ivanti

Patch for Windows® Servers

powered by Shavlik

Administration Guide

9.3

Copyright Notice

This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti"), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.ivanti.com.

Copyright © 2003-2017, Ivanti. All rights reserved.

Ivanti and its logos are registered trademarks or trademarks of Ivanti, Inc. and its affiliates in the United States and/or other countries. Other brands and names may be claimed as the property of others.

Last updated: 4/20/2017

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Contents

Contents **3**
Welcome to Ivanti Patch for Windows® Servers, powered by Shavlik **16**
Patch Management 16
Asset Inventory 16
Power Management 17
ITScripts 17
Editions of the Program **19**
Ivanti Patch for Windows® Servers, Full Edition 19
Ivanti Patch for Windows® Servers, Trial Edition 19
Ivanti Patch for Windows® Servers, Government Edition 19
What's New? **20**
System Requirements **21**
Obtaining the Software **28**
Installing the Prerequisites **29**
Automatic Installation 29
Manual Installation 29
SQL Server Pre-Installation Notes **30**
What You Need to Know About SQL Server Before Installing Ivanti Patch for Windows® Servers 30
Performing a New Installation **32**
HTTP Proxy Post-Installation Notes **39**
SQL Server Post-Installation Notes **40**
Manually Configuring a Remote SQL Server to Accept Machine Account Credentials 40
Allowing Other Users Access to the Program 42
Performing Periodic Maintenance on the Database 43
Starting Ivanti Patch for Windows® Servers **44**
Activating Ivanti Patch for Windows® Servers **45**
Version and License Information **49**
Application and Version Information 49
Export Information 49
Open Source License 49
Technical Support 49
Data Versions and Product End of Life Notification 49
How Licenses are Tracked **51**
Navigating the Interface **52**
Major Program Features **54**
Viewing Charts **60**
Menu Commands **61**
Editing the Database Description **64**
For Data Rollup Configurations 65
Help System **67**
Command-line Option **68**
About Machine Groups **69**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About the My Test Machines Group **70**
Creating Machine Groups **71**
Organizing Machine Groups **72**
Performing Actions on Machine Groups **74**
Right-Click Menu 74
Searching Machine Groups **75**
Working with a Machine Group **77**
Machine Group Dialog: Top Section **78**
Machine Group Dialog: Middle Section **80**
Machine Group Dialog: Bottom Section **81**
Adding Machines by Name to a Machine Group **87**
Adding an Individual Machine Name 87
Importing Machine Names From an External Source 87
Adding Domains to a Machine Group **90**
Adding an Individual Domain Name 90
Importing Domain Names From an External Source 90
Adding Machines by IP Address to a Machine Group **93**
Adding an Individual IPv4 Address 93
Adding a Range of IPv4 Addresses 93
Adding an IPv6 Address 93
Importing IP Addresses from an External Source 94
Adding Organizational Units to a Machine Group **95**
Adding an Individual Organizational Unit 95
Importing OUs from an External Source 95
Defining Nested Groups **98**
How to Add Virtual Machines to a Machine Group **99**
Adding Virtual Machines Hosted by a Server **100**
Logging on to an ESX or Virtual Infrastructure Server **103**
Adding Offline Virtual Machines That Reside On Workstations **104**
Viewing Servers and Virtual Machines in a Machine Group **107**
Excluding Certain Machines **108**
Linking Files to a Machine Group **109**
Introducing the Virtual Inventory Feature **111**
vCenter Server and ESXi Hypervisor Requirements **113**
vCenter Server Requirements and Recommendations 113
ESXi Hypervisor Scanning Requirements 113
ESXi Hypervisor Deployment Requirements and Recommendations 113
Adding, Editing, or Removing vCenter Servers and ESXi Hypervisors **116**
Adding vCenter Servers and ESXi Hypervisors 116
Editing or Removing vCenter Servers and ESXi Hypervisors 117
Customizing the Column Headers **118**
Viewing Information About a vCenter Server **121**
vCenter Server Top Pane Summary **123**
Searching for Hypervisors While Viewing a vCenter Server **124**
Tips for Using the Search Tool 124

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing Actions on ESXi Hypervisors **125**
Viewing a Summary of the ESXi Hypervisor's Virtual Machines and Virtual Machine Templates **126**
Performing Actions on Virtual Machines **128**
Viewing Bulletin Status **129**
How to Deploy Bulletins to Your Managed Hypervisors **132**
Using the ESXi Hypervisors List **133**
Viewing a Summary of the ESXi Hypervisor's Virtual Machines and Virtual Machine Templates **134**
Performing Actions on a Hypervisor's Virtual Machines **136**
Viewing Bulletin Status on Unmanaged Hypervisors **138**
Deploying Bulletins to Unmanaged Hypervisors **142**
How to Initiate a Scan of an ESXi Hypervisor **145**
Scanning One or More Managed ESXi Hypervisors 145
Scanning a Managed or Unmanaged ESXi Hypervisor 145
Viewing Scan Results 146
Initiating a Bulletin Deployment to an ESXi Hypervisor **147**
Configuring an ESXi Bulletin Deployment **148**
Viewing ESXi Hypervisor Deployment Results **152**
Using the Bulletins Tab to View Bulletin Deployment Results 152
Supplying Scan Credentials for Target Machines **154**
Defining Credentials **159**
Potential Security Implications When Sharing Credentials **162**
Managing Credentials **163**
Credential Precedence for Physical Machines and Online Virtual Machines **168**
Initiating actions from the home page, from a machine group, or from a favorite 168
Initiating an agent installation from a machine group 168
Initiating actions from Machine View or Scan View 169
Initiating an agent installation from Machine View or Scan View 169
Credential Precedence for Offline Hosted Virtual Machines **170**
Initiating actions from the home page, from a machine group, or from a favorite 170
Initiating actions from Machine View or Scan View 170
Creating Favorites **172**
Performing Actions on a Favorite **174**
Why You Might Use Multiple Administrators **175**
Scenario 1: Two or More Administrators on the Same Console Machine 175
Scenario 2: Two or More Consoles Sharing One Database 176
How Ivanti Patch for Windows® Servers Manages Multiple Administrators **178**
Potential Issues When Using Multiple Administrators **179**
Usage Issues 179
Credential Issue 179
Virtual Inventory Consideration 180
Best Practices When Using Multiple Administrators **181**
How Role-Based Administration Works **182**
Assigning User Roles **183**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Enabling and Disabling Role-Based Administration **185**
Enabling Role-Based Administration 185
Disabling Role-Based Administration 186
Determining the Currently-Assigned Role **187**
Show Me How to Get Started! **188**
How Do I . . .?: Get Started Scanning and Patching **190**
How Do I . . .?: Automate Scheduled Patching **193**
How Do I . . .?: Track Deployment Status **194**
Tracking Patch Deployments 194
Monitoring Post-patch Machine Status 194
How Do I . . .?: Download Approved Patches **195**
How Do I . . .?: Scan and Patch ESXi Hypervisors **196**
How Do I . . .?: Set Up and Monitor Agents **197**
How Do I . . .?: Use The Asset Inventory Feature **198**
How Do I . . .?: Use The Power Management Feature **200**
How Do I . . .?: Use The ITScripts Feature **202**
How Do I . . .?: Collect Data for Technical Support **203**
Installation Log Files 203
Program Log Files 203
How Do I . . .?: Use A Distribution Server **205**
How Do I . . .?: Generate Reports **207**
How Do I . . .?: View How-to Tutorials **209**
Virtual Machine Overview **210**
Online Virtual Machines 210
Offline Virtual Machines 210
Virtual Machine Templates 211
Power State and Credential Requirements for Successful Scans and Deployments to Virtual Machines **212**
Notes About Virtual Machines **214**
Requirements 214
General Notes 214
Patch Deployments 215
Agents 216
Notes About Virtual Machine Templates **217**
General Notes 217
Patch Deployments 217
Roadmap of Tasks for Virtual Machines and Virtual Machine Templates **219**
Patch Tasks 219
Asset Management Tasks 220
Power Management Tasks 220
What Sets Ivanti Patch for Windows® Servers Apart from the Others? **221**
Features 221
Security and Integrity 221
Scanning Engine Overview **223**
Enumerating Machines in Domains **224**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Determining Patch Status **225**
File Version Analysis **226**
Determining Patch Replacements **227**
Identifying Explicitly Installed Patches **228**
Identifying Effectively Installed Patches **229**
Patch Scanning Overview **230**
Scans Are Performed As Background Tasks 230
Scanning Considerations 230
Patch Scanning Prerequisites **231**
When scanning your local (console) machine 231
When scanning a remote machine, you must meet all the requirements for the local scan above, plus the following: 231
Special note regarding Simple File Sharing 232
How to Initiate a Patch Scan **233**
From the Home Page 233
From a Machine Group 234
From a Favorite 235
From Machine View or Scan View 236
From the API 237
Scheduling Patch Scans Using the Run Operation Dialog **238**
Monitoring a Patch Scan **241**
Monitoring a Scheduled Patch Scan **242**
Scan History **243**
Patch Options Menu **244**
About Patch Scan Templates **245**
Predefined Patch Scan Templates **246**
Creating or Editing a Patch Scan Template **247**
Organizing Patch Scan Templates **253**
Managing a Patch Scan Template **255**
Specifying a Default Patch Scan Template **256**
About Patch View **257**
Navigating Patch View **258**
Filtering Patch View by Patch Type **260**
Filtering Patch View by Product Vendor **262**
Exporting Patches **263**
Customizing the Patch View Column Headers **264**
Understanding the Top Pane **267**
Searching Patch View **268**
Tips for Using the Search Tool 268
Filtering Patch View **269**
Custom Filters 269
Example 270
Performing Actions on Patches **271**
Right-Click Menu 271
Keyboard Shortcuts 272

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Patch Details **273**
Viewing Machines Affected by a Selected Patch **275**
About Patch Groups **276**
Creating and Editing a Patch Group **277**
Performing Actions on Patch Groups 278
Using a Patch Group **280**
About Third-Party Applications **282**
How to Scan for Third-Party Applications **283**
Accessing Patch Scan Results (Scan View) **284**
Machines Scanned 284
Machines Not Scanned 284
Navigating the Scan View Grid **286**
Customizing the Column Headers **287**
Scan View Scan Summary **291**
Machine Group Information is Dynamic **293**
Searching for Machines in the Top Pane **294**
Tips for Using the Search Tool 294
Using Smart Filter **295**
Default Filters 295
Custom Filters 296
Performing Actions on Machines **298**
Right-Click Menu 298
Keyboard Shortcuts 300
Viewing Patch Summaries in Scan View **301**
Performing Actions on Patches **304**
Keyboard Shortcuts 305
Viewing Patch Information **306**
Viewing Machines Affected by a Selected Patch **308**
Downloading Patches and Service Packs **309**
How to Download Different Language Versions of a Patch **310**
Patch Downloads Are Performed As Background Tasks **311**
Patch Deployment Overview **312**
Patch Deployments Are Performed As Background Tasks 312
Patch Deployment Prerequisites **313**
Patch Deployment Security **315**
Testing the Deployment **316**
How to Perform a Test Deployment 316
Deploying One or More Patches to a Machine **318**
Deploying All Missing Patches to a Machine **319**
From the Top Pane of Machine View or Scan View 319
From the Middle Pane of Machine View or Scan View 319
Deploying Patches to Multiple Machines **321**
Deploying Third-Party Applications **322**
Deploying Patches to Virtual Machines and to Virtual Machine Templates **324**
Deploying Service Packs **328**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deploying Patches to All Members of a Domain **329**
Scheduling and Configuring a Deployment **330**
Automatically Deploying Patches **333**
Monitoring the Deployment **336**
Tips for Monitoring Patch Deployments to Virtual Machines 336
Viewing Deployment Results **338**
Canceling a Deployment **339**
Deployment History **340**
About Deployment Templates **341**
Creating or Editing a Deployment Template **342**
Organizing Patch Deployment Templates **344**
Deployment Template: General Tab **346**
Deployment Template: Pre-Deploy Reboot Tab **348**
Deployment Template: Post-Deploy Reboot Tab **350**
Deployment Template: Email Tab **354**
Deployment Template: Custom Actions Tab **356**
Deployment Template: Distribution Servers Tab **358**
Deployment Template: Hosted VMs/Templates Tab **361**
Deployment Template: Used By Tab **363**
Managing a Deployment Template **364**
About the Deployment Tracker **365**
About the Deployment Tracker Dialog **366**
Canceling a Task **368**
Uninstalling Patches **369**
Overview of the Custom Patch XML Process **370**
Creating a New Custom XML File **371**
Creating a Custom Product **373**
Creating a Custom Bulletin **377**
Creating a Custom Patch **379**
Scan Information Tab **381**
Deployment Information Tab **388**
Saving and Validating Your Changes **391**
Changing a Custom XML File **392**
Specifying Which Custom XML Files to Use **393**
Removing a Custom XML File 394
Viewing Custom Patches and Products **395**
Asset Inventory Overview **397**
How-To Information 397
Software Asset Scan Information 397
Hardware Asset Scan Information 398
Ivanti Patch for Windows® Servers's Advantages Over Other Asset Tools 398
Asset Management Scan Requirements **399**
Asset Scans are Performed as Background Tasks **401**
Scanning Considerations 401
Creating a New Asset Scan Template **402**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How to Initiate an Asset Scan **405**
Scheduling Asset Scans Using the Run Operation Dialog **409**
Monitoring an Asset Scan **411**
Monitoring a Scheduled Asset Scan **412**
Viewing Asset Scan Results **413**
Power Management Overview **414**
How-To Information 414
Extremely Flexible Implementation Options 414
Agentless vs. Agent-based 416
Power Management Requirements **417**
General Requirements 417
Sleep and Hibernate Requirements 417
Wake-on-LAN (WoL) Requirements 417
Power Status Scan Requirements 418
Creating and Editing a Power State Template **419**
How to Initiate Power Management Tasks **424**
Scheduling Power Management Tasks Using the Run Operation Dialog **430**
Sleep and Hibernation Implementation Notes **432**
Wake-on-LAN Implementation Notes **434**
Shutdown Implementation Notes **436**
Machine Restart Implementation Notes **437**
Monitoring a Power Task **438**
Monitoring a Scheduled Power Task **439**
Initiating and Monitoring a Power Status Scan **440**
Initiating a Power Status Scan 440
Monitoring a Power Status Scan 440
Viewing Power Status Scan Results **442**
Using Patch Deployments to Perform Power Tasks **445**
About Machine View **446**
Accessing Machine View **447**
Navigating Machine View **448**
Customizing the Column Headers **449**
Machine View Top Pane Summary **453**
Understanding Patch Count Data **456**
Machine Group Information is Dynamic **457**
Searching for Machines in the Top Pane **458**
Tips for Using the Search Tool 458
Using Smart Filter to Filter Information in the Top Pane **459**
Default Filters 459
Custom Filters 460
Example 461
Performing Actions on Machines **462**
Right-Click Menu 462
Keyboard Shortcuts 464
Viewing Patch Summaries in Machine View **465**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing Actions on Patches **469**
Keyboard Shortcuts 470
Viewing Software Asset Summaries **471**
Viewing Hardware Asset Summaries **472**
Viewing Patch Information **473**
Viewing Machines Affected by a Selected Patch **475**
Typical Uses of Machine View **476**
What is Event History? **477**
Searching for Event Entries **479**
Tips for Using the Search Tool 479
Using the Event History Smart Filter **480**
Default Filters 480
Custom Filters 480
Manage Items **482**
Accessing Machine Properties **483**
Managing Individual Machine Properties **484**
Managing Multiple Machine Properties **487**
About the Operations Monitor **490**
About the Scheduled Console Tasks Manager **493**
How to Access the Scheduled Console Tasks Manager 493
About the Scheduled Remote Tasks Manager **495**
How to Access the Scheduled Remote Tasks Manager 495
Manually Installing and Uninstalling the IvantiScriptLogic Scheduler **498**
Display Options **500**
Notifications and Warnings Options **502**
Patch Options **504**
Scheduling Options **507**
Agents Options **509**
Download Options **511**
Email Options **517**
Data Rollup Options **519**
Why Use a Distribution Server? **521**
Determining How Many Distribution Servers to Use **523**
Do You Need a Distribution Server? 523
If You Need Distribution Servers, How Many? 523
Configuring a New or Existing Distribution Server **524**
How to Access Your Distribution Servers 524
Configuring System Account Permissions **529**
Synchronizing Distribution Servers **532**
Creating a Status Report 532
Automatically Synchronizing Distribution Servers 533
Manually Synchronizing Selected Distribution Servers 534
Assigning IP Addresses to Distribution Servers **536**
Database Maintenance **538**
Scheduled Snapshot Maintenance **542**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Protect Cloud Synchronization Overview **545**
Protect Cloud Synchronization Requirements and Usage Notes **547**
Requirements 547
Usage Notes 548
How to Enable Protect Cloud Synchronization **549**
Protect Cloud Sync Options **550**
Logging Options **552**
Internet Proxy Options **554**
ITScripts Options **556**
Email Overview **558**
Populating the Address Book **559**
Defining a New Contact 559
Defining a New Email Group 559
Deleting an Existing Contact or Group 560
Automatically Sending Email Reports and Notifications **561**
Templates 561
Machines and Machine Groups 561
Manually Sending Email Reports and Notifications **562**
Using Disconnected Mode **563**
Be Careful if Your Site Uses Agents 563
Possible Issue with .NET Framework Prerequisite 563
Managing Data Files and Missing Patches in Disconnected Mode **564**
Data File Locations 564
Downloading Missing Patches 564
Available Reports **565**
Reports Dialog **569**
Pick a Report 569
Pick Filtering Options 569
View the Report 570
Scheduling a Report 570
Generating a Report from a Data Rollup Console 570
Advanced Filtering **571**
Exporting Reports **572**
How to Schedule a Report **574**
How to Access the Scheduling Dialog 574
Report Tab 575
Schedule Tab 576
Email Tab 576
Scheduling the Report 576
Why Use Multiple Consoles? **578**
What is a Data Rollup Console Configuration? **579**
Implementing a Data Rollup Configuration **580**
On the Central Console 580
On Each Remote Console 580
Watching For Data Rollup Activity **581**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

What is an Unattended Console Configuration? 582
Implementing an Unattended Console Configuration 584
On the Distribution Server 584
On Each Unattended Console 584
Ongoing Maintenance 585
What is a Disconnected Console Configuration? 586
Tasks Performed by the Central Console 588
Tasks Performed by the Remote Consoles 589
Configuring the Central Console in a Disconnected Configuration 590
I. (Optional) Configure the Data Rollup Service 590
II. Set Up a Distribution Server 590
III. Update the Distribution Server with the Latest Files 590
Configuring the Remote Consoles in a Disconnected Configuration 591
I. (Optional) Configure the Data Rollup Service 591
II. Set Up a Distribution Server 591
III. Create a Machine Group of the Machines at This Site 591
IV. Specify Where to Download Files 591
V. Create a Patch Scan Template 592
VI. Create a New Favorite and Schedule a Periodic Scan 592
Multiple Console Configuration with Agents 593
Agentless vs. Agent-based Solutions 595
Agentless Solution 595
Agent-based Solution 595
Summary 596
When Should I Use Agentless and Agent-based Solutions? 597
For Patch Management and Asset Management Tasks 597
For Power Management Tasks 597
What Exactly is Ivanti Patch for Windows® Servers Agent? 599
How the Agent Process Works 601
Preparing to Use Ivanti Patch for Windows® Servers Agent 603
I. (Optional) Set Up and Synchronize a Distribution Server 603
II. Create and Configure a Ivanti Patch for Windows® Servers Agent Policy 603
III. Install the Agent on the Desired Machines 604
How to Install Ivanti Patch for Windows® Servers Agent from the Console 605
For Machines That Have Been Previously Scanned 605
For Machines That Have Not Been Previously Scanned 606
Manually Installing Ivanti Patch for Windows® Servers Agent 608
Requirements 608
Installation Procedure 608
Installing Agents from the Cloud 614
Requirements 614
Installation Instructions 614
Configuring Proxy Server Settings for Ivanti Patch for Windows® Servers Agent 618
Creating and Using a Manual Installation Script 620
Troubleshooting Agent Installation Errors 622

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Managing Your Agents **623**
Monitoring Ivanti Patch for Windows® Servers Agent Actions **626**
Determining Which Machines Have Ivanti Patch for Windows® Servers Agent **627**
Ongoing Maintenance Tasks **628**
Using an Agent on a Machine **629**
Administrator Tools within the Client Program 630
Uninstalling Ivanti Patch for Windows® Servers Agent **632**
Using Machine View to Uninstall Agents 632
Manually Uninstalling Ivanti Patch for Windows® Servers Agent 632
Creating a New Ivanti Patch for Windows® Servers Agent Policy **634**
Configuring General Settings for a Ivanti Patch for Windows® Servers Agent Policy **635**
Creating a New Patch Task **640**
Creating a New Asset Task **649**
Creating a New Power Task **652**
About Service Pack Groups **655**
Notes About Service Pack Groups 655
Creating and Editing a Service Pack Group **656**
Using a Service Pack Group **659**
Copy, Delete, or Rename a Service Pack Group **660**
ITScripts and Windows PowerShell™ Overview **661**
ITScripts Requirements **664**
License Requirements 664
Script Requirements 664
Console Requirements 665
Target Machine Requirements When Using PowerShell Remoting or Opening a PowerShell Prompt 665
Target Machine Requirements When NOT Using PowerShell Remoting 666
Managing ITScripts **667**
Creating an ITScripts Template **671**
How to Execute a Script **674**
Scheduling Scripts Using the Run Operation Dialog **679**
Using the Run console ITScripts Dialog **682**
Monitoring the Execution of a Script **684**
Monitoring a Scheduled Script **685**
ITScripts Results View **686**
Performing Actions on Script Results **688**
Right-Click Menu 688
Run Results vs Machine Results 688
Double-Click Shortcut 690
Keyboard Shortcuts 690
Searching for Script Results **691**
Tips for Using the Search Tool 691
Using the Script Result Smart Filter **692**
Default Filters 692
Custom Filters 692

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Example ... 693
Opening a Windows PowerShell Prompt ... 695
Creating a Custom Script ... 697
Understanding RDP ... 698
RDP Requirements ... 699
How to Initiate a Remote Desktop Connection ... 701
Assigning Aliases to the Console ... 704
Migration Tool ... 707
Using the API Feature ... 708
What is the Issue? ... 709
Overview of the Solution ... 710
Major steps in the process ... 710
Before and after views of your certificate environment ... 710
Requirements and Exceptions ... 713
Requirements of the New Sub-Authority Certificate ... 713
Exceptions ... 713
Step 1: How to Issue a New Certificate Using Your Own CA ... 714
Step 2: Let the New Certificate Percolate Through Ivanti Patch for Windows® Servers ... 716
30 day waiting period ... 716
Bypassing the 30 day waiting period ... 716
Step 3: Commit the New Sub-Authority Certificate ... 717
Automatic commit process ... 717
Manual commit process ... 717
What happens after the commit is issued? ... 718
IAVA Overview ... 719
IAVA XML File ... 719
Creating an IAVA Report ... 720
Performing an IAVA Patch Scan ... 723
Reporting Errors and Checking for Possible Solutions ... 726
Check Online for a Solution ... 726
Privacy and Security Concerns ... 727
Obtaining Support ... 728
Index ... 729

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Welcome to Ivanti Patch for Windows® Servers, powered by Shavlik

Welcome to Ivanti Patch for Windows® Servers, a unified IT management platform used for managing and protecting Windows-based machines and VMware ESXi Hypervisors. Ivanti Patch for Windows® Servers provides you with one centralized and common interface that you can use to perform several essential IT management functions.

Patch Management

Ivanti Patch for Windows® Servers' industry-leading patch management function provides the ability to scan all Windows-based machines and VMware ESXi hypervisors in your network and assess the current patch status of those machines. After a scan is performed you can generate reports that provide additional details about the patch "health" of each machine. Ivanti Patch for Windows® Servers can then be used to easily and automatically bring each machine up to date. You simply instruct the program to download and deploy the desired patches to the machines of your choosing. You can even dictate when the deployment will occur and if and when each machine should be restarted. In addition, Ivanti Patch for Windows® Servers can provide email alerts that notify you when patches are available and it can email the results of scans and other information you wish to share with selected users.

The patch management function can be performed with or without agents. This unique blending of agentless and agent-based technologies gives you maximum flexibility while minimizing management overhead.

To get started: How Do I Get Started Scanning and Patching?

Asset Inventory

The asset inventory function enables you to track your software and hardware assets. The function works with both physical and virtual machines. You can perform scans to detect and categorize the software and hardware contained on your physical and online virtual machines. Detailed information about your software and hardware virtual assets is available immediately following a scan. You also have the ability to create reports that can be used to track your asset inventory over time.

Like the patch management function, the asset inventory function can be performed with or without agents.

To get started: How Do I Use the Asset Inventory Feature?

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Power Management

Power management is only available with Ivanti Patch for Windows® Servers Advanced or as an add-on to Ivanti Patch for Windows® Servers Standard. If you do not have access to this function, contact your sales representative to upgrade your Ivanti Patch for Windows® Servers license.

The power management function enables you to control the power state of the machines in your organization. The primary reasons for using power management are to:

- Prepare your machines for maintenance tasks
- Reduce noise and power consumption
- Reduce operating costs
- Prolong battery life

You can shut down, restart, or awaken machines either immediately or on a scheduled basis. When you perform a scheduled restart you also have the ability to specify what power state to put the machines in: fully powered on, in sleep mode, or in hibernate mode. The power management function can be performed with or without agents.

To get started: How Do I Use the Power Management Feature?

ITScripts

Portions of the ITScripts function are only available with Ivanti Patch for Windows® Servers Advanced. If you do not have full access to this function, contact your sales representative to upgrade your Ivanti Patch for Windows® Servers license.

The ITScripts function enables you to execute PowerShell scripts against the machines and machine groups you have already defined in Ivanti Patch for Windows® Servers. With this scripting feature you can:

- Access to free scripts and all pre-defined scripts provided by Ivanti
- Execute scripts against target machines
- Execute scripts from the console
- Create PowerShell templates
- Import custom scripts
- Share your custom scripts with the ITScripts community
- Execute scripts immediately

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- Schedule script execution to run at some time in the future
- Execute scripts with or without the Windows PowerShell remoting features
- View the results of all scripts that have been initiated from Ivanti Patch for Windows® Servers

To get started: How Do I Use the ITScripts Feature?

Copyright © 2004 - 2017 Ivanti All rights reserved.

This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti"), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.ivanti.com.

Ivanti and its logos are registered trademarks or trademarks of Ivanti, Inc. and its affiliates in the United States and/or other countries. Other brands and names may be claimed as the property of others.

Help file version info: Ivanti Patch for Windows® Servers 9.3, April 2017

Editions of the Program

Ivanti Patch for Windows® Servers is available within two different product bundles.

- Ivanti Patch for Windows® Servers Standard: This is the basic product offering that includes patch management, asset inventory, and a limited number of scripts for IT management. You can purchase additional keys for separately licensed add-on features.
- Ivanti Patch for Windows® Servers Advanced: This is the full-featured product offering that includes patch management, asset inventory, power management and full ITScript capabilities.

There are several different editions of Ivanti Patch for Windows® Servers. Each edition provides a different level of capabilities. To determine which edition you are running, select **Help > About** to view program details.

This section provides a synopsis of each available edition.

Ivanti Patch for Windows® Servers, Full Edition

This is the full edition of the program. With Ivanti Patch for Windows® Servers you can scan for missing patches, deploy missing patches, and view the results of these actions. You also have access to all the other features provided by your program license (Ivanti Patch for Windows® Servers Standard or Ivanti Patch for Windows® Servers Advanced).

Ivanti Patch for Windows® Servers, Trial Edition

Ivanti Patch for Windows® Servers is available on a trial basis. This enables you to test all the capabilities of Ivanti Patch for Windows® Servers, but only for 60 days. You are also limited to 50 license seats. When the trial license expires the program will stop refreshing its XML data files and many of the program features will no longer be available.

Ivanti Patch for Windows® Servers, Government Edition

When you purchase the Government Edition of Ivanti Patch for Windows® Servers you will receive a license key that enables you to use the Information Assurance Vulnerability Alert (IAVA) Reporter. The IAVA-specific files are automatically installed when Ivanti Patch for Windows® Servers Standard or Ivanti Patch for Windows® Servers Advanced is installed. For more information about IAVA, see IAVA Overview.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

What's New?

For a complete list of the new features, enhancements, and bug fixes included in this version, see the Ivanti Patch for Windows® Servers Release Notes: https://help.ivanti.com/sh/help/en_US/PWS/93/rn-pws-9-3.pdf.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

System Requirements

You must meet the following requirements when installing the Ivanti Patch for Windows® Servers console and performing actions on client machines.

CONSOLE

Restrictions

- An NTFS file system is required on the console machine
- If you install the console on a domain controller that uses LDAP certificate authentication, you may need to configure the server to avoid conflict issues between the SSL certificate and the Ivanti Patch for Windows® Servers program certificate. There is no easy way to configure this on a Windows Server 2003-based domain controller and this combination is not recommended for use as a console.
- If you install the console on two or more machines that share a database, all of the console machines must have unique security identifiers (SIDs) in order to prevent user credential problems. Machines are likely to have the same SIDs if you make a copy of a virtual machine or if you ghost a machine.

Processor

- Minimum: 2 processor cores 2 GHz or faster
- Recommended: 4 processor cores 2 GHz or faster (for 250 - 1000 seat license)
- High performance: 8 processor cores 2 GHz or faster (for 1000+ seat license)

Memory

- Minimum: 2 GB of RAM
- Recommended: 4 GB of RAM (for 250 - 1000 seat license)
- High performance: 8 GB of RAM (for 1000+ seat license)

Video

- 1024 x 768 screen resolution or higher (1280 x 1024 recommended)

Disk Space

- 100 MB for application
- 2 GB minimum, 10 GB or more recommended for patch repository

Operating System (one of the following)

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Ivanti Patch for Windows® Servers supports 64-bit versions of the listed operating systems. 32-bit versions are not supported for the console.

- Windows Server 2016 Family, excluding Server Core and Nano Server
- Windows Server 2012 Family R2 Cumulative Update 1 or later, excluding Server Core
- Windows Server 2012 Family, excluding Server Core
- Windows Server 2008 Family R2 SP1 or later, excluding Server Core
- Windows 10 Pro, Enterprise or Education Edition
- Windows 8.1 Cumulative Update 1 or later, excluding Windows RT
- Windows 7 SP1 or later, Professional, Enterprise, or Ultimate Edition

Database

- Use of a Microsoft SQL Server database [SQL Server 2008 or later]

  If you do not have a SQL Server database, the option to install either SQL Server 2016 SP1 Express Edition (if it is supported) or SQL Server 2014 Express Edition will be provided during the prerequisite software installation process.
- Size: 1.5 GB

Prerequisite Software

- Use of Microsoft SQL Server 2008 or later
- Microsoft .NET Framework 4.6.2 or later
- Microsoft Visual C++ Redistributable for Visual Studio 2015
- Windows Management Framework 4.0 (contains Windows PowerShell 4.0, which is required for the ITScripts feature): This prerequisite does not apply to Windows 8.1 or later and Windows Server 2012 R2 or later, as PowerShell 4.0 is already included with these operating systems.

Windows Account Requirements

- In order to access the full capabilities of Ivanti Patch for Windows® Servers, you must run under an account with administrator privileges

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Configuration Requirements

- When performing an asset scan of the console machine, Windows Management Instrumentation (WMI) service must be enabled and the protocol allowed to the machine. In Windows Firewall, on Windows XP/Windows 2003 machines the service is called Remote Administration, and on more recent Windows machines the service is called Windows Management Instrumentation (WMI)/Remote Administration.

CLIENTS (AGENTLESS)

Operating Systems (32- and 64-bit versions of any of the following)

- Windows XP Professional (**Note:** Can deploy patches to Windows XP Family SP3 or later)
- Windows XP Tablet PC Edition
- Windows XP Embedded
- Windows Server 2003, Enterprise Edition (**Note:** Can deploy patches to Windows Server 2003 Family SP2 or later)
- Windows Server 2003, Standard Edition
- Windows Server 2003, Web Edition
- Windows Server 2003 for Small Business Server
- Windows Server 2003, Datacenter Edition
- Windows Vista, Business Edition
- Windows Vista, Enterprise Edition
- Windows Vista, Ultimate Edition
- Windows 7, Professional Edition
- Windows 7, Enterprise Edition
- Windows 7, Ultimate Edition
- Windows Server 2008, Standard
- Windows Server 2008, Enterprise
- Windows Server 2008, Datacenter
- Windows Server 2008, Standard - Core
- Windows Server 2008, Enterprise - Core
- Windows Server 2008, Datacenter - Core

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- Windows Server 2008 R2, Standard
- Windows Server 2008 R2, Enterprise
- Windows Server 2008 R2, Datacenter
- Windows Server 2008 R2, Standard - Core
- Windows Server 2008 R2, Enterprise - Core
- Windows Server 2008 R2, Datacenter - Core
- Windows 8
- Windows 8 Pro
- Windows 8 Enterprise
- Windows 8.1
- Windows 8.1 Enterprise
- Windows Server 2012, Foundation Edition
- Windows Server 2012, Essentials Edition
- Windows Server 2012, Standard Edition
- Windows Server 2012, Datacenter Edition
- Windows Server 2012 R2, Essentials Edition
- Windows Server 2012 R2, Standard Edition
- Windows Server 2012 R2, Datacenter Edition
- Windows 10 Pro
- Windows 10 Enterprise
- Windows 10 Education
- Windows Server 2016, Essentials Edition
- Windows Server 2016, Standard Edition (excluding Server Core and Nano Server)
- Windows Server 2016, Datacenter Edition (excluding Server Core and Nano Server)

Virtual Machines (offline virtual images created by any of the following)

- VMware ESXi 5.0 or later (VMware Tools is required on the virtual machines)

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- VMware vCenter (formally VMware VirtualCenter) 5.0 or later (VMware Tools is required on the virtual machines)
- VMware Workstation 9.0 or later
- VMware Player

Configuration Requirements

- Remote Registry service must be running
- Simple File Sharing must be turned off
- Server service must be running
- NetBIOS (TCP 139) or Direct Host (TCP 445) ports must be accessible
- Windows Update service must not be disabled; rather, it must be set to either **Manual** or **Automatic** in order to successfully deploy patches. In addition, the Windows Update setting on each target machine (**Control Panel > System and Security > Windows Update > Change settings**) should be set to **Never check for updates**.
- Remote Desktop connections must be allowed in order for the console to make an RDP connection with the target machine.
- When performing an asset scan, Windows Management Instrumentation (WMI) service must be enabled and the protocol allowed to the machine (TCP port 135). In Windows Firewall, on Windows XP/Windows 2003 machines the service is called Remote Administration, and on more recent Windows machines the service is called Windows Management Instrumentation (WMI)/Remote Administration. See Asset Scan Requirements for more details.

Products Supported (for patch program)

- See https://www.ivanti.com/en-US/support/supported-products for the current list

Disk Space (for patch program)

- Free space equal to five times the size of the patches being deployed

Supported Languages (for patch program)

- Arabic, Chinese (Simplified), Chinese (Traditional), Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hebrew, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese (Brazil), Portuguese (Portugal), Russian, Spanish, Swedish, Thai, Turkish

CLIENTS RUNNING WITH AN AGENT



An NTFS file system is required on agent machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Processor

- 500 MHz or faster CPU

Memory

- Minimum: 256 MB RAM
- Recommended: 512 MB RAM or higher

Disk Space

- 30 MB for Ivanti Patch for Windows® Servers Agent client
- 2 GB or more for patch repository

Operating Systems (any of the following except home editions)

- Windows Vista Family
- Windows 7 Family
- Windows 8 Family, excluding Windows RT
- Windows 10 Family
- Windows Server 2008 Family
- Windows Server 2008 Family R2
- Windows Server 2012 Family
- Windows Server 2012 Family R2
- Windows Server 2016 Family

Configuration Requirements

- Workstation service must be running

PORT REQUIREMENTS

These are the default port requirements. Several of the port numbers are configurable.

	Inbound Ports (Basic NAT Firewall)								
	TCP 80	**TCP 135**	**TCP 137-139 or TCP 445 (Windows file sharing/directory services)**	**TCP 443**	**TCP 3121**	**TCP 3122**	**TCP 4155**	**TCP 5120**	**TCP 5985**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Client System		X (For asset scans)	X	X				X (For listening agents)	X	X (For WinRM protocol)
Console System						X	X			
Distribution Server	X		X	X	X					

	Outbound Ports (Highly Restricted Network Environment)						
	TCP 80	**TCP 137-139 or TCP 445 (Windows file sharing/directory services)**		**TCP 443**	**TCP 3121**	**TCP 5120**	**UDP 9**
Client System	X (For agents)	X	X	X (For cloud agents)	X (For agents and Deployment Tracker)		
Console System	X	X	X	X (For cloud sync)		X	X (For WoL and error reporting)

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Obtaining the Software

Ivanti Patch for Windows® Servers is available for download from our Web-based download center: https://www.ivanti.com/en-US/resources/downloads. The download center always has the most recent version of Ivanti Patch for Windows® Servers that is available.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Installing the Prerequisites

This topic explains how to obtain and install the prerequisites needed by Ivanti Patch for Windows® Servers.

Automatic Installation

The prerequisites can be automatically installed during the Ivanti Patch for Windows® Servers installation.

Manual Installation

If you prefer to download and install the prerequisites yourself, you may do so using the following URLs. Your operating system may already contain many of the prerequisites, so only install the prerequisites that you are missing.

SQL Server 2016 Express Edition SP1

Only required if you don't already have a full or express edition of SQL Server.

https://www.microsoft.com/en-us/sql-server/sql-server-editions-express

.NET Framework 4.6.2

https://www.microsoft.com/en-us/download/details.aspx?id=53345

https://www.microsoft.com/en-us/download/details.aspx?id=53344 (for disconnected environments)

Visual C++ 2015 Redistributable (x64)

https://www.microsoft.com/en-us/download/details.aspx?id=53840

Windows Management Framework 4.0

http://www.microsoft.com/en-us/download/details.aspx?id=40855

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

SQL Server Pre-Installation Notes

Ivanti Patch for Windows® Servers will store all scan and patch deployment results in an SQL Server database. The SQL Server backend enables real-time collaboration and knowledge management amongst all individuals responsible for performing patch management tasks. Some of the benefits to using the SQL Server database include:

- High performance when scanning either a handful of machines or many machines
- Storage of data on a remote machine
- Ability for multiple Ivanti Patch for Windows® Servers consoles to share templates, comments, reports, and scan results

What You Need to Know About SQL Server Before Installing Ivanti Patch for Windows® Servers

Before installing Ivanti Patch for Windows® Servers, please review the following SQL Server notes:

- Microsoft SQL Server is required.

  If you do not have SQL Server, either Microsoft SQL Server 2016 SP1 Express Edition (if supported) or SQL Server 2014 Express Edition SP1 will be installed for you on the console machine by the Ivanti Patch for Windows® Servers installation process.

- If you will be using an Express Edition of Microsoft SQL Server, you should consider downloading and installing Microsoft SQL Server Management Studio Express. This free software can be used to perform backups and to manage your database.
- Installation of SQL Express may fail if you have a SQL Native Client previously installed. It is strongly recommended you uninstall SQL Native Client using **Add or Remove Programs** before running the installation program.
- You must have access to the specified SQL Server. The program will support either Windows authentication or SQL Server authentication to access the specified SQL server. Although administrative access is not required, this account does need permissions to create and populate the product database on the specified SQL Server. In addition, the Ivanti Patch for Windows® Servers console machine background services must be able to access the SQL Server. All background services run using the LocalSystem account on the console. If you are using Integrated Windows Authentication on a remote server, be sure to use the machine account when defining the console login account on SQL Server.

  For security purposes, Ivanti recommends using Windows authentication where possible. For information on configuring a remote SQL Server to accept Windows authentication credentials from the Ivanti Patch for Windows® Servers console, see SQL Server Post-Installation Notes.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- In order to create the database, the user account you specify during the installation process must be assigned the **db-creator** role.
- If you are using SQL Server on a remote machine, you must configure the server to allow remote connections. This can be done using SQL Server Configuration Manager.
- If you want to use a clustered configuration for redundancy purposes it must be configured prior to installation. You then reference the virtual clustered instance during the installation process. Clustered configurations are not supported with SQL Server Express Editions.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

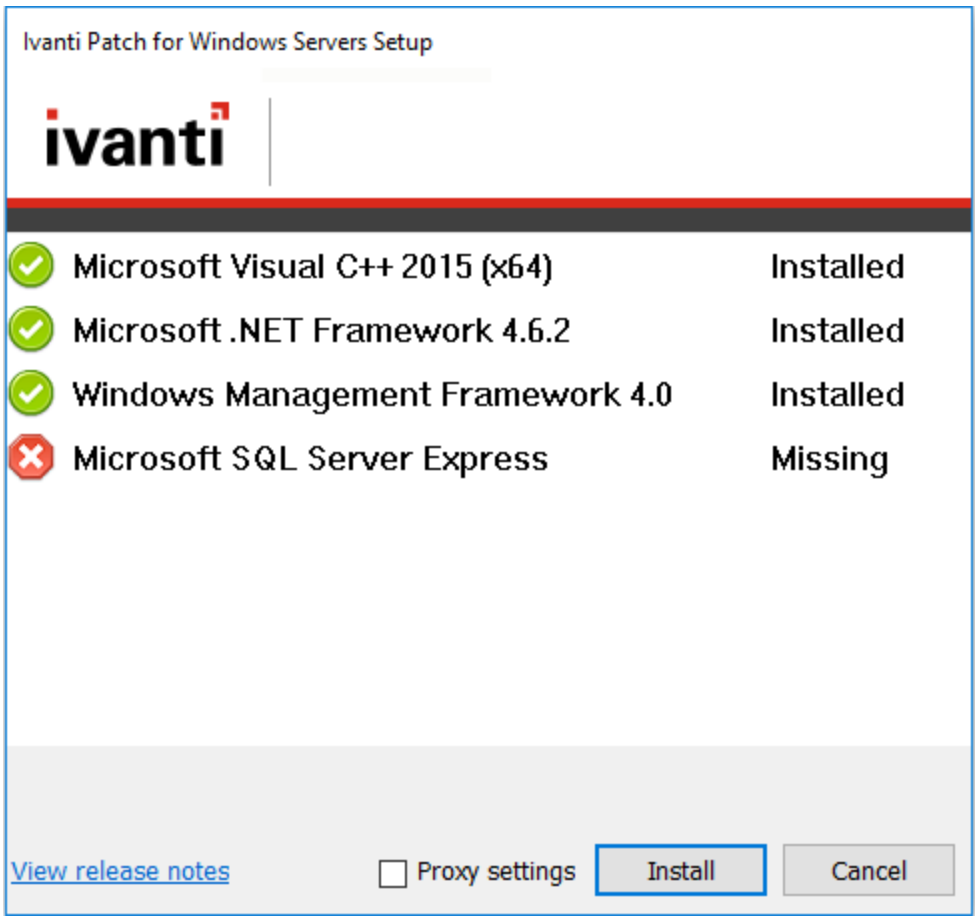
Performing a New Installation

If you are installing on a disconnected machine and are missing any of the prerequisite software, you must download the software from a connected machine and then manually install it on the disconnected console before you begin the installation process.

1. Begin the installation process by double-clicking the Ivanti Patch for Windows® Servers executable file.

   If you receive a prompt indicating that a reboot is required, click **OK** and the installation process will automatically resume after the reboot.

   If you are missing any prerequisites they are displayed in the **Setup** dialog. If you are not missing any prerequisites you will skip Step 2 - Step 4 and go directly to the **Welcome** dialog described in Step 5.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

2. If you are required to enter a user name and password each time you launch your browser and browse the Internet, enable the **Proxy settings** check box, click the link, and type the necessary credentials.

   It may be necessary to specify a domain as part of your user name (for example: mydomain\my.name). These settings can be modified later by going to **Tools > Options > Proxy**.

   It also may be necessary to modify your HTTP proxy information after the installation is complete. See HTTP Proxy Post Installation Notes for details.

3. Click the **Install**button to install any missing prerequisites.

   A few of the prerequisites require a reboot after they are installed. In this case the installation program will request a system reboot before continuing. The installation program will restart automatically following the reboot.

4. (Conditional) If you were missing any prerequisites that required a reboot, to continue with the installation after the reboot click **Install**.

5. Read the information on the **Welcome** dialog and then click **Next**.

   The license agreement is displayed. You must agree to the terms of the license agreement in order to install the program.

6. To continue with the installation click **Next**.

   The **Destination Folder** dialog is displayed.

7. If you want to change the default location of the program, click the browse button and choose a new location.

   TIP: If you want a shortcut icon to be created and placed on your desktop, enable the **Create a shortcut on the desktop** check box.

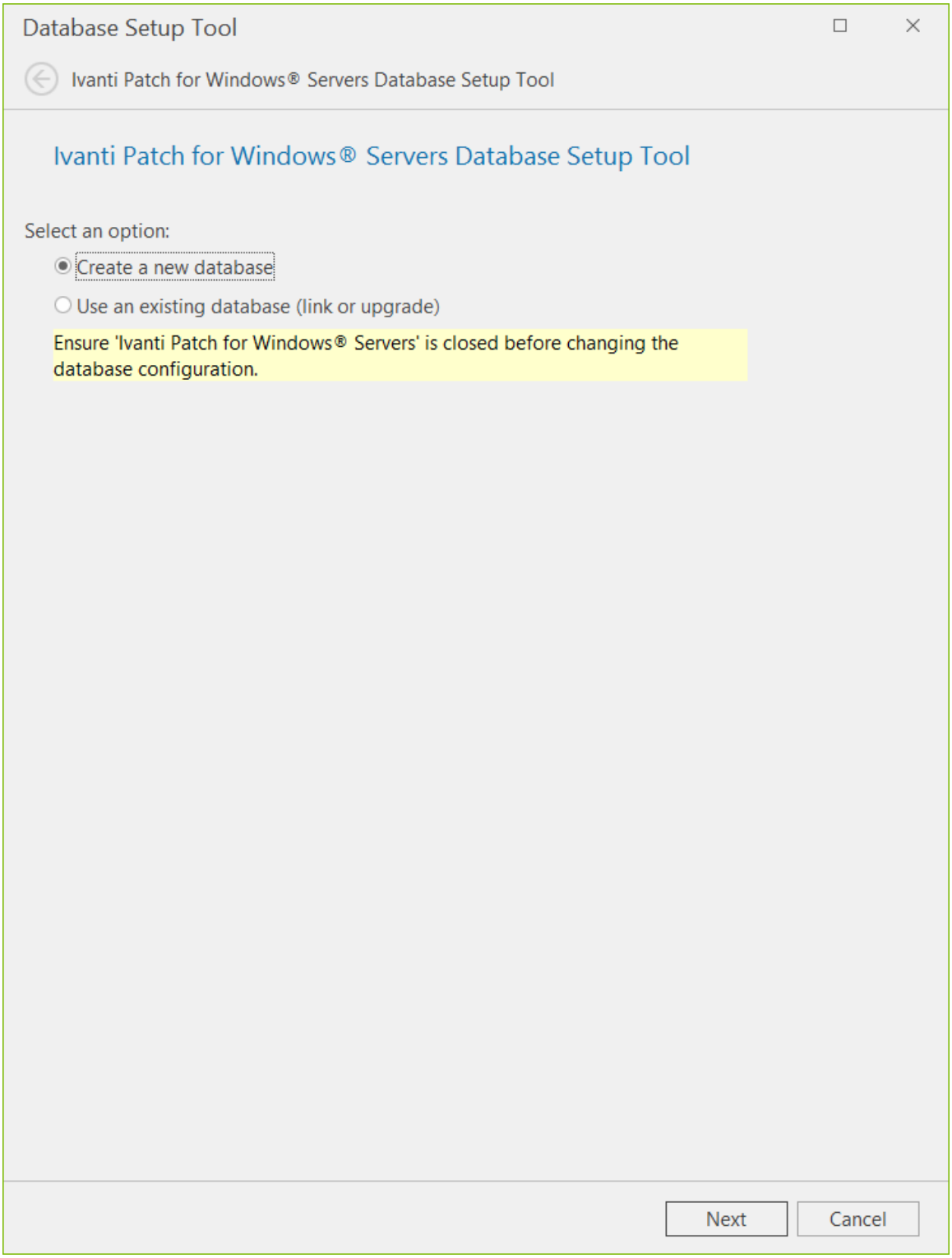
   Click **Next**. The **Product Improvement Program** dialog is displayed. Read the description and decide if you agree to participate in the program. The program enables Ivanti to collect product usage information that will help improve future versions of the product.

   When you are done, click **Next**. The **Ready to install** dialog is displayed.

8. To begin the installation click **Install**.

   Near the end of the installation process the **Database Setup Tool** dialog is displayed.

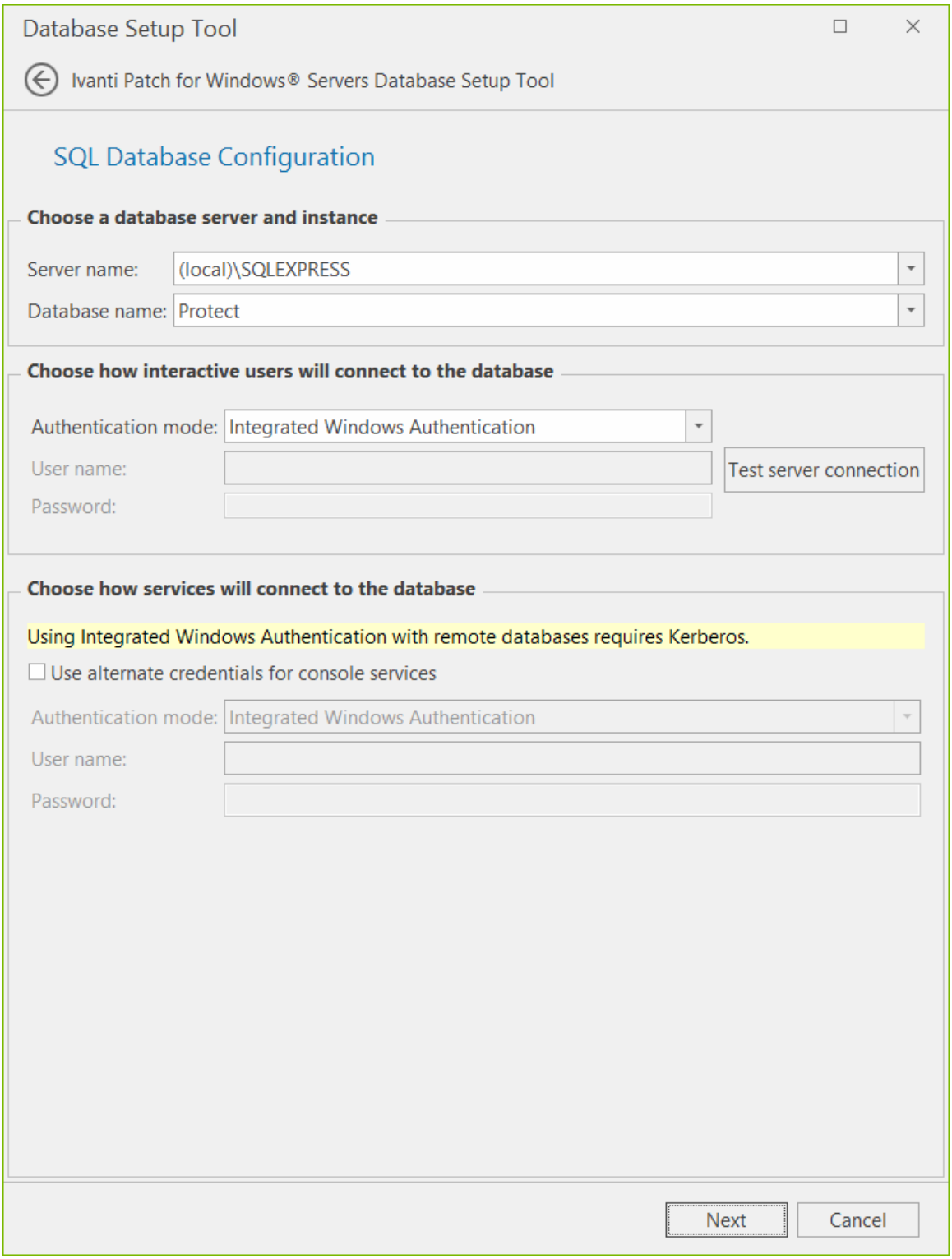
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



9. If you have a previously installed Ivanti Patch for Windows® Servers database that you wish to use, select **Use an existing database** and then click **Next**. Otherwise, select **Create a new database** and then click **Next**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

A dialog similar to the following is displayed:



10. Use the boxes provided to define how users and services will access the SQL Server database.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Choose a database server and instance

- **Server name:** You can specify a machine or you can specify a machine and the SQL Server instance running on that machine (for example: *machinename*\SQLExpress). If SQL Server is already installed, this box will be automatically populated with the local SQL Server instance name.
- **Database name:** Specify the database name you want to use. The default database name is **ProtectScans**.

Choose how interactive users will connect to the database

Specify the credentials you want the program to use when a user performs an action that requires access to the database.

- **Integrated Windows Authentication:** This is the recommended and default option. Ivanti Patch for Windows® Servers will use the credentials of the currently logged on user to connect to the SQL Server database. The **User name** and **Password** boxes will be unavailable.
- **Specific Windows User:** Select this option only if the SQL Server database is on a remote machine. This enables you to provide a specific Windows user name and password combination. This option will have no effect if the database is on the local (console) machine (see Supplying Credentials for more information about local machine credentials). All Ivanti Patch for Windows® Servers users will use the supplied credentials when performing actions that require interaction with the remote SQL Server database.
- **SQL Authentication:** Select this option to enter a specific SQL Server user name and password combination that will be used to log on to the specified SQL Server.

CAUTION! If you supply SQL authentication credentials and have not implemented SSL encryption for SQL connections, the credentials will be passed over the network in clear text.

- **Test Server Connection:** To verify that the program can use the supplied interactive user credentials to connect to the SQL Server database, click this button.

Choose how services will connect to the database

Specify the credentials you want the background services to use when making the connection to the database. These are the credentials that the results importer, agent operations, and other services will use to log on to SQL Server and provide status information.

- **Use alternate credentials for console services:**
  - If the SQL Server database is installed on the local machine you will typically ignore this option by not enabling this check box. In this case the same credentials and mode of authentication that you specified above for interactive users will be used.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- You will typically only enable this check box if the SQL Server database is on a remote machine. When the database is on a remote machine you need an account that can authenticate to the database on the remote database server.

- **Authentication method:** Available only if **Use alternate credentials for console services** is enabled.

  - **Integrated Windows Authentication:** Selecting this option means that the machine account will be used to connect to the remote SQL Server. The Kerberos network authentication protocol must be available in order to securely transmit the credentials. The User name and Password boxes will be unavailable.

If you choose Integrated Windows Authentication the installation program will attempt to create a SQL Server login for the machine account. If the account creation process fails, see SQL Server Post-Installation Notes for instructions on manually configuring a remote SQL Server to accept machine account credentials. Do this after you complete the Ivanti Patch for Windows® Servers installation process but before you start the program.

  - **Specific Windows User:** Select this option to enter a specific Windows user name and password combination. Ivanti Patch for Windows® Servers's background services will use these credentials to connect to the SQL Server database. This is a good fallback option if for some reason you have difficulties implementing integrated Windows authentication.

  - **SQL Authentication**: Select this option to provide a specific SQL Server user name and password combination for the services to use when logging on to SQL Server.

11. After providing all the required information, click **Next**.

If the installation program detects a problem with any of the specified credentials, an error message will be displayed. This typically indicates that a user account you specified does not exist. Make a correction and try again.

The program will create, link to, or upgrade the database. When the database operation is complete the **Database Complete** dialog is displayed.

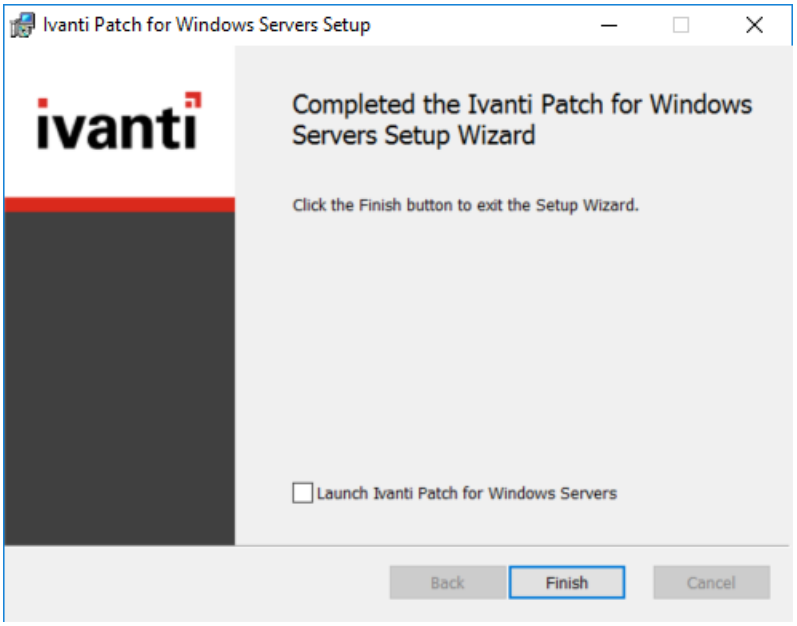
12. Click **Next**.

    The **Installation Complete** dialog is displayed.

13. Click **Finish**.

    The **Completed** dialog is displayed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



14. If you want to start Ivanti Patch for Windows® Servers immediately, enable the **Launch Ivanti Patch for Windows® ServersLaunch Patch Authority Ultimate** check box and then click **Finish**; otherwise, just click **Finish**.
15. See HTTP Proxy Post-installation Notes and SQL Server Post-installation Notes.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

HTTP Proxy Post-Installation Notes

If your location uses an HTTP proxy to access the Internet, please note the following requirements:

- You must enable the **Bypass proxy server for local addresses** check box in the browser's proxy server settings. To access these settings, on the **Tools** menu in Internet Explorer, click **Internet Options**, click the **Connections** tab, and then click **LAN Settings**. Enabling the **Bypass proxy server for local addresses** check box specifies that the proxy server should not be used when the Ivanti Patch for Windows® Servers console connects to a computer on the local network.
- The consoles services will not read or reference any per-user proxy address information. To configure proxy addresses for console services, you must manually modify the **STServiceHost.exe.config** file to include a default proxy XML tag that defines the proxy, bypass local and bypasslist. You do this by adding the following XML beneath the base <configuration> element.

```
<system.net>
 <defaultProxy>
  <bypasslist>
   <add address="127.0.0.1" />
   <add address="::1" />
   <add address="RollupConsoleNameOrIPAddress" />
  </bypasslist>
  <proxy bypassonlocal="True" proxyaddress="http://ProxyNameOrIP:Port"
/>
 </defaultProxy>
</system.net>
```

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

SQL Server Post-Installation Notes

Manually Configuring a Remote SQL Server to Accept Machine Account Credentials

The manual process described here is required only if the automated account creation process failed during product installation.

If you are using Integrated Windows Authentication to access a remote SQL Server, in order for Ivanti Patch for Windows® Servers to interact properly with the server you must configure the server to accept machine account credentials. The best time to do this is immediately after you have installed Ivanti Patch for Windows® Servers but before you actually start the program. You can, however, perform these steps after starting the program. Any scans you initiate prior to this that require interaction with a remote SQL Server database will probably fail.

This section describes how to configure a remote SQL Server to accept Windows authentication (machine account) credentials from the Ivanti Patch for Windows® Servers console. For security purposes, Ivanti recommends using Windows authentication where possible. Microsoft SQL Server Management Studio is used as the editor in the following examples but you can use a different tool if you prefer.

1. The Ivanti Patch for Windows® Servers console and SQL Server must be joined to the same domain or reside in different domains that have a trusted relationship.

   This is so the console and the server can compare credentials and establish a secure connection.

2. On SQL Server, create a new login account for Ivanti Patch for Windows® Servers to use.

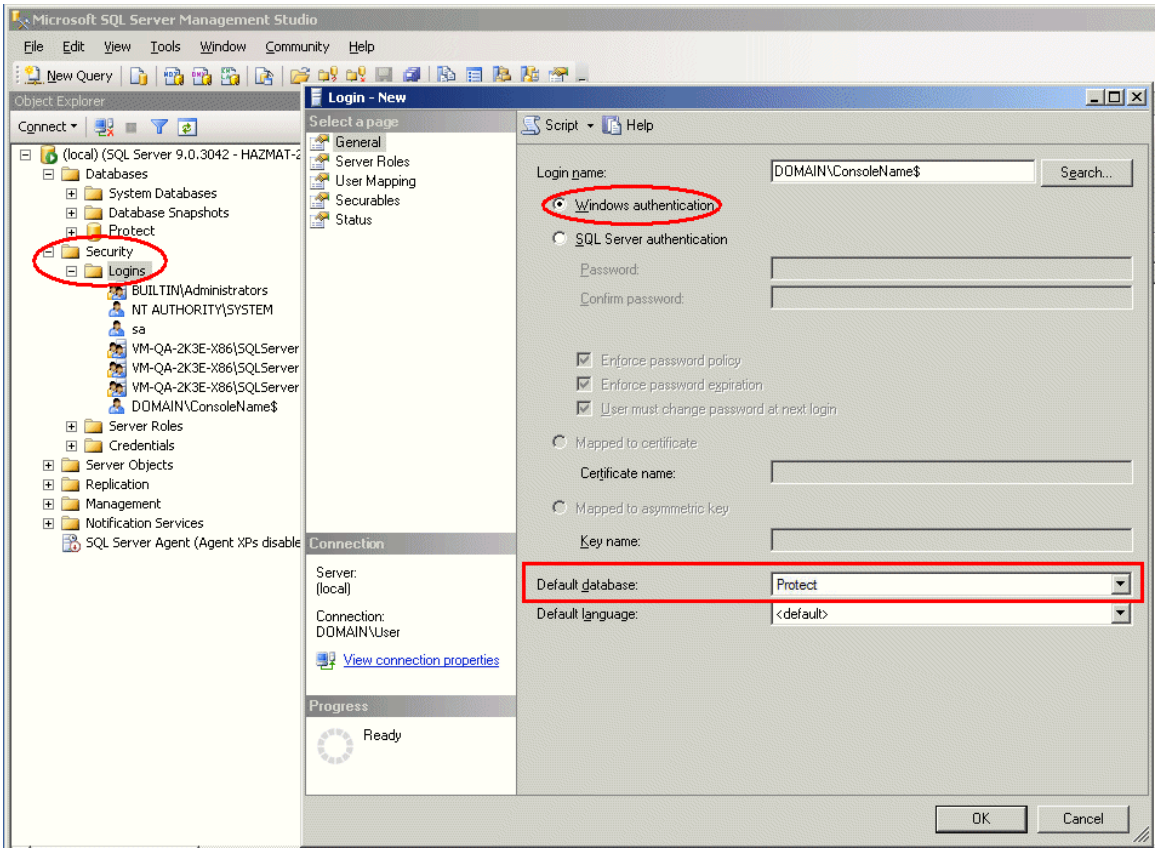
   You must have *securityadmin* privileges in order to create an account.

   To do this: Within the **Security** node, right-click **Logins** and select **New Login**. Type the login name using a SAM-compatible format (domain\machine name). The machine account is your console's machine name and must contain a trailing $.

   Do not use the **Search** option. You must manually type the name because it is a special name.

   Make sure you choose **Windows Authentication** and that the **Default database** box specifies the Ivanti Patch for Windows® Servers database.

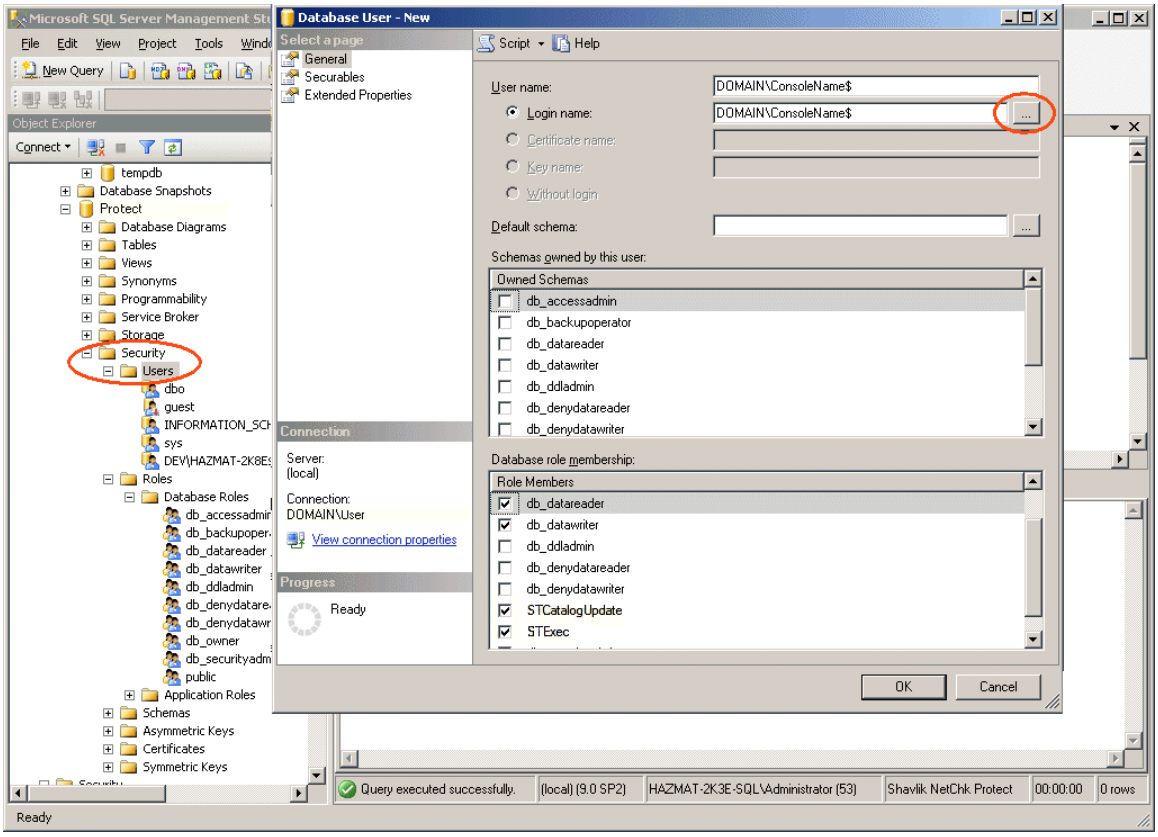
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



3. For your Ivanti Patch for Windows® Servers database, create a new user login using the console machine account.

   Right-click the **Users** folder, select **New User**, browse to find the **Login name**, and then paste the name in the **User name** box. Assign the user the **db_datareader**, **db_datawriter**, **STCatalogUpdate**, and **STExec** roles.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



4. Start Ivanti Patch for Windows® Servers.
5. Perform any troubleshooting as necessary.
    - You can use the SQL Server activity monitor to determine if connection attempts are successful when performing a patch scan.
    - If you ran Ivanti Patch for Windows® Servers before creating the SQL Server user account, some services may fail to connect to SQL Server. You should select **Control Panel** > **Administrative Tools** > **Services** and try restarting the services.
    - If the connection attempts are failing you can view the messages in the SQL Server logs to determine why the failures are occurring.

Allowing Other Users Access to the Program

This section also applies if you are using the role-based administration feature.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

If you wish to allow other users access to the program, you may need to configure SQL Server so that those users have the necessary database permissions. Specifically, when using Windows integrated authentication, users without administrative rights on the database machine must be granted read and write permission to all tables and views. They must also be granted execute permission to all stored procedures in the Ivanti Patch for Windows® Servers application database. They may not otherwise be able to start Ivanti Patch for Windows® Servers.

One way to grant these permissions is to assign your users the *db_owner* role. For security reasons, however, this may not be the best solution. A safer alternative is to grant execute permission at the database level. You do this by assigning the users in question to the *STExec* role.

Performing Periodic Maintenance on the Database

Ivanti Patch for Windows® Servers provides the ability to perform periodic maintenance on the database by automatically removing old scans, rebuilding index files, and performing backups. See Database Maintenance for details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Starting Ivanti Patch for Windows® Servers

In order to access the full capabilities of Ivanti Patch for Windows® Servers, you must run under a Windows account with administrator privileges.

You can start Ivanti Patch for Windows® Servers two ways:

- Tap or double-click the **Ivanti Patch for Windows® Servers** icon on your desktop
- Select **Start > Ivanti Patch for Windows® Servers >Ivanti Patch for Windows® ServersScriptLogic Corporation > Patch Authority Ultimate**

After starting the program the home page is displayed. See Navigating the Interface for detailed information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Activating Ivanti Patch for Windows® Servers

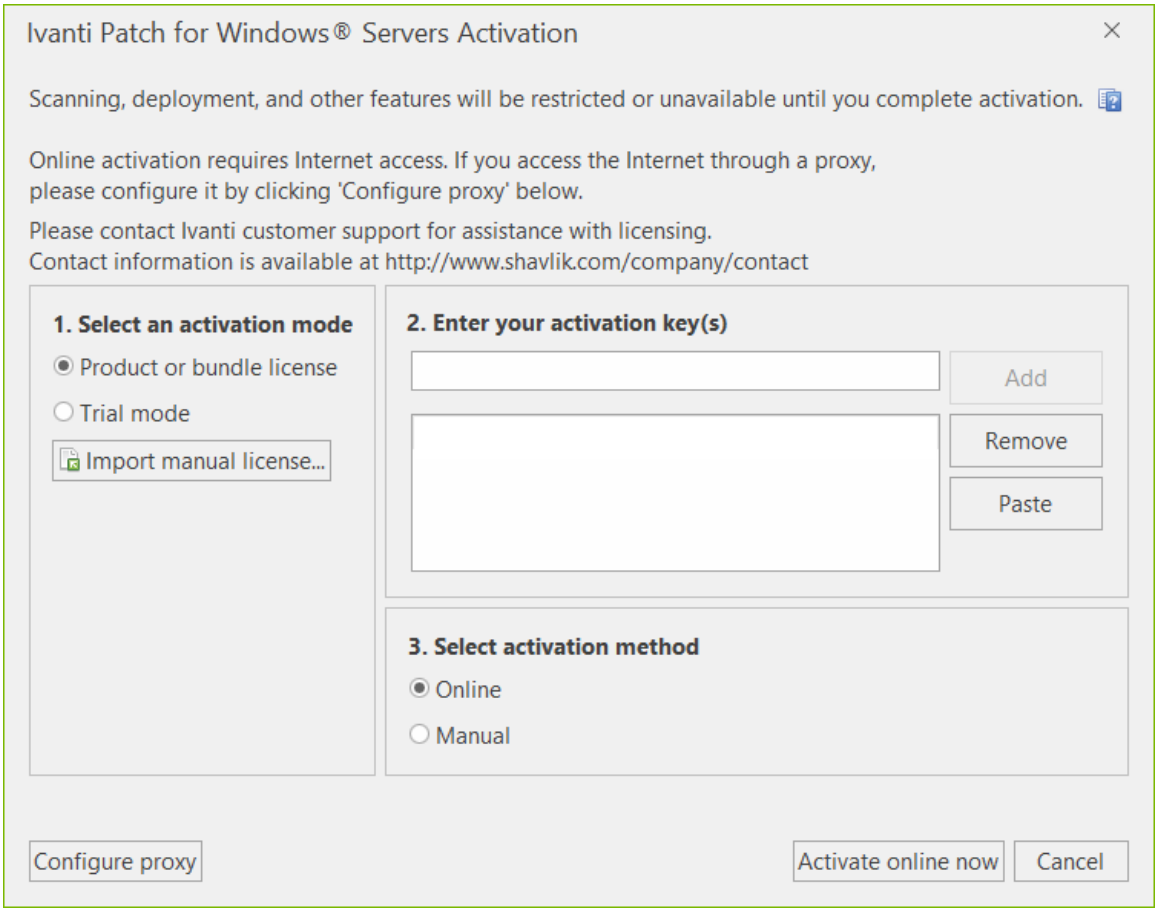
Until you activate Ivanti Patch for Windows® Servers you are very limited in the actions you are allowed to perform. You activate the program by entering one or more activation keysa valid activation key. To activate Ivanti Patch for Windows® Servers:

1. If you have an electronic copy of your license key(s) copy it to your computer's clipboard.

   Your license key is typically sent to you in an email from Ivanti when you purchase the product.

2. From the Ivanti Patch for Windows® Servers menu select **Help > Enter/refresh license key**.

   The **Activation** dialog is displayed.



3. (Optional) If you didn't copy the key into your computer's clipboard until after you launched this dialog, click **Paste**.

   You can also manually type your activation key if you prefer.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

4. (Optional) If your organization uses a proxy server, click **Configure proxy** and provide the credentials necessary for the activation process to reach the activation server.

   If you are required to enter a user name and password each time you launch your browser and access the Internet, it typically means you are using a proxy server.

IF YOU HAVE AN INTERNET CONNECTION

1 Select an activation mode.

   - **Product or bundle license:** Selecting this option enables you to specify one or more activation keys. If you receive multiple keys be sure to paste them all in the **Enter your activation key(s)** box. Each key represents a different edition (Standard, Advanced), add-on, license seat count (workstation, server), or expiration date. The keys are additive so the resulting product license will be a compilation of all features and seat counts provided by the individual keys.
   - **Product or bundle license:** Enables you to enter your license key.
   - **Trial mode:**Enables you to test all the capabilities of Ivanti Patch for Windows® Servers, but only for 60 days. You are also limited to 50 license seats. When the trial license expires the program will stop refreshing its data files and many of the program features will no longer be available.
   - **Import manual license:** Enables you to import a license that was generated by the Ivanti web portal. This is used only by console machines that are not connected to an external network. See the following section for more details.Enables you to import a license that was emailed to you by Shavlik. This is used only by console machines that are not connected to an external network. See the following section for more details.

2. Verify that your activation key is specified in the **Enter your activation keys** box.

   If not, copy your key to your computer's clipboard and then click **Paste**.

3. Select **Online** activation.
4. Click **Activate online now**.

   If the activation is successful the message **Patch for Windows® ServersPatch Authority Ultimateproduct activation successfully completed** is displayed near the bottom of the dialog.

5. Click **Close**.

IF YOU DO NOT HAVE AN INTERNET CONNECTION (DISCONNECTED NETWORK MODE)

This procedure will not work if you are at a secure site that does not allow files to be transferred out of the secure environment. For this case, see the section below titled *If You are Activating from Within a Secure Disconnected Network*.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

1 Select an activation mode (either **Product or bundle license** or **Trial mode**).

2. Paste or type your key into the **Enter your activation key(s)** box.
3. Select **Manual** activation.
4. Click **Create request**.

   Two files are generated and saved to the desktop of your console computer: an XML file named **LicenseInfo.xml** and a text file named **DisconnectedLicenseInfo.txt**. The XML file is used in this procedure; the text file can be ignored.

5. Move the XML activation request file to a computer that has an Internet connection.
6. On the Internet-connected computer, open a browser and go to https://license.shavlik.com/OfflineActivation.
7. Upload the **LicenseInfo.xml** activation request file.

   The web portal will process the license information and generate a license file.

8. Download the processed license file and move it to the console computer.
9. Within Ivanti Patch for Windows® Servers, select **Help > Enter/refresh license key**.
10. On the Ivanti Patch for Windows® Servers **Activation** dialog click **Import manual license**.
11. Go to the location of the processed license file and then click **Open**.

    Ivanti Patch for Windows® Servers will process the file and the program will be activated.

1 Paste or type your key into the **Enter your activation key(s)** box.

2. Select **Manual** activation.
3. Click **Create request**.

   An XML file named LicenseInfo.xml is generated and saved to the desktop of your console computer. This file contains the information needed to make an offline activation request.

4. Move the XML file to a computer that has an Internet connection.
5. Email the file to support@scriptlogic.com.

   Ivanti will process the license information and email you back the processed license file.

6. When you receive the processed license file, move the file to the console computer.
7. Within Ivanti Patch for Windows® Servers, select **Help > Enter/refresh license key**.
8. On the Ivanti Patch for Windows® Servers**Activation** dialog click **Import offline license**.
9. Go to the location of the processed license file and then click **Open**.

   Ivanti Patch for Windows® Servers will process the file and the program will be activated.

IF YOU ARE ACTIVATING FROM WITHIN A SECURE DISCONNECTED NETWORK

Use this activation procedure if you are at a secure site that does not allow files to be transferred out

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

of the secure environment.

1 Select an activation mode (either **Product or bundle license** or **Trial mode**).
2. Paste or type your key into the **Enter your activation key(s)** box.
3. Select **Manual** activation.
4. Click **Create request**.

   Two files are generated and saved to the desktop of your console computer: an XML file named **LicenseInfo.xml** and a text file named **DisconnectedLicenseInfo.txt**. The text file is used in this procedure; the XML file can be ignored.
5. Open the **DisconnectedLicenseInfo.txt** file and carefully copy the information contained in it to a piece of paper.
6. On an Internet-connected computer, open a browser and go to https://license.shavlik.com/OfflineActivationhttps://license.scriptlogic.com.
7. Manually enter the activation request data and then click **Submit**.

   The web portal will process the data and generate a license file.
8. Download the processed license file and move it to the console computer.
9. Within Ivanti Patch for Windows® Servers, select **Help > Enter/refresh license key**.
10. On the Ivanti Patch for Windows® Servers**Activation** dialog click **Import manual license**.
11. Go to the location of the processed license file and then click **Open**.

    Ivanti Patch for Windows® Servers will process the file and the program will be activated.

TRACKING YOUR LICENSE

You can easily find out information about your license by selecting **Help > About Ivanti Patch for Windows® Servers**. For more information see How Licenses are Tracked.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Version and License Information

Selecting **Help > About Ivanti Patch for Windows® Servers** will provide a variety of information about Ivanti Patch for Windows® Servers.

Application and Version Information

The center portion of the **Help > About** dialog is used to view both application and version information. To toggle between both views, click either the **Version Info** or **App Info** button (the button name changes each time it is clicked).

- **App Info**: Displays application information for Ivanti Patch for Windows® Servers and information about the database being used by the program, including:
  - **Program Version**: Displays both the version and the edition of the program being used.
  - **Administration Role:** If role-based administration is enabled, displays the current role assignment.
  - **License Key and Licensed Capabilities**: Displays license key information and identifies which features are enabled.
  - **Configured Database**: Displays the current database being used.
- **Version Information**: Displays version information about each of the program components being used by the program. This can be helpful if you ever need to perform any troubleshooting of the program as you can quickly determine if you are using the most current data.

Export Information

To save the version information to a Notepad file, click **Export info**.

Open Source License

To view license information for the open source packages distributed with Ivanti Patch for Windows® Servers, click **Open Source license**.

Technical Support

To learn about technical support options, click **Tech support**.

Data Versions and Product End of Life Notification

The **Data Versions** area on the right shows the current versions of the definition files being used by the program.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

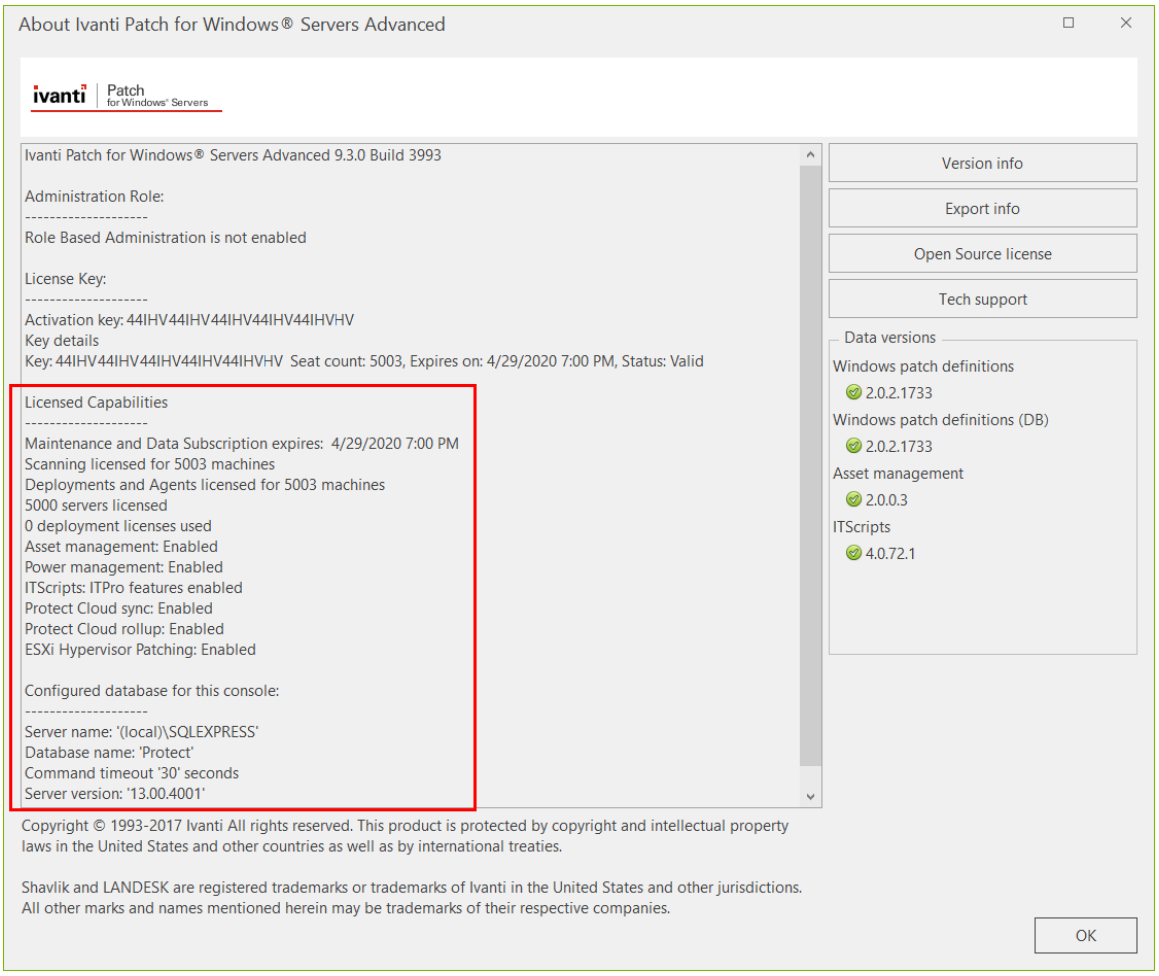
In addition, if the version of Ivanti Patch for Windows® Servers that you are using is nearing its end of life (EOL) date, the EOL date will be displayed. No new updates to the XML patch data file will be provided after the EOL date, rendering the program ineffective. You should upgrade to the latest version of the program well in advance of the EOL date. As an aid, if an EOL date has been announced for your version of the program, a notification will be displayed when you start Ivanti Patch for Windows® Servers. The notification will indicate when the version will expire and it will provide a link to get the latest version.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Licenses are Tracked

When a patch deployment is performed, Ivanti Patch for Windows® Servers records the machine name in the database if it does not already exist. From there, the number of remaining seats available for deployment is reduced by one for each target. If you elect to use Ivanti Patch for Windows® Servers Agent, each agent machine is allocated a license and also counts against the total number of license seats available. If the same machine is managed in both an agentless and agent-based manner, that machine is counted only once. Similarly, when scanning virtual machines, a machine is counted only once even if it is scanned both in online (powered on) mode and offline (powered off) mode.

You can easily find out how many license seats have been used by choosing **Help > About Ivanti Patch for Windows® Servers**.

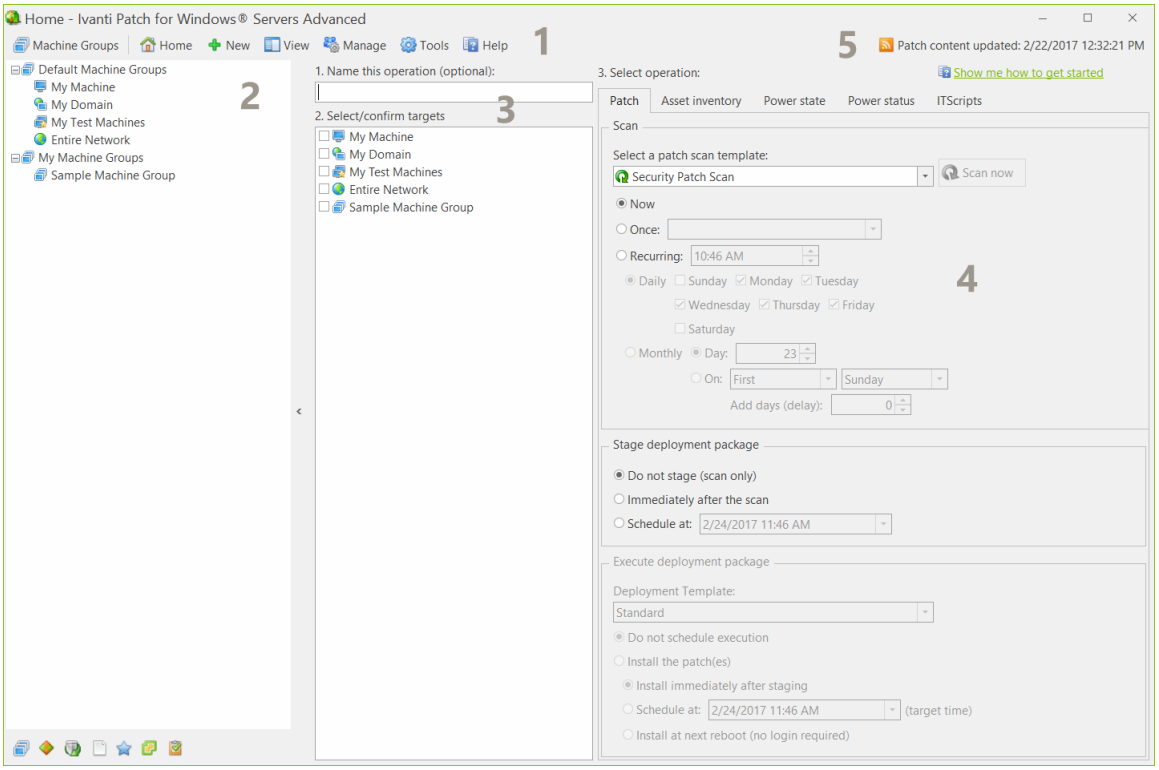


Power management (including Wake-on-LAN) and portions of the ITScripts function require either a Ivanti Patch for Windows® Servers Advanced license or a separate power management add-on license key if you are using Ivanti Patch for Windows® Servers Standard.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

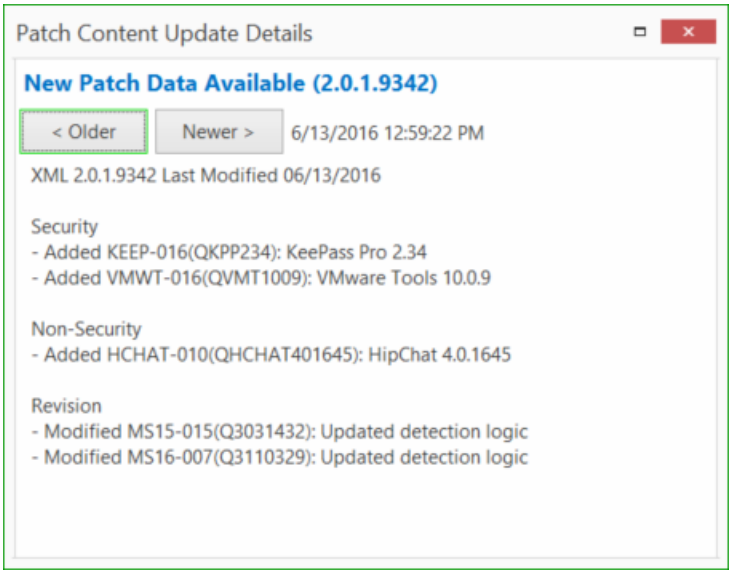
Navigating the Interface

The Ivanti Patch for Windows® Servers interface is designed to be simple yet powerful, enabling you to perform any number of activities quickly and easily. An annotated interface is shown here. For information about each area of the interface, see the table that follows.



1	The menu bar provides quick access to many of the functions of the program.
2	The navigation pane displays whatever primary feature is currently selected. There can be only one feature active at a time. In this example the Machine Groups feature is the active feature. You can collapse the navigation pane by clicking the icon. This maximizes the size of the right-hand pane.

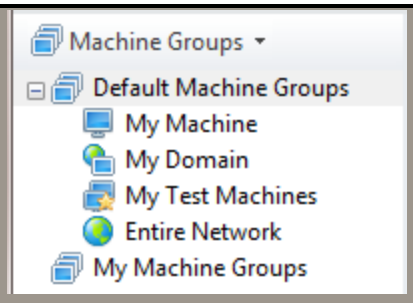
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

3	This area is used to select the machine group(s) you want to perform an operation on.
4	This area enables you to quickly configure and initiate patch, asset, power and ITScripts operations.
5	The date that the patch content was last updated is displayed in the upper-right corner of the home page. This is a configurable item and can be disabled using the **Tools > Options > Display > Show patch content release date** check box. If you click the date, the **Patch Content Update Details** dialog is displayed. Use this dialog to view more detailed information about the current patch data and about previous patch data releases. This newsfeed will also be used to display important security-related news and messages from Ivanti. 

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Major Program Features

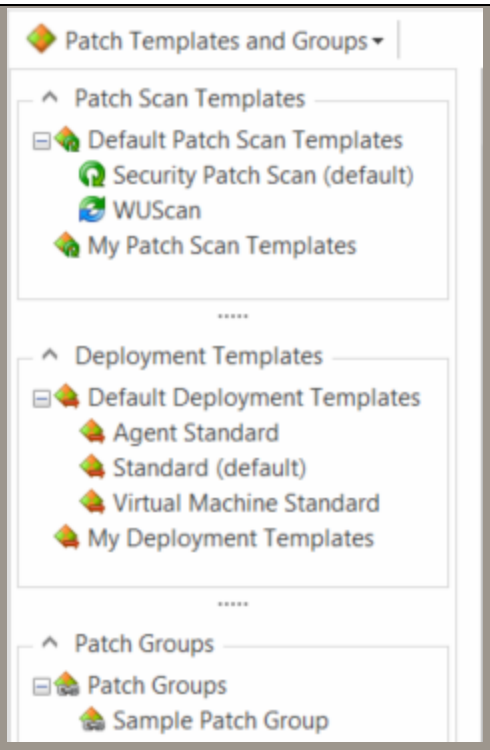
The following program features are available using the selection box located at the top of the navigation pane.



Machine groups are used to define the machines you want included in a particular scan. Many actions within the program are performed using machine groups. The Machine Groups pane contains the following:

- **My Machine:** A default group consisting of only the console machine.
- **My Domain:** A default group consisting of the machines in the local domain.
- My Test Machines: A default group that is initially empty. You should add machines to this group that represent a 'smaller' view of your actual network environment and use the group to perform tests.
- **Entire Network:** A default group consisting of all machines visible on the network.
- **My Machine Groups:** Contains a list of your custom machine groups. To create a custom machine group, select **New > Machine Group**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

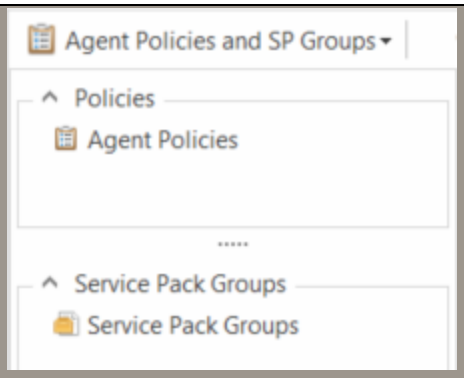
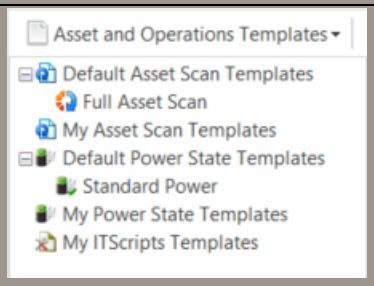


The **Patch Templates and Groups** list contains three types of items.

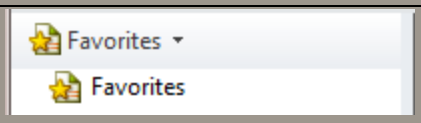
- A patch scan template defines exactly how a patch scan will be performed. The available patch scan templates are:
  - **Security Patch Scan:** Scans for missing and installed security patches.
  - **WUScan:** Scans for both security patches and non-security patches.

  To create your own custom patch scan template, select **New > Patch Scan Template**.
- A deployment template provides a way to save desired settings for patch deployment and have them quickly available for future deployments. To view the settings for the three default templates, click **Agent Standard**, **Standard**, or **Virtual Machine Standard**. To create a new template, select **New > Deployment Template**.
- A patch group is a collection of patches that you wish to scan for and/or deploy. Patch groups can represent required or mandatory patches that have been approved for your organization. To create a new group, select **New > Patch Group**.

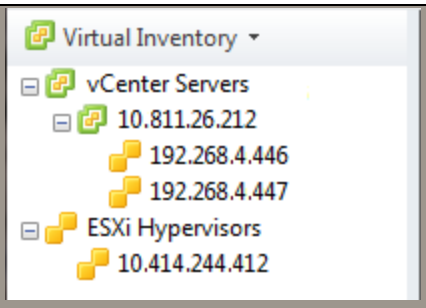
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	The **Agent Policies and SP Groups** list contains two types of items. • An agent policy defines exactly what an agent can and cannot do. With Ivanti Patch for Windows® Servers Agent you can create as many different agent policies as is needed. A policy can be used to scan for missing patches, to determine software and hardware assets, and to perform power state tasks. To create a new agent policy, select **New > Agent Policy**. • A service pack (SP) group is a collection of service packs that you wish to deploy using agents. Service pack groups can represent required or mandatory SPs that have been approved for your organization. To create a new group, select **New > Service Pack Group**.
	The **Asset and Operations Templates** list supports the use of a number of different types of templates. • An asset scan template defines exactly how an asset scan will be performed. The default asset scan template is configured to perform a software and hardware scan. You can also create your own unique asset scan template by selecting **New > Asset Scan Template**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

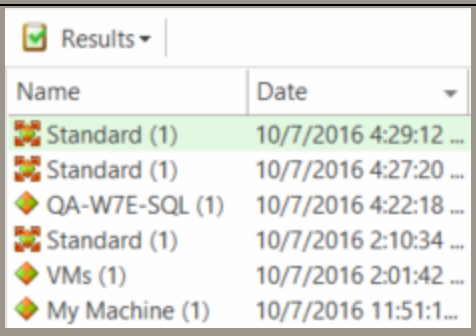
	• A power state template defines what power management tasks should be performed. The default power state template is named **Standard Power** and is configured to initiate a restart of the selected machines. It enables a logged on user to extend the reboot in one minute increments up to 10 minutes. You can also create your own unique power state template by clicking **New > Power State Template**. Power management (including Wake-on-LAN) requires either a Ivanti Patch for Windows® Servers Advanced license or a separately purchased add-on license key. • An ITScripts template specifies which script to execute and what parameter values and mode to use when executing the script. You can create an ITScripts template by clicking **New > ITScripts Template**. Portions of the ITScripts function require a Ivanti Patch for Windows® Servers Advanced license .
	A favorite is a collection of machines to scan and a choice of how to scan them. To create a new favorite, select **New > Favorite**. Select the machine groups you want to scan and then select the desired scan template.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



The Virtual Inventory list is used to manage and track the vCenter Servers and the ESXi hosts that are used in your organization. You can use the Virtual Inventory feature to:

- Add vCenter Servers and ESXi hosts to Ivanti Patch for Windows® Servers
- View basic configuration information about the vCenter Servers and the ESXi hosts
- Perform a patch scan of the managed and unmanaged ESXi hosts
- View the security bulletins that have already been installed on the managed and unmanaged ESXi hosts
- View the security bulletins that are missing on the managed and unmanaged ESXi hosts
- Deploy the patches associated with each missing security bulletin
- Power on and off the virtual machines that reside on your managed and unmanaged ESXi hosts
- Add the virtual machines and virtual machine templates to a new or existing machine group



A history of the patch scans, patch deployments, and power status scans that you have performed is available in the **Results** list. The number of days' worth of items displayed in the **Results** list is configured using **Tools > Options > Display**.

To view the results of a scan or deployment, select the desired item. Detailed information about scans will be presented in Scan View and detailed information about deployments will be presented in Deployment Tracker.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	You can right-click on an item to either delete it from the list or to rename it. Here's a quicker method for deleting many items at once from any of these lists: 1. Select **Manage > Items**. 2. On the summary screen that appears select the items you want to delete. 3. Click **Delete Selected**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Charts

You access the charts page by selecting **View > Charts**. The charts page displays a number of charts that show the security status of your network at the time of the most recent machine scans. Two charts are displayed at a time. You can toggle through all the available charts by clicking **Previous** and **Next**. If you want certain charts to always be displayed or never be displayed you can do so by clicking **Options**.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Menu Commands

The menu commands that are available are dependent upon your particular product license.

The Ivanti Patch for Windows® Servers menus enable you to do the following:

New:

- **Agent Policy**: Create a new agent policy
- **Asset Scan Template**: Create a new asset scan template
- **Deployment Template:** Create a new deployment template
- **Favorite:** Create a new favorite
- **ITScripts Template**: Create a new ITScripts template
- **Machine Group:** Create a new machine group
- **Patch Group:** Create a new patch group
- **Patch Scan Template:** Create a new patch scan template
- **Power State Template**: Create a new power state template
- **Service Pack Group**: Create a new service pack group
- **Import Machine Group**: Imports an existing group definition from an encrypted XML file
- **Import Patch Group**: Imports an existing patch group definition from a text file
- **Add vCenter Server/ESXi Hypervisor**: Add a vCenter Server or an ESXi Hypervisor to your virtual inventory

View:

- **Charts:** Displays a number of charts that show the security status of your network at the time of the most recent machine scans
- **Machines:** Displays current information about every machine in your network that has been previously scanned
- **Patches:** Provides detailed information about patches for the various operating systems and applications scanned for by Ivanti Patch for Windows® Servers
- **ITScript results:** Displays information about the scripts that have been executed on your target machines
- **Event History:** Displays log entries that are generated by background operational events

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **Operations Monitor:** Launches the Ivanti Patch for Windows® Servers Operations Monitor, which tracks a number of different background tasks
- **Deployment Tracker**: Launches Ivanti Patch for Windows® Servers Deployment Tracker, which tracks deployment tasks that are currently in progress
- **Refresh:** Refresh the information displayed in the right-hand pane

Manage:

- **Address Book**: Displays the address book used to store the names and email addresses of contacts you wish to send reports
- **Credentials**: Launches the Credential Manager, which manages all credentials used within the program
- **Items**: Displays a list of all prior scans and patch deployments
- **ITScripts**: Launches the Script Catalog Manager, which enables you to specify which scripts are approved for use within your organization
- **User Role Assignment**: Used to assign specific roles to specific administrators
- **Custom Patches**: Used to create and manage custom patches, products, and bulletins
- **Scheduled Remote Tasks**: This is a legacy menu item that no longer applies to version 9.3 or later. You now access the Scheduled Remote Tasks Manager from Machine View or Scan View by right-clicking on a machine and then selecting **View scheduled tasks**. For more information, see About the Scheduled Remote Tasks Manager.
- **Scheduled Console Tasks:** Launches the Scheduled Console Tasks Manager, which is used to monitor the status of tasks that have been scheduled to run on the console

Tools:

- **Edit database description**: Launches the Edit Database Description dialog, which is used to change the name the program uses when referring to the database
- **Console alias editor**: Launches the Console Alias Editor dialog, which is used to assign trusted names and IP addresses to the console certificate
- **Create report**: Launches the Report Gallery, which is used to generate a variety of reports on any of the scans and patch deployments that have been performed
- **Schedule report:** Launches the Schedule Report dialog
- **Custom Patch Editor**: Used to create and manage custom patches, products, and bulletins

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **Run console ITScripts**: Enables you to select and run those scripts that run on the console machine but not against target machines
- **Auto-update definitions**: Automatically downloads new data definition files immediately before performing a new scan. Enabling this check box will also enable the **Auto-update definitions (before scans)** check box on the **Tools > Options > Downloads** dialog.
- **Options**: Launches the Options dialog, which enables you to configure a number of different program options

Help:

- **Enter/refresh license Key**: Enables you to activate the program or to upgrade your program license
- **Check for program updates**: Checks if a new version of the program is available
- **Product Improvement Program**: Enables the capture of product usage information

  The Product Improvement Program enables Ivanti to collect product usage information. The program is anonymous and no personal, machine, network, or licensing information is collected. If you choose to participate, you agree to share system information (such as operating system, processor, and memory installed), product information (such as version number), and feature usage information (such as agents, asset management, and power management). This information will help us to improve future versions of the product. The information is sent only a few times a year and the process will not impact your network.
- **Refresh files**: Downloads new versions of the XML files and the command files used by the program
- **View how-to tutorials**: Provides links to a website that contains tutorials that show you how to perform certain tasks
- **View help**: Display the Help contents tab
- **Submit a feature request**: Links to a webpage that enables you to provide feedback on Ivanti products
- **About Ivanti Patch for Windows® Servers**: Displays program version information

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Editing the Database Description

You can change the name the program uses when referring to the database. This serves two purposes:

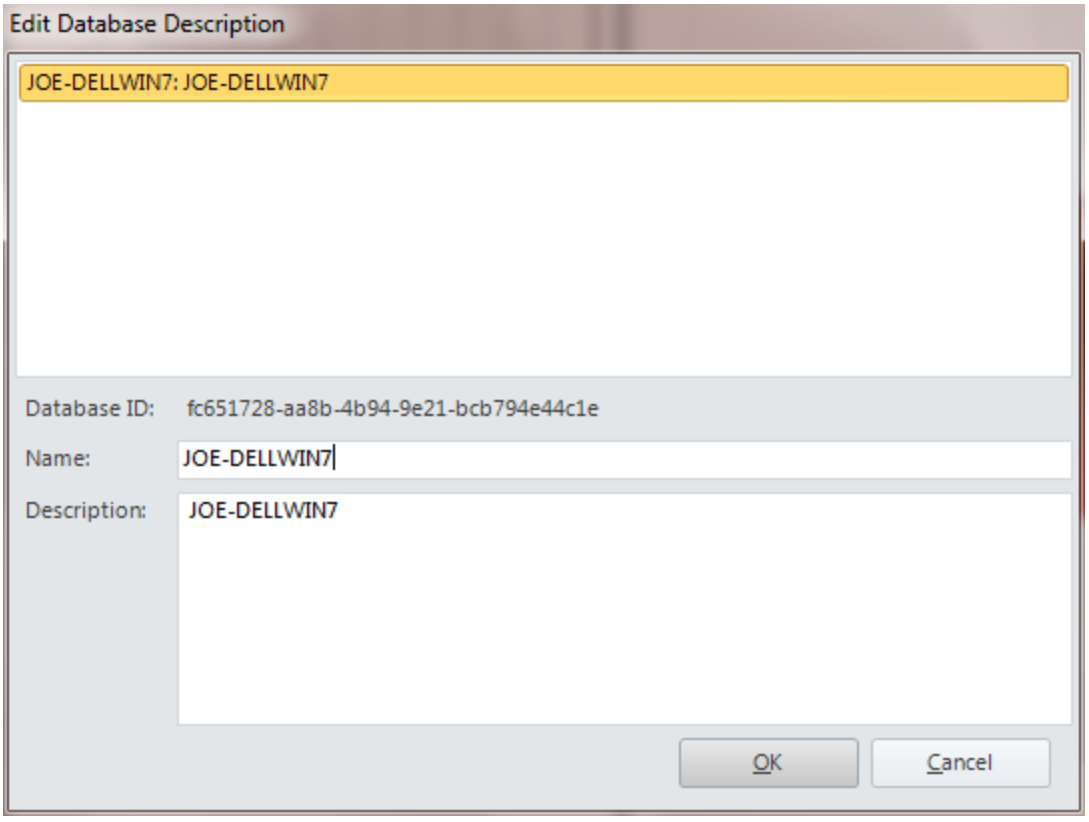
- It enables you to assign a user-friendly name to use for all references to the database. By default the name for the database is the console computer name. If there is only one console using the database then the default name may be fine. But in some cases the default name may not have much meaning to you and you'll want to change the name.
- It helps avoid confusion if the database is on a remote server or if two or more consoles are using the same database.

This does not change the actual name of the database; rather, it simply provides a user-friendly name for the program to use when referring to the database.

To edit the console name:

1. Select **Tools > Edit database description**.

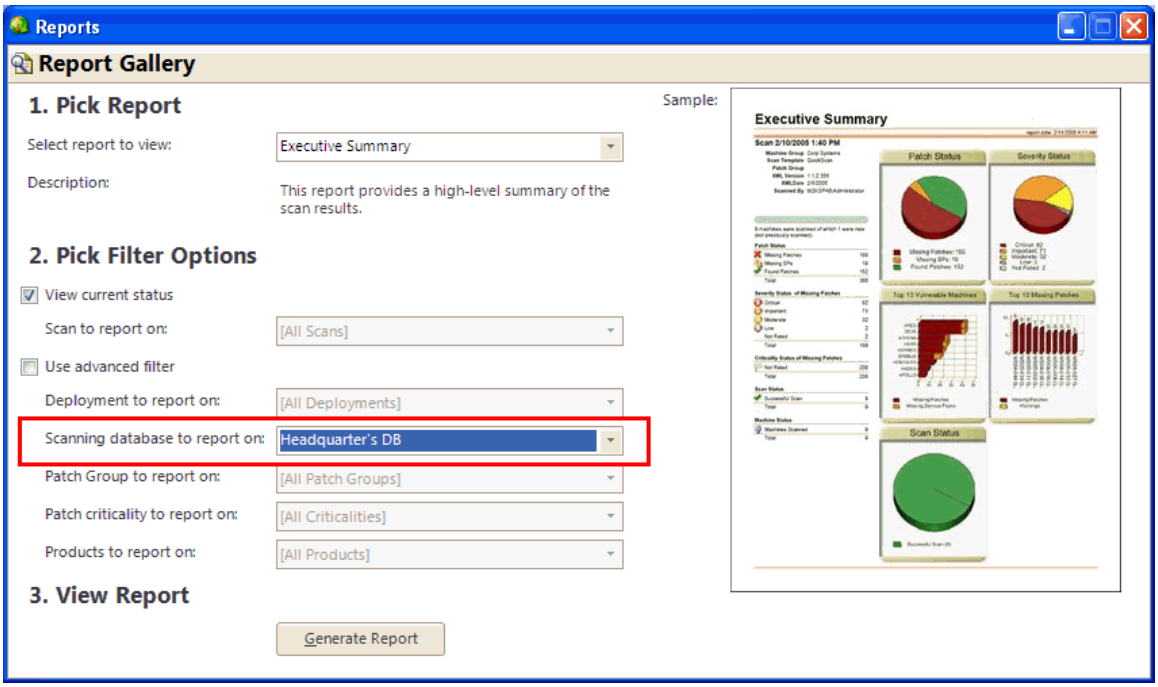
   A dialog similar to the following is displayed.



2. Change the name and description as desired.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

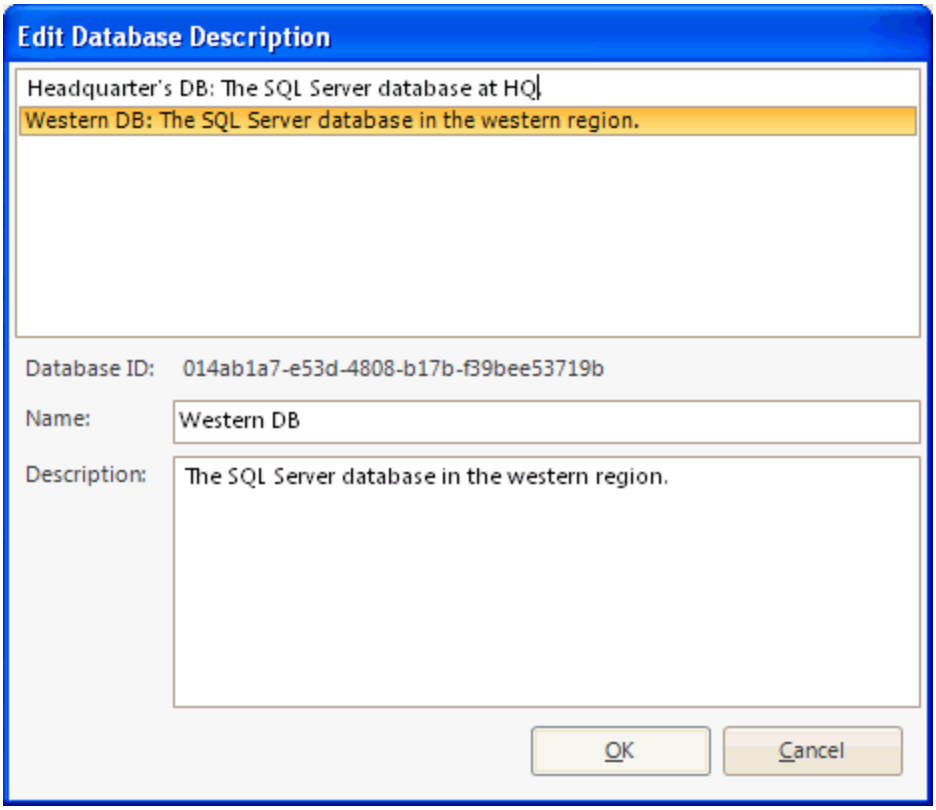
The program will use the new, friendly name whenever it refers to the database. The new name will be used in any reports you generate for the console. For example, if you changed the name to "Headquarters DB" you would see the following:



For Data Rollup Configurations

This feature is particularly useful in data rollup configurations (see What is a Data Rollup Configuration), where one database (the database associated with the central console) receives results that are rolled up to it from other remote databases. An entry is automatically generated in the central console's **Edit Database Description** dialog whenever a remote database imports the central console's data rollup settings. Once an entry is generated, its name and description can be modified, if desired.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Help System

A robust Help system is available for the program. To access the Help system, select **Help > View help**.

Context-sensitive help is also available for many of the various program windows and dialogs. Simply click the context-sensitive help icon () or press **F1** to view information specific to the window or dialog currently being displayed.

If you are a non-English user, a localized version of the Help system is available if have an Internet connection and you specify **On the web** for the **View help topics** display option.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

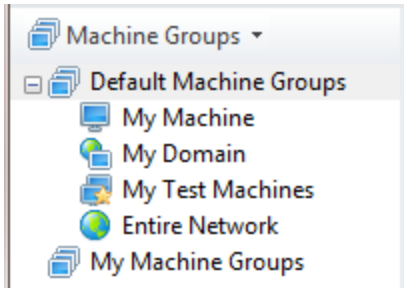
Command-line Option

Ivanti Patch for Windows® Servers can be operated from a command prompt using **C:\Program Files\LANDESK\Shavlik Protect\hfcli.exeC:\Program Files\ScriptLogic\PatchAuthority\hfcli.exe**. To view all available commands, type **hfcli -?**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About Machine Groups

Ivanti Patch for Windows® Servers uses machine groups to keep track of the machines that are included in a particular scan. Even the local machine **My Machine** is considered a machine group. Among the predefined machine groups are:



My Machine	This group includes only the local machine.
My Domain	Includes all of the machines that are a part of the domain to which the scanning computer is joined.
My Test Machines	A group of machines that represent a 'smaller' view of your actual network environment. A machine of each type that is typically scanned should be added to this group and used for testing purposes.
Entire Network	Includes all machines currently viewable in the discoverable network.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About the My Test Machines Group

One hard lesson that many administrators have learned is the importance of testing new implementations before rolling them out to critical production systems. In anticipation of this need we have created a default group for you to use for this purpose.

You can use this group just like any other. Simply add either lab machines or low priority production systems to it. You should take care to make sure that you have a representative mix of machines in the group in order to cover the production systems on your network.

For instructions on adding machines to this group, see Machine Group Pane: Middle Section.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating Machine Groups

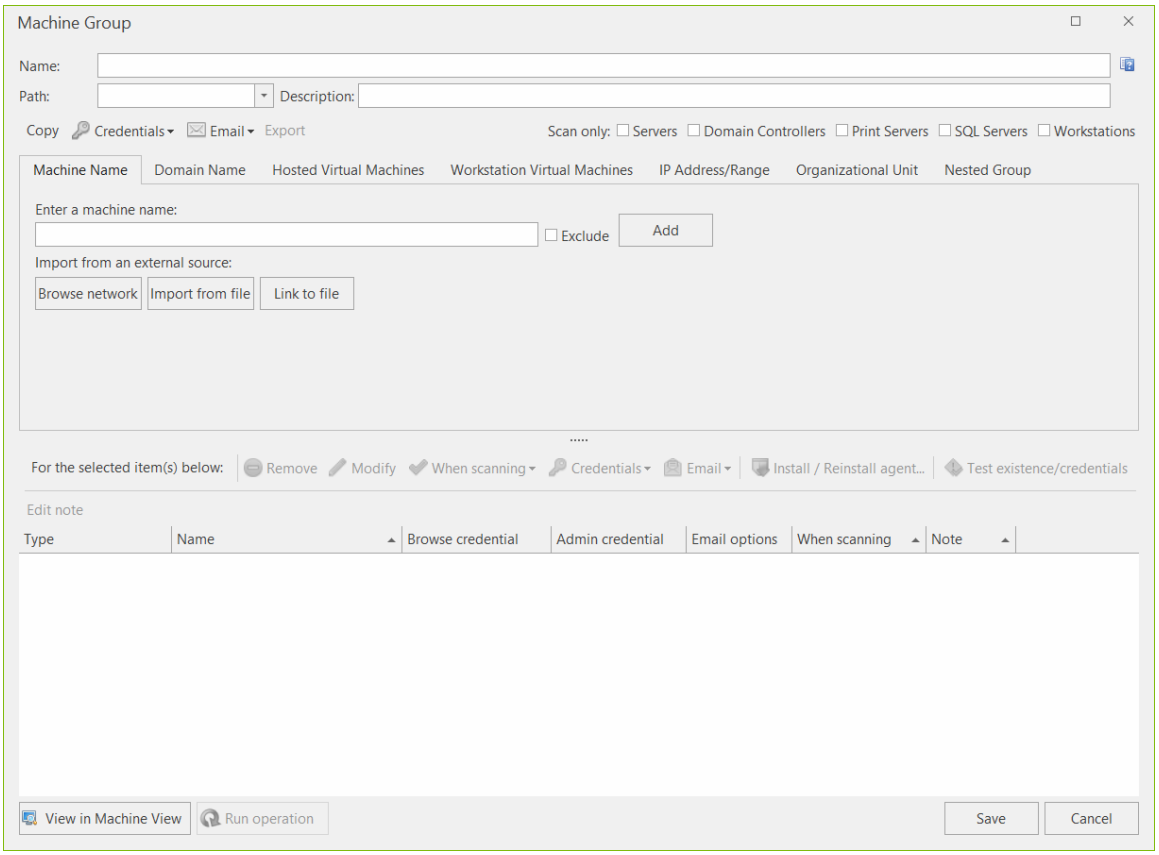
To import an existing machine group, select **New > Import Machine Group**.

There are two ways to create a new machine group:

- From the main menu, select **New > Machine Group**
- In the navigation pane, right-click on either the **Default Machine Groups** list or the **My Machine Groups** list and then select **New Machine Group**

The **Machine Group** dialog is displayed. You must provide a name for the new machine group. If you want to add the group to a new or existing folder in the navigation pane, type a folder path into the **Path** box; see Organizing Machine Groups for more information. You can also provide an optional description that identifies the purpose of the group.

For information on configuring the new machine group, see Machine Group Dialog: Middle Section.

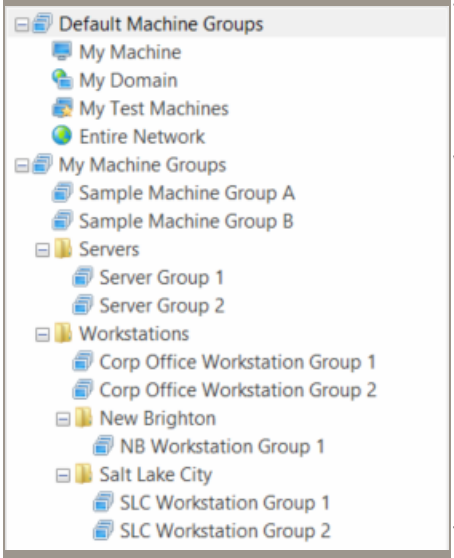


Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Organizing Machine Groups

If you create many machine groups, you should consider organizing the groups into logical folders. Doing so will enable you to quickly locate and manage your groups. You can create as many folders and sub-folders as needed within the **My Machine Groups** list in the navigation pane. For example, you might choose to organize your groups based on the types of machines they contain, by location, etc.

Sample Organizational Scheme



To create a new folder, in the Machine Group dialog, type a folder path into the **Path** box. You can specify as many folder levels as needed by using a backslash (\) to separate the levels in the name. The folder will be created when you save the machine group. If you do not specify a path, the machine group will be contained at the root level of the **My Machine Groups** list.

Folder path examples:

- \Servers
- \Workstations
- \Workstations\Location A
- \Workstations\Location B

To assign a machine group to a different folder, do one of the following:

A machine group can only belong to one folder.

- In the Machine Group dialog, type a new folder path into the **Path** box
- In the navigation pane, click and drag the machine group to a different folder
- Right-click the machine group and select **Edit path**

To assign a folder and its contents to a different folder:

- Click and drag the folder to another existing folder.

The folder you move becomes a sub-folder.

To delete a folder, do one of the following:

- Change or remove the folder name in the **Path** box of all machine groups contained in that folder

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



- Click and drag the machine groups to a different folder
- Delete all machine groups contained in the folder path

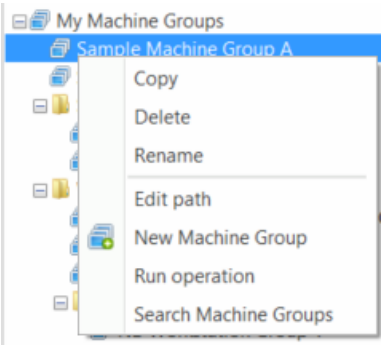
The folder will be automatically deleted when the last machine group is removed from the folder.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing Actions on Machine Groups

Right-Click Menu

You can right-click on any machine group in the navigation pane and perform a number of different actions. For example:



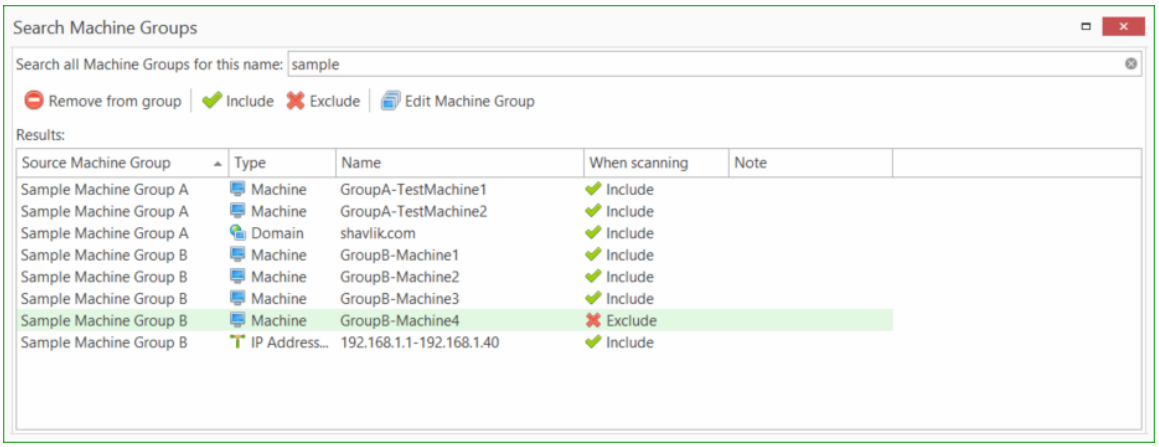
Copy	Makes a copy of the selected machine group. Type a name for the new group and then click **Save**.
Delete	Deletes the selected machine group.
Rename	Enables you to rename the selected machine group.
Edit path	Enables you to change the folder path of the selected group. Doing so will relocate the machine group to a different folder in the **My Machine Groups** list in the navigation pane. For more details, see Organizing Machine Groups.
New Machine Group	Enables you to create a new machine group. See Creating a New Machine Group for more details.
Run operation	Enables you to initiate a patch, asset, power or ITScripts operation on the machine group.
Search Machine Groups	Enables you to search for alphanumeric characters in any of your existing machine groups. See Searching Machine Groups for details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Searching Machine Groups

You can search for names in any of your existing machine groups. This enables you to quickly locate specific machines and machine groups. This is especially useful for determining if a machine belongs to more than one machine group.

To initiate a search, right-click on any machine group in the navigation pane and select **Search Machine Groups**. The **Search Machine Groups** dialog is displayed. For example:



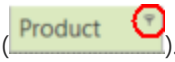
In the **Search all Machine Groups for this name** box, type the alphanumeric characters you want to find. Any machines or machine groups matching the search criteria will be displayed. Here are some tips for using the search tool:

- The search will look for matching characters in all columns except the **Type** column.
- All partial matches are displayed. For example, if you type *Test* as your search criteria, any machine with "test" in its name will be considered a match (e.g. TestMachine1, ContestantMachine, etc.).
- A semicolon (;) can be used to concatenate multiple search terms into one search string. For example, specifying "server;workstation" will return all machines containing either of the two terms.
- The use of wildcards is not allowed.

In addition, you can use the following buttons or right-click menu options to perform the following actions.

Remove from group	Deletes the selected machine from its machine group. You can use the Crtl or Shift keys to select multiple machines and delete all of the machines from the selected groups at once. If you want to delete a specific machine from all its groups:

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	1. Hover over the **Name** column header and in the upper-right corner click the column filter icon (). 2. In the column filter menu, select the desired machine name. 3. Multi-select all occurrences of the machine. 4. Click **Remove from group**.
Include	Includes the machine in any scans performed on the machine group. See the **When scanning** column for the current status.
Exclude	Excludes the machine from any scans performed on the machine group. For more information, see Excluding Certain Machines.
Edit Machine Group	Enables you to edit the selected machine group.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

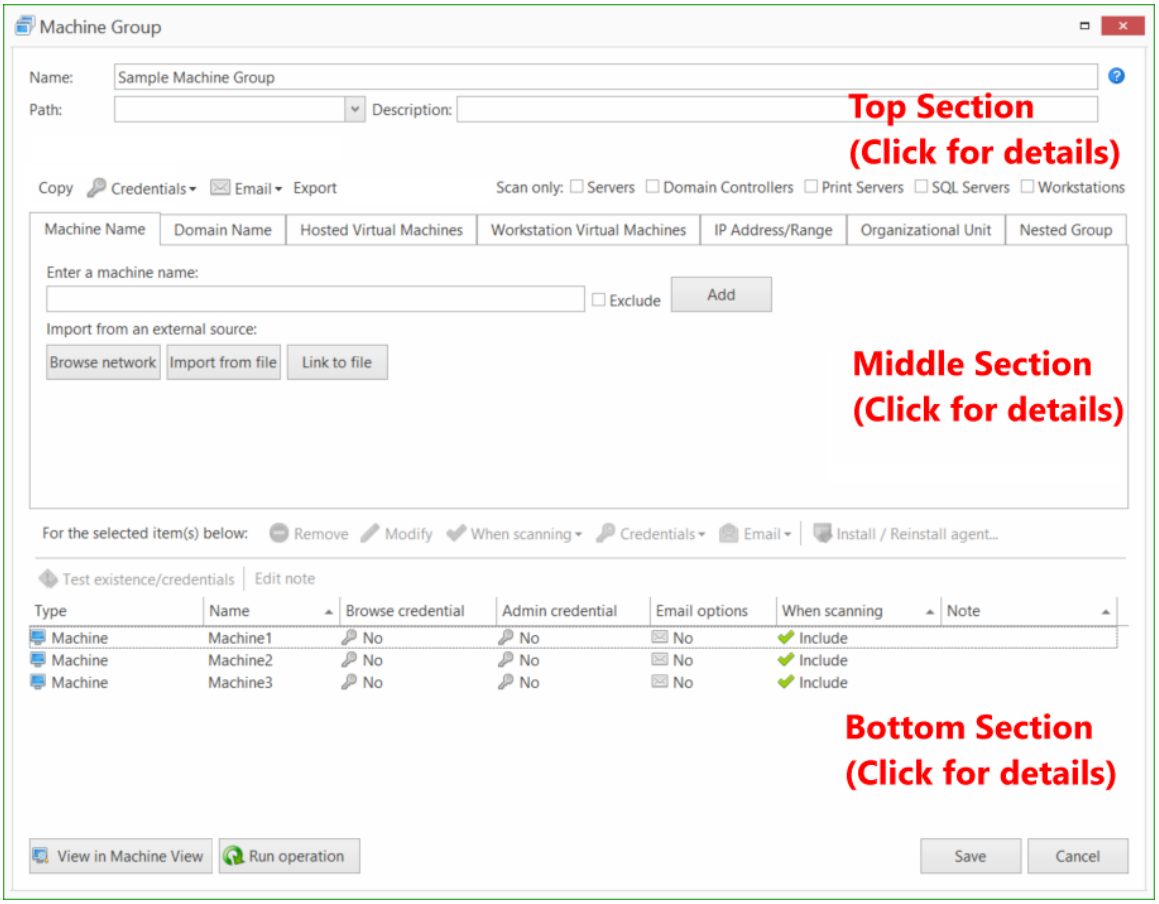
Working with a Machine Group

When a machine group is selected in the navigation bar, the details for it are shown in a separate dialog. The dialog is logically separated into three functional sections:

- Top section: Contains buttons, links, and filters that apply to the entire machine group.
- Middle section: Enables you to add machines to the group.
- Bottom section: Enables you to perform actions on individual machines within the group.

For example, here are the details for a group named *Sample Machine Group*.

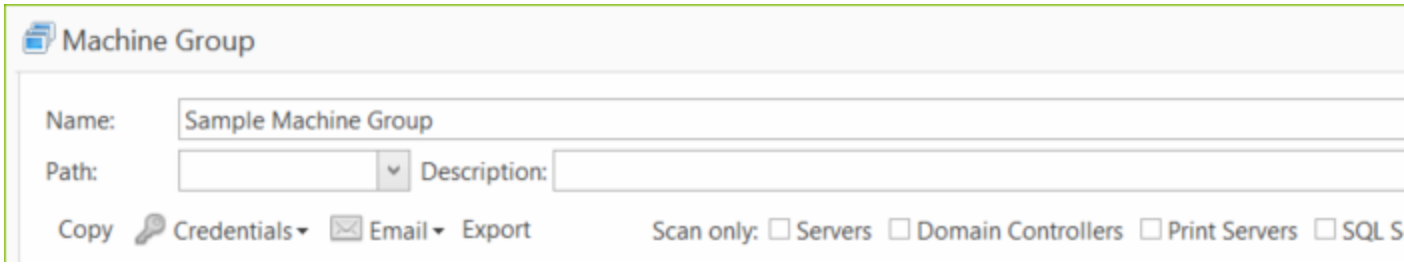
For more details about the three sections of the machine group dialog, click on the sections shown in the following figure.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Machine Group Dialog: Top Section

When viewing a machine group, the top section of the machine group dialog contains buttons, links, and filters that apply to the entire group.



This section contains the following items:

- **Name:** Provide a descriptive name for the new machine group.
- **Path:** If you want to add the group to a new or existing folder in the navigation pane, type a folder path into the **Path** box; see Organizing Machine Groups for more information.
- **Description:** Provide a description that identifies the purpose of the group.
- There are several buttons that apply to the group as a whole.

Copy	Copies the current machine group to a new group. Type a name for the new group and then click **OK**.
Credentials	Enables you to select one of the following options: • **Set credentials:** Enables you to assign common credentials to every machine in the group. Be sure the credential you select includes the domain name when defining the user name (for example: SampleDomain\Sample.Name). When credentials are assigned, the button name will change to the name of the assigned credential. For more information see Defining Credentials. • **Remove credentials:** Enables you to remove any credentials defined for the group. When credentials are not defined the icon will be dimmed ( ).

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Email	Defines email options for the entire group. The email options enable you to define which reports (if any) will be automatically sent— and to whom they will be sent— whenever this group is used in a scan. To specify which reports should be automatically sent and to whom they should be sent: 1. Click **Email > Set email**. 2. In the **Automated Email Settings** dialog, select a report in the **Reports** list. 3. In the **Report recipients** list, select the groups and/or individuals you want to email the report to. 4. Repeat Step 2 and Step 3 for each report you want to be automatically sent. 5. When finished, click **Close**.
Export	TIP: To import an existing machine group, select **New > Import Machine Group**. Enables you to export the group definition to an encrypted XML file. This file can be imported into another machine group on the same console or on a different console. You will be asked to supply a passphrase when exporting a group file. This is done to secure the contents of the file and prevent an unauthorized person from learning about your network topology, from discovering your machine credentials, etc.
	Displays online Help information about machine groups.

- **Scan only**: There are a variety of filters that can be applied to the machines in this group.

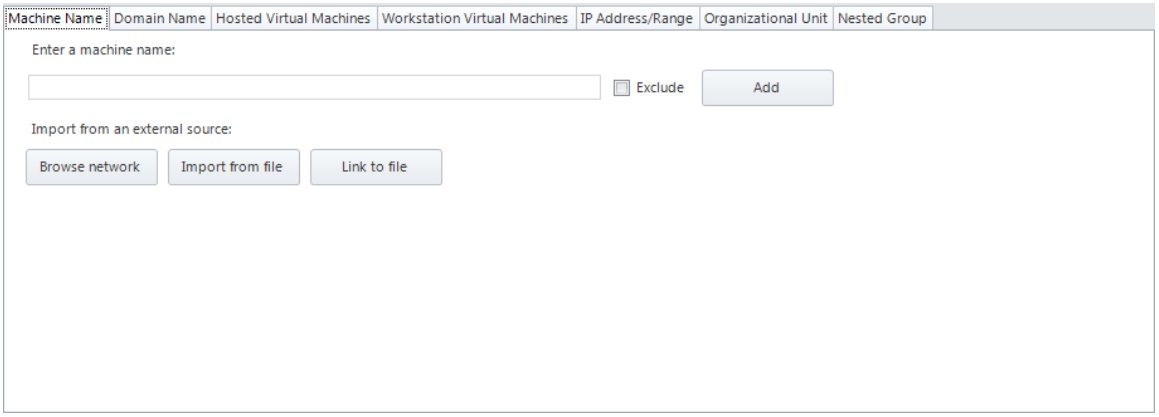
  Filters enable you to specify the types of machines you want included in a scan. For example, if you want to scan all the print servers within a domain, you would specify the desired domain on the **Domain Name** tab and then in the **Scan only** area you would select **Print Servers**. All other machine types are ignored.

  To specify one or more machine types, simply enable the check box in front of the machine type (s) you want included in the scan. If no check boxes are enabled then no filters are applied.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Machine Group Dialog: Middle Section

When viewing a machine group, the middle section of the machine group dialog enables you to add machines to the group.



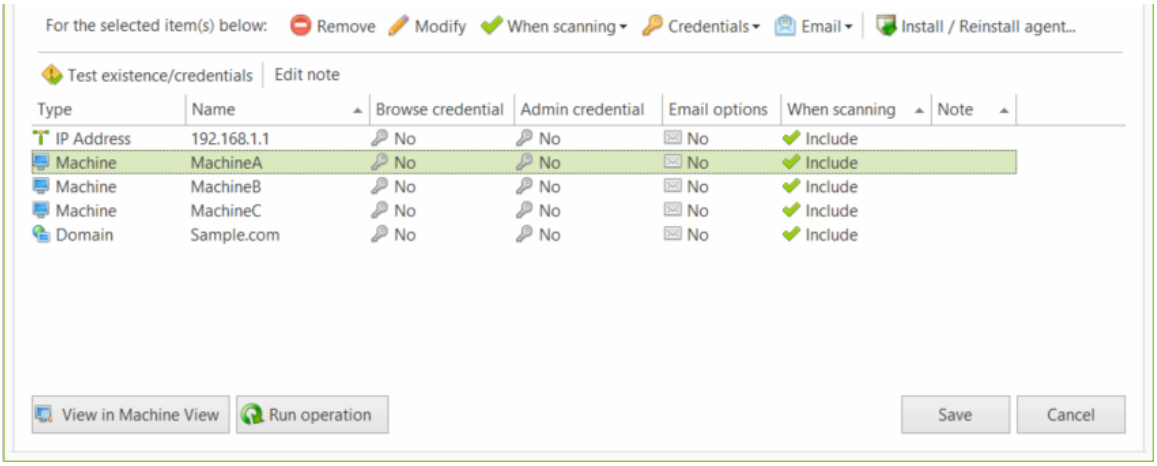
You can add machines a number of different ways. See the following topics for details:

- Adding Machines by Name
- Adding Domains
- Adding Virtual Machines
- Adding Machines by IP Address
- Adding Organizational Units
- Defining Nested Groups

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Machine Group Dialog: Bottom Section

When viewing a machine group, the bottom section of the machine group dialog displays the machines that are currently members of the group. The bottom section also enables you to perform actions on individual machines within the group.



The bottom section contains the following items and capabilities:

- Machine-level buttons: Buttons that perform actions on individual machines within the group.

> These actions can also be performed by right-clicking on one or more machines.

Remove	Removes the selected machines from the current machine group.
Modify	Enables you to modify the name or IP address of an existing group item. The item is displayed in the middle pane, allowing you to modify the name and then add the item back to the group using the new name.
When Scanning	**Include:** The selected machines will be included when scans are performed on this machine group. **Exclude:** The selected machines will be excluded when scans are performed on this machine group.
Credentials	- **Set Admin Credentials:** The ability to provide administrative credentials for the selected machines in the group. Credentials assigned to individual machines will take precedence over credentials assigned to the group.

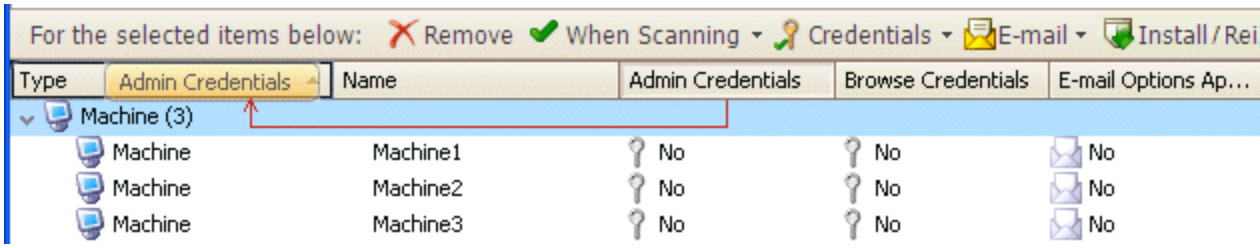
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	When credentials are applied to the selected machines, the name of the assigned credential is displayed next to the icon. - **Set Browse Credentials:** Applies only to domains and organizational units. Enables you to provide browse credentials that are used to locate all machines in a specific domain or OU. These credentials may be different than the administrator credentials used to connect to the machines in the domain or OU. When credentials are applied, the name of the assigned credential is displayed next to the icon. - **Remove:** Removes specified credentials from the selected machines. The credentials icon will become dimmed (). Any group-specific credentials will still be applied to the machines. For more information on setting credentials see Defining Credentials.
Email	**Set email:** Defines email options for the selected machines. Defining email options for individual machines overrides any email options defined for the group. The email options enable you to define which reports (if any) will be automatically sent—and to whom they will be sent— whenever the machines are used in a scan. To specify which reports should be automatically sent and to whom they should be sent: 1. In the **Automated Email Settings** dialog, select a report in the **Reports** list. 2. In the **Report Recipients** list, select the groups and/or individuals you want to email the report to. 3. Repeat Step 1 and Step 2 for each report you want to be automatically sent. 4. When finished, click **Close**. **Remove email:** Removes all email settings currently applied to the selected machines.
Install/Reinstall Agent	Installs Ivanti Patch for Windows® Servers Agent on the selected machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• The machines must be added to the machine group using a machine name, domain name, or IP address. You cannot use the **Install / Reinstall Agent** button to install agents on machines that were added as organizational units, nested groups, or IP address ranges. • The machines must be online and connected to the network. If the console cannot make a connection to a machine the install will fail for that machine. See Installing Agents from the Console for more details.
Test existence/credentials	Performs a power status scan to verify the existence of the selected machines and to verify that the credentials defined for the selected machines can be used to access the machines.
Edit note	Enables you to add a note to one or more machines in the group. For example, you might use a note to indicate why a certain machine is being excluded from scans that are performed on the group. • To edit an existing note: Select the note, click **Edit note**, and modify the text. • To remove an existing note: Select the note, click **Edit note**, and replace the text with a space.

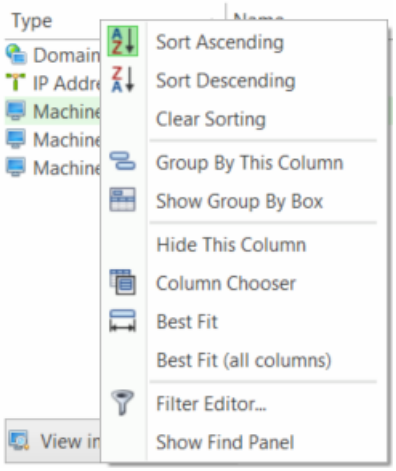
- The ability to display the machines in the group a number of different ways.
  - You can click on a column heading to sort the table by that information.
  - You can reorder the columns by clicking and dragging the column headers to new locations. For example, if you want administrator credential information to be displayed in the first column, simply click on the **Admin Credentials** column header and drag it to the first column.



> When reordering columns, the column header you are moving will always be placed in front of the column you drag it to.

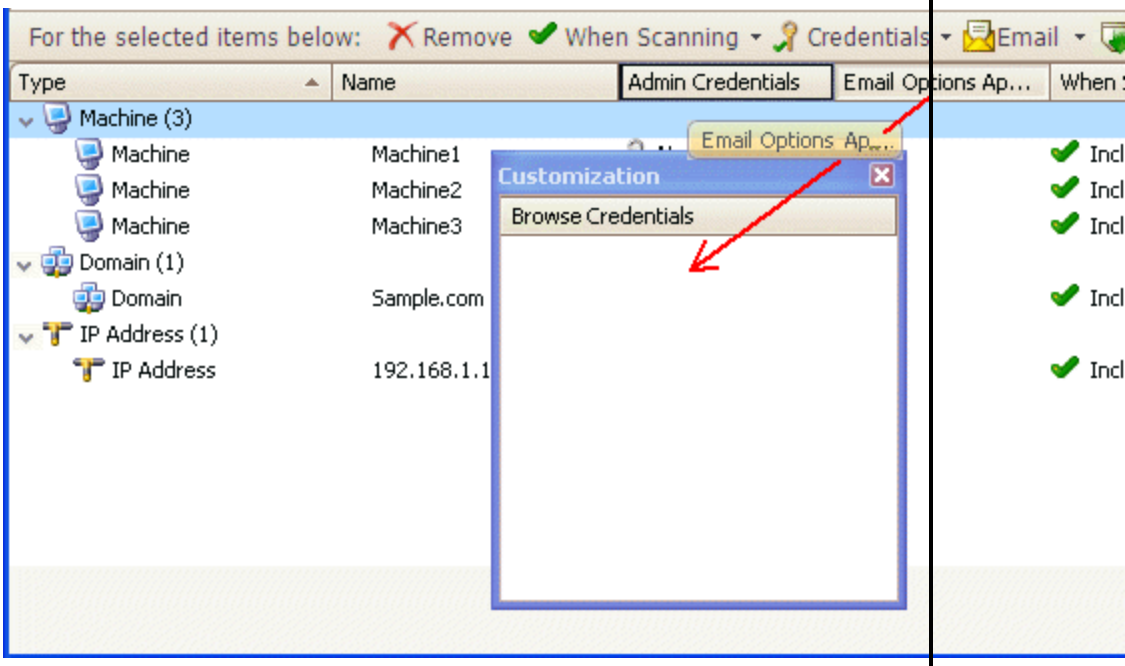
  - You can right-click within a column header and perform a number of additional actions.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Sort Ascending	Sorts the selected column in ascending order.
Sort Descending	Sorts the selected column in descending order.
Clear Sorting	Clears the sorting criteria currently set for this column.
Group By This Column	Groups the table using the data in the selected column. It does this by moving the data into expandable lists that are located in the body of the grid. One expandable list will be created for each possible column value. If you perform this action on any subsequent columns, that data will be presented as nested groups at increasingly lower levels within the expandable lists. If **Show Group By Box** is enabled, this will also create a "Group By" box in the area immediately above the column headers. TIP: To turn off the **Group By This Column** feature and revert to the original view: Enable **Show Group By Box**, drag the Group By boxes back to the column header and then right-click in the column header and select **Hide Group By Box**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Show Group By Box / Hide Group By Box	Displays or hides an area immediately above the column headers that contains "Group By" boxes. One Group By box will be displayed for each column header for which **Group By This Column** is currently enabled. You can also drag column headers to and from this area. The table will be grouped according to the data in the box. If there are two or more boxes then the grouping will be nested, with the left-most box presented at the highest level, the second box presented at the second level, etc.
Hide This Column	Removes the column from the table. You can add the column back to the table using the **Column Chooser**
Column Chooser	Enables you to add and remove information from the table. When you select **Column Chooser** the **Customization** dialog is displayed. This dialog is used to store the columns you currently don't want displayed within the table. Simply click and drag the desired column headers from the table to the **Customization** dialog. For example, if you decide you don't want **Browse Credentials Applied** and **Email Options Applied** information displayed in the table, simply drag those column headers into the **Customization** dialog.  If you decide you want an item back in the table, simply click and drag it from the **Customization** dialog back to the table.
Best Fit	Resize the width of the selected column so that all information in the column is displayed in the optimal amount of space.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

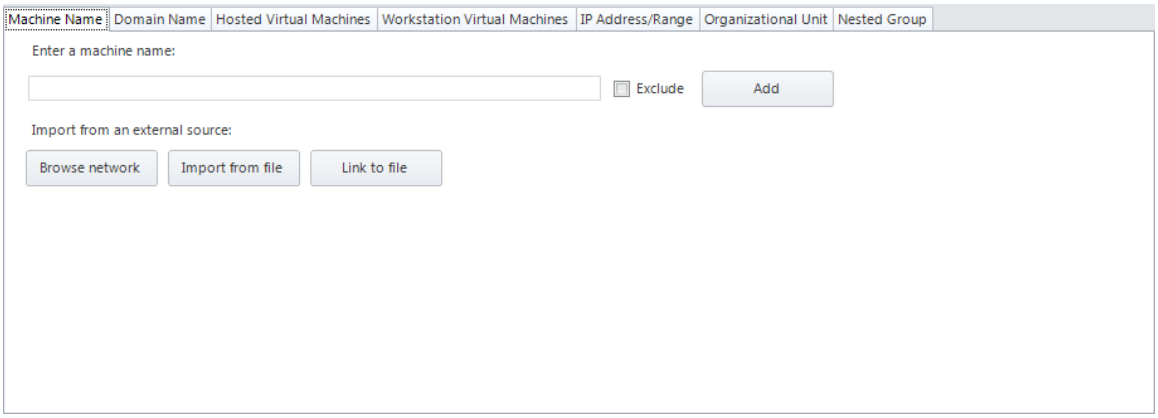
Best Fit (all columns)	Resize the width of all columns in the table so that information in the columns is displayed in the optimal amount of space.
File Editor	The **Filter Editor** dialog will show any filters that are currently active in the column headers. You can use the editor to modify the existing filter criteria and to build new criteria using the available filter conditions and logical operators.
Show Find Panel / Hide Find Panel	Displays or hides a search box that you can use to find specific patches or text related to any of the patches contained in the patch data file. Here are a few tips for using the search box: • The search works only on the information currently visible in the grid • All partial matches are displayed • The use of wildcards is not allowed

- **View in Machine View:** Displays this group in Machine View, which shows the most recent scan information for every machine in the group.
- **Run operation** button: Enables you to initiate an operation (a patch scan, a power management task, etc.) on all machines in the machine group.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Adding Machines by Name to a Machine Group

One of the ways that a machine can be added to a machine group is by machine name. Like most other tasks in Ivanti Patch for Windows® Servers, there are many ways that you can add a machine name to a machine group.



Adding an Individual Machine Name

The easiest way to add a machine to a machine group is as follows:

1. Select the **Machine Name** tab.
2. Type the name of the machine in the **Enter a machine name** box.

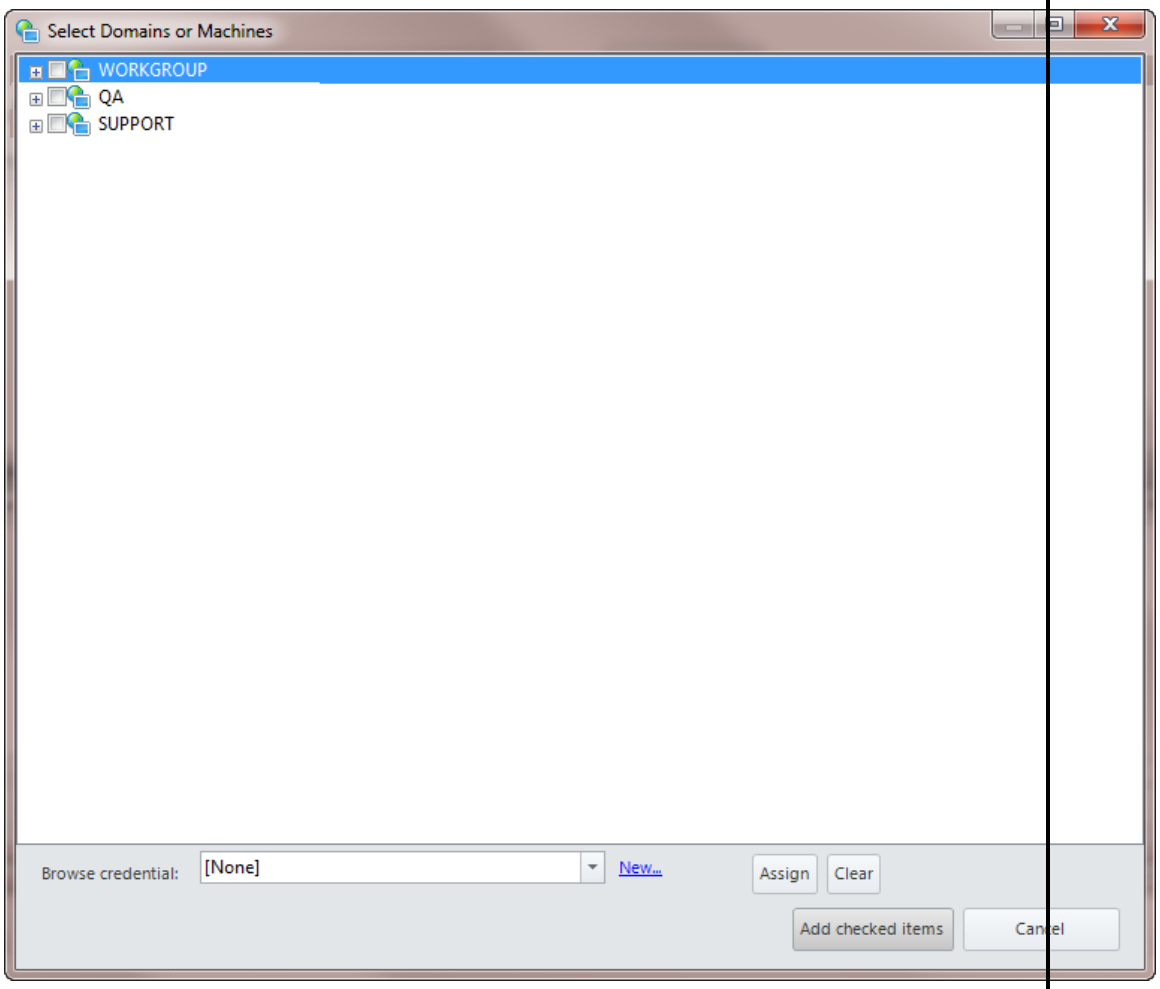
   You can specify either the individual machine name or the fully qualified domain name.
3. Click **Add**.

If you want to specifically exclude a machine, enable the **Exclude** check box before you click **Add**. The machine will be added to the machine list but will not be included in any scans. See Excluding Certain Machines for more information.

Importing Machine Names From an External Source

You can also add machines by using the following buttons to import machine names from an external source.

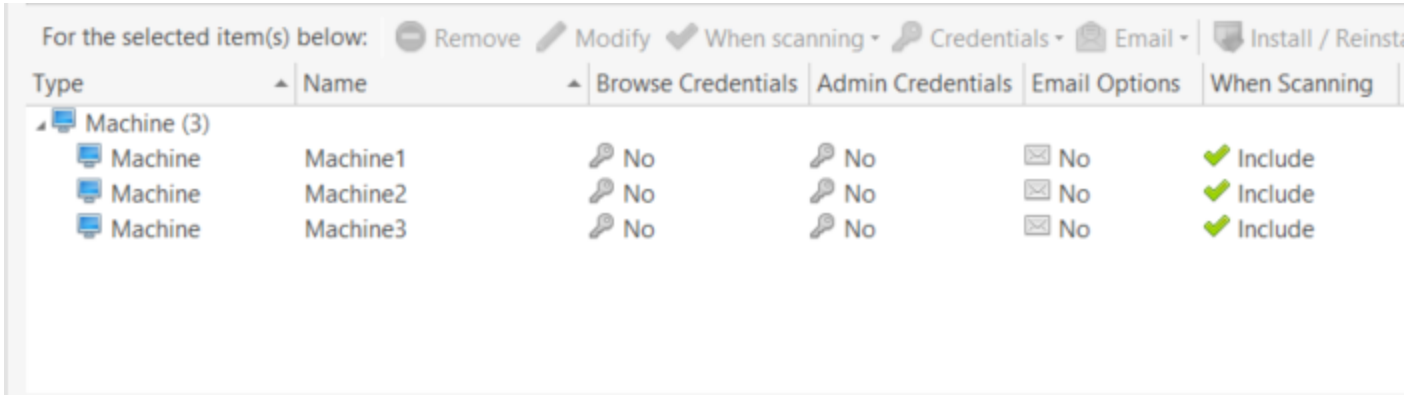
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Browse network	This button opens a separate dialog that lists the contents of your Microsoft network. Locate the machines you would like to add to the custom group, place a check mark in the check boxes, and then click **Select**. If you need to supply credentials in order to enumerate one or more nodes, in the **Browse credential** box at the bottom of the dialog select the appropriate credential and then click **Assign**. If you need to define a new credential, see Defining Credentials. 
Import from file	You can import a list of machines from a previously created text file. The text file can be created manually or it can be created using any network-based tool available to you. Each machine name in the text file must be separated by either a carriage return or a comma.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Link to file	Machine names can also be dynamically linked to a text file rather than imported. Linking a file to a machine group is different than importing its contents. Importing contents is a one-time operation after which the information from the file becomes a part of the machine group. When you link a file to a machine group, any changes that you make to the file are automatically reflected in the next scan. See Linking Files to Machine Groups for more information.

When machines are added or imported by name, the new entries are displayed within the bottom section of the machine group pane.

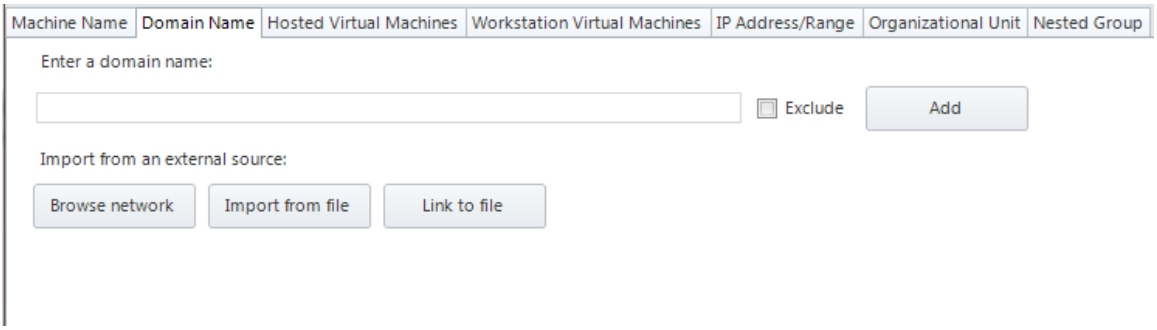


TIP: The recommended best practice is to always supply credentials for the machines in the machine group. See Supplying Credentials for more details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Adding Domains to a Machine Group

Another way that machines can be added to a machine group is by domain. Adding a domain to a machine group will result in all machines that are members of the domain being made a part of the group.



Adding an Individual Domain Name

The easiest way to add a domain to a machine group is as follows:

1. Select the **Domain Name** tab.
2. Type the name of the domain in the **Enter a domain name** box.
3. Click **Add**.

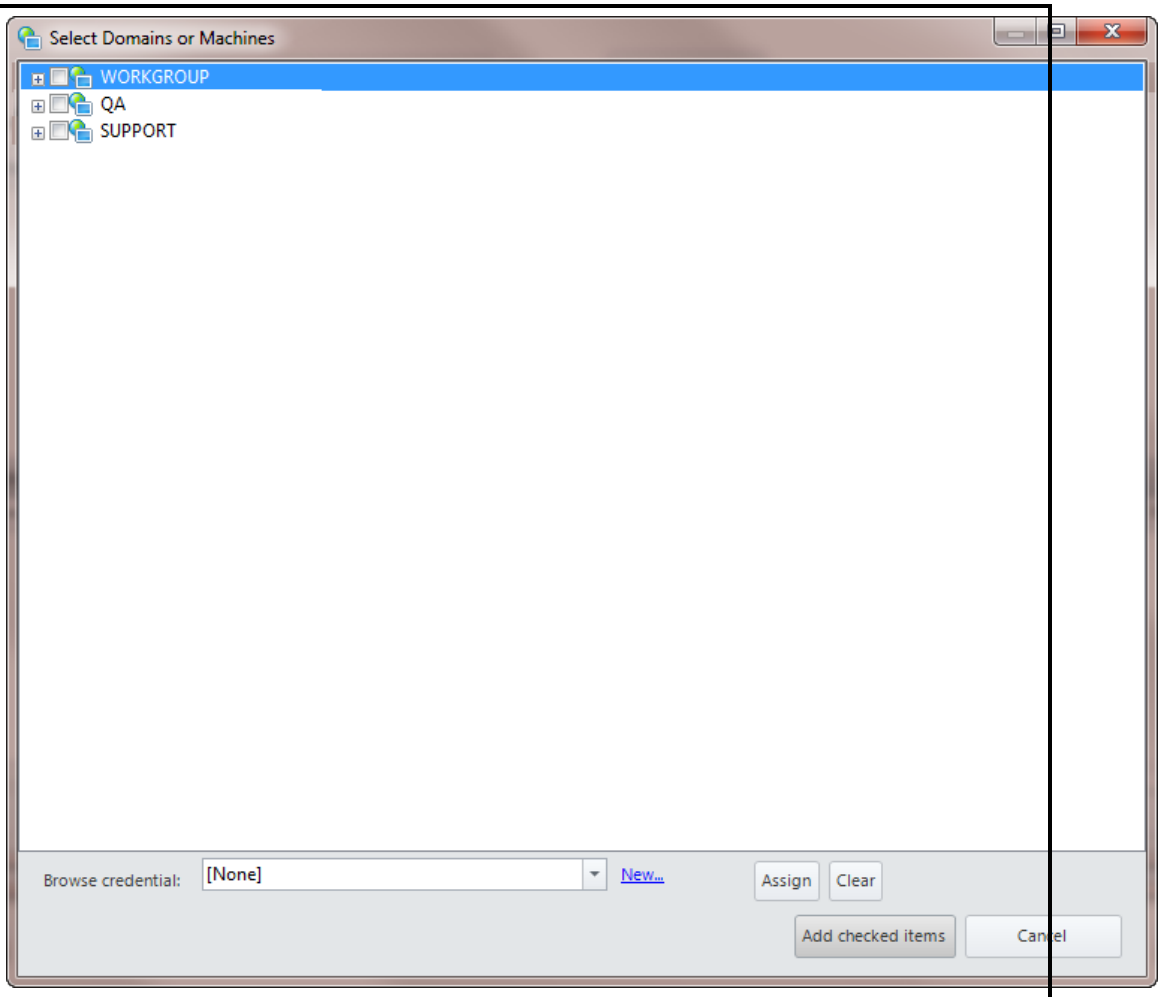
If you want to specifically exclude a domain, enable the **Exclude** check box before you click **Add**. The domain will be added to the machine list but will not be included in any scans. See Excluding Certain Machines for more information.

Importing Domain Names From an External Source

You can also add domains by using the following buttons to import domain names from an external source.

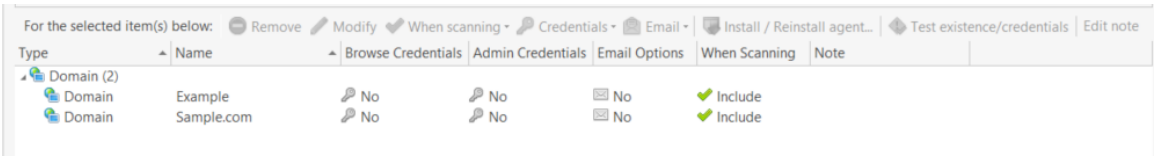
Browse network	This button opens a separate dialog that lists the contents of your Microsoft network. Locate the domains you would like to add to the custom group, place a check mark in the check boxes, and then click **Select**. If you need to supply credentials in order to enumerate one or more nodes, in the **Browse credential** box at the bottom of the dialog select the appropriate credential and then click **Assign**. If you need to define a new credential, see Defining Credentials.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	
Import from file	You can import a list of domain names from a previously created text file. The text file can be created manually or it can be created using any network-based tool available to you. Each domain name in the text file must be separated by either a carriage return or a comma.
Link to file	Domain names can also be dynamically linked to a text file rather than imported. Linking a file to a machine group is different than importing its contents. Importing contents is a one-time operation after which the information from the file becomes a part of the machine group. When you link a file to a machine group, any changes that you make to the file are automatically reflected in the next scan. See Linking Files to Machine Groups for more information.

When domains are added or imported by name, the new entries are displayed within the bottom section of the machine group pane.

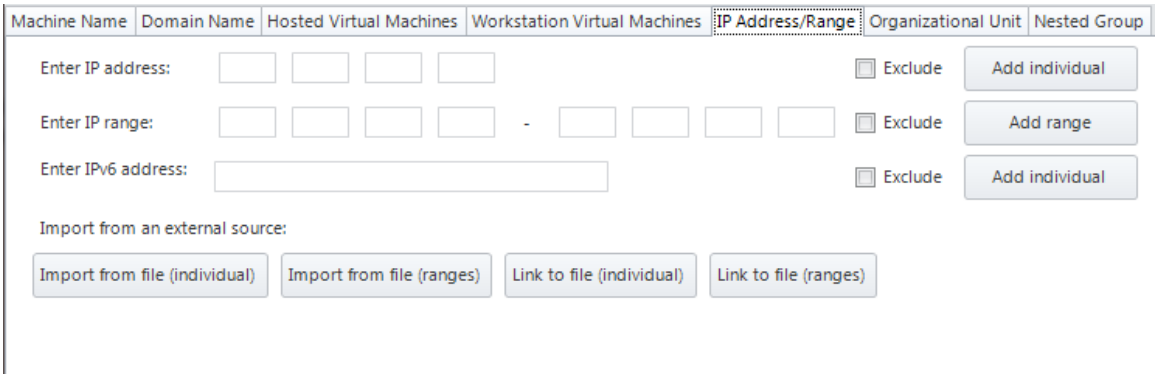
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Adding Machines by IP Address to a Machine Group

Machines can be added to a machine group by entering individual IP addresses or by defining a range of IP addresses.



Adding an Individual IPv4 Address

1. Select the **IP Address/Range** tab.
2. Type the IP address in the **Enter IP address** box.
3. Click **Add individual**.

If you want to specifically exclude an IP address, enable the **Exclude** check box before you click **Add individual**. The IP address will be added to the machine list but will not be included in any scans. See Excluding Certain Machines for more information.

Adding a Range of IPv4 Addresses

1 Select the **IP Address/Range** tab.

2. Type the starting and ending IP addresses in the **Enter IP range** boxes.
3. Click **Add range**.

Adding an IPv6 Address

1 Select the **IP Address/Range** tab.

2. Type the IPv6 address in the **Enter IPv6 address** box.
3. Click **Add individual**.

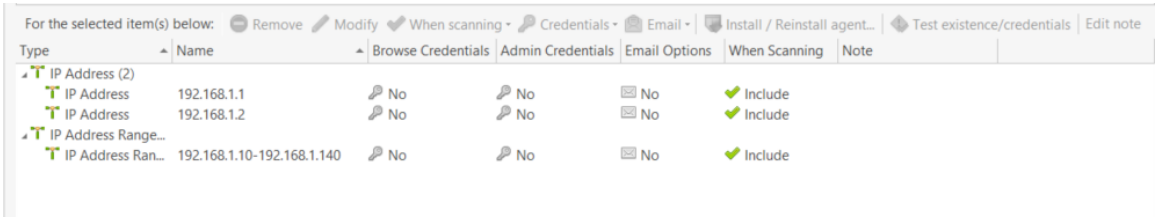
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Importing IP Addresses from an External Source

You can also add IP addresses by using the following buttons to import the addresses from an external source.

Import from file (individual) and **Import from file (ranges)**	You can import a list of individual IP addresses or a list of IP address ranges from a previously created text file. The text file can be created manually or it can be created using any network-based tool available to you. Each IP address in the text file must be separated by either a carriage return or a comma. When defining an IP range, include a dash between the beginning and ending IP address: `172.16.1.1-172.16.1.255`
Link to file (individual) and **Link to file (ranges)**	IP addresses can also be dynamically linked to a text file rather than imported. Linking a file to a machine group is different than importing its contents. Importing contents is a one-time operation after which the information from the file becomes a part of the machine group. When you link a file to a machine group, any changes that you make to the file are automatically reflected in the next scan. See Linking Files to Machine Groups for more information.

When IP addresses are added, the new entries are displayed within the bottom section of the machine group pane.

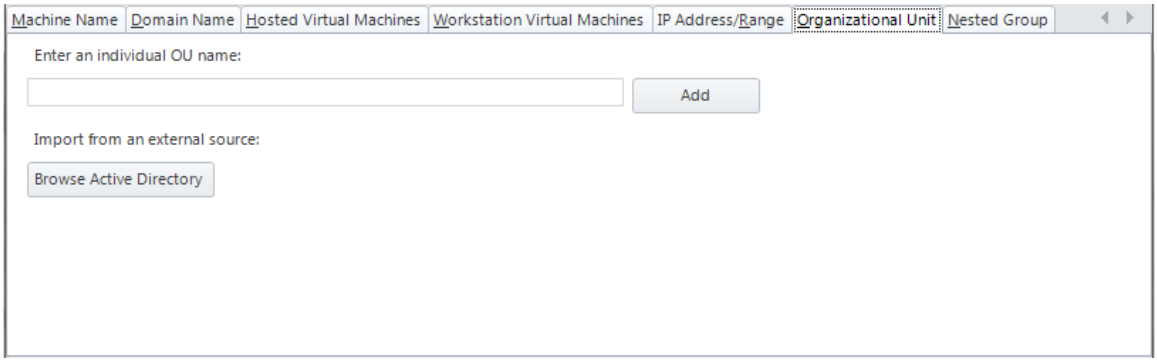


The recommended best practice is to always supply credentials for the machines in the machine group. See Supplying Credentials for more details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Adding Organizational Units to a Machine Group

Companies often split up Active Directory entities by creating multiple Organizational Units (OUs). A machine group in Ivanti Patch for Windows® Servers can be configured to include specific organization units from Active Directory. For example, you might create a machine group that includes all machines from the 'Sales' organizational unit.



Adding an Individual Organizational Unit

The easiest way to add an organizational unit to a machine group is as follows:

1. Select the **Organizational Unit** tab.
2. Type the name of the organizational unit in the **Enter an individual OU name** box.

   An OU is added in full LDAP format. For example, to add the Sales OU from the domain example.com, the format is 'ou=sales,dc=example,dc=com'. If you specify a parent OU, all children OUs will be included in the scan.
3. Click **Add**.

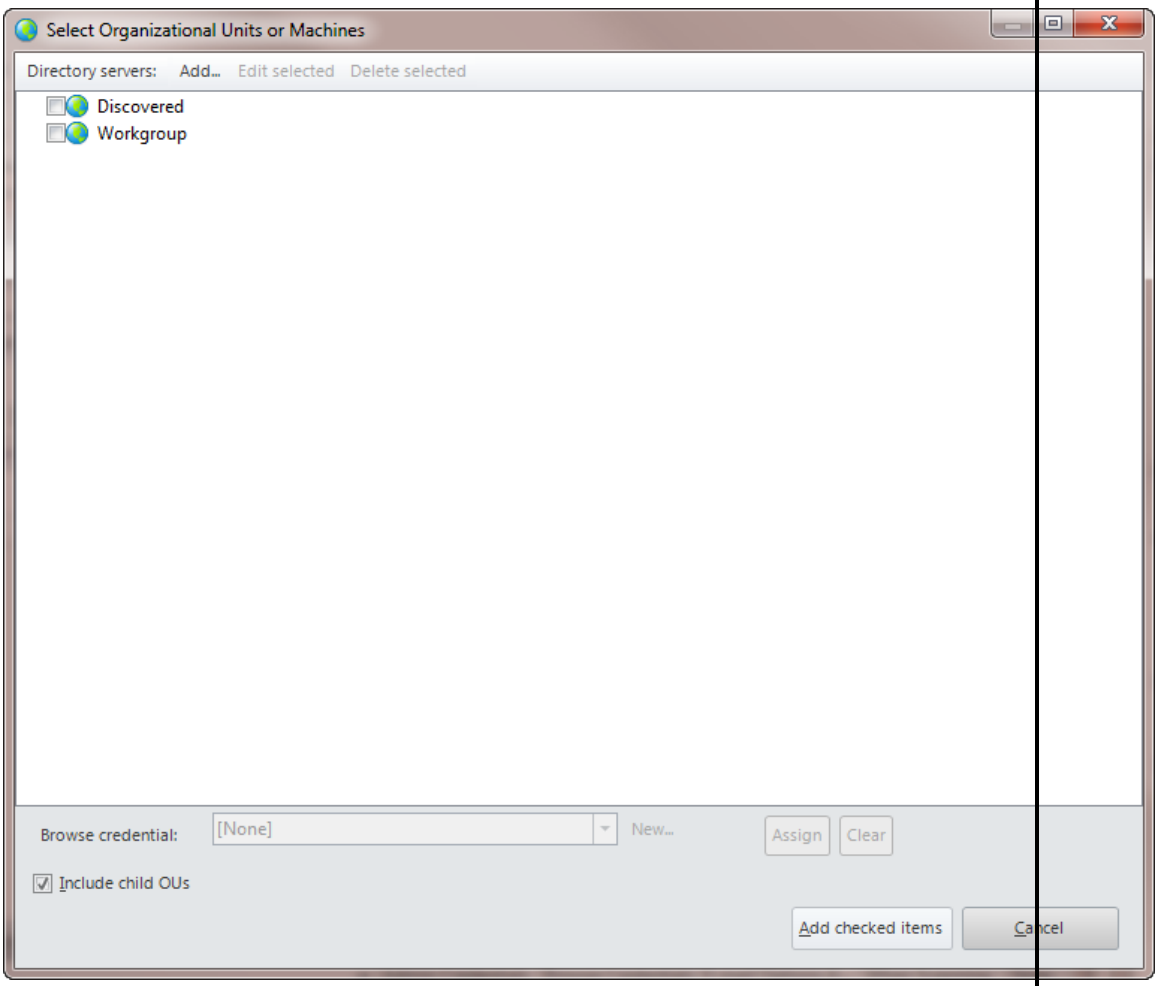
Importing OUs from an External Source

You can also add organizational units by using the **Browse Active Directory** button to import organizational unit names from an external source.

Browse Active Directory	This button opens a separate dialog that lists the contents of your Active Directory network. Locate the organizational units and/or machines you would like to add to the custom group, place a check mark in the desired check boxes, and then click **Add checked items**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- If your Active Directory network is not listed, click **Add** to manually define the network.
- If you need to supply credentials in order to browse the Active Directory OUs on the available domains, in the **Browse credential** box at the bottom of the dialog select the appropriate credential and then click **Assign**.

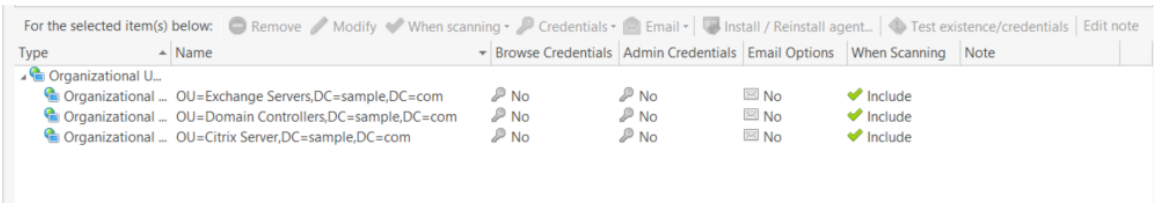


Add	Enables you to add an Active Directory forest that is not broadcasting its availability. You will need to provide credentials that are authorized to enumerate the forest. You can then add any items within that forest.
Edit Selected	Enables you to edit the selected entry.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Delete Selected	Enables you to delete the selected entry.
Browse Credential	To set credentials to use for browsing an Active Directory hierarchy on a remote domain: 1 Select the domain. 2. Select the proper credential. If you need to define a new credential, see Defining Credentials. 3. Click **Assign.**
Include Child OUs	If enabled, for every parent OU selected, all children OUs will also be included in the machine group.
Clear	Removes the credentials currently defined for the selected domain.

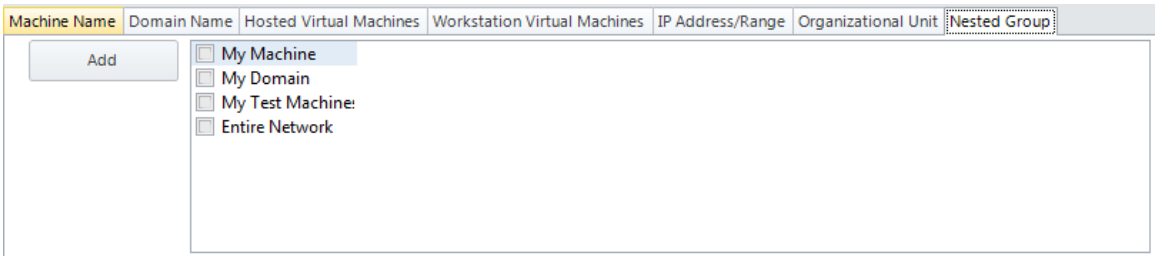
When organizational units are added, the new entries are displayed within the bottom portion of the machine group pane.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

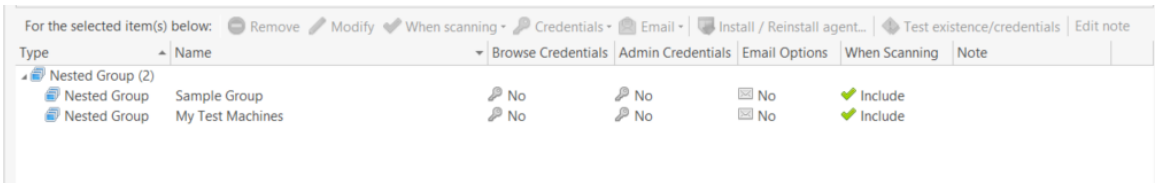
Defining Nested Groups

You can use nested groups when configuring a machine group. A nested group is a group that consists of one or more other groups.



All currently defined machine groups are listed except the machine group you are currently configuring. To add one or more nested groups, simply enable the check boxes of the desired groups and then click **Add**.

When one or more nested groups are added, the new entries are displayed within the bottom portion of the machine group pane.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How to Add Virtual Machines to a Machine Group

Virtual machines can be added to a machine group. The recommended best practice is to create a machine group consisting of nothing but virtual machines. You can, however, add both physical machines and virtual machines to the same machine group if you wish.

There are four different ways to add virtual machines to a machine group:

- If virtual machines are hosted by a server you can add the server to the machine group. This effectively adds all virtual machines hosted by the server to the machine group. The virtual machines can be in either online or offline mode.

  The server will also be added to the Virtual Inventory list, which is used to manage your ESXi Hypervisors.

- If virtual machines are hosted by a server you can add individual virtual machines to the machine group. The virtual machines can be in either online or offline mode.

  You can also add virtual machine templates that may be hosted on a server.

- If virtual machines reside on individual workstations, you may consider adding the machines to the group twice to ensure that each virtual machine is successfully scanned regardless of its current power state (online or offline).

  - You can add the full path names or directory names of the offline virtual machines to the machine group using the Workstation Virtual Machines tab. The virtual machines defined using this tab are scanned only if they are in offline mode.
  - You can add the virtual machines to the machine group using the **Machine Name** tab, the **Domain Name** tab, or the **IP Address/Range** tab. Virtual machines defined using these tabs are scanned only if they are in online mode.

For overview information about scanning for and deploying patches to virtual machines, see Virtual Machine Overview.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

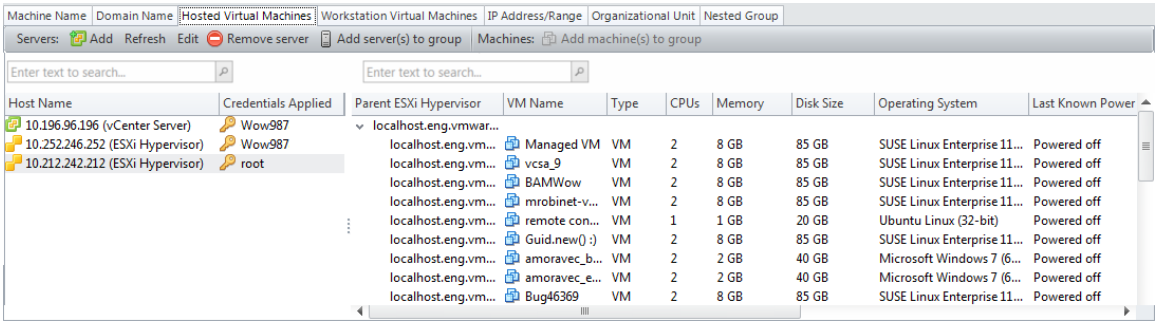
Adding Virtual Machines Hosted by a Server

Many organizations will host their virtual machines on one or more VMware servers. Doing so provides the means to manage the virtual machines in an organized fashion. There are two main types of VMware servers:

- **VMware ESX/ESXi Server**: A server dedicated to hosting and managing multiple virtual machines. VMware ESX/ESXi servers (also referred to as ESXi hosts or ESXi Hypervisors) are typically used in small- and medium-sized organizations that want to control multiple virtual machines from one location. The server often runs on a dedicated blade computer that is using a VMware operating system.
- **VMware vCenter Server**: This type of server is typically used by large organizations that need to manage multiple VMware ESX/ESXi servers, each of which may be running multiple VMware images. For example, you can quickly move a highly-utilized virtual machine from a busy ESXi server to another less busy ESXi server.

TIP: For information on managing your vCenter Servers and ESXi Hypervisors, see Using the Virtual Inventory Feature.

You can use the **Hosted Virtual Machines** tab to log on to these servers and select the virtual machines you want to include in your machine group. The virtual machines can be in either offline or online mode. You can also use this tab to add virtual machine templates that may be hosted on a server. Finally, you can also add the servers themselves to the group.



1. Log on to the desired server by clicking **Add**.

   See Logging on to a Server for information on logging on to a server. The credentials you use to log on to the server are called *browse credentials*. They will be used to connect to the server and to enumerate the machines hosted by the server.

   After a connection is made the server is displayed in the left-hand pane. The virtual machines hosted by the server are displayed in the right-hand pane. At this point you can either add the server itself to the group or you can add individual virtual machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

You must have server permission set on the datacenter, the folder, or the individual virtual machines in order for the machine to be displayed. If you don't have permission for a specific virtual machine it will not be displayed in the right-hand pane.

TIP: The server will also be displayed in the Virtual Inventory list.

2. Add the server and/or individual hosted machines to the group.
   - To add one or more servers to the group, select the server(s) in the left-hand pane and click **Add Server(s) to Group**.

     How a server in a machine group is treated depends on how the group is used. If you perform a patch scan on the group, all of the virtual machines hosted by the server will be scanned. If you perform a bulletin scan or run a script against the group, only the server is affected.When you perform a patch scan on the group, all of the virtual machines hosted by the server will be scanned.
   - To add individual hosted machines to the group, in the right-hand pane select the virtual machines you want to add and then click **Add Machine(s) to Group**.

   The server and/or the virtual machines are added to the bottom pane of the machine group. Be sure to supply any credentials that may be needed for the individual machines.

   You can also add virtual machine templates to the machine group. Templates are identified by a unique icon ( ). For complete details see Notes About Virtual Machine Templates.

You can log on to multiple servers at the same time. All virtual machines found on the servers are displayed in the right-hand table. The server table identifies the server type (VI = Virtual Infrastructure server, ESX = ESX server) and the server name. The virtual machine table contains a large amount of information about each virtual machine, including:

- **Parent ESX Server**: The name of an ESX server being used to host virtual machines.
- **VM Name**: The name of a virtual machine being managed by a server.
- **CPUs**: The number of Central Processing Units (CPUs) available to the virtual machine.
- **Memory**: The amount of memory (MB) allocated to the virtual machine.
- **Disk Space**: The amount of disk space (GB) allocated to the virtual machine.
- **Operating System**: The operating system being used on the virtual machine.
- **Last Known Power State**: The last known state of the virtual machine (Powered On, Powered Off, or Suspended)

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **IP Address**: The IP address of the virtual machine.
- **Host Name**: The name of the machine on the network that is hosting the virtual machine.

You can reorder the columns in both tables by clicking and dragging the column headers to new locations. You can also click within a column header and sort the column in ascending or descending order.

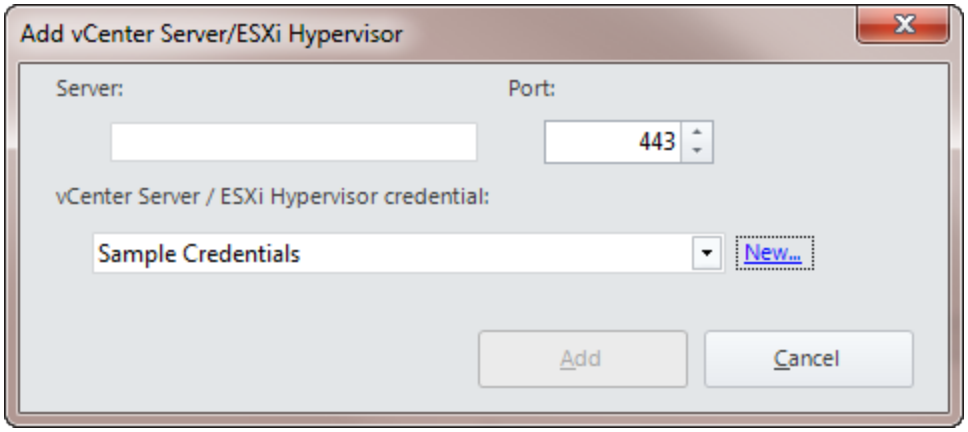
The **Hosted Virtual Machines** tab contains the following buttons:

Add Server	Enables you to log on to a VMware ESX server or virtual infrastructure server. After a successful logon the server and its hosted virtual machines are displayed and available for selection.
Refresh Server	Reconnects to the selected server and updates the list of virtual machines hosted by the server.
Edit Server	Allows you to edit the information used to connect to the selected server.
Remove Server	Removes the selected server from the table. All virtual machines hosted by the server will be removed from the right-hand table.
Add Server (s) To Group	In the left-hand pane, select the desired server(s) and then click **Add Server(s) To Group**. The server is added to the bottom pane. When you add a server, it effectively adds all virtual machines hosted by that server to the machine group.
Add Machine (s) To Group	To add individual virtual machines to the machine group, select the desired virtual machines in the right-hand table and then click **Add Machine(s) To Group**. You can add an individual virtual machine even if the server being used to host the virtual machine is already contained in the machine group. Although the virtual machine in this case would technically be listed twice, it will only be scanned once. This applies for all duplicate entries.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Logging on to an ESX or Virtual Infrastructure Server

When you click **Add** or **Edit** on the **Hosted Virtual Machines** tab the **Add vCenter Server/ESXi Hypervisor** dialog is displayed.



Server	Type the full path name or IP address of the vCenter Server or ESXi Hypervisor that you want to add to Ivanti Patch for Windows® Servers.
Port	The port number used when making a connection to the vCenter Server or ESXi Hypervisor. The default value is 443.
vCenter Server / ESXi Hypervisor credential	Select a credential that has access to the vCenter Server or ESXi Hypervisor, or click **New** to define a new credential. For more information, see Defining Credentials.
Add	After you have specified all necessary information, click **Add**. The program will search for all ESXi Hypervisors being managed by the vCenter Server and for all virtual machines hosted on the ESXi Hypervisor(s) and use that information to populate the table.

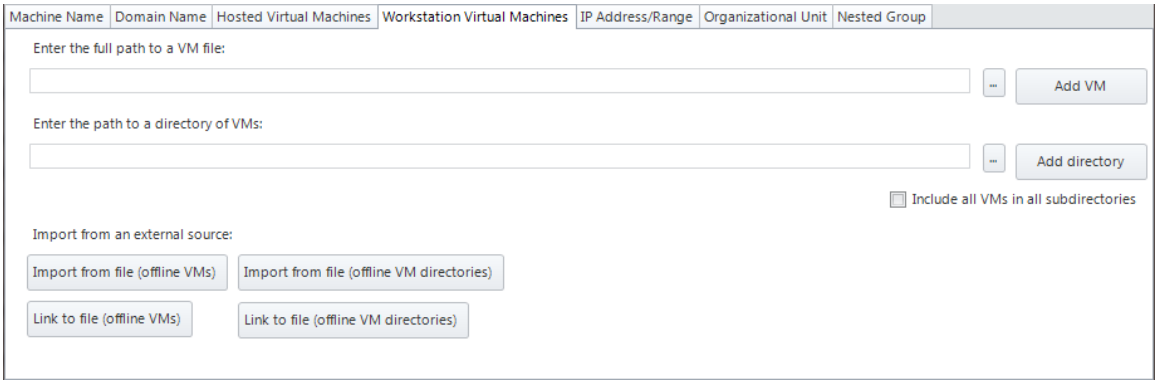
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Adding Offline Virtual Machines That Reside On Workstations

Some virtual machines may reside on individual workstations. Any machine using VMware Workstation software is capable of supporting a virtual machine. The virtual machines may reside almost anywhere, including hard drives, network drives, jump drives, etc. You use the **Workstation Virtual Machines** tab to add these stand-alone offline virtual machines to a machine group.

This tab is used to specify the offline identity of each virtual machine. If a virtual machine added here is online when a scan is performed, a mounting error will occur and the scan of that machine will fail.

TIP: If you want to be absolutely sure that all your virtual machines are successfully scanned, simply add the same machines to the group a second time using one of the other tabs (**Machine Name**, **Domain Name**, or **IP Address/Range**). This duplication assures that each virtual machine will be successfully scanned regardless of its power state (online or offline).



The virtual machines specified here are the actual images and you must therefore specify the full path name. Once the virtual machine is added to a machine group you should also specify the credentials used to connect to that virtual machine. This is different from virtual machines hosted by a server. On a server you can simply reference a file that points to the actual virtual machine, letting the server manage the path and credential information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Adding a virtual machine residing on a workstation	There are two ways to add an offline virtual machine that is hosted on a workstation: • In the **Enter the full path to a VM file** box, type the full path name of the virtual machine. You must specify the full path name and not just the name of the virtual machine. The name must contain a valid image extension (such as .vmx) and must not contain any illegal characters (such as @, ", etc.). When possible, avoid using network drive letters; the recommended practice is to instead specify the Uniform Naming Convention (UNC) path. For example: *machinename**sharename**directory**machine.vmx*. **- OR -** • Click the Browse button () and locate the virtual machine by browsing your local machine and your network for the desired file. Once the virtual machine is defined, click **Add VM** to add it to the machine group list.
Adding a directory of virtual machines	There are two ways to add a directory of offline virtual machines: • In the **Enter the path to a directory of VMs** box, type the full path name of the directory. When possible, avoid using network drive letters. The recommended practice is to specify the Uniform Naming Convention (UNC) path. For example: *virtual**directory*\. **- OR -** • Click the Browse button () and locate the directory by browsing your local machine and your network for the desired directory. If you want the program to recursively search all subdirectories for virtual machines when performing a scan, enable the **Include all VMs in all subdirectories** check box. Once the directory is defined, click **Add directory** to add it to the machine group list.  Adding a large number of virtual machines that are all hosted on the same workstation could cause a connection limit error to occur when scanning the virtual machines. See Notes About Virtual Machines for more information.
Import from file (offline VMs)	You can import a list of offline virtual machines from a previously created text file. 1. Click **Import from file (offline VMs)**. 2. Navigate to the location of the text file and then click**Open**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	The text file can be created manually or it can be created using any network-based tool available to you. When creating the text file, each virtual machine name must be separated by either a carriage return or a comma. For example: `D:\VMware Images\VM-MAF-FR-XPP\winXPPro.vmx, D:\VMware Images\VM-QA-EN-2KS-4\win2000Serv.vmx, Z:\VMware Images\WinXP_EN_gold_2\winXPPro.vmx`

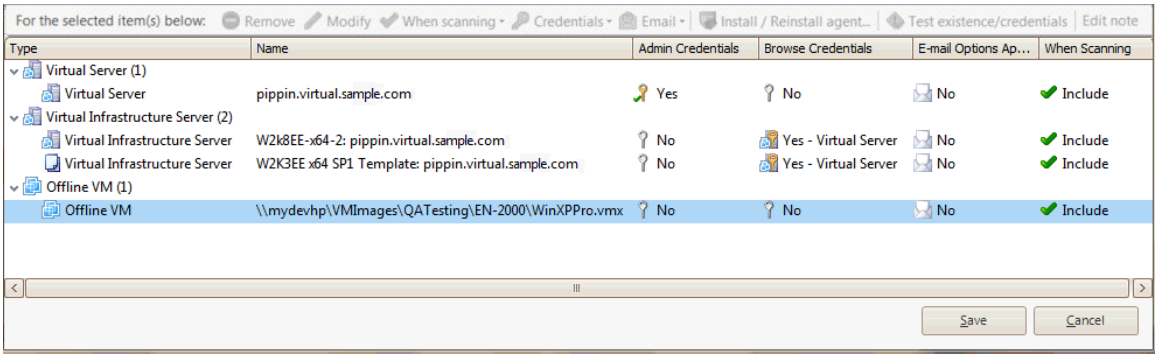
Import from file (offline VM directories)	You can import a list of virtual machine directories from a previously created text file.
	1 Click **Import from file (offline VM directories)**.
	2. Navigate to the location of the text file and then click **Open**.
	The text file can be created manually or it can be created using any network-based tool available to you. When creating the text file, each directory name must be separated by either a comma or a carriage return. For example:
	`D:\VMware Images\VM-MAF-FR-XPP, D:\VMware Images\VM-QA-EN-2KS-4`
	`Z:\VMware Images\WinXP_EN_gold_2`

Link to file (offline VMs) and **Link to file (offline VM directories)**	Offline virtual machines and virtual machine directories can be dynamically linked to a text file rather than imported. Linking a file to a machine group is different than importing its contents. Importing contents is a one-time operation after which the information from the file becomes a part of the machine group. When you link a file to a machine group, any changes that you make to the file are automatically reflected in the next scan. See Linking Files to Machine Groups for more information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Servers and Virtual Machines in a Machine Group

When servers, virtual machines, and virtual machine templates are added to a machine group, the new entries are displayed within the bottom section of the machine group dialog.



The recommended best practice is to always supply credentials for the VMware servers, the virtual machine templates, and the workstation virtual machines. See Supplying Credentials for details. Be careful if you have multiple console administrators, as different administrators are likely to provide different server credentials.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

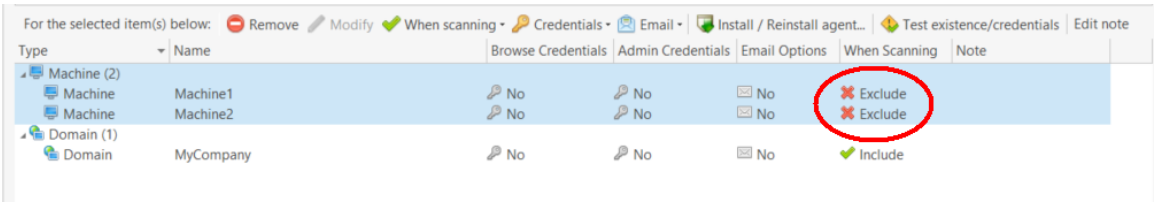
Excluding Certain Machines

You can define a number of machines you want to exclude. This is especially useful for defining a machine group that consists of all but a few machines from a large group of machines. For example, if you want to create a machine group that consists of all but two machines in a domain, you simply add the domain and then specify the two machines you want to exclude.

Machines can be added to the "exclude list" by machine name, by domain name, or by IP address. When specifying the name or IP address, simply enable the **Exclude** check box before you click **Add**. Excluded machines are identified in the machine group list by an **Exclude** icon.

If you create a group of excluded machines and then add that group to a nested group, the exclusions will be honored.

To specify how Ivanti Patch for Windows® Servers will react if two machine groups with opposing include/exclude definitions are used in the same scan operation, see the **Always enforce machine group exclusions** check box.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Linking Files to a Machine Group

Ivanti Patch for Windows® Servers provides a dynamic mechanism for keeping a machine group current. This is especially useful if your machine list changes from time to time and you want an easy way to update it. Linking a file to a machine group is different than importing its contents. Importing contents is a one-time operation after which the information from the file becomes a part of the machine group.

When you link files to a machine group, any changes that you make to the files are reflected upon the next scan. In other words, if you add machines to and delete machines from a linked file between scans, any new machines added to the file will be scanned while any machines removed will not.

When defining a machine group you can link to files containing machine names, domains, IP addresses, and virtual machines. The following table describes how to create each particular link file.

Link Machine File	Provide the name of a file containing machine names. One machine name per line with a carriage return at the end. **Sample:** `machine1`↵ `machine2`↵ `dc`↵ `mail`↵ `dbserver`
Link Domain File	Provide the name of a file containing domain names. One domain name per line with a carriage return at the end. **Sample:** `example`↵ `yourcompany`↵ `corp`↵ `redmond`↵ `dmz`
Link Virtual Machine File	Provide the name of a file containing virtual machines. One virtual machine name per line with a carriage return at the end, or separate each name by a comma. **Sample:** `D:\VMware Images\VM-MAF-FR-XPP\winXPPro.vmx, D:\VMware Images\VM-QA-EN-2KS-4\win2000Serv.vmx`↵ `Z:\VMware Images\WinXP_EN_gold_2\winXPPro.vmx`

Copyright © 2017, Ivanti. All Rights Reserved. Terms of Use.

Link IP Address File	Provide the name of a file containing IP addresses. One IP address per line with a carriage return at the end. You cannot combine individual IP addresses and IP ranges in the same file. **Sample:** `192.168.29.132`↵ `10.1.1.10`↵ `172.16.1.5`
Link IP Range File	Provide the name of a file containing IP ranges. IP ranges in the format of x.x.x.x-y.y.y.y are acceptable. One per line with a carriage return at the end. **Sample:** `192.168.29.1-192.168.29.5`↵ `172.16.2.20-172.16.2.99`

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Introducing the Virtual Inventory Feature



Show Me!

To view a video tutorial on this topic, click the video icon on the left.

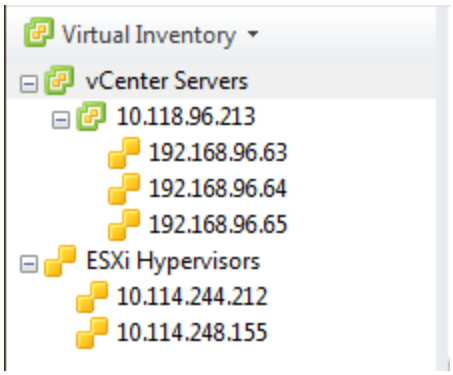
For information on managing your online and offline virtual machines, see Roadmap of Tasks for Virtual Machines.

The Virtual Inventory feature is used to manage and track the vCenter Servers and the ESXi hypervisors (ESXi hosts) that are used in your organization. It may also help you discover virtual machines you didn't even know you had. You can use the Virtual Inventory feature to:

- Add vCenter Servers and ESXi hypervisors to Ivanti Patch for Windows® Servers
- View basic configuration information about the vCenter Servers and the ESXi hypervisors
- Perform a scan of the managed and unmanaged ESXi hypervisors
- View the security bulletins that have already been installed on the managed and unmanaged ESXi hypervisors
- View the security bulletins that are missing on the managed and unmanaged ESXi hypervisors
- Deploy any missing security bulletins to the ESXi hypervisors
- Power on and off the virtual machines that reside on your managed and unmanaged ESXi hypervisors
- Add the virtual machines and virtual machine templates to a new or existing machine group

The vCenter Servers and the ESXi hypervisors that are currently defined to Ivanti Patch for Windows® Servers can be viewed by selecting **Virtual Inventory** at the top of the navigation pane. The **vCenter Servers** list shows the vCenter Servers you are using and the ESXi hypervisors they are managing. The **ESXi Hypervisors** list shows the hypervisors that are not being managed by a vCenter Server. It is possible for a managed hypervisor to appear in both lists if you import the hypervisor as a standalone device and you also import the vCenter Server that is managing the hypervisor.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

vCenter Server and ESXi Hypervisor Requirements

The functions provided by the Virtual Inventory feature are designed for use with the following VMware vSphere licensed environments: VMware vSphere Essentials, Essentials Plus, Standard, and Standard with Operations Management. While the functions can be used in enterprise-level environments, the user experience and performance has been optimized for use in small and medium-sized business environments.

vCenter Server Requirements and Recommendations

- The vCenter Servers that are added to the Virtual Inventory list must be at VMware vCenter Server 5.0 or later
- You must have valid credentials for the vCenter Server
- You must be able to connect to the vCenter Server
- If the hypervisors in your organization are managed by a vCenter Server, you should add those hypervisors to Ivanti Patch for Windows® Servers by adding the managing vCenter Server. The scanning and deployment actions you take on the hypervisors are more complete when performed through a vCenter Server.

ESXi Hypervisor Scanning Requirements

You must meet the following requirements in order to successfully scan an ESXi hypervisor:

- You must have valid credentials for the ESXi hypervisor
- You must be able to connect to the ESXi hypervisor
- The hypervisor must be using ESXi version 5.0 or later
- Your firewall must be configured to allow an HTTP Client connection

ESXi Hypervisor Deployment Requirements and Recommendations

You must meet the following requirements in order to successfully deploy bulletins to ESXi hypervisors:

- The Ivanti Patch for Windows® Servers console must be online
- The ESXi hypervisor must be online in order to access assessment data and download updates
- The hypervisor must be using ESXi version 5.0 or later

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- Port 443 must be open on the hypervisor
- The latest version of VMware Tools is required on all virtual machines running on the hypervisor
- You must have previously scanned the ESXi hypervisor to identify the missing bulletins
- You can only deploy bulletins to one ESXi hypervisor at a time in a single deployment. You can, however, start multiple deployments to different hypervisors and have them run concurrently (do not do this if the hypervisors are being managed by the same vCenter Server).
- You cannot schedule deployments
- For vCenter Servers using fully automated Distributed Resources Scheduler (DRS), during a deployment Ivanti Patch for Windows® Servers will attempt to put the ESXi hypervisor into maintenance mode and allow DRS to manage the virtual machines. Ivanti Patch for Windows® Servers will not support DRS for vCenter Servers that have their DRS automation level set to **Manual** or **Partially Automated** because these DRS settings require user intervention at the vSphere client level. In this case Ivanti Patch for Windows® Servers may suspend or shut down the virtual machines, or it may cancel the deployment.
- You should not attempt to patch a hypervisor that contains a vCenter Server or vCenter Server Appliance without first moving the vCenter Server to another hypervisor. Consider using DRS to move the vCenter Server.
- You should not attempt to patch a hypervisor that contains the Ivanti Patch for Windows® Servers console without first moving the console to another hypervisor. Consider using DRS to move the console.
- You must use a role that contains the following permissions on the ESXi hypervisor:
    - Global
        - Act as vCenter Server
        - Cancel task
        - Diagnostics
        - Licenses
        - Log event
        - Proxy
    - Host: Configuration
        - Connection
        - Maintenance

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

    - Power
    - Query patch
    - System Management
    - System resources
- Host: Replication
- Resource
- Scheduled task
- Sessions
- Tasks
- vApp
- vCenter Inventory Services (v5.1 or later)
- vService (v5.0 or later)
- Virtual machine

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

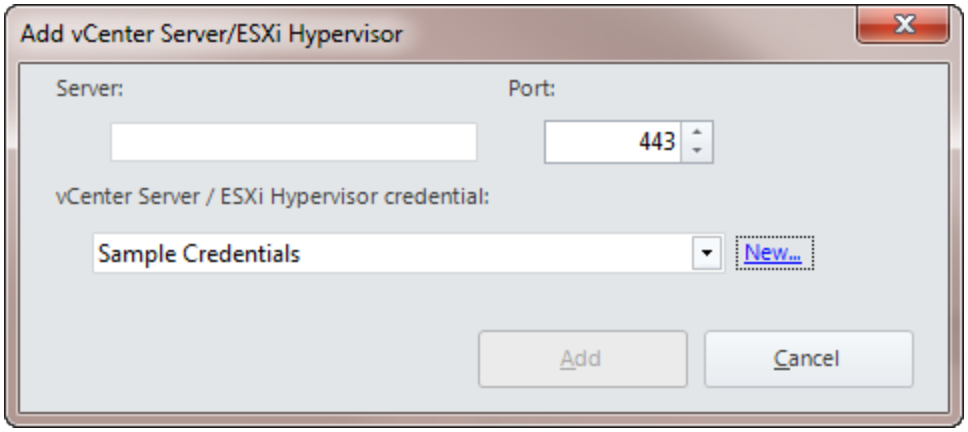
Adding, Editing, or Removing vCenter Servers and ESXi Hypervisors

Adding vCenter Servers and ESXi Hypervisors

To add a vCenter Server or an ESXi hypervisor to Ivanti Patch for Windows® Servers:

1. From the main menu select **New > Add vCenter Server/ESXi Hypervisor**.
2. Specify the server, port, and credential information.
3. Click **Add**.

The item is added to the **Virtual Inventory** list. It is also automatically added to the **Hosted Virtual Machines** tab of your existing and future machine groups.



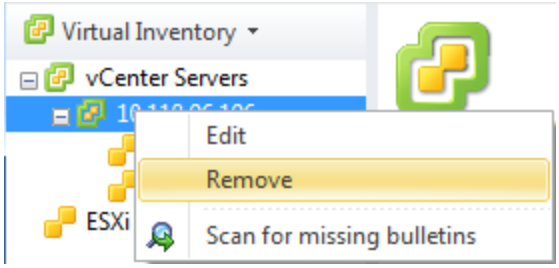
Server	Type the full path name or IP address of the vCenter Server or ESXi hypervisor that you want to add to Ivanti Patch for Windows® Servers.
Port	The port number used when making a connection to the vCenter Server or ESXi hypervisor. The default value is 443.
vCenter Server / ESXi Hypervisor credential	Select a credential that has access to the vCenter Server or ESXi hypervisor, or click **New** to define a new credential. For more information, see Defining Credentials.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Add	After you have specified all necessary information, click **Add**. If the item is an unmanaged ESXi hypervisor, the program will add the hypervisor and all virtual machines hosted on the hypervisor to the **Virtual Inventory** list. If the item is a vCenter Server, the program will search for all ESXi hypervisors being managed by the vCenter Server and it will add the vCenter Server, the hypervisors, and the hosted VMs to the **Virtual Inventory** list.

Editing or Removing vCenter Servers and ESXi Hypervisors

In the Virtual Inventory list, use the right-click menu to edit or remove a vCenter Server or an ESXi hypervisor.



You cannot use the right-click menu to edit or remove individual ESXi hypervisors that are being managed by a vCenter Server. These two right-click menu items apply to vCenter Servers and to hypervisors that are NOT being managed by a vCenter Server (the hypervisors contained in the **ESXi Hypervisors** list).

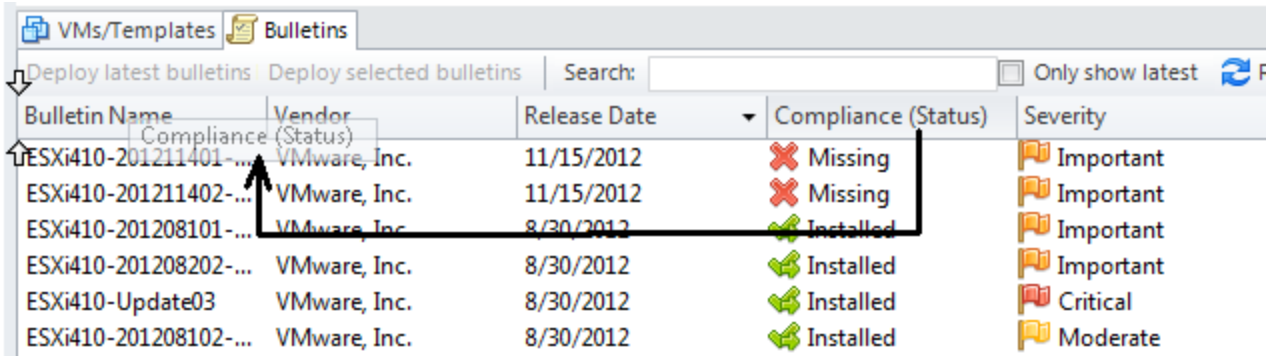
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Customizing the Column Headers

You can easily customize the way information is displayed within any of the Virtual Inventory panes.

- You can reorder the columns by clicking and dragging the column headers to new locations.

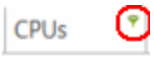
  For example, if you want missing bulletin information to be displayed in the first column, simply click on the **Compliance (Status)** column header and drag it to the first column.



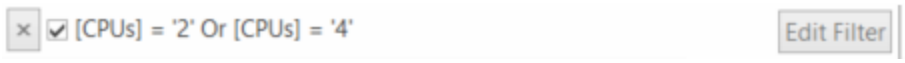
> TIP: When reordering columns, the column header you are moving will always be placed in front of the column you drag it to.

- You can apply filters to one or more column headers.

  Hover over a column header and then click the filter icon located in the upper-right corner. For example:

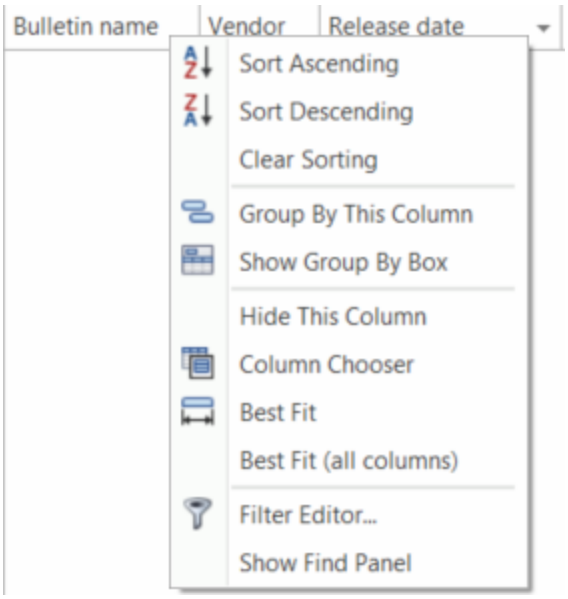


  Use the filter menu to select which of the values currently contained in the column should be displayed. When you apply a column filter, the filter definition will be displayed beneath the pane. You can use this to confirm which column filters have been applied and to edit the filter. For example:



- You can right-click within a column header and perform a number of additional actions.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Sort Ascending	Sorts the selected column in ascending order.
Sort Descending	Sorts the selected column in descending order.
Clear Sorting	Clears the ascending or descending sorting criteria currently set for a column.
Group By This Column	Groups the table using the data in the selected column. It does this by moving the data into expandable lists that are located in the body of the grid. One expandable list will be created for each possible column value. If you perform this action on any subsequent columns, that data will be presented as nested groups at increasingly lower levels within the expandable lists. If **Show Group By Box** is enabled, this will also create a "Group By" box in the area immediately above the column headers. TIP: To turn off the **Group By This Column** feature and revert to the original view: Enable **Show Group By Box**, drag the Group By boxes back to the column header and then right-click in the column header and select **Hide Group By Box**.
Show Group By Box / Hide Group By Box	Displays or hides an area immediately above the column headers that contains "Group By" boxes. One Group By box will be displayed for each column header for which **Group By This Column** is currently enabled. You can also drag column headers to and from this area.

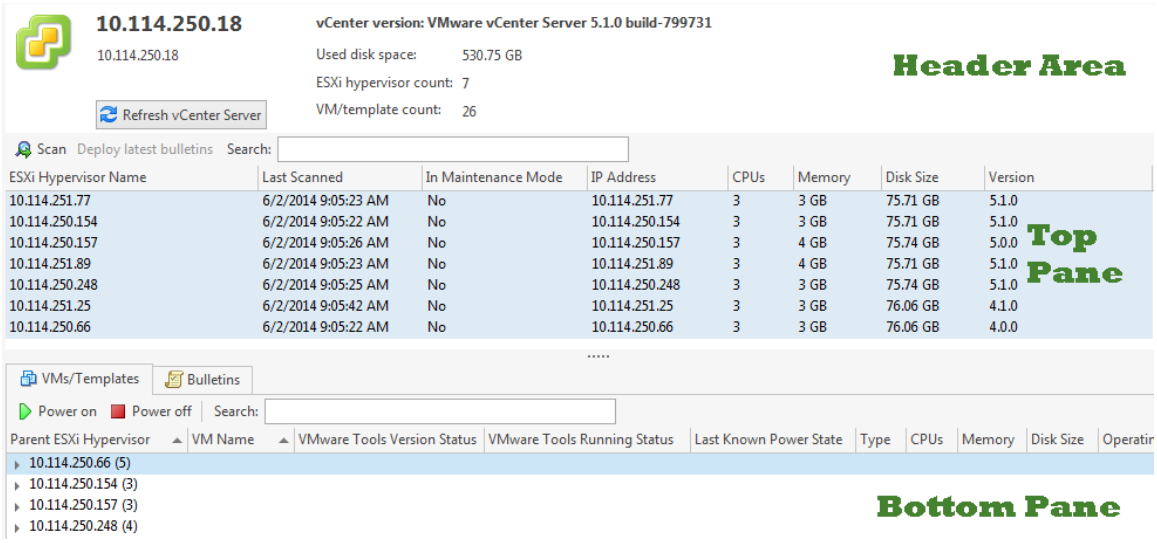
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	The table will be grouped according to the data in the box. If there are two or more boxes then the grouping will be nested, with the left-most box presented at the highest level, the second box presented at the second level, etc.
Hide This Column	Removes the column from the table. You can add the column back to the table using the **Column Chooser**.
Column Chooser	Enables you to add and hide information within a pane. When you select **Column Chooser** the **Customization** dialog is displayed. This dialog is used to store the columns you don't currently want displayed within the pane. Simply click and drag the desired column headers from the table to the Customization dialog. If you decide you want an item back in the table, simply click and drag it from the Customization dialog back to the table.
Best Fit	Resize the width of the selected column so that the header text is displayed in the optimal amount of space.
Best Fit (all columns)	Resize the width of all columns in the table so that the header text is displayed in the optimal amount of space.
File Editor	The **Filter Editor** dialog will show any filters that are currently active in the column headers. You can use the editor to modify the existing filter criteria and to build new criteria using the available filter conditions and logical operators.
Show Find Panel / Hide Find Panel	Displays or hides a search box that you can use to find specific patches or text related to any of the patches contained in the patch data file. Here are a few tips for using the search box: • The search works only on the information currently visible in the grid • All partial matches are displayed • The use of wildcards is not allowed

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Information About a vCenter Server

When you select a vCenter Server in the Virtual Inventory list, information about that vCenter Server is displayed in a header area and in two panes. Both panes display unique information and provide unique functionality. The two panes are interrelated—the information presented in the bottom pane is dependent on what is selected in the top pane. This "top down" approach means you use the top pane to view overview information about the hypervisors being managed by the vCenter server, and you use the bottom pane to drill down to more detailed information about specific hypervisors.



- The header area provides basic configuration information about the selected vCenter server.
- The top pane displays the ESXi hypervisors that are being managed by the selected vCenter Server. See the following topics for information on using the top pane:
  - Searching the List of Hypervisors
  - Scanning One or More Hypervisors
  - Deploying Bulletins to a Hypervisor
  - Customizing the Column Headers
- The bottom pane contains two tabs: The **VMs/Templates** tab displays information about the virtual machines and virtual machine templates that are contained on the selected ESXi hypervisor(s). The **Bulletins** tab shows the status of the security bulletins that have been issued for the selected hypervisor(s). See the following topics for information on using the bottom pane:
  - Powering On and Off the Virtual Machines and Virtual Machine Templates

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- Adding the Virtual Machines to a Machine Group
- Searching the List of Virtual Machines
- Applying Missing Bulletins to an ESXi Hypervisor
- Customizing the Column Headers

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

vCenter Server Top Pane Summary

The top pane contains basic information about each ESXi hypervisor that is being managed by the vCenter Server. Click on a column heading to sort the table by that information.

ESXi Hypervisor Name	Last Scanned	In Maintenance Mode	IP Address	CPUs	Memory
10.114.251.77	6/2/2014 9:05:23 AM	No	10.114.251.77	3	3 GB
10.114.250.154	6/2/2014 9:05:22 AM	No	10.114.250.154	3	3 GB
10.114.250.157	6/2/2014 9:05:26 AM	No	10.114.250.157	3	4 GB
10.114.251.89	6/2/2014 9:05:23 AM	No	10.114.251.89	3	4 GB
10.114.250.248	6/2/2014 9:05:25 AM	No	10.114.250.248	3	3 GB
10.114.251.25	6/2/2014 9:05:42 AM	No	10.114.251.25	3	3 GB

ESXi Hypervisor Name	The name or IP address of the ESXi hypervisor.
Last Scanned	Shows the date and time that the ESXi hypervisor was last scanned.
In Maintenance Mode	Indicates if the ESXi hypervisor was in maintenance mode at the time of the last scan.
IP Address	The IP address of the ESXi hypervisor.
CPUs	The number of CPUs contained on the ESXi hypervisor.
Memory	The amount of memory contained on the ESXi hypervisor.
Disk Size	The amount of total disk space contained on the ESXi hypervisor.
Version	The software version of the ESXi hypervisor.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Searching for Hypervisors While Viewing a vCenter Server

You can easily search for hypervisors contained in the top pane. All searches are performed using the Search tool.



To initiate a search you simply type the search criteria in the **Search** box. Only those hypervisors that match the search criteria are displayed; all other hypervisors are hidden.

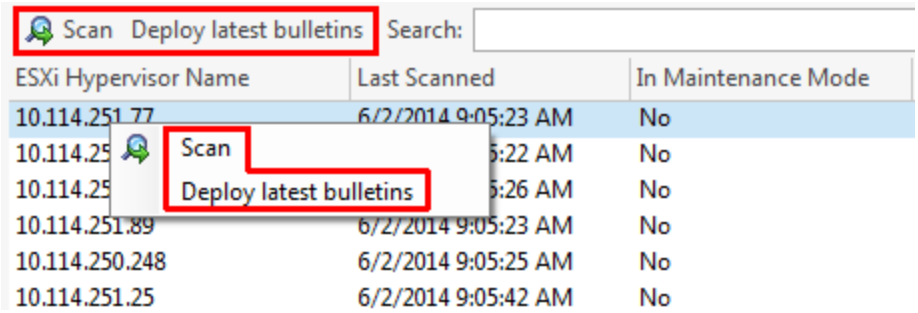
Tips for Using the Search Tool

- The Search tool works only on the information currently visible in the top pane.
- The search will be performed on all information in the pane, not just the **ESXi Hypervisor Name** column.
- All partial matches are displayed. For example, if you search for hypervisors named *Test*, any hypervisor with "test" in its name will be considered a match (e.g. TestHypervisor1, Contest, etc.).
- A semicolon (;) can be used to concatenate multiple search terms into one search string. For example, specifying "192.168;10.112" will return all items containing either of the two terms.
- The use of wildcards in the Search tool is not allowed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing Actions on ESXi Hypervisors

You can perform a number of different actions on the ESXi hypervisors that are being managed by a vCenter Server. You simply select the desired ESXi hypervisors and then either use the buttons along the top of the table or use the right-click menu.



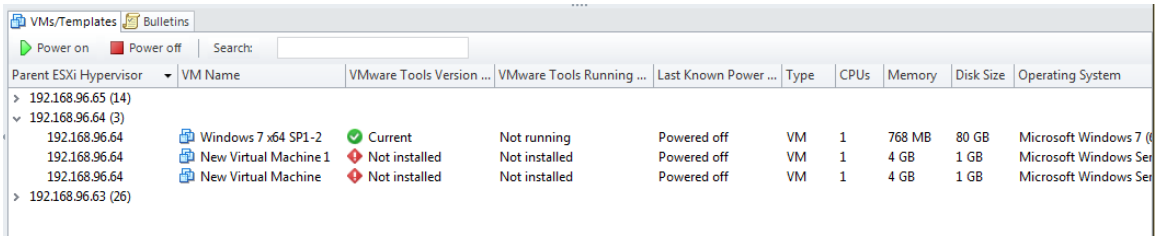
Scan	Enables you to initiate a scan of the selected ESXi hypervisors. The Operations Monitor is used to monitor the status of the hypervisor scan. The results of the scan can be found on the **Bulletins** tab. Remember to refresh the **Bulletins** tab to view the most current information.
Deploy latest bulletins	Enables you to deploy bulletins currently missing on the selected ESXi hypervisor. If this option is not available it means one of the following: the ESXi hypervisor has not been previously scanned, there are multiple ESXi hypervisors selected (you can only deploy bulletins to one hypervisor at a time), or all bulletins have been applied. For more information on deploying bulletins to an ESXi hypervisor, see Configuring an ESXi Deployment.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing a Summary of the ESXi Hypervisor's Virtual Machines and Virtual Machine Templates

The **VMs/Templates** tab displays summary information about the virtual machines and virtual machine templates that are contained on the ESXi hypervisor(s) selected in the top pane. If multiple hypervisors are selected in the top pane, this tab will display virtual machine information for all the selected hypervisors.

You can customize the way information is displayed within this pane. See Customizing the Column Headers for information.



Power on	See Performing Actions on Virtual Machines.
Power off	See Performing Actions on Virtual Machines.
Search	Enables you to search for virtual machines contained on the tab. To initiate a search you simply type the search criteria in the **Search** box. Only those virtual machines that match the search criteria are displayed; all other virtual machines are hidden. • The Search tool works only on the information currently visible on the tab. • The search will be performed on all information on the tab, not just the VM Name column. • All partial matches are displayed. For example, if you search for virtual machines named Test, any virtual machine with "test" in its name will be considered a match (e.g. TestVM1, Contest, etc.). • The use of wildcards in the Search tool is not allowed.

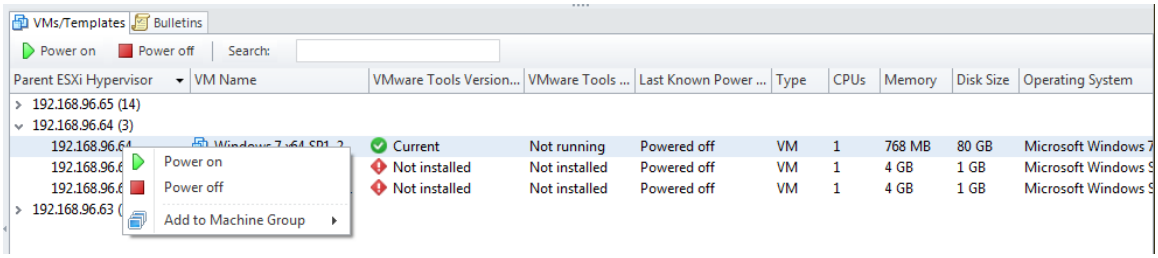
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Parent ESXi Hypervisor	The name or IP address of the ESXi hypervisor that is hosting the virtual machine or virtual machine template.
VM Name	The virtual machine name.
VMware Tools Version Status	VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine. This column identifies the version of VMware Tools currently in use on the virtual machine.
VMware Tools Running Status	Indicates if VMware Tools is running on the virtual machine.
Last Known Power State	The last known state of the virtual machine (Powered on, Powered off, or Suspended).
Type	Indicates if the device is a virtual machine (VM) or a VM template.
CPUs	The number of Central Processing Unit (CPUs) available to the virtual machine.
Memory	The amount of memory (MB) allocated to the virtual machine.
Disk Size	The amount of disk space (GB) allocated to the virtual machine.
Operating System	The operating system being used on the virtual machine.
IP Address	The IP address of the virtual machine.
Hostname	The name of the machine on the network that is hosting the virtual machine.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing Actions on Virtual Machines

The **VMs/Templates** tab can be used to power on and off your virtual machines. You can also add the virtual machines to a new or existing machine group. To do this you simply select the desired virtual machines and then either use the buttons along the top of the tab or use the right-click menu.



Power on	Enables you to immediately power on the selected virtual machine(s). The Operations Monitor is used to monitor the status of the power operation. To view the updated power state, refresh the information displayed on the tab by selecting **View > Refresh**.
Power off	Enables you to immediately power off the selected virtual machine(s). The Operations Monitor is used to monitor the status of the power operation. To view the updated power state, refresh the information displayed on the tab by selecting **View > Refresh**.
Add to Machine Group	Enables you to add the selected machines to a new machine group or to an existing machine group. See Creating A New Machine Group for more information. IMPORTANT! Machines you add to the machine group are automatically assigned the associated machine credentials. (Hosted virtual machines are the exception, they are assigned the last known machine group credentials.) If no machine credentials are available, no credentials will be assigned and the default credentials will be used in any subsequent scans. If the default credentials are not valid for the machines, and if the account credentials of the person currently logged on to the program are also not valid for the machines, scans of the machines you just added to the group will fail. To prevent scanning errors, always supply credentials for machines you add to a machine group. See Supplying Credentials for more information.

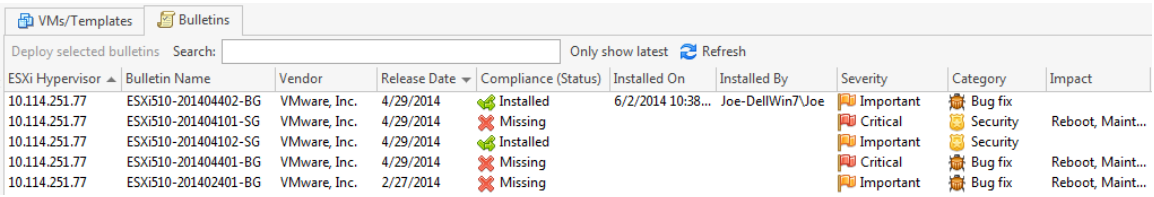
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Bulletin Status

The **Bulletins** tab displays the status of the security bulletins that have been issued for the ESXi hypervisor(s) selected in the top pane. If multiple hypervisors are selected in the top pane, this tab will display bulletin information for all selected hypervisors.

A bulletin that is scheduled for deployment is considered to be still missing. This status will change after the bulletin is successfully installed and the screen is refreshed.

You can customize the way information is displayed within this tab. See Customizing the Column Headers for information.



Deploy selected bulletins	See How to Deploy Bulletins to Your Managed Hypervisor.
Search	Enables you to search for bulletins contained on the tab. To initiate a search you simply type the search criteria in the **Search** box. Only those bulletins that match the search criteria are displayed; all other bulletins are hidden. • The Search tool works only on the information currently visible on the tab. • The search will be performed on all information on the tab, not just the **Bulletin Name** column. • All partial matches are displayed. For example, if you search for bulletins named *Test*, any bulletin with "test" in its name will be considered a match (e.g. Testbulletin1, Contest, etc.). • The use of wildcards in the Search tool is not allowed.
Only show latest	If enabled, filters the contents of the tab so that the only bulletins displayed are those that are not replaced by newer bulletins. Use this check box to identify the vulnerabilities that have not yet been addressed.
Refresh	Updates the bulletin information that is displayed on the tab.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

ESXi Hypervisor	The name or IP address of the ESXi hypervisor.
Bulletin Name	The bulletin name.
Vendor	Identifies the name of the vendor that released the bulletin.
Release Date	The original publication date of the bulletin that corrects this vulnerability.
Compliance (Status)	Indicates the bulletin status at the time the scan was performed.
Installed On	Shows the date and time that the bulletin was installed. This information will not be available if the bulletin was installed using a different Ivanti Patch for Windows® Servers database or if the bulletin was not installed by Ivanti Patch for Windows® Servers.
Installed By	Shows the name of the user who installed the bulletin. This information will not be available if the bulletin was installed using a different Ivanti Patch for Windows® Servers database or if the bulletin was not installed by Ivanti Patch for Windows® Servers.
Severity	Indicates the severity level of the vulnerability that is corrected by this bulletin. The severity level can be one of the following: • **Critical:** Vulnerabilities that can be exploited by an unauthenticated remote attacker or vulnerabilities that break guest/host operating system isolation. The exploitation results in the compromise of confidentiality, integrity, availability user data, or processing resources without user interaction. Exploitation could be leveraged to propagate an Internet worm or execute arbitrary code between virtual machines and the host. • **Important:** Vulnerabilities whose exploitation results in the compromise of confidentiality, integrity, or availability of user data and processing resources. Such flaws could allow local users to gain privileges, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

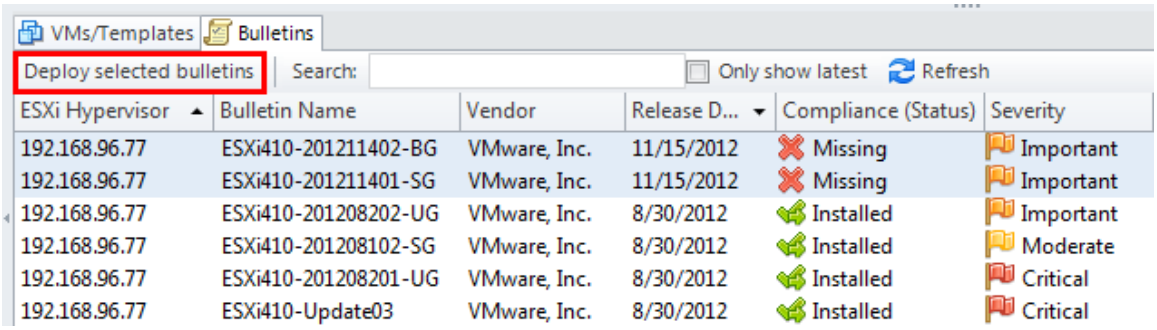
	• **Moderate:** Flaws where the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios could still lead to some compromise of the confidentiality, integrity, or availability of user data and processing resources. These are the types of vulnerabilities that could have had a critical impact or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations. • **Low:** All other issues that have a security impact. Vulnerabilities where exploitation is believed to be extremely difficult, or where successful exploitation would have minimal impact.
Category	The bulletin category can be one of the following: • **Security:** The bulletins that belong to this category fix one or more potential security vulnerabilities. The bulletin may also contain bug fixes. • **Bug fix:** The bulletins that belong to this category contain one or more bug fixes. • **Other:** For backward compatibility. For example, for updates without a category specified or for obsolete categories.
Impact	Indicates the impact that applying the bulletin will have on the virtual machine and hypervisor.
Replaced By	The bulletin that contains a more recent update for the vulnerability.
Summary	Provides a short description of the bulletin.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How to Deploy Bulletins to Your Managed Hypervisors

The **Bulletins** tab can be used to deploy missing bulletins to your managed ESXi hypervisors. You simply select the desired bulletin(s) and then click **Deploy selected bulletins**. Note that because you can only deploy bulletins to one hypervisor at a time, if you select bulletins from two or more hypervisors, the **Deploy selected bulletins** button will no longer be available. For more information on the bulletin deployment process, see Configuring an ESXi Deployment.

TIP: Use the **Only show latest** check box to view only those bulletins that are not replaced by newer bulletins.

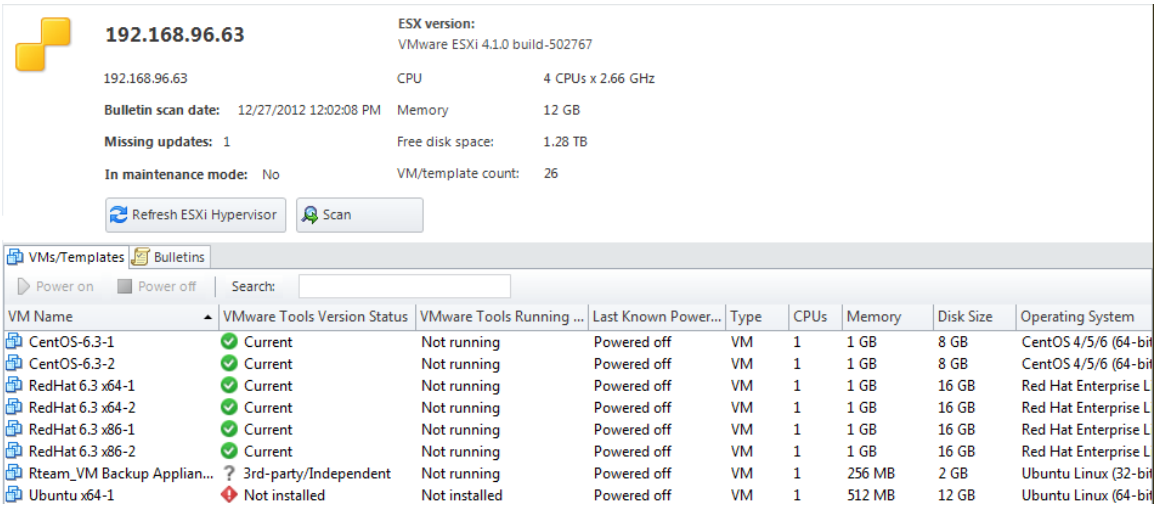


Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Using the ESXi Hypervisors List

The **ESXi Hypervisors** list contains those hypervisors that are not being managed by a vCenter Server. When you select an individual hypervisor in this list or in the vCenter Servers list, information about that ESXi hypervisor is displayed in a header area and on two tabs in the lower pane.

- The header area provides basic configuration information about the selected ESXi hypervisor. It also contains a **Scan** button that enables you to initiate a bulletin scan of the ESXi hypervisor. For more information, see How to Initiate a Scan of an ESXi Hypervisor.
- The **VMs/Templates** tab displays information about the virtual machines and virtual machine templates that are contained on the selected ESXi hypervisor. You can use this tab to power the virtual machines on and off, and you can add the virtual machines to a machine group.
- The **Bulletins** tab shows the status of the security bulletins that have been issued for the ESXi hypervisor(s). You can also use this tab to deploy missing bulletins to your ESXi hypervisors.

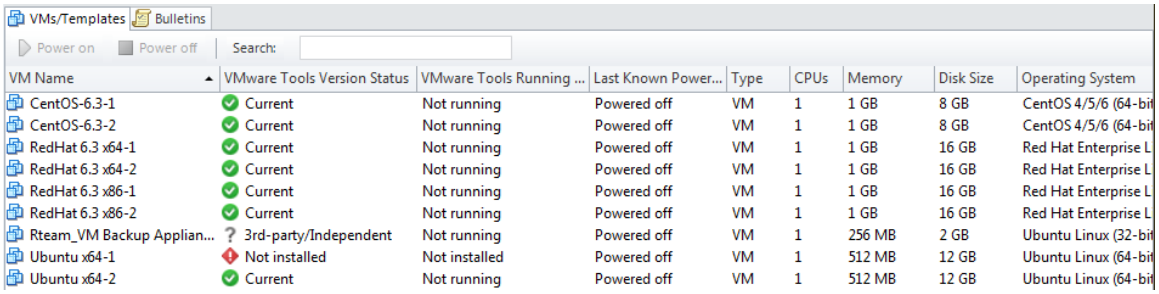


Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing a Summary of the ESXi Hypervisor's Virtual Machines and Virtual Machine Templates

The **VMs/Templates** tab displays summary information about the virtual machines and virtual machine templates that are contained on the selected ESXi hypervisor.

You can customize the way information is displayed within this pane. See Customizing the Column Headers for information.



Power on	See Performing Actions on Virtual Machines.
Power off	See Performing Actions on Virtual Machines.
Search	Enables you to search for virtual machines contained on the tab. To initiate a search you simply type the search criteria in the **Search** box. Only those virtual machines that match the search criteria are displayed; all other virtual machines are hidden. • The Search tool works only on the information currently visible on the tab. • The search will be performed on all information on the tab, not just the **VM Name** column. • All partial matches are displayed. For example, if you search for virtual machines named *Test*, any virtual machine with "test" in its name will be considered a match (e.g. TestVM1, Contest, etc.). • The use of wildcards in the Search tool is not allowed.
VM Name	The virtual machine name.

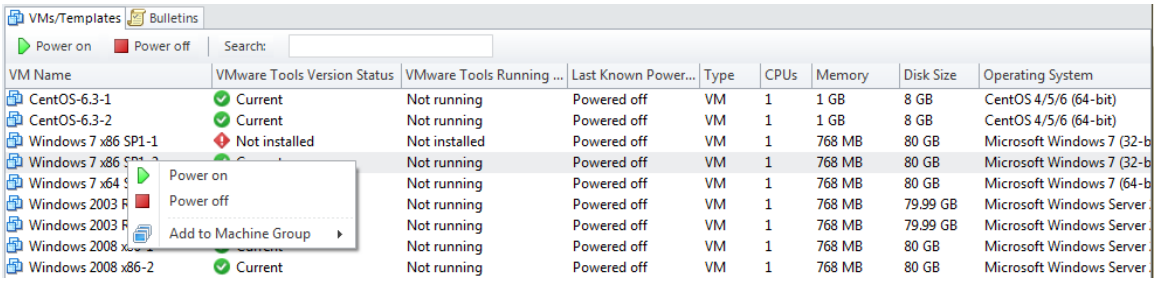
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

VMware Tools Version Status	VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine. This column identifies the version of VMware Tools currently in use on the virtual machine.
VMware Tools Running Status	Indicates if VMware Tools is running on the virtual machine.
Last Known Power State	The last known state of the virtual machine (Powered on, Powered off, or Suspended).
Type	Indicates if the device is a virtual machine (VM) or a virtual machine template.
CPUs	The number of Central Processing Unit (CPUs) available to the virtual machine.
Memory	The amount of memory (MB) allocated to the virtual machine.
Disk Size	The amount of disk space (GB) allocated to the virtual machine.
Operating System	The operating system being used on the virtual machine.
IP Address	The IP address of the virtual machine.
Hostname	The name of the machine on the network that is hosting the virtual machine.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing Actions on a Hypervisor's Virtual Machines

The **VMs/Templates** tab can be used to power on and off the virtual machines that are contained on the selected hypervisor. You can also add the virtual machines and templates to a new or existing machine group. To perform these actions you simply select the desired virtual machines and/or templates and then either use the buttons along the top of the tab or use the right-click menu.



Power on	Enables you to immediately power on the selected virtual machine(s). The Operations Monitor is used to monitor the status of the power operation. To view the updated power state, refresh the information displayed on the tab by selecting **View > Refresh**.
Power off	Enables you to immediately power off the selected virtual machine(s). The Operations Monitor is used to monitor the status of the power operation. To view the updated power state, refresh the information displayed on the tab by selecting **View > Refresh**.
Add to Machine Group	Enables you to add the selected machines to a new machine group or to an existing machine group. See Creating A New Machine Group for more information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



IMPORTANT! Machines you add to the machine group are automatically assigned the associated machine credentials. (Hosted virtual machines are the exception, they are assigned the last known machine group credentials.) If no machine credentials are available, no credentials will be assigned and the default credentials will be used in any subsequent scans. If the default credentials are not valid for the machines, and if the account credentials of the person currently logged on to the program are also not valid for the machines, scans of the machines you just added to the group will fail. To prevent scanning errors, always supply credentials for machines you add to a machine group. See Supplying Credentials for more information.

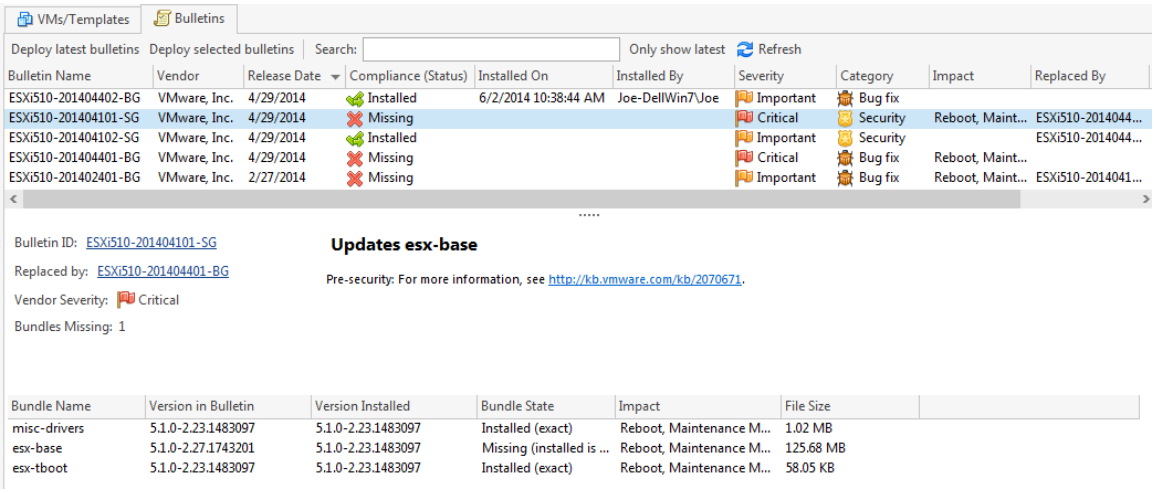
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Bulletin Status on Unmanaged Hypervisors

The **Bulletins** tab displays the status of the security bulletins that have been issued for the selected ESXi hypervisor. If you select a bulletin, information about it is displayed in the bottom pane.

A bulletin that is scheduled for deployment is considered to be still missing. This status will change after the bulletin is successfully installed and the screen is refreshed.

You can customize the way information is displayed within this tab. See Customizing the Column Headers for information.



Deploy latest bulletins **Deploy selected bulletins**	See Deploying Bulletins to Unmanaged ESXi Hypervisors.
Search	Enables you to search for bulletins contained on the tab. To initiate a search you simply type the search criteria in the **Search** box. Only those bulletins that match the search criteria are displayed; all other bulletins are hidden. • The Search tool works only on the information currently visible on the tab. • The search will be performed on all information on the tab, not just the **Bulletin Name** column.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• All partial matches are displayed. For example, if you search for bulletins named *Test*, any bulletin with "test" in its name will be considered a match (e.g. TestBulletin1, Contest, etc.). • The use of wildcards in the Search tool is not allowed.
Only show latest	If enabled, filters the contents of the tab so that the only bulletins displayed are those that are not replaced by newer bulletins. Use this check box to identify the vulnerabilities that have not yet been addressed.
Refresh	Updates the information that is displayed on the tab.
Bulletin Name	The bulletin name.
Vendor	Identifies the name of the vendor that released the bulletin.
Release Date	The original publication date of the bulletin that corrects this vulnerability.
Compliance (Status)	Indicates the bulletin status at the time the bulletin scan was performed.
Installed On	Shows the date and time that the bulletin was installed. This information will not be available if the bulletin was installed using a different Ivanti Patch for Windows® Servers database or if the bulletin was not installed by Ivanti Patch for Windows® Servers.
Installed By	Shows the name of the user who installed the bulletin. This information will not be available if the bulletin was installed using a different Ivanti Patch for Windows® Servers database or if the bulletin was not installed by Ivanti Patch for Windows® Servers.
Severity	Indicates the severity level of the vulnerability that is corrected by this bulletin. The severity level can be one of the following:

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **Critical:** Vulnerabilities that can be exploited by an unauthenticated remote attacker or vulnerabilities that break guest/host operating system isolation. The exploitation results in the compromise of confidentiality, integrity, availability user data, or processing resources without user interaction. Exploitation could be leveraged to propagate an Internet worm or execute arbitrary code between virtual machines and the host. • **Important:** Vulnerabilities whose exploitation results in the compromise of confidentiality, integrity, or availability of user data and processing resources. Such flaws could allow local users to gain privileges, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service. • **Moderate:** Flaws where the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios could still lead to some compromise of the confidentiality, integrity, or availability of user data and processing resources. These are the types of vulnerabilities that could have had a critical impact or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations. • **Low:** All other issues that have a security impact. Vulnerabilities where exploitation is believed to be extremely difficult, or where successful exploitation would have minimal impact.
Category	The bulletin category can be one of the following:

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

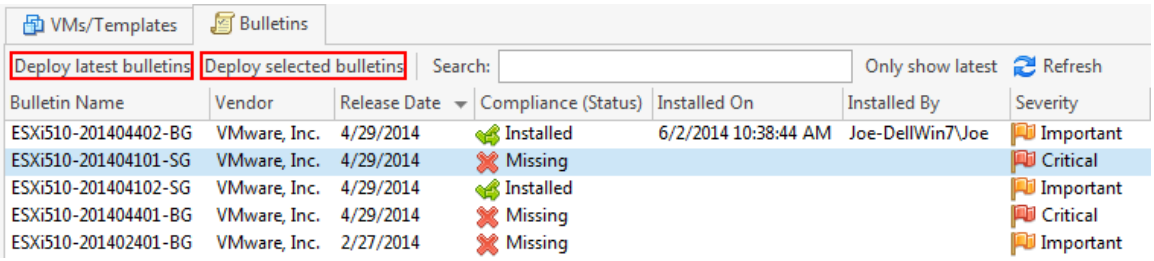
	• **Security:** The bulletins that belong to this category fix one or more potential security vulnerabilities. The bulletin may also contain bug fixes. • **Bug fix:** The bulletins that belong to this category contain one or more bug fixes. • **Other:** For backward compatibility. For example, for updates without a category specified or for obsolete categories.
Impact	Indicates the impact that applying the bulletin will have on the virtual machine and hypervisor.
Replaced By	The bulletin that contains a more recent update for the vulnerability.
Summary	Provides a short description of the bulletin.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deploying Bulletins to Unmanaged Hypervisors

The **Bulletins** tab can be used to deploy missing bulletins to your ESXi hypervisors and to view information about the bulletins.

To apply one or more bulletins, select the desired bulletins and then use the buttons along the top of the table.

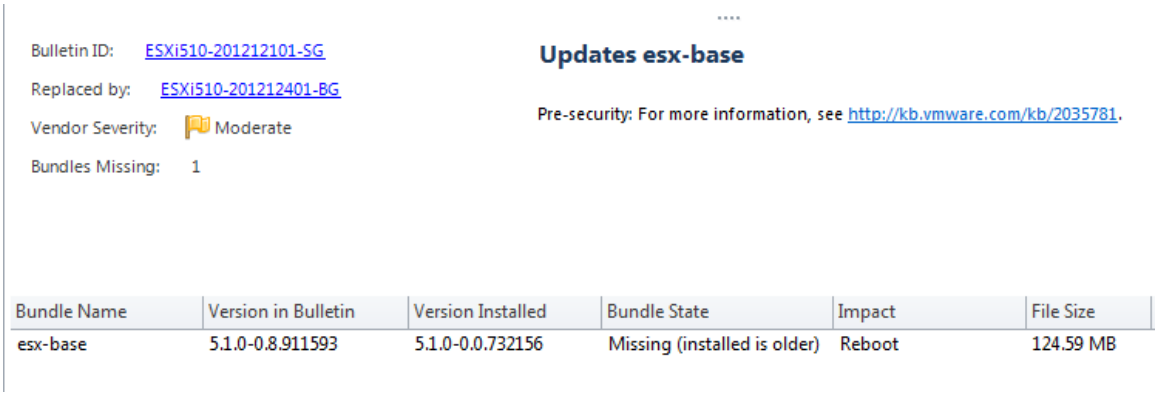


Deploy latest bulletins	Initiates the deployment of all bulletins that are missing on the ESXi hypervisor. This will include only those bulletins that have not been replaced by newer bulletins. For more information on the bulletin deployment process, see Configuring an ESXi Deployment. TIP: Use the **Only show latest** check box to see which bulletins will be deployed if you click **Deploy latest bulletins**.
Deploy selected bulletins	Initiates the deployment of the selected bulletins. For more information on the bulletin deployment process, see Configuring an ESXi Deployment.

Viewing Bulletin Details

The bottom pane displays detailed information about the bulletin that is selected in the top pane of the **Bulletins** tab. Detailed information will not be displayed if multiple bulletins are selected.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Bulletin ID	Provides a link to the VMware Knowledge Base article that describes the threat addressed by this bulletin.
Replaced by	If shown, indicates that the bulletin has been replaced by a newer bulletin. A link is provided to the VMware Knowledge Base article that describes the newer bulletin.
Vendor Severity	Indicates the severity level of the vulnerability that is corrected by this bulletin. The severity level can be one of the following: • **Critical:** Vulnerabilities that can be exploited by an unauthenticated remote attacker or vulnerabilities that break guest/host operating system isolation. The exploitation results in the compromise of confidentiality, integrity, availability user data, or processing resources without user interaction. Exploitation could be leveraged to propagate an Internet worm or execute arbitrary code between virtual machines and the host. • **Important:** Vulnerabilities whose exploitation results in the compromise of confidentiality, integrity, or availability of user data and processing resources. Such flaws could allow local users to gain privileges, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service. • **Moderate:** Flaws where the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios could still lead to some compromise of the confidentiality, integrity, or availability of user data and processing resources. These are the types of vulnerabilities that could have had a critical impact or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **Low:** All other issues that have a security impact. Vulnerabilities where exploitation is believed to be extremely difficult, or where successful exploitation would have minimal impact.
Bundles Missing	The number of bundles that will be installed if the selected bulletin is installed.
Bundle Name	The base name of the bundle within the bulletin. The base name does not include the version information.
Version in Bulletin	The version of the bundle that is specified in the bulletin.
Version Installed	The version of the bundle that is currently installed. The installed version may be older, newer, or the same as the version specified in the bundle. If blank, then no version of this bundle is currently installed.
Bundle State	The state indicate how the installed version compares with the required version. The bundle state can be one of the following: • **Installed (exact):** The installed version of the bundle is the same as the version specified in the bulletin. • **Installed (installed is newer):** The installed version of the bundle is newer that the version specified in the bulletin. • **Missing (not installed):** No version of the bundle is currently installed. • **Missing (installed is older):** The installed version of the bundle is older that the version specified in the bulletin.
Impact	Indicates the impact that applying the bulletin will have on the hypervisor.
File Size	The size of the installation bundle file.

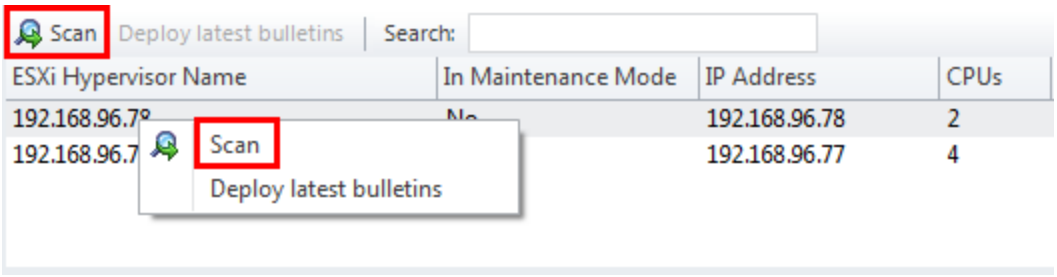
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How to Initiate a Scan of an ESXi Hypervisor

There are multiple ways to initiate a scan of your ESXi hypervisors.

Scanning One or More Managed ESXi Hypervisors

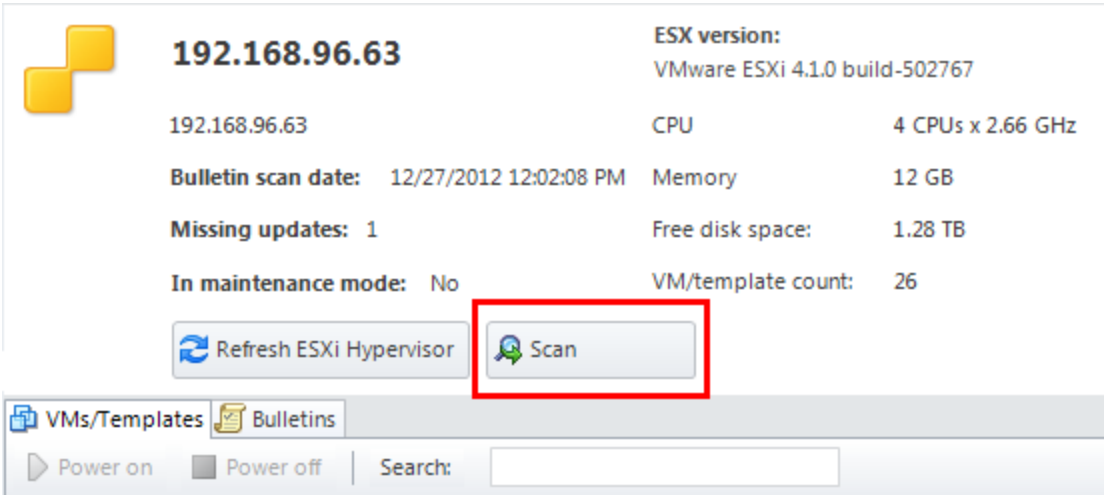
1. In the **vCenter Servers** list, select the desired vCenter Server.
2. In the top pane, select the desired ESXi hypervisor(s).
3. Initiate the scan using either the **Scan** button along the top of the table or the right-click menu.



Scanning a Managed or Unmanaged ESXi Hypervisor

1 In the **vCenter Servers** list or the ESXi Hypervisors list, select the desired ESXi hypervisor.

2. In the header area, click **Scan**.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Scan Results

The Operations Monitor is used to monitor the status of the hypervisor scan. The bulletins discovered during the scan can be found on the **Bulletins** tab of your managed or unmanaged hypervisor. Remember to select **View > Refresh** to view the most current information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Initiating a Bulletin Deployment to an ESXi Hypervisor

1. In the **vCenter Servers** list or the **ESXi Hypervisors** list, select the desired ESXi hypervisor.
2. On the **Bulletins** tab, select the desired bulletin(s).

   You can deploy an individual bulletin, multiple bulletins, or all missing bulletins to a single ESXi hypervisor.
3. Click either **Deploy latest bulletins** or **Deploy selected bulletins**.
   - **Deploy latest bulletins:** Initiates the deployment of all bulletins that are missing on the ESXi hypervisor. This will include only those bulletins that have not been replaced by newer bulletins.

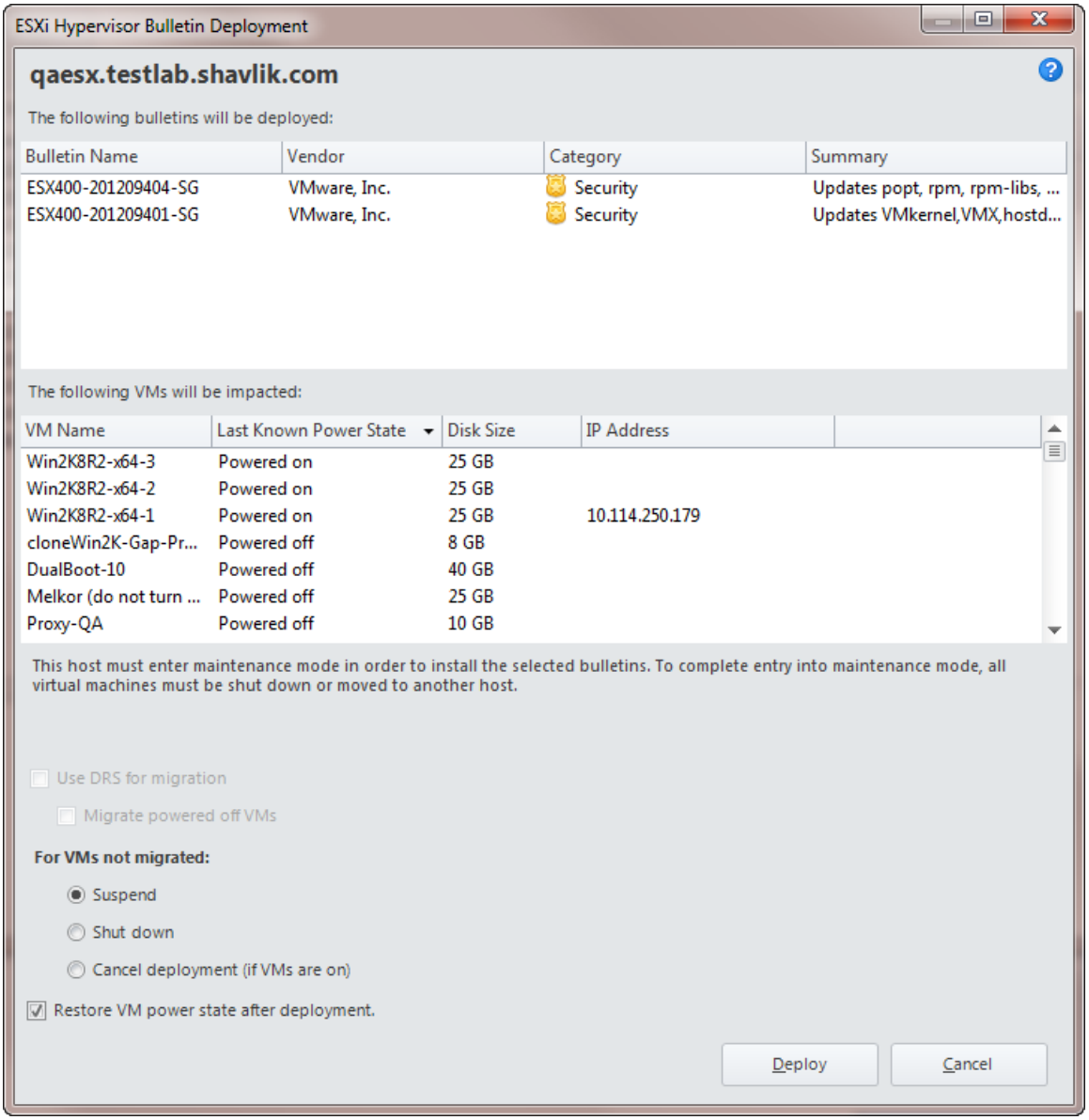
     TIP: Use the **Only show latest** check box to see which bulletins will be deployed if you click **Deploy latest bulletins**.
   - **Deploy selected bulletins:** Initiates the deployment of the selected bulletins.

This will launch the **ESXi Hypervisor Deployment** dialog, which you will use to configure the deployment.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Configuring an ESXi Bulletin Deployment

When an ESXi hypervisor deployment is initiated the **Bulletin Deployment** dialog is displayed. This dialog enables you to specify how the ESXi hypervisor and the virtual machines contained on the hypervisor will be affected during the bulletin deployment.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

The following bulletins will be deployed	Specifies which bulletins are about to be deployed.
The following VMs will be impacted	Shows the virtual machines that are hosted by the ESXi hypervisor. Each of the virtual machines may be affected because most deployments require that hosted virtual machines be powered off or moved to another host prior to the bulletin deployment to the hypervisor. The **Last Known Power State** column shows the power state each virtual machine was in at the time of the most recent scan.
	The following options apply only if one or more of the bulletins being deployed will have an impact on the virtual machines and hypervisor.
Use DRS for migration	If the ESXi hypervisor must enter maintenance mode to deploy the bulletin(s), and if the vCenter Server that is managing this hypervisor is configured to use VMware Distributed Resource Scheduler (DRS), you have the option to allow DRS to migrate the hypervisor's virtual machines to different hypervisors before beginning the deployment process. If you choose not to use DRS, the hypervisor's virtual machines power state will be modified according to the **For VMs not migrated** setting. When the hypervisor update is complete, virtual machines that were migrated to other hosts are not automatically migrated back to this host. If load balancing is enabled, however, DRS will likely migrate some virtual machines back to this host soon after the deployment completes.
Migrate powered off VMs	If enabled, virtual machines that are powered off will be included in a Distributed Resource Scheduler (DRS) migration. If left unchecked, powered off virtual machines will not migrate and cannot be powered on until this hypervisor update is complete.
For VMs not migrated	Indicates what power state to place the hypervisor's virtual machines into if Distributed Resource Scheduler (DRS) is not available or if DRS fails to migrate one or more virtual machines. DRS will be used to migrate a virtual machine only if the following conditions are met: • The hypervisor is managed by a vCenter Server • The hypervisor is in a cluster • DRS is enabled on the cluster • The hypervisor automation level is Fully Automated, or the hypervisor uses the default automation level and the default automation level is Fully Automated.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	Even if all these conditions are met, migration may fail because other hosts are not available or vSphere HA admission control policies prohibit the migration. The action selected here applies to all powered-on virtual machines that are not configured for migration and virtual machines that fail to migrate for other reasons. • **Suspend**: The hypervisor's virtual machines will be placed into a suspended state before the hypervisor enters maintenance mode. • **Shut down**: The hypervisor's virtual machines will be shut down before the hypervisor enters maintenance mode. • **Cancel deployment (if VMs are on)**: The deployment will be canceled if any of the hypervisor's virtual machines are powered on.
Restore VM power state after deployment	If enabled, each virtual machine on the hypervisor that was suspended or shut down during the deployment will be restored to its current power state following the deployment.
Deploy	When you are ready to deploy your bulletins using the selected deployment options, click this button. The Operations Monitor is used to monitor the status of the ESXi Hypervisor bulletin deployment. The following occurs during a bulletin deployment to an ESXi hypervisor: 1. The bulletins are downloaded from the vendor's website and staged to the hypervisor. 2. If any selected bulletin requires that the hypervisor enter maintenance mode or be restarted, the hypervisor's virtual machines that are not configured for DRS migration are suspended or powered off. 3. The hypervisor enters maintenance mode, triggering DRS to begin migrating virtual machines that are properly configured. 4. Virtual machines that fail to migrate are suspended or shut down, or the deployment is canceled, based on the selection made in **For VMs not migrated**. 5. When the migration and/or shut down of virtual machines is complete, the bulletins are installed. 6. The hypervisor is restarted if a reboot is required. 7. The virtual machines that were suspended or powered off during the deployment will be powered on if **Restore VM power after deployment** is enabled. 8. The deployment is recorded in the Event History log. 9. The results are reflected on the **Bulletins** tab after selecting **View > Refresh**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing ESXi Hypervisor Deployment Results

There are three places to view the results of a bulletin deployment to an ESXi hypervisor.

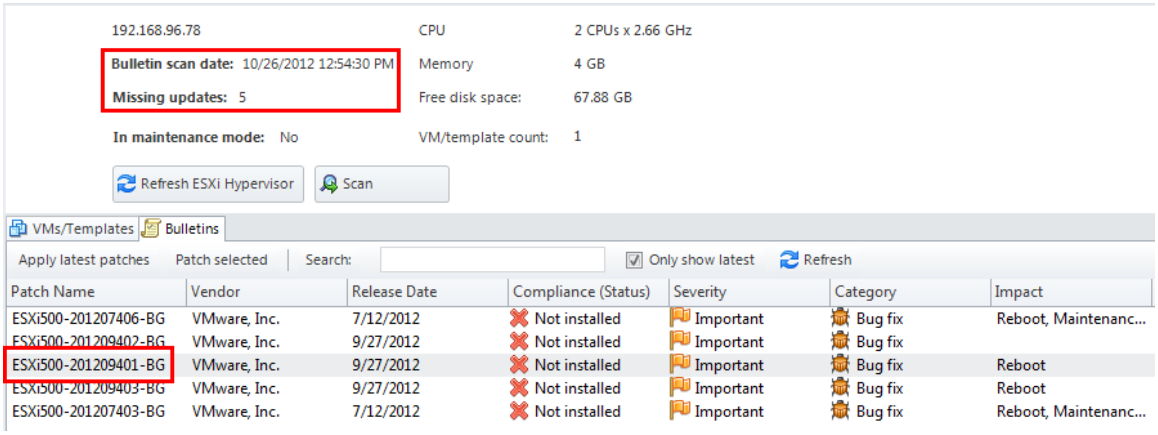
- From the Operations Monitor
- From the Event History log
- From the ESXi hypervisor **Bulletins** tab

Using the Bulletins Tab to View Bulletin Deployment Results

While viewing a vCenter Server or an ESXi hypervisor, select **View > Refresh** to see the most current information. The information in the header area and on the **Bulletins** tab will be updated to reflect the successful bulletin deployment.

Example: Before deployment

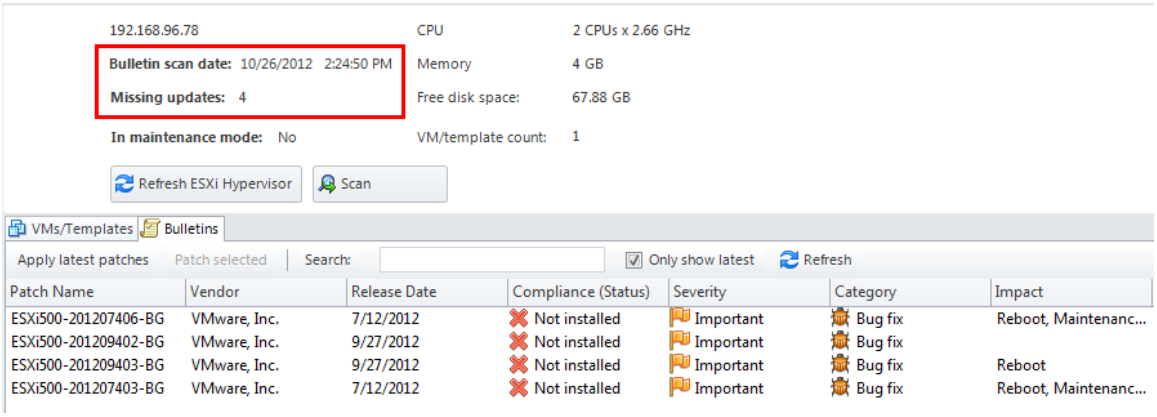
The ESXi hypervisor shown here is missing five bulletins, including bulletin **ESXi500-201209401-BG**. To simplify things the **Only show latest** check box is enabled, which means that the only bulletins being displayed are those that have not been replaced by newer bulletins and whose vulnerabilities have not been addressed.



Example: After deployment

The ESXi hypervisor is now missing only four bulletins, and bulletin **ESXi500-201209401-BG** is no longer included in the list. Note that the **Bulletin scan date** information has also changed; this is because a new bulletin scan is one of the last steps that are performed during the bulletin deployment process.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Supplying Scan Credentials for Target Machines

Browse credentials are slightly different from the scan credentials described in this section. Browse credentials are used by servers, domains, and organizational units to enumerate machines but do not actually authenticate to the individual machines. See Adding Virtual Machines Hosted by a Server and Machine Group Dialog: Bottom Section for information on specifying browse credentials.

In addition, Ivanti Patch for Windows® Servers also uses a scheduler credential for all tasks scheduled to be run on the console. You set this credential from the **Scheduled Console Tasks** dialog.

This section provides information on how to define new scan credentials and how to assign the credentials to target machines. Credentials consist of a user name and password pair used to authenticate the program to specified target machines. One credential can be associated with any number of operations or entities. The credentials are stored with strong encryption techniques and are not available to anyone except the user who provided them.

The scan credentials you supply will be used to access remote machines, perform any scans, and push any necessary files. The supplied credentials will NOT be used to:

- Authenticate to the local (console) machine

  Rather, the program uses the credentials of the currently logged on user to authenticate to resources on the local machine. Therefore, in order to perform tasks on the local machine, make sure you log on using an account that has administrator and local machine access rights.

- Perform a patch deployment

  The machine credentials that you supply are used to provide access to the remote machine and to push the necessary patch deployment files. The actual deployment, however, will be run under the remote machine's Local System account.

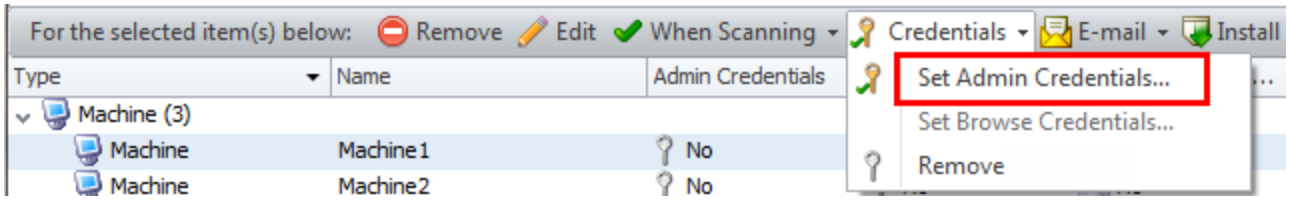
You use a machine group to initially assign scan credentials to target machines. You can assign credentials to individual machines, to all machines in a machine group, or both. After a machine has been scanned and is contained in Ivanti Patch for Windows® Servers's database of managed machines, you can use the **Machine Properties** dialog to assign different credentials if desired.

IMPORTANT! If there are two or more administrators using Ivanti Patch for Windows® Servers, each administrator should provide their own machine credentials. For details see Potential Issues When Using Multiple Admins.

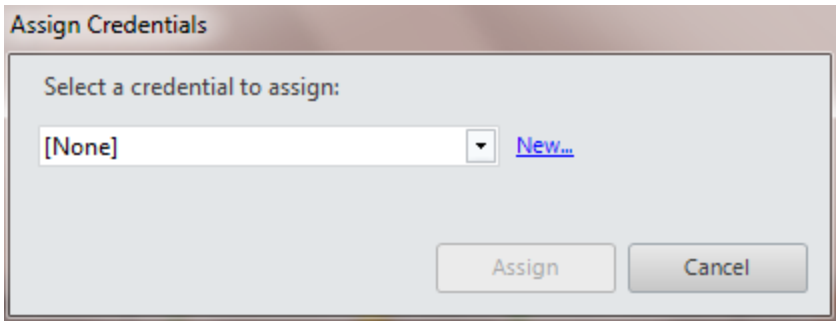
ASSIGNING CREDENTIALS TO INDIVIDUAL MACHINES IN A MACHINE GROUP

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

To assign credentials to one or more machines in a machine group, in the bottom pane select the machines and then select **Credentials** > **Set Admin Credentials**.



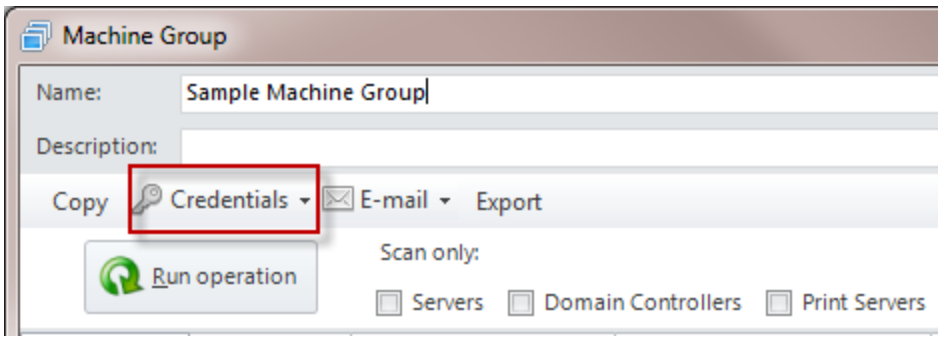
On the **Assign Credentials** dialog, select from the list of available credentials or click **New** to define new credentials.



When credentials are applied to the selected machines, the name of the assigned credential is displayed next to the icon.

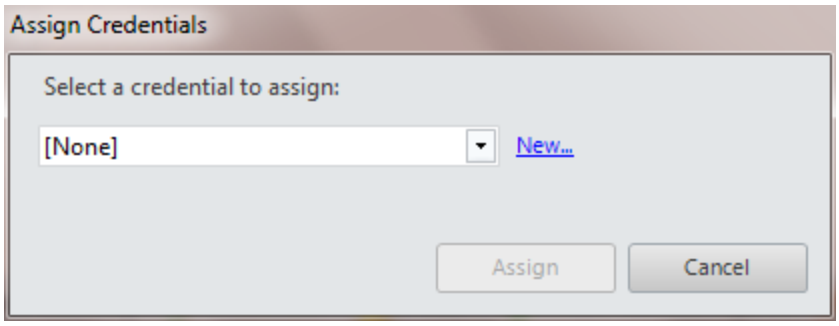
ASSIGNING CREDENTIALS TO ALL MACHINES IN A GROUP

To assign credentials to all machines in a machine group, in the top pane select **Credentials** > **Set Credentials**.



On the **Assign Credentials** dialog, select from the list of available credentials or click **New** to define new credentials.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

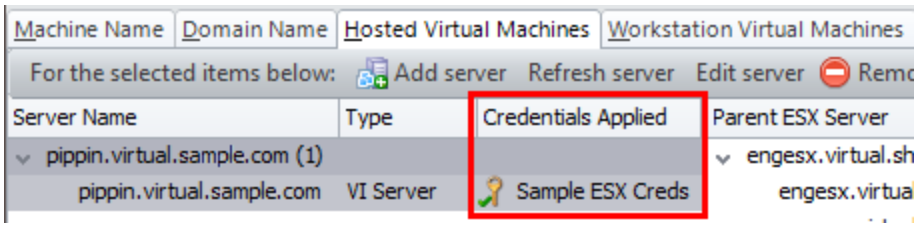


When credentials are assigned, the button name will change to the name of the assigned credential.

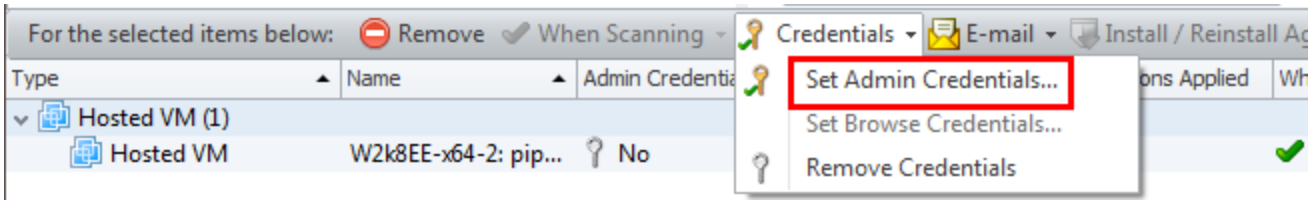
ASSIGNING CREDENTIALS TO VIRTUAL MACHINEStual Machines

There are several different tabs that can be used to add virtual machines to a machine group. The credentials that will be used to scan and/or deploy patches to these machines depends on how the machines are defined to the group and on the current power state of each machine.

- **Hosted Virtual Machines** tab: Used to add virtual machines that are hosted by a server. The credentials used to scan each machine depends on the current power state of the machine.
  - A hosted virtual machine that is *offline* at the time of a scan will be accessed using the server's browse credentials. Any individual credentials supplied for the machine are ignored.



  - A hosted virtual machine that is *online* at the time of a scan will be accessed using scan credentials for that machine. See *Assigning Credentials to Individual Machines in a Machine Group*, above.



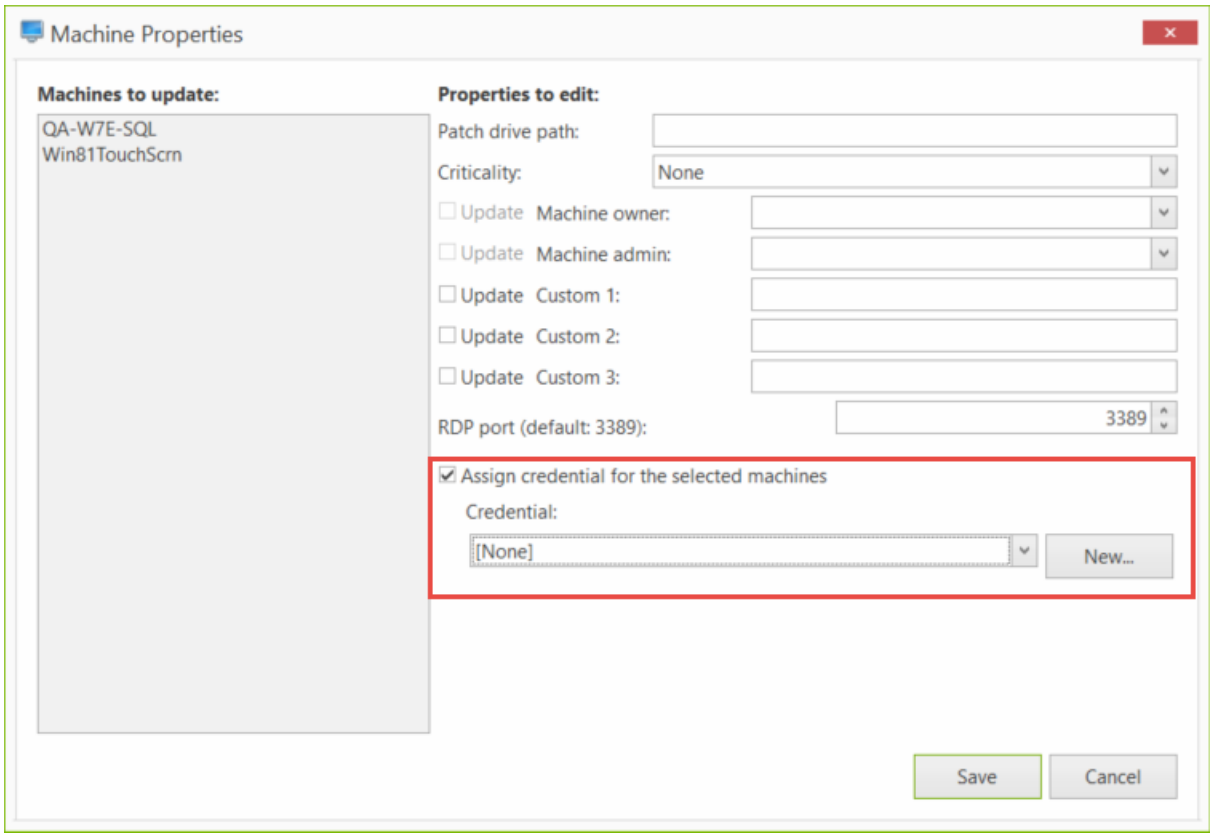
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **Workstation Virtual Machines** tab: Used to add *offline* virtual machines that reside on individual workstations. You should assign individual machine credentials for each virtual machine defined using this tab. If appropriate, credentials can also be assigned at the machine group level. The credentials are used during the mounting process and provide permission for Ivanti Patch for Windows® Servers to access the virtual machine files on the workstation. See *Assigning Credentials to Individual Machines in a Machine Group*, above.
- **Machine Name** tab, **Domain Name** tab, or **IP Address/Range** tab: Used to add virtual machines that reside on individual workstations and that are *online* at the time of a scan. See *Assigning Credentials to Individual Machines in a Machine Group*, above.

ASSIGNING NEW CREDENTIALS TO MACHINES AFTER THEY HAVE BEEN SCANNED

After one or more machines have been scanned and are contained in Ivanti Patch for Windows® Servers's database of managed machines, you can use the **Machine Properties** dialog to assign different credentials or to remove credentials.

There may be several reasons for providing different credentials to machines after a scan has been performed. If you have multiple administrators in your organization and each is responsible for a different domain, they will need to set their own credentials before performing an action. Or, your organization's policy may be to separate scan (assessment) duties from deployment duties, in which case different credentials are probably required.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

See also:

Credential Precedence for Physical Machines and Online VMs

Credential Precedence for Offline Hosted VMs

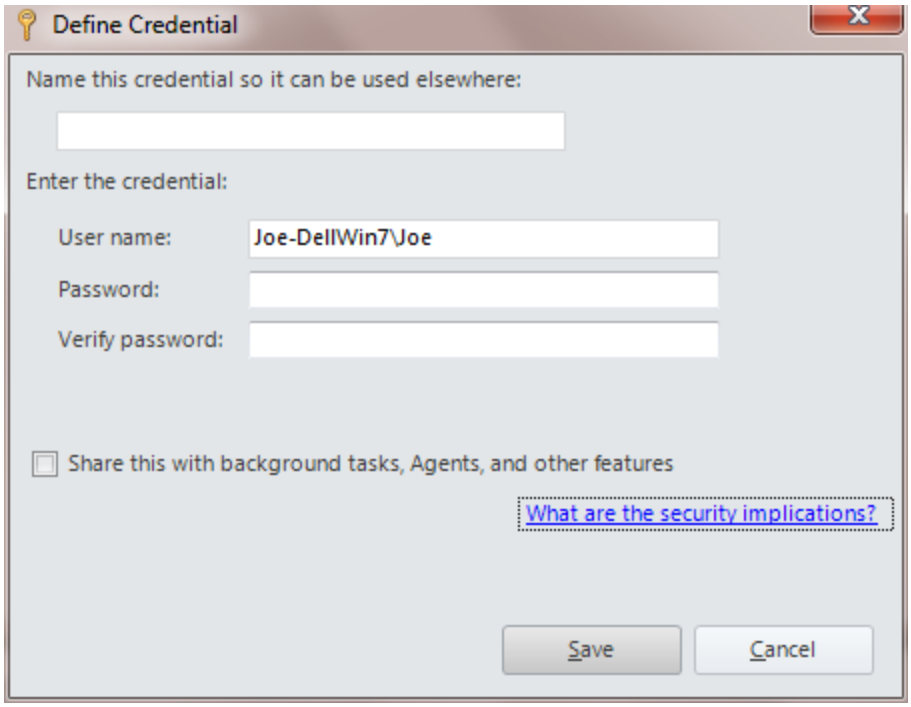
Deploying Patches to Virtual Machines

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Defining Credentials

The **Define Credential** dialog can be accessed anywhere a credential is used within the Ivanti Patch for Windows® Servers interface (for example, from a machine group, from the **Credentials Manager**, etc.). It is used to specify a new user name and password pair that collectively define one credential. The credential is stored with strong encryption techniques. Only the administrator that creates the credential will be able to decrypt the credential and access it from within the program. If you elect to share the credential, however, it will be made available to other administrators as well as to Ivanti Patch for Windows® Servers service components.

Credentials may be automatically defined for you during a product upgrade or when importing a machine group. Any credentials that are found during these processes are preserved and will be assigned friendly names according to their usage. The term *Discovery filter* is the friendly name assigned by the program to a machine group credential that it identifies during an upgrade or import process. Feel free to change the name to something that more closely reflects the usage of the credential in your organization.



Name this credential so it can be used elsewhere	Provide a friendly name for this credential that describes exactly where it should be used.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

User name	Type a user name that has access to the machine(s). When specifying the user name: • If you need to specify a domain as part of the credentials be sure to include the domain name as part of the user name. For example, if you enter User@<Domain>, <Domain>\User, or a fully qualified user name, Ivanti Patch for Windows® Servers will use the domain account rights. • If you enter <Target Machine>\User, Ivanti Patch for Windows® Servers will use the target's local account rights. • If you do not include a domain or machine as part of the user name, the name will be qualified to the target machine (<targetmachinename>\User). • Microsoft Windows .alias name formats (for example: '.\username') are supported by Ivanti Patch for Windows® Servers.
Password	Type the password for the user.
Verify password	Retype the password to verify you specified it correctly.
Share this with background tasks, agents, and other features	If enabled, this credential will be available to all Ivanti Patch for Windows® Servers administrators and can be used to specify credentials for service components within the program. The service components within Ivanti Patch for Windows® Servers that require a shared credential include the following: • Proxy service • Email service • Agent Internet proxy • Distribution servers • TrustedHost list access when running remote scripts Why is it necessary to share a credential? Credentials are encrypted, so you must share a credential so that the service components can decrypt and access it when needed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Example: If you select **Tools > Options > Proxy** and attempt to assign **Service credentials**, only shared credentials are available for selection. The service must have a copy of the credential in order to decrypt it.

It is recommended that you create a service account to perform these service functions rather than using a domain administrator account. See Potential Security Implications When Sharing Credentials for more information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Potential Security Implications When Sharing Credentials

When you share a credential, that credential becomes available to all other administrators for use with Ivanti Patch for Windows® Servers service components. For example, if Administrator A creates a shared credential and assigns it to the proxy service, Administrator B is free to assign that same shared credential to other service areas of the program.

Therefore:

- Only share those credentials that are needed by Ivanti Patch for Windows® Servers service components.
- **DO NOT** share credentials that allow access to secure areas of your organization.

When you share a credential, that credential becomes available to all other administrators for use with Ivanti Patch for Windows® Servers service components. For example, if Administrator A creates a shared credential and assigns it to the proxy service, Administrator B is free to assign that same shared credential to other service areas of the program.

Therefore:

- Only share those credentials that are needed by Ivanti Patch for Windows® Servers service components.
- **DO NOT** share credentials that allow access to secure areas of your organization.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

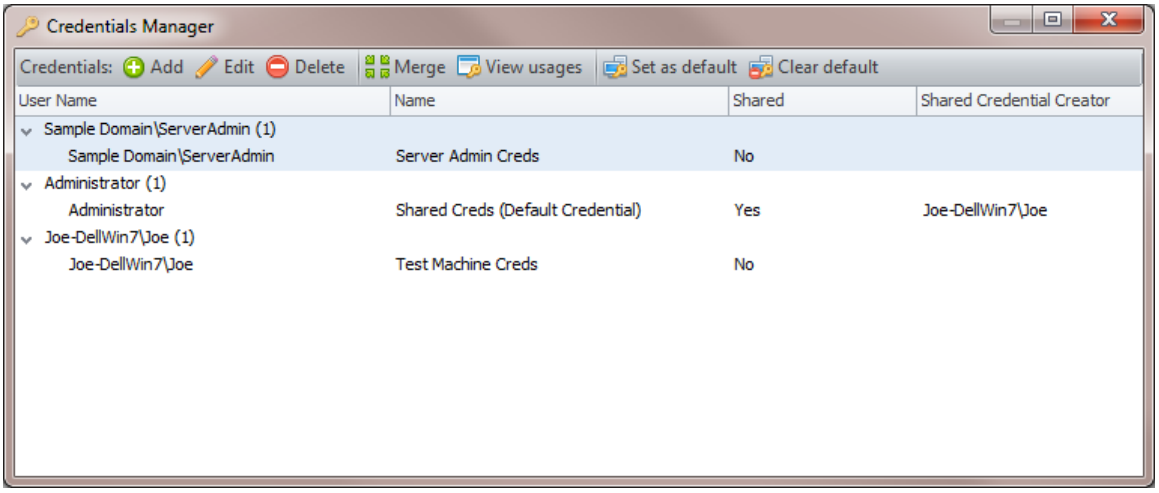
Managing Credentials

IMPORTANT! If there are two or more administrators using Ivanti Patch for Windows® Servers, each administrator should provide their own machine credentials. For details see Potential Issues When Using Multiple Admins.

The Credentials Manager is used to manage all credentials used within the program. It is also used to set the default credential for the program.

Although you can supply new credentials from several different areas of the program, all of the credentials can be edited and deleted from this single location. This greatly simplifies the credentials management process. For example, if a password that is used to authenticate a specific group of machines changes, you simply use the Credentials Manager to update the associated credential. All items assigned to that credential are automatically updated with the new password.

To manage the credentials used by the program, select **Manage > Credentials**.

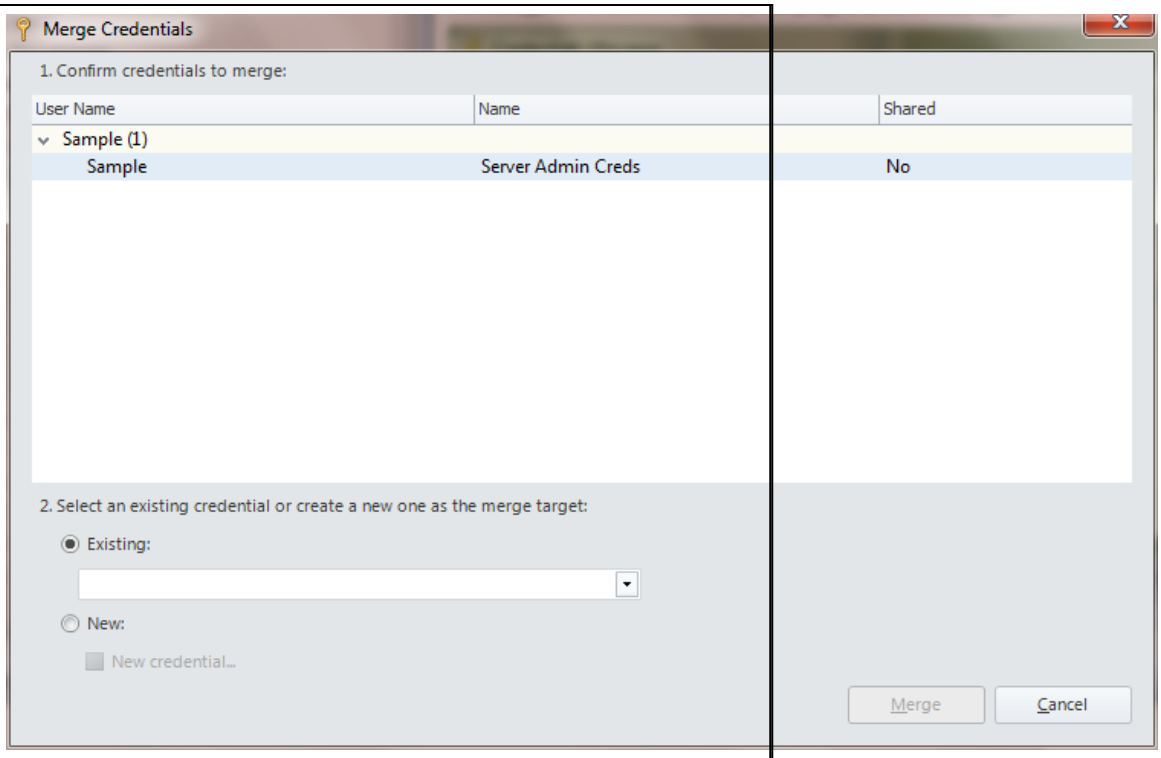


Add	Enables you to add a new credential. See Defining Credentials for details.
Edit	Enables you to modify the selected credential. See Defining Credentials for details.
Delete	Deletes the selected credential. You can delete multiple credentials at the same time. When you delete a credential the following occurs: • The credential itself is deleted • All usages of the credential throughout the program are deleted

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• If it is a shared credential, the shared credential and all its usages are deleted CAUTION! Any items using the deleted credential will no longer be assigned a credential. Before you delete a credential you should browse your machine groups to verify the credential is not being used.
Merge	TIP: This credential cleanup tool will typically be used immediately following an upgrade from an earlier version of Ivanti Patch for Windows® Servers that does not contain the Credentials Manager. Enables you to merge one or more credentials that contain the same user name and password with another credential entry that also contains the same user name and password. Or you can merge several different credentials into one new credential that is effective in all situations. By eliminating duplicate and unneeded credentials you reduce confusion and lessen the chance for human error. 1. On the **Credentials Manager** dialog select the credential(s) you want to merge with another credential. 2. Click**Merge**. The **Merge Credentials** dialog is displayed

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



3. At the bottom of the dialog do one of the following:
   - Select an existing credential: The credential(s) specified in the **Confirm credentials to merge** list will be merged with the credential you select here.
   - Create a new credential: The credential(s) specified in the **Confirm credentials to merge** list will be merged with the new credential you create here.

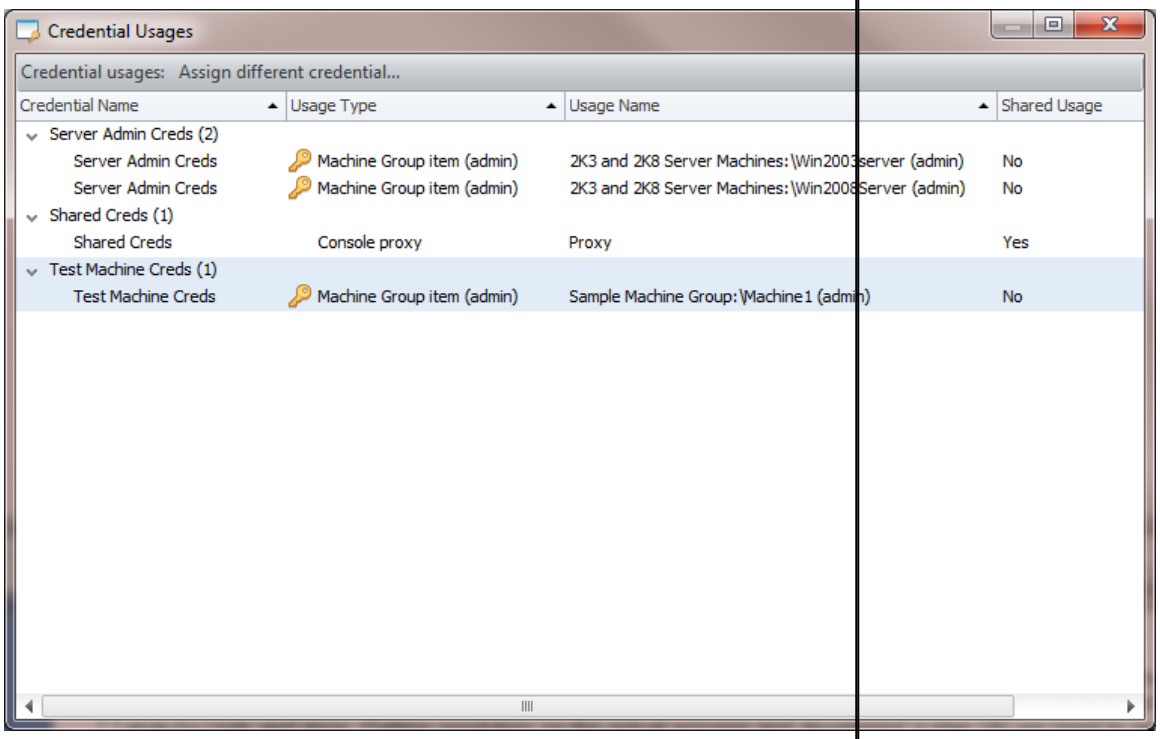
   A shared credential can only be merged with another shared credential. Therefore, if any of the credentials in the **Confirm credentials to merge** list are shared, then (1) only shared credentials will be offered for selection in the **Existing** box, and (2) any new credential you create will automatically be defined as a shared credential.

4. Click **Merge**.
5. Read the message on the confirmation dialog and if you agree with the merger, click **Merge**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

View usages

Enables you to see how and where the selected credentials are being used in the program. Only those credentials that are currently being used in the program will be displayed in the **Credential Usages** dialog. A credential may be listed multiple times if it is used in different areas of the program.



You can right-click on any list item and perform a number of different actions.

- **Assign different credential:** Enables you to assign a different credential to the selected item(s). You can assign a different credential to multiple items at once but only if they all have the same **Shared Usage** value (Yes or No).
- **Expand all:** Expands all lists.
- **Collapse all:** Collapses all lists.
- **Export selected credential usages to CSV:** Export information about the selected items to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Set as default	Assigns the selected credential as the default credential. The program will use the default credential if other credentials are missing or invalid. See Credential Precedence for information on when the default credential is used.
Clear default	Removes the default credential assignment.
User Name	Displays the user name portion of each credential.
Name	Displays the unique name assigned to each credential.
Shared	Displays whether the credentials are shared credentials. The information in this column is directly related to the **Share this with background tasks, Agents, and other features** check box on the **Define Credential** dialog.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Credential Precedence for Physical Machines and Online Virtual Machines

Initiating actions from the home page, from a machine group, or from a favorite

The home page, machine groups and favorites can be used to initiate patch scans, asset scans,power management actions, and to execute scripts. When performing these actions, Ivanti Patch for Windows® Servers will attempt to authenticate to each machine using a variety of credentials and will do so using the following strategy:

1. If one or more of the following are available, try to authenticate using the credential with the highest precedence, where the precedence order is as follows:
   - Machine-level credentials (see the **To Individual Machines in a Machine Group** section in Supplying Credentials for Machines)
   - Group-level credentials (see the **To All Machines in a Machine Group** section in Supplying Credentials for Machines)
   - Default credentials (see Managing Credentials)

   Example: If machine-level credentials are not available but group-level and default credentials are available, the program will use the group-level credentials.
2. If the credential used above does not work, then Integrated Windows Authentication (the credentials of the person currently logged on to the program) will be used.

If neither of these credentials work the scans and the power management tasks will fail.

One suggestion is to make your default credentials the same as the account credentials you typically use to log on to the program. This will eliminate problems that may occur if you forget to assign credentials.

Initiating an agent installation from a machine group

When using a machine group to push install the Ivanti Patch for Windows® Servers Agent service to connected target machines, the credentials used by the program follows the same strategy as above with one major exception -- integrated credentials will not be used. So the agent installation must be successful using machine-level, group-level, default, or explicitly supplied credentials.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Initiating actions from Machine View or Scan View

When initiating a scan, a patch deployment or a power management action from Machine View or Scan View, the program will attempt to authenticate to the target machines using a variety of credentials and will do so using the following strategy:

1. If one or more of the following are available, try to authenticate using the credential with the highest precedence, where the precedence order is as follows:
   - Any manually or automatically assigned managed machine credentials (see the **To Individual Machines in a Machine Group** section in Supplying Credentials for Machines and the **Credential** option on the **Manage Machine Properties** dialog)
   - Default Credentials (used if the machine credentials are missing)
2. If the credential used above does not work, then Integrated Windows Authentication (the credentials of the person currently logged on to the program) will be used.

> Integrated credentials will not work for deployments to offline virtual machines or for rescans.

If neither of these credentials work then the action will fail.

Initiating an agent installation from Machine View or Scan View

When using Machine View or Scan View to push install the Ivanti Patch for Windows® Servers Agent service to connected target machines, the credentials used by the program follows the same strategy as immediately above with one major exception -- integrated credentials will not be used. So the agent installation must be successful using managed machine credentials, default credentials, or explicitly supplied credentials.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Credential Precedence for Offline Hosted Virtual Machines

Initiating actions from the home page, from a machine group, or from a favorite

The home page, machine groups and favorites can be used to initiate patch scans, asset scans,power management actions, and to execute scripts. When performing these actions, Ivanti Patch for Windows® Servers will attempt to authenticate to each offline hosted virtual machine using the browse credentials.

Initiating actions from Machine View or Scan View

When initiating a scan, a patch deployment or a power management action from Machine View or Scan View, the credentials that will be used to authenticate to an offline virtual machine depends on the power state of the machine when it was initially scanned.

If a machine was originally scanned in offline mode

The program will attempt to authenticate using the browse credentials.

If a machine was originally scanned in online mode

The program will attempt to authenticate using a variety of credentials and will do so using the following strategy:

1. Try using any manually or automatically assigned managed machine credentials (see the *Assigning Credentials to Virtual Machines* section in Supplying Credentials for Machines.
2. If the following are available, try to authenticate using the credential with the highest precedence, where the precedence order is as follows:
   - (a) The administrator credential from the machine group. If the administrator credential exists but fails, the default credentials will not be tried.
   - (b) Default Credentials (used if the scan credentials are invalid or missing (for example, if an agent performed the scan rather than the console))
3. If the credentials used above do not work, then Integrated Windows Authentication (the credentials of the person currently logged on to the program) will be used.

> Integrated credentials will not work for deployments to offline virtual machines or for rescans.

If none of these credentials work then the action will fail.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

See also:

Deploying Patches to Virtual Machines

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

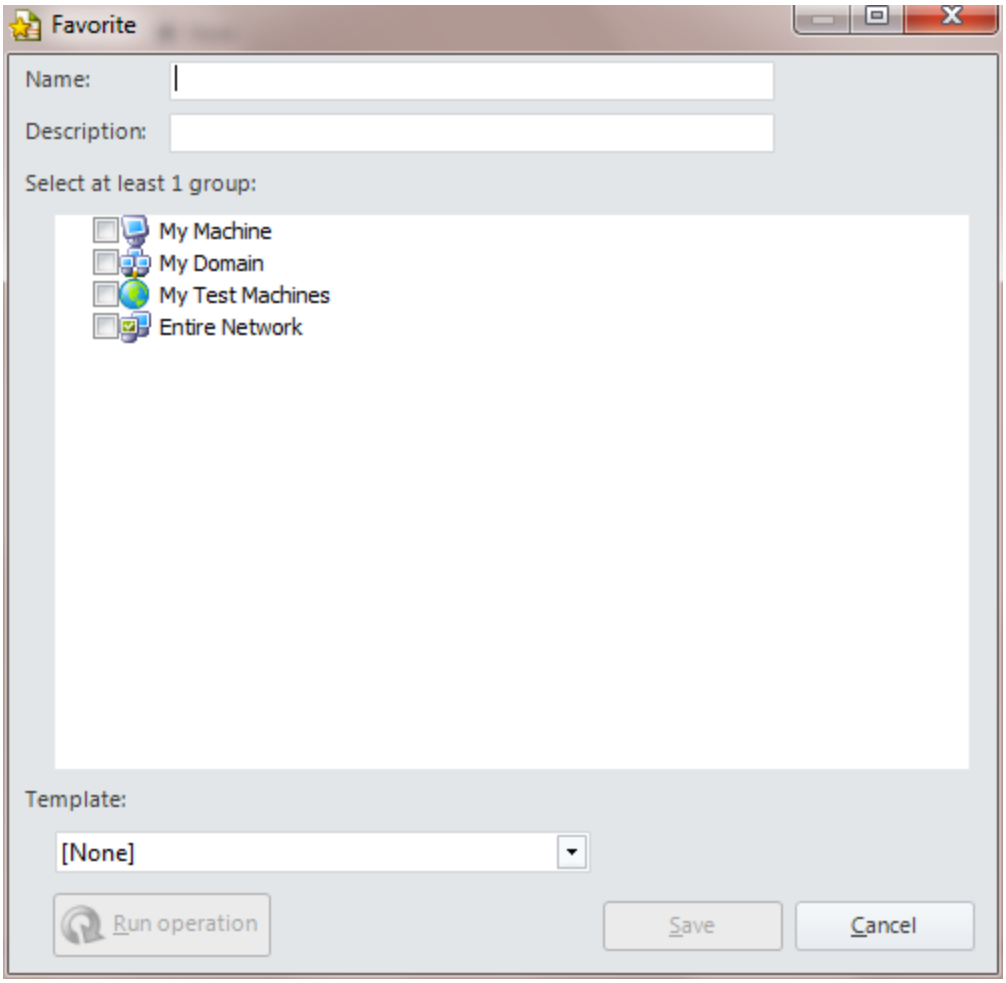
Creating Favorites

A favorite is a marriage between machine groups and a template. It consists of one or more machine groups and one template (a patch scan template, an asset scan template, or a power template). You select one or more machine groups and then select a template that specifies what operation to perform on the machines.

To create a new favorite:

1. From the main menu select **New** > **Favorite**.

   The **Favorite** dialog is displayed.



2. Give the favorite a unique name (e.g. "Domain Controllers").
3. If desired, provide a description.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

For example "This favorite consists of only domain controllers and will be scanned using the Security Patch Scan template".

4. In the **Select at least 1 group** list, select which machine groups you would like to include in this favorite.

   If you elected to exclude certain machines from one or more machine groups, the exclusions will apply to all machine groups you include in this favorite.

5. Select the template you want to use when performing the desired operation on the machines.
6. Click **Save**.

   A new entry will appear in the **Favorites** pane.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing Actions on a Favorite

When you select a favorite from the **Favorites** list the **Favorite** dialog is displayed. It shows the current configuration of the favorite. If you want to immediately perform an operation using this favorite, click **Run operation**. To edit the configuration, simply make the desired changes and then click **Save**.

You can also right-click a favorite and perform the following actions:

Copy	Makes a copy of the selected favorite. The new favorite will contain the same settings as the selected favorite.
Delete	Deletes the selected favorite.
Rename	Enable you to rename the favorite.
Scan	Initiates a scan of the machines specified within the favorite. Initiating a scan from a favorite is an easy way to schedule a scan for a later time or date.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Why You Might Use Multiple Administrators

Ivanti Patch for Windows® Servers will allow two or more administrators to access the program at the same time. There are two basic scenarios in which multiple administrators might be used.

For more information see:

- How Ivanti Patch for Windows® Servers Manages Multiple Administrators
- Potential Issues When Using Multiple Administrators
- Best Practices When Using Multiple Administrators

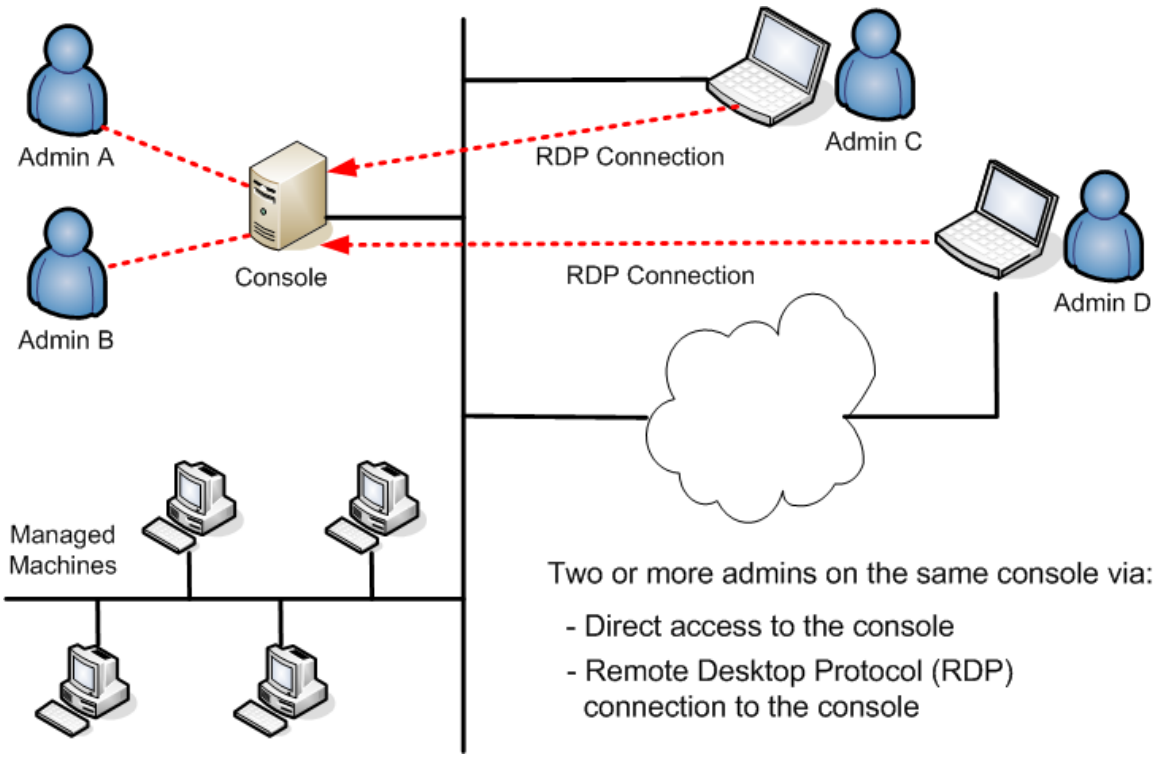
Scenario 1: Two or More Administrators on the Same Console Machine

It is very common for two or more administrators to use a single Ivanti Patch for Windows® Servers console. For example:

- Your company might assign a primary and a backup Ivanti Patch for Windows® Servers administrator
- Your company might assign a different administrator to manage each unique domain within the organization
- Your company might assign a different administrator to manage each physically distinct office location

The following figure illustrates how multiple administrators might access a Ivanti Patch for Windows® Servers console.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

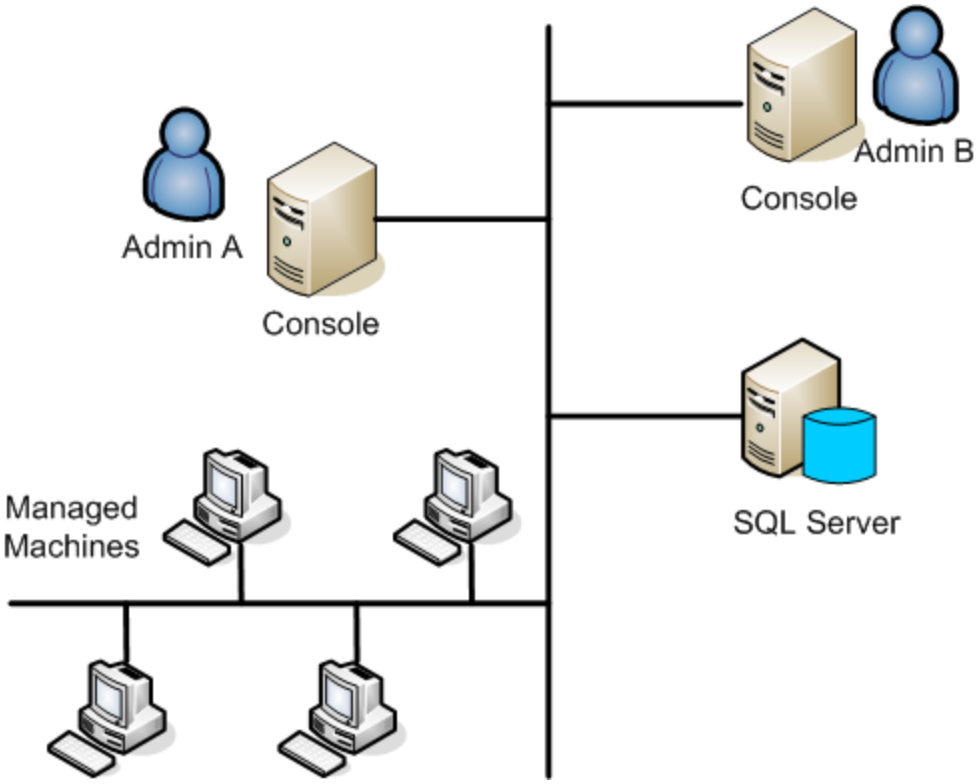


Scenario 2: Two or More Consoles Sharing One Database

To understand why you might choose to use more than one console, see Why Use Multiple Consoles?

The following figure illustrates a typical two console scenario with a different administrator assigned to each console.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

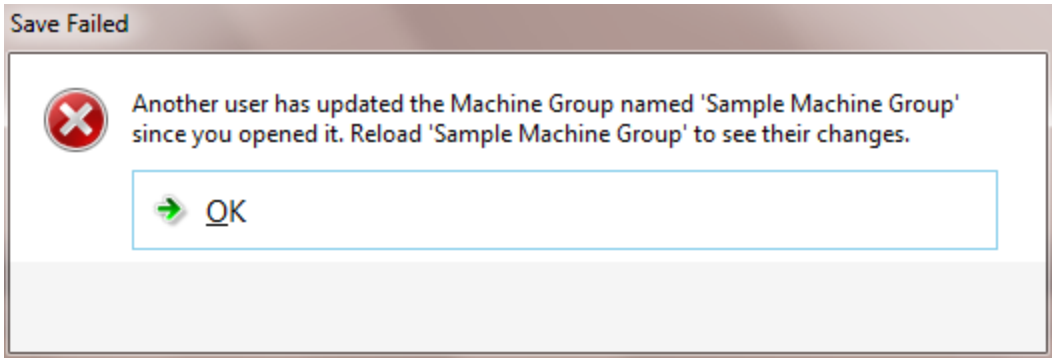


Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Ivanti Patch for Windows® Servers Manages Multiple Administrators

Ivanti Patch for Windows® Servers contains a number of built-in checks to guard against simultaneous and conflicting commands from different administrators. For example:

- The program will not allow duplicate group names or template names
- The program will not allow simultaneous updates to any groups, templates, distribution servers, or agent policies by different administrators. If this situation should occur the second administrator will receive a warning message.



- Only one console will be authorized to use the Database Maintenance tool. If an administrator at another console wants to perform maintenance on the database, that administrator must take ownership of that task before the program will allow the administrator to continue.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Potential Issues When Using Multiple Administrators

Usage Issues

You must take a few common sense precautions when using multiple administrators. Even though Ivanti Patch for Windows® Servers contains a number of built-in safety checks, it cannot guard against all possibilities. The program may act in unpredictable ways if the following occur:

- If two administrators try to scan the same machine group or ESXi Hypervisor at the same time.

  The machines will be scanned twice, causing potential performance issues. In addition, there may be administrative rights errors due to the multiple connections.

- If two or more administrators try to deploy patches or bulletins to the same machine at the same time.

The most likely result is that one deployment task will succeed and the other will fail. But because the deployment that succeeds will likely perform a restart of the target machines, the machines may be in an unknown state when the other deployment fails.

Credential Issue

When you create credentials and assign them to machines, those credentials belong to your administrator account. If a different administrator (Administrator B) logs on and uses Ivanti Patch for Windows® Servers, they will not have access to the machine credentials you provided. The second administrator must provide their own machine credentials.

One of the ways this can be confusing is if Administrator B fails to provide their own machine credentials and tries to schedule a patch deployment from a scan that was performed by Administrator A. The deployment can be successfully scheduled if default credentials are available, but the actual patch deployment will likely fail because the patch deployment requires machine credentials -- credentials that were provided by Administrator A but that are not available to Administrator B.

Recommendations:

- Each administrator should create their own credentials and assign them to machines
- Each administrator should define default credentials that are the same as their logon credentials. This will eliminate some of the problems that may occur if the administrator forgets to assign machine credentials.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Virtual Inventory Consideration

Unlike machine groups (which can be viewed by all administrators), vCenter Servers and ESXi Hypervisors can only be viewed by the administrator that added them to Ivanti Patch for Windows® Servers. If two different administrators want to manage the same vCenter Server or ESXi Hypervisors, both administrators must add the item to the **Virtual Inventory list**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Best Practices When Using Multiple Administrators

Recommendations

- You should upgrade your hardware platform by increasing the number of processors and the amount of installed memory on the console machine. This will increase performance in those instances when two or more administrators are logged on at the same time and performing tasks.
    - Minimum suggested hardware requirements for two administrators: 2 processor cores and 4 GB RAM
    - For each additional administrator, add 1 processor core and 1 GB RAM
    - For a high performance system, use 16 processor cores and 32 GB RAM
- When two administrators log on to the same console they must use different accounts. The same account can be used only when logging on to different consoles.
- If you edit a group that is typically used by another administrator you should notify that person about the change.
- Each administrator should create their own credentials and assign them to machines.
- Each administrator should define default credentials that are the same as their logon credentials. This will eliminate problems that may occur if the administrator forgets to assign machine credentials.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Role-Based Administration Works

This feature is not available to (unlicensed) users.

You can assign different roles to different users of Ivanti Patch for Windows® Servers . This enables you to make the program available to a wide variety of people within your organization while maintaining control over its use. The role assigned to a user determines what that particular user can do.

Here's how it works. When Ivanti Patch for Windows® Servers is launched it checks if role-based administration is enabled. If so, the program then looks to see if the current user has been assigned a role. If the user has been assigned a role, the program grants that user access to only those features allowed by their role. For example, you may have a number of users who are allowed to create reports, but only one or two users who have permission to deploy patches.

Features that are not available due to role limitations will be either grayed out or removed from the interface. If a user has not been assigned a role they will not be able to start the program. It is not possible for a user to switch roles while within the program.

Role-based administration is initially disabled. Until you enable this feature, all users will have full access to the program. You enable and configure role-based administration via the **Manage > User Roles Assignment** menu. See Assigning User Roles and Enabling and Disabling Role-based Administration for detailed information.

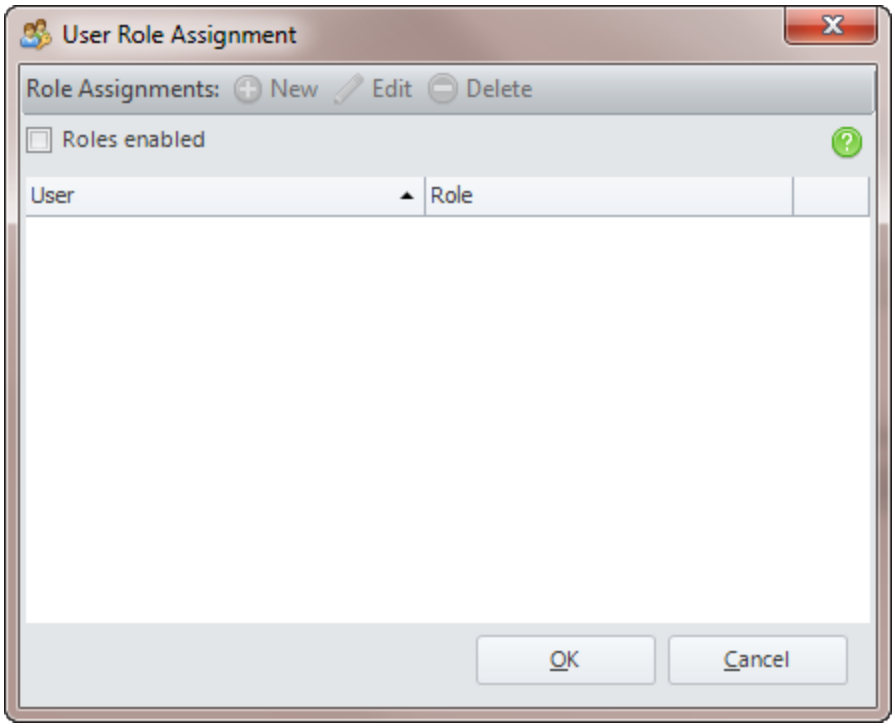
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Assigning User Roles

You can assign roles to as many users as needed. At least one user must be assigned the administrator role.

1. Select **Manage > User Role Assignment**.

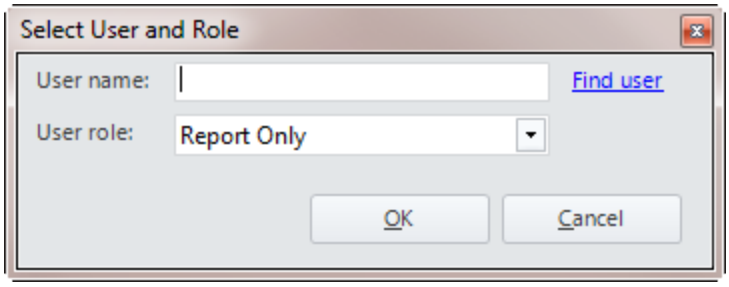
   The **User Role Assignment** dialog is displayed.



   If the buttons on the dialog are unavailable it means you do not have permission to modify the user role assignments. Only a user assigned the **Administrator** role can modify the roles.

2. Click **New**.

   The **Select User and Role** dialog is displayed.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

3. Type a user name and then select the role you want to assign to that user.
   - When specifying the user name you must use the following format: *domain\user*.
   - If you are unsure of the correct domain and user name, you can view a list of all available domains and users by clicking **Find User**. The resulting dialog enables you to conduct either a quick search of just the *Users* organizational unit or a more comprehensive search of the entire active directory.
   - Role definitions:
     - **Administrator:** Full access to all features of the program. Only an administrator user can modify the roles assigned to other users.

     CAUTION! If you assign the **Administrator** role to only one user, make sure you know how to log on to the console machine using that user. Otherwise it is possible to lock yourself out from certain features, with the only solution being to reinstall the program.

     - **Full User:** Access to all features except for the ability to administer roles.
     - **Scan and Report Only:** Can perform patch scans and can generate reports.
     - **Deploy and Report Only:** Can perform patch deployments and can generate reports.
     - **Report Only:** Can generate reports
4. Click **OK**.

All configured users must have access to the database. If users without administrative rights on the console machine receive an error when starting Ivanti Patch for Windows® Servers, it probably means they don't have the necessary SQL Server permissions. See SQL Server Preinstallation Notes for more information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Enabling and Disabling Role-Based Administration

Enabling Role-Based Administration

Simply defining one or more users and assigning them roles does not automatically enable the role-based administration feature. The program allows you to predefine several users without actually enabling the feature. You will not be able to enable role-based administration, however, without having at least one user assigned to the *Administrator* role.

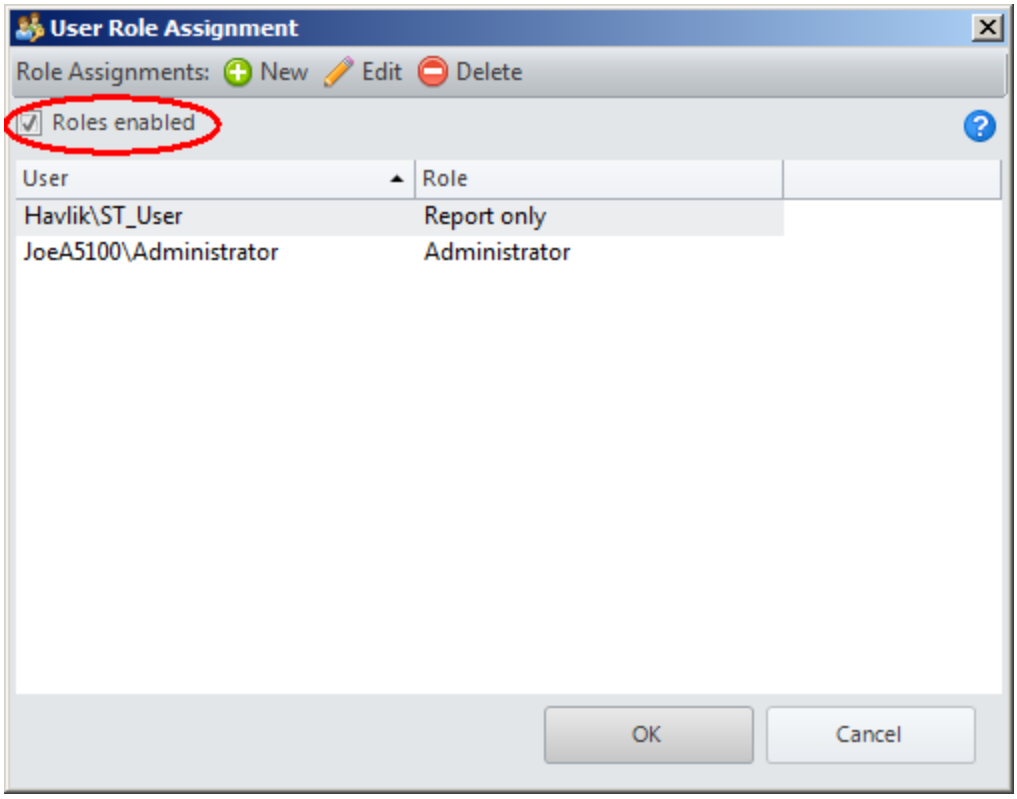
To enable role-based administration:

1. Select **Manage > User Role Assignment**.

   The **User Role Assignment** dialog is displayed.

2. Enable the **Roles Enabled** check box.

   You must have defined at least one user with the *Administrator* role in order to enable role-based administration. See Assigning User Roles for detailed information.



3. Click **OK**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Role-based administration takes effect the next time the program is launched.

Disabling Role-Based Administration

To disable role-based administration:

1. Clear the **Roles Enabled** check box.
2. Click **OK**.

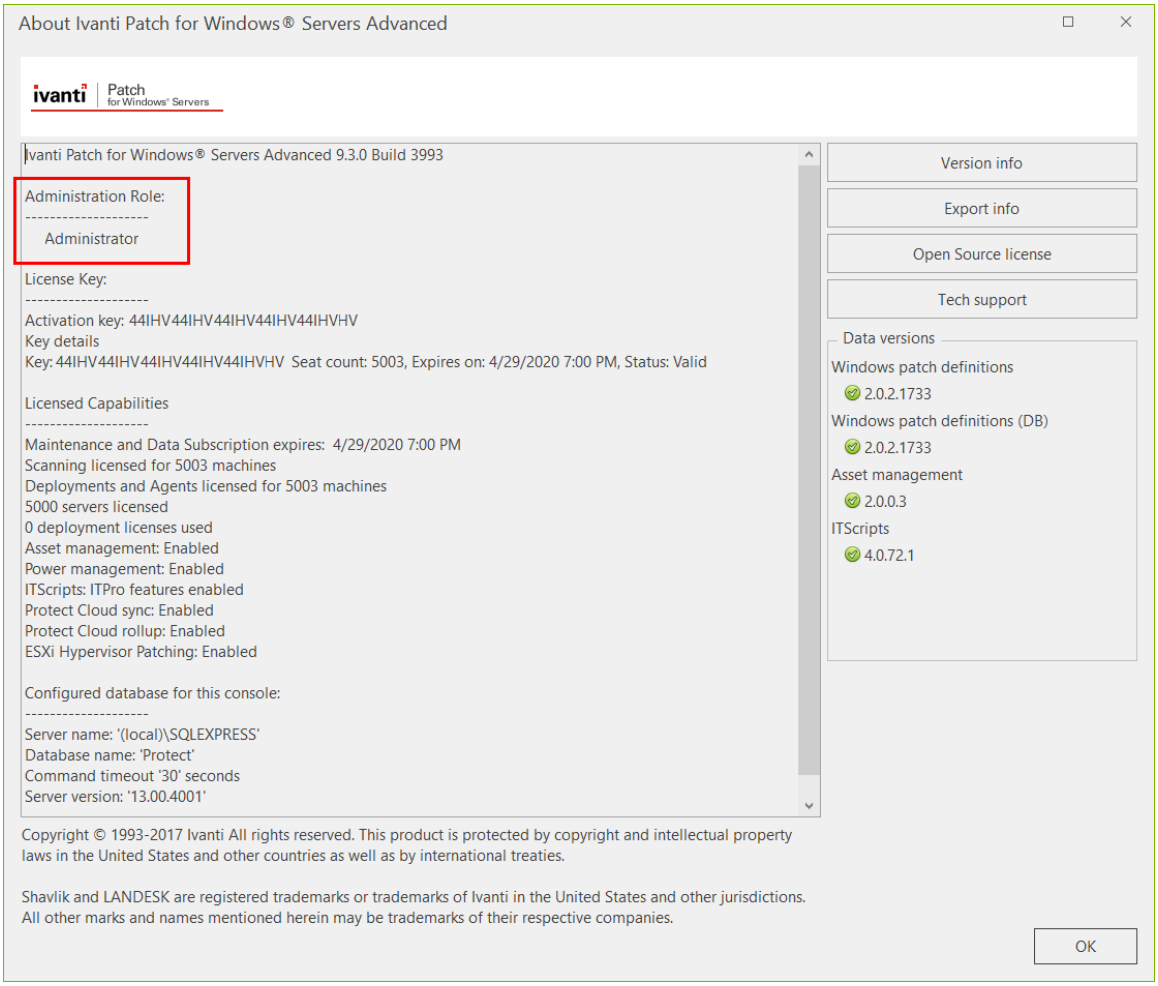
After disabling role-based administration, the next time that Ivanti Patch for Windows® Servers is launched all users will have full access to the program. Any users that are defined in the **User Role Assignment** dialog will remain but their role assignments will be ignored.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Determining the Currently-Assigned Role

Information about the currently-assigned role is available in the **About Ivanti Patch for Windows® Servers** dialog.

1. Select **Help > About Ivanti Patch for Windows® Servers**.
2. In the upper portion of the dialog you will be able to view the current role assignment.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Show Me How to Get Started!

Most tasks in Ivanti Patch for Windows® Servers are simple to perform, you just need to know how to get started!

The following table lists a number of the most commonly performed tasks in Ivanti Patch for Windows® Servers. For each task you can click the **Read a Help Topic** link to view the associated Help topics, or you can click the **View a Video Tutorial** link to view the associated "How-to" video.

Task Category	Read a Help Topic	View a Video Tutorial
Patch Management	Scan for and Deploy Patches	Ivanti Help Channel on YouTube
	Track Deployment Status	Ivanti Help Channel on YouTube
	Automate Scheduled Patching	Ivanti Help Channel on YouTube
	Create a Custom Patch XML File	Ivanti Help Channel on YouTube
Asset Inventory	Use the Asset Inventory Feature	Ivanti Help Channel on YouTube
Power Management	Use the Power Management Feature	Ivanti Help Channel on YouTube
Agents	Create an Agent Policy	Ivanti Help Channel on YouTube
	Install an Agent Policy	Ivanti Help Channel on YouTube
	Implementing Cloud-based Synchronization	Ivanti Help Channel on YouTube
Virtual Machines	Deploying ESXi Hypervisor Bulletins	Ivanti Help Channel on YouTube
	Manage Your Virtual Machines	Ivanti Help Channel on YouTube
ITScripts	Use the ITScripts Feature	Ivanti Help Channel on YouTube
Distribution Servers	Use a Distribution Servers	Ivanti Help Channel on YouTube
General Operation	Generate Reports	
	Manage Credentials	
	Initiate a Remote Desktop Connection	

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Most tasks in Ivanti Patch for Windows® Servers are simple to perform, you just need to know how to get started!

The following table lists a number of the most commonly performed tasks in Ivanti Patch for Windows® Servers. For each task you can click the **How Do I . . . ?** link to view the associated Help topics.

Task Category	How Do I . . . ?
Patch Management	Get Started Scanning and Patching
	Automate Scheduled Patching
	Track Deployment Status
	Download Approved Patches
Virtual Machines	Manage Virtual Machines: Roadmap of Tasks
General Operation	Set Up and Monitor Agents
	Collect Data for Tech Support
	Use a Distribution Server
	Generate Reports
	Manage Credentials

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Do I . . .?: Get Started Scanning and Patching



Show Me!

To view a video tutorial on this topic, click the video icon on the left.

Scanning for and deploying missing patches is easy! You simply do the following:

1

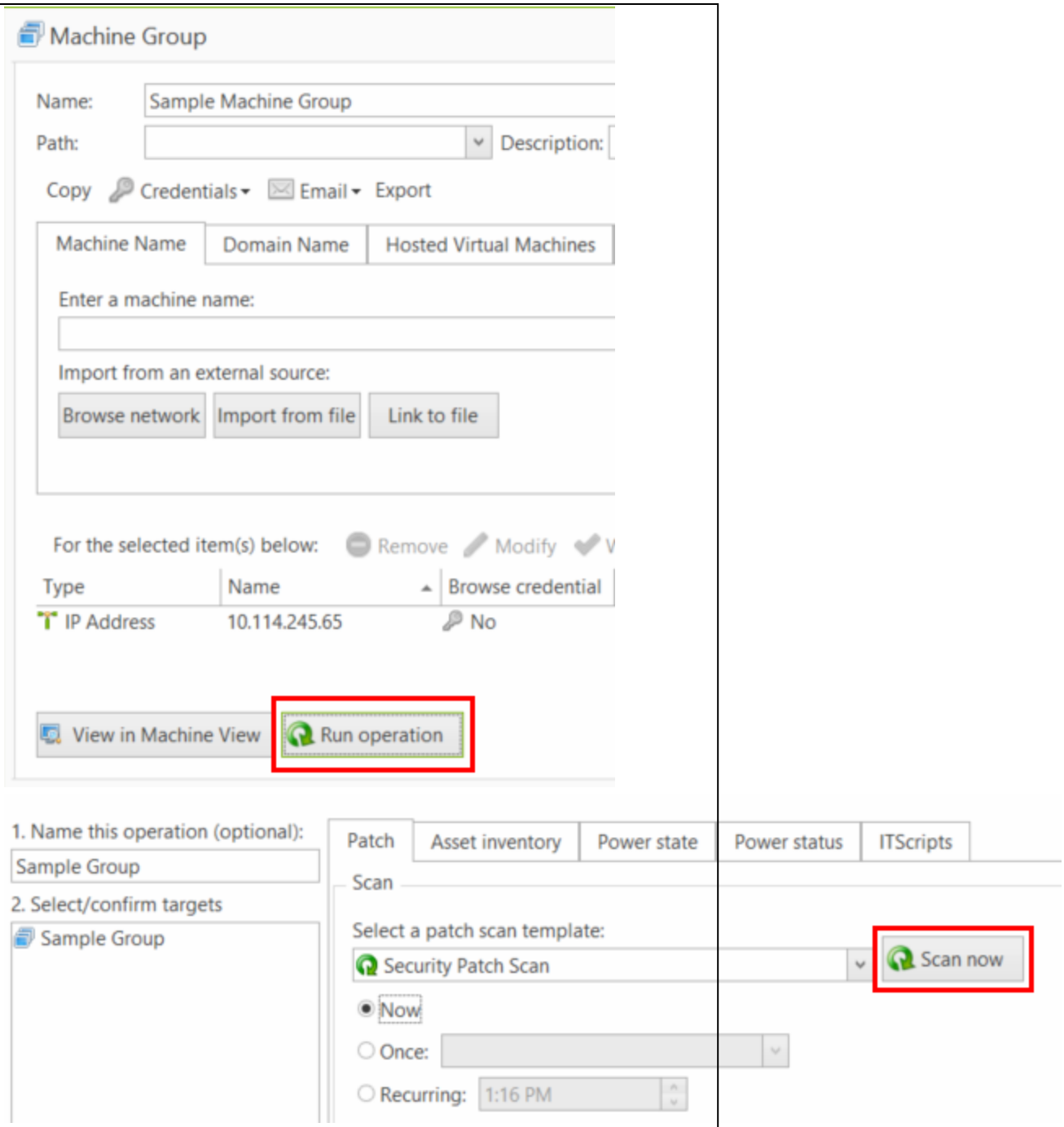
A) Create and Configure a Machine Group

The quickest way to evaluate many machines at once is to create and configure a machine group. For details, see Creating a New Machine Group, Configuring a Machine Group, and Supplying Credentials for Target Machines.

B) Perform a Scan of the Machine Group

After creating and configuring the machine group, to initiate a patch scan you simply click **Run Operation**. On the **Run Operation** dialog, verify the default options and then click **Scan Now**. This will immediately begin a scan of all machines in the machine group. (For other options see How to Initiate a Patch Scan.)

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



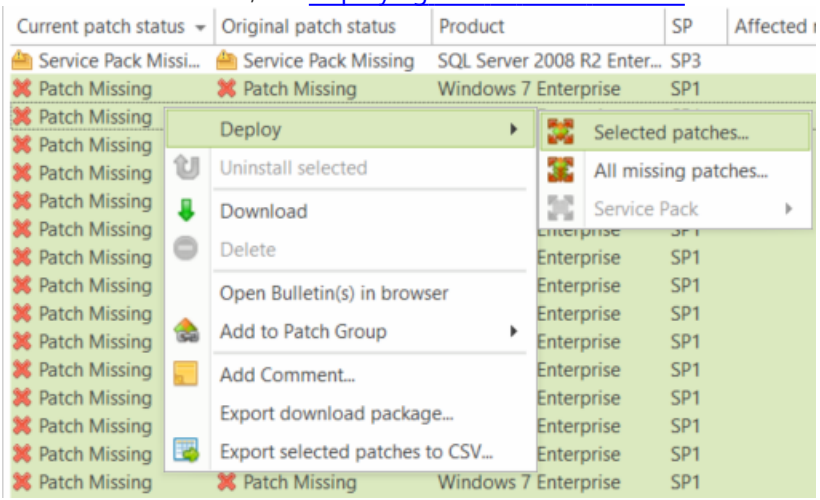
2 Review the Scan Results

Scan results are available immediately following a successful scan. For details, see Accessing Patch Scan Results.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

3 Deploy Any Missing Patches

You can immediately deploy any patches that are missing on your machines. For details, see Deploying One or More Patches.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Do I . . .?: Automate Scheduled Patching



Show Me!

To view a video tutorial on this topic, click the video icon on the left.

A scheduled scan enables you to specify exactly when a scan should be performed. You can configure Ivanti Patch for Windows® Servers to automatically perform recurring scheduled scans and to automatically deploy any missing patches it detects during a scan.

1. (Optional) Create a custom patch group and a custom patch scan template.

   This step is necessary if you want to control exactly which patches you scan for and deploy. You do this by first creating a patch group that contains just your approved patches, and then using it as a patch filter in a custom patch scan template.

   If the scheduled scan is something you intend to perform regularly (for example, to coincide with Microsoft's monthly patch release), you will also have to update the patch group on a regular basis.

2. (Optional) Create a custom machine group or a favorite.

   Using one of the default machine groups will work, too.

3. (Optional) Create a deployment template.

   Using one of the default templates will work, too.

4. Initiate a scan from the home page, from a machine group, or from a favorite.
5. On the **Run Operation** dialog, choose the **Recurring** option and specify when you want the scheduled scans to be performed.

   You can schedule a scan to run once at a specific time, or you can schedule a recurring scan. See Scheduling Patch Scans for complete details.

6. Enable the **Auto-deploy patches after scan** check box.
7. Select the desired deployment template and specify when the deployment should occur.
8. Click **Schedule**.
9. If prompted, select credentials that can be used to schedule the job on the console machine.
10. Use the Scheduled Console Tasks Manager to review scheduled scans.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Do I . . .?: Track Deployment Status



Show Me!

To view a video tutorial on this topic, click the video icon on the left.

Tracking Patch Deployments

It is very simple to track the status of patch deployment tasks.

- Scheduled patch deployments can be managed using the Scheduled Task Manager.
- Active patch deployments can be monitored using the Ivanti Patch for Windows® Servers Deployment Tracker.
- When a deployment is finished, you can review the status of the deployment by selecting the deployment in the Patch Results pane in the navigation bar.

Monitoring Post-patch Machine Status

To verify the status of the updated machine(s), simply perform a new scan and review the updated results using Machine View.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Do I . . .?: Download Approved Patches

There are a couple of reasons for downloading patches in advance of a patch deployment:

- If you are using one or more distribution servers to store patches you wish to deploy, you must download the patches to the console's patch download directory before you can copy them to the desired distribution servers. See Synchronizing Servers for more details.
- It will speed the deployment process. The act of deploying one or more patches will automatically download those patches not already resident in the patch download directory, but downloading them in advance will make the deployment process much faster.

Ivanti Patch for Windows® Servers provides a number of different ways to download patches.

- From within the top pane of Patch View, select the desired patches, right-click the patches, and then select **Download > Patches**.
- From within an approved patch group, click **View in Patch View**. From the resulting patch view, select all the patches, right-click the patches, and then select **Download > Patches**.
- From within the middle pane of Scan View, right-click the selected patches and select **Download Selected**.
- From within the middle pane of Machine View, right-click the selected patches and select **Download Selected**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Do I . . .?: Scan and Patch ESXi Hypervisors

The Virtual Inventory feature is used to scan and patch the ESXi hypervisors (ESXi hosts) that are used in your organization. The process is simple:

1. Add your managed and unmanaged ESXi hypervisors to Ivanti Patch for Windows® Servers.
2. Perform a scan of the managed and unmanaged ESXi hypervisors.
3. View the security bulletins that are missing on the managed and unmanaged ESXi hypervisors.
4. Initiate a deployment of any missing security bulletins.
5. Specify how the ESXi hypervisor and the virtual machines contained on the hypervisor will be affected during the bulletin deployment.
6. View the deployment results.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Do I . . .?: Set Up and Monitor Agents



Show Me!

To view a video tutorial on this topic, click the video icon on the left.

Setting up and using agents consists of the following general steps:

1	**Create and Configure an Agent Policy** An agent policy defines exactly what an agent can or cannot do. With Ivanti Patch for Windows® Servers Agent you can create as many different agent policies as is needed. This provides a great deal of flexibility, enabling you to assign different agent policies to different machines in your organization. A policy can be used to scan for missing patches, to determine software and hardware assets, and to perform power state tasks. See Creating a New Agent Policy for complete information.
2	**Install the Agent Policy On the Desired Machines** Agents can be push-installed from the console to the desired target machines, or they can be installed manually.
3	**Monitor the Agents as They Protect Your Machines** You can monitor the agents from the console or you can use the Ivanti Patch for Windows® Servers Agent client program to perform additional actions directly on the agent machine.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Do I . . .?: Use The Asset Inventory Feature



Show Me!

To view a video tutorial on this topic, click the video icon on the left.

The asset inventory feature enables you to track your software, hardware, and virtual assets. You can perform scans to detect and categorize the software and hardware contained on your physical and online virtual machines. You can also scan for the properties of your online and offline virtual machines.

To use the asset inventory feature you do the following:

1. Determine if you want to use the default asset scan template or a custom asset scan template.

   See Creating a New Asset Scan Template for information on creating your own unique asset scan templates.

2. Initiate an asset scan of the desired machines.

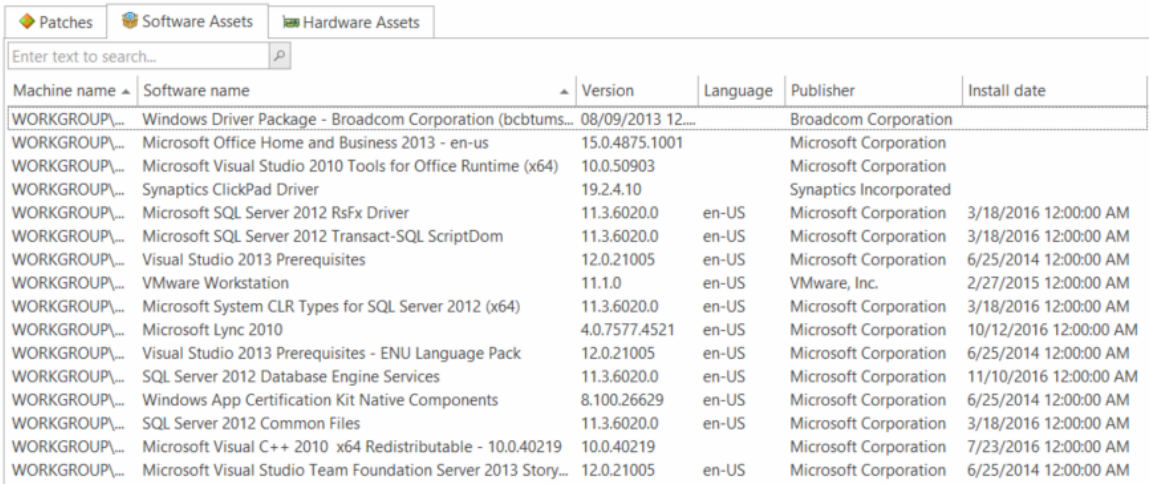
   Asset scans can be initiated from the home page, from a machine group, from a favorite, or from Machine View. See How to Perform Asset Scans for details.

3. View the asset scan results.

   Asset scan results are available within Machine View. See the following for details:

   - Viewing Software Asset Summaries
   - Viewing Hardware Asset Summaries

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Machine name	Software name	Version	Language	Publisher	Install date
WORKGROUP\...	Windows Driver Package - Broadcom Corporation (bcbtums...	08/09/2013 12....		Broadcom Corporation	
WORKGROUP\...	Microsoft Office Home and Business 2013 - en-us	15.0.4875.1001		Microsoft Corporation	
WORKGROUP\...	Microsoft Visual Studio 2010 Tools for Office Runtime (x64)	10.0.50903		Microsoft Corporation	
WORKGROUP\...	Synaptics ClickPad Driver	19.2.4.10		Synaptics Incorporated	
WORKGROUP\...	Microsoft SQL Server 2012 RsFx Driver	11.3.6020.0	en-US	Microsoft Corporation	3/18/2016 12:00:00 AM
WORKGROUP\...	Microsoft SQL Server 2012 Transact-SQL ScriptDom	11.3.6020.0	en-US	Microsoft Corporation	3/18/2016 12:00:00 AM
WORKGROUP\...	Visual Studio 2013 Prerequisites	12.0.21005	en-US	Microsoft Corporation	6/25/2014 12:00:00 AM
WORKGROUP\...	VMware Workstation	11.1.0	en-US	VMware, Inc.	2/27/2015 12:00:00 AM
WORKGROUP\...	Microsoft System CLR Types for SQL Server 2012 (x64)	11.3.6020.0	en-US	Microsoft Corporation	3/18/2016 12:00:00 AM
WORKGROUP\...	Microsoft Lync 2010	4.0.7577.4521	en-US	Microsoft Corporation	10/12/2016 12:00:00 AM
WORKGROUP\...	Visual Studio 2013 Prerequisites - ENU Language Pack	12.0.21005	en-US	Microsoft Corporation	6/25/2014 12:00:00 AM
WORKGROUP\...	SQL Server 2012 Database Engine Services	11.3.6020.0	en-US	Microsoft Corporation	11/10/2016 12:00:00 AM
WORKGROUP\...	Windows App Certification Kit Native Components	8.100.26629	en-US	Microsoft Corporation	6/25/2014 12:00:00 AM
WORKGROUP\...	SQL Server 2012 Common Files	11.3.6020.0	en-US	Microsoft Corporation	3/18/2016 12:00:00 AM
WORKGROUP\...	Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	10.0.40219		Microsoft Corporation	7/23/2016 12:00:00 AM
WORKGROUP\...	Microsoft Visual Studio Team Foundation Server 2013 Story...	12.0.21005	en-US	Microsoft Corporation	6/25/2014 12:00:00 AM

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Do I . . .?: Use The Power Management Feature



Show Me!

To view a video tutorial on this topic, click the video icon on the left.

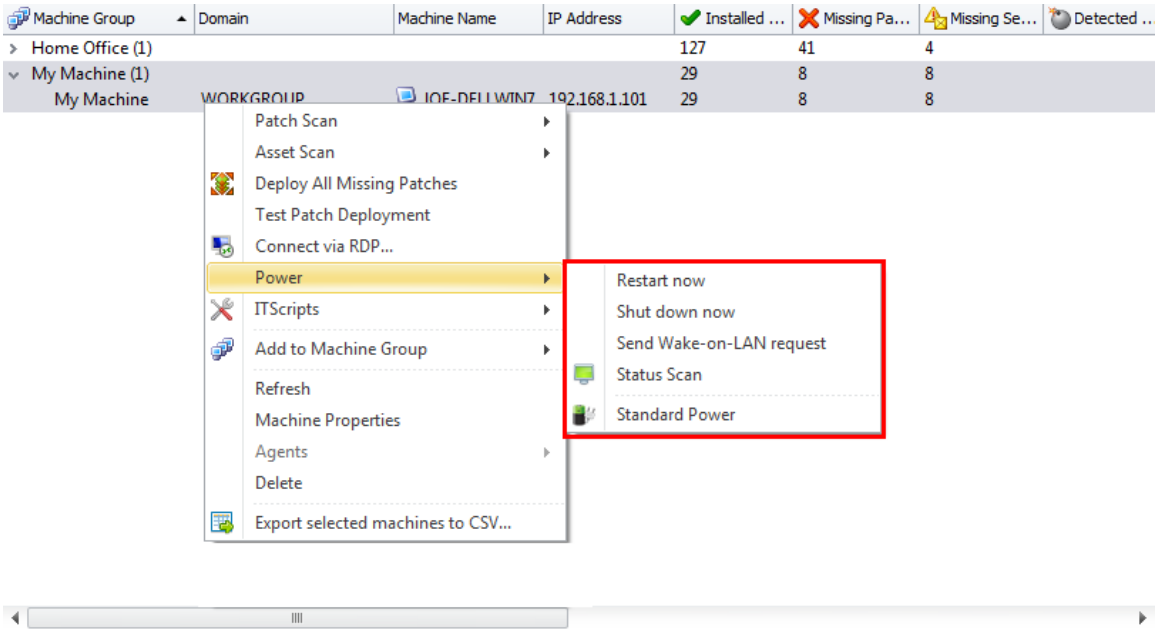
The power management feature enables you to control the power state of the machines in your organization. The primary reasons for using power management are to:

- Prepare your machines for maintenance tasks
- Reduce power and noise consumption
- Reduce operating costs
- Prolong battery life

To use the power management feature you do the following:

1. Initiate power management commands from either Machine View or Scan View.

   Use the right-click menu to immediately restart, shut down, or wake up machines. See How to Initiate Power Management Tasks for details.



2. Track the status of power commands using the Operations Monitor.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

See Monitoring a Power Task for details.

3. To schedule a restart or a shutdown you use a power management template.

   See:

   - Creating and Editing a Power State Template
   - How to Initiate Power Management Tasks
   - Scheduling Power Management Tasks

4. Before using the Wake-on-LAN feature be sure to read Wake-on-LAN Implementation Notes.

   You can use the Wake-on-LAN feature to wake up machines that are sleeping, hibernating, or powered off. For example, you might want to wake up your machines during a maintenance window so they can receive critical security updates. Or you might schedule a wake-up call for a group of machines that you put to sleep the night before so they are ready for the work day.

5. Power management tasks can also be performed by agents.

   See Creating and Configuring a Power Task for details.

6. Perform a power status scan to verify the updated power status of your machines.

   See Performing a Power Status Scan and Viewing Power Status Scan Results.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Do I . . .?: Use The ITScripts Feature



Show Me!

To view a video tutorial on this topic, click the video icon on the left.

The ITScripts feature enables you to execute PowerShell scripts against the machines and machine groups you have already defined in Ivanti Patch for Windows® Servers.

To use the ITScripts feature you do the following:

1. Review the ITScripts Overview topic to familiarize yourself with the capabilities of this feature.
2. Use the Script Catalog Manager to specify which scripts are approved for use within your organization.
3. Execute the desired script from within the Ivanti Patch for Windows® Servers interface.
4. Review the results using ITScript Results View.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Do I . . .?: Collect Data for Technical Support

If you ever have a question or issue with Ivanti Patch for Windows® Servers that requires help from the Ivanti Technical Support staff, please have the following information available when opening a support request or calling:

- What version of Ivanti Patch for Windows® Servers are you using? Please include the build number (available via **Help > About Ivanti Patch for Windows® Servers**).
- What operating system is the console installed on? Please include the service pack level.
- What operating system(s) are the target machines running? Please include the service pack level and architecture version (32-bit or 64-bit).
- What exactly were you doing when the issue occurred, or what exactly do you want to do? Please be as descriptive as possible.
- Provide your Ivanti Patch for Windows® Servers license key.
- Provide screen shots or text of any on-screen errors.

Installation Log Files

The installation logs are located in the following directory: C:\Users\user name\AppData\Local\Temp

There are three installation log files within the directory:

- Main installation log file: ProtectSetup_date_time.log PAUSetup_date_time.log
- Prerequisite installation log file: PreSetupdate.log
- Windows Installer log file: ProtectInstall_date_time.log PAUInstall_date_time.log

Program Log Files

If necessary, you may be asked to capture program log files.

1. Select **Tools > Options > Logging** and in the **User Interface** and **Services** boxes specify **All**.
2. Restart the program.
3. Recreate the issue.

   Please note the steps you took to recreate the issue. Also note the date and time of day so our analysts know where to look in the log files.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

4. Once the issue is recreated, and before you close or restart the program, make a copy of all the logs and include them in your email correspondence.

The logs are located in the following directory: **C:\ProgramData\LANDESK\Shavlik Protect\LogsScriptLogic Corporation\Patch Authority Ultimate\Logs**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Do I . . .?: Use A Distribution Server



Show Me!

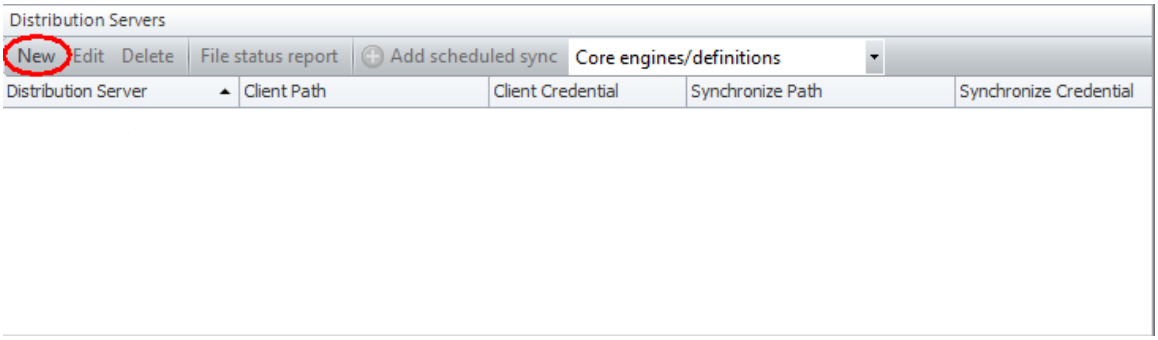
To view a video tutorial on this topic, click the video icon on the left.

Distribution servers can be used as an alternate location for storing the scan engines, the XML data files, and the patches used by Ivanti Patch for Windows® Servers. There are a number of reasons you may want to use a distribution server. For details, see Why Use a Distribution Server?

To use a distribution server you do the following:

1. Create and configure a new distribution server.

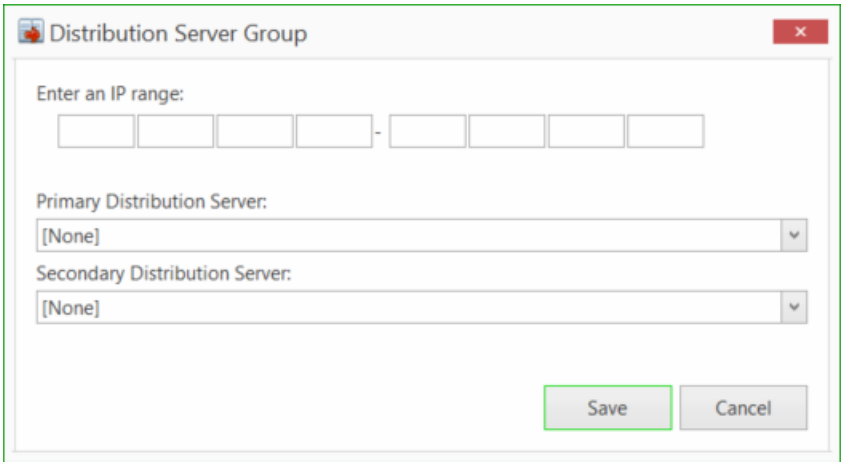
   Select **Tools > Options > Distribution Servers** and then click **New**. For details, see Configuring Distribution Servers.



2. Define which target machines will use the distribution server.

   In the **IP Ranges** pane, click **New** and then specify the IP ranges you want to associate with the server. For details, see Assigning IP Addresses to Servers.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



3. Update the distribution server with the latest files.

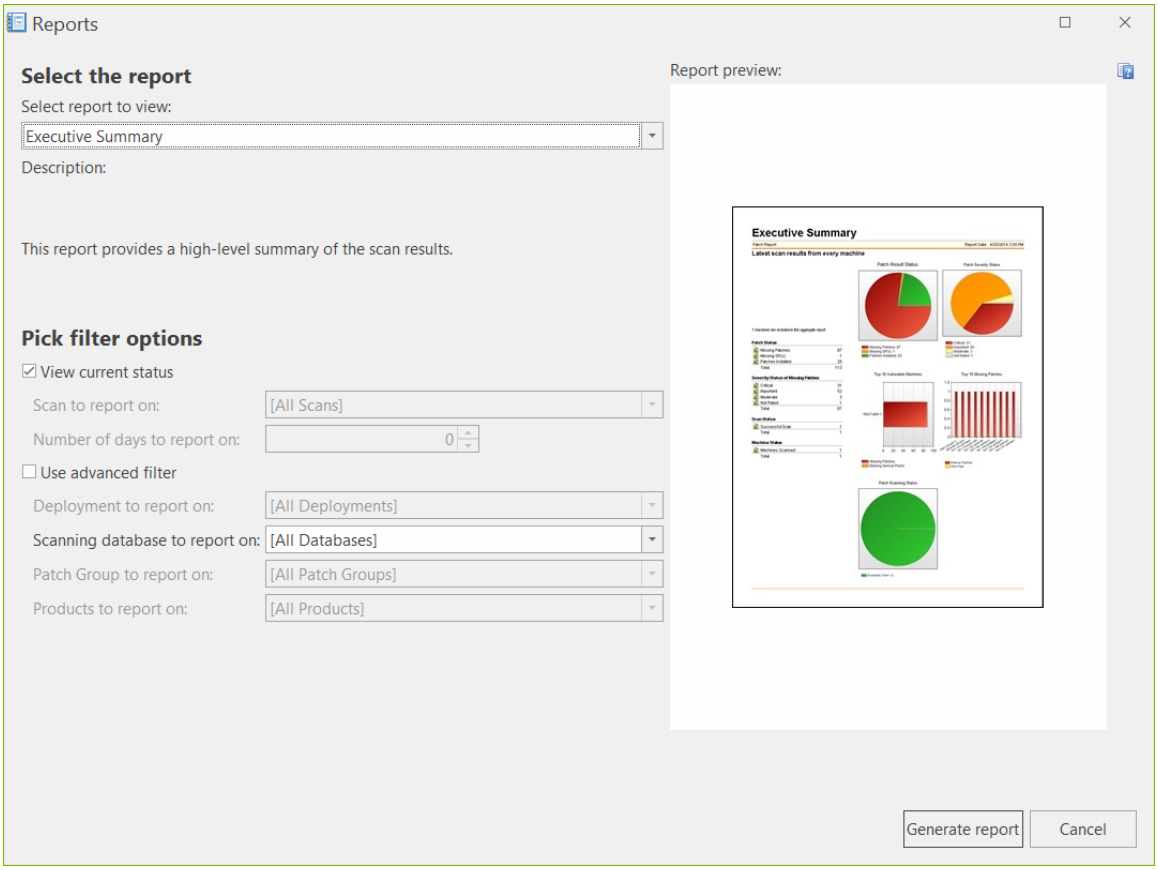
   You do this by synchronizing the distribution server with the console. For details, see Synchronizing Servers.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Do I . . .?: Generate Reports

There are a number of different reports you can generate to view the state of the machines in your network.

1. Select **Tools > Create report** from the main menu.
2. Select a report from the drop-down list at the top of the **Reports** dialog.



   For a list of all available reports, see Overview of Reports.

3. Select your filtering options.

   For details, see Report Gallery.

4. Click **Generate report**.

   The report is generated and displayed within the report viewer.

5. (Optional) If you elected to use advanced filtering, specify the advanced filtering options.

   For details, see Advanced Filtering.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

6. If desired, export the report to a number of different formats.

   For details, see Exporting Reports.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How Do I . . .?: View How-to Tutorials

To view video tutorials that show you how to perform a number of common tasks within Ivanti Patch for Windows® Servers, please go to the Ivanti Help channel on YouTube.

This channel contains a number of video tutorials. The tutorials walk you through the product interface, showing you exactly how easy it is to use Ivanti Patch for Windows® Servers and how to get the maximum benefit from the product.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Virtual Machine Overview



Show Me!

To view a video tutorial on this topic, click the video icon on the left.

TIP: For information on managing and tracking the vCenter Servers and the ESXi hosts that are used in your organization, see Introducing the Virtual Inventory Feature.

A virtual machine is not actually a physical machine but rather a software environment (usually an operating system) designed to emulate a physical machine. A virtual machine can run programs just like a physical machine. The physical machine used to host the virtual machine can often support multiple virtual machines.

Ivanti Patch for Windows® Servers can scan for and deploy patches to the virtual machines on your network regardless of whether they are online or offline. It can also perform a software asset scan of your online and offline virtual machines.

Online Virtual Machines

A virtual machine that is online and running is treated by Ivanti Patch for Windows® Servers the same as a physical machine. Patch scans and asset scans will be performed in the same manner as on a physical machine. Any patches that may be missing can also be deployed in the same manner to both your physical machines and your online virtual machines. This means that your online virtual machines are protected by the latest software patches just like your physical machines.

Offline Virtual Machines

Ivanti Patch for Windows® Servers also enables you to scan and patch offline virtual machines. Offline virtual machines are those that aren't powered on when a patch scan or an asset management scan is performed. These virtual machines may be powered on for only a few hours or days a month and then powered off until they are needed again the next month. It's important to ensure that these systems are patched so that when they are brought online they don't place your network at risk.

Ivanti Patch for Windows® Servers makes it easy to scan these offline virtual machines. When you initiate a scan of a machine group that contains offline virtual machines, Ivanti Patch for Windows® Servers will perform a full assessment of the offline virtual machines and display the scan results alongside the results for running systems. Offline virtual machines will be differentiated in the scan results by a unique icon ( ). The scan results may even identify offline virtual machines that you don't know about. When viewing machines in Machine View the **Offline Scan** column in the top pane will indicate if a virtual machine was offline at the time of the scan.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Patching offline virtual machines is similarly simple. You simply highlight the machines and patches you'd like to install and then select **Deploy** from the Ivanti Patch for Windows® Servers menu. For offline virtual machines that are hosted on a server, the machines will be powered on, the patches installed, and the machines powered back down. For virtual machines that reside on workstations, the patches will be copied to the offline virtual machines and will be installed the moment that the virtual machine is started (or according to the scheduled patch deployment time).

Virtual Machine Templates

Virtual servers and virtual workstations are often created using a template. Templates enable you to quickly create new virtual machines that conform to your particular configuration requirements. A template that is offline poses no danger to your organization. A template that is brought online, however, is no different than an online virtual machine. It can perform tasks just like any other virtual machine, and it can also contain the same viruses, spyware, and other types of malware that target improperly patched machines. For this reason it is critical that your virtual machine templates receive the same patch management care as your physical and virtual machines.

Ivanti Patch for Windows® Servers enables you to patch your virtual machine templates. You simply add your templates to a machine group and Ivanti Patch for Windows® Servers will take care of the rest. For complete details on the virtual machine template scan and deployment process, see Notes About Virtual Machine Templates.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Power State and Credential Requirements for Successful Scans and Deployments to Virtual Machines

An offline virtual machine (workstation-based or hosted on a server) is a file or set of files. To scan or deploy to an offline virtual machine requires permissions to the file system where the files reside. An online virtual machine is almost indistinguishable from a physical machine. To scan or deploy patches to an online virtual machine requires credentials for an administrator account on the virtual machine operating system.

Because of these differences between online and offline virtual machines, you may need to provide two sets of credentials – one for when the virtual machine is in the online state and one for when it is in the offline state.

For workstation virtual machines, if you wish to scan and/or deploy to the virtual machine in either its online or offline state, you should add the virtual machine to the machine group twice:

- For its online state, enter the machine identifier and online credentials in the machine group as you would any physical machine – on the **Machine Name**, **Domain Name**, **IP Address/Range**, or **Organizational Unit** tab.
- For its offline state, enter the information and credentials for the virtual machine file locations on the **Workstation Virtual Machines** tab.

For hosted virtual machines, you only need to specify the machine once, on the **Hosted Virtual Machines** tab. Separate credentials, however, are still required to access the machine in either the online or offline state. The browse credentials you enter when connecting to the VMware server are used when the machine is in the offline state. You should enter online credentials for each hosted virtual machine using the **Set Admin Credentials** option in the bottom pane of the machine group editor.

The following table summarizes the credentials used for various machine types.

Machine Type	Machine State	Machine Group Tab Used to Define the Virtual Machine	Credentials Required
Physical Machine	Online	Machine Name, Domain Name, IP Address/Range, Org Unit	Machine or machine group credentials

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Workstation VM	Online	Machine Name, Domain Name, IP Address/Range, Org Unit	Machine or machine group credentials
Workstation VM	Offline	Workstation Virtual Machines	Machine or machine group credentials
Hosted VM	Online	Hosted Virtual Machines	Machine or machine group credentials
Hosted VM	Offline	Hosted Virtual Machines	Browse credentials (the creds used to log on to the VM server)



Integrated credentials will not work for deployments to offline virtual machines.

If you specify both online and offline credentials for virtual machines, you will be able to scan and deploy to those virtual machines whether they are online or offline.

For more information, see Deploying Patches to Virtual Machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

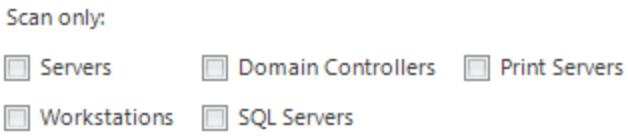
Notes About Virtual Machines

Requirements

- Dual boot systems (for example, a virtual machine with two partitions, each containing a different operating system) are not supported.
- When scanning offline virtual machines that are supported by VMware, please keep in mind the following:
  - You cannot mount encrypted virtual disks.
  - You cannot mount a virtual disk if any of its .vmdk files are compressed or have read-only permissions.
  - You cannot mount a virtual disk that is currently being used by a running or suspended virtual machine.
  - Linked clones and compressed images are not supported.

General Notes

- Only the current state of the virtual machine will be scanned and patched. Snapshots of virtual machines are not scanned or patched.
- A virtual machine is counted only once against the total number of license seats available, even if it is scanned both in online (powered on) mode and offline (powered off) mode.
- In machine groups and in scan results, special icons will distinguish an offline virtual machine ( ) from a physical machine or an online virtual machine ( ) and from a virtual machine template ( ).
- Avoid using network drive letters when defining offline virtual machines in a machine group. The recommended practice is to instead specify the Uniform Naming Convention (UNC) path. This comes into play when performing a scheduled scan on an offline virtual machine. Network drive mappings are session-specific, so it is very possible that a specified mapping will no longer exist when the scheduled scan process is run.
- Within a machine group, the **Scan only** filters do not apply to offline virtual machines or to virtual machine templates.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- It is possible for two offline virtual machines to have the same domain and computer name. This will be the case if you clone a virtual machine and do not change either the computer name or domain on one or both machines. In this situation, of the two duplicate virtual machines, only the last one scanned will be visible in Machine View. The machines displayed in Machine View are keyed on domain and computer name and duplicates are not allowed.
- Virtual machines that are offline (powered off) will be mounted before they are scanned. Virtual machines that are online (powered on) do not need to be mounted as they are treated no differently than a physical machine.
- When performing a patch scan or an asset scan, a virtual machine that was added to a machine group as an offline virtual machine but that is online at the time of a scan will be scanned if it is hosted on an ESX server and if the proper credentials are available in order to access that machine. Online virtual machines that are hosted on workstations will fail to mount and will not be scanned.
- When scanning multiple offline virtual machines that are hosted on one workstation, it is possible to reach the connection limit for that workstation. If the connection limit is reached an error will occur and the scans will fail. The maximum number of simultaneous connections supported varies for each Windows OS.

Patch Deployments

- When deploying patches to an offline virtual machine that is hosted on a server, the virtual machine will be powered on, the patches installed, and the virtual machine powered down. See Deploying Patches to Virtual Machines for more details.
- When deploying patches to an offline virtual machine that is hosted on a server, VMware tools must be installed on the virtual machine.
- When deploying patches to an offline virtual machine that is hosted on a server, the following VMware server permissions are required in order to manage snapshots and to change the power state of the machine during the deployment process:
  - VirtualMachine.State.CreateSnapshot
  - VirtualMachine.State.RemoveSnapshot
  - VirtualMachine.Interact.PowerOn
  - VirtualMachine.Interact.PowerOff
  - VirtualMachine.Interact.DeviceConnection (to disable/enable the network card)
- When deploying patches to an offline virtual machine that resides on a workstation, the new deployment job will overwrite any older deployment jobs that have not yet been performed. For this reason you should deploy all desired patches in a single deployment.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Example: You deploy Patch A to a workstation-based offline virtual machine. The virtual machine is still offline a month later when you deploy Patches B and C. Because the first deployment job was never executed it gets overwritten and only Patches B and C are now scheduled for deployment. To avoid this you simply include Patch A along with Patches B and C in the second deployment job.

One way to manage this is to use a patch group to define the patches you want deployed to your workstation-based offline virtual machines. When new patches are identified you simply add them to the list of patches in the patch group. This is particularly useful when specifying a patch group within a patch scan template and then enabling the **Auto-deploy patches after scan** check box on the **Run Operation** dialog. See Creating a New Patch Scan Template and Using the Run Operation Dialog for more details about these options.

Agents

- Ivanti Patch for Windows® Servers Agent operations are not supported on offline virtual machines.
- If you install Ivanti Patch for Windows® Servers Agent on an online virtual machine and then later scan the virtual machine while it is in an offline state, Ivanti Patch for Windows® Servers may report the wrong agent status for that image. For example, it may show that the agent is not installed, or it may let you attempt to uninstall the agent. This occurs because Ivanti Patch for Windows® Servers Agent operations are not supported on offline virtual machines. The correct status will be reported once the virtual machine is brought back online and rescanned by Ivanti Patch for Windows® Servers.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Notes About Virtual Machine Templates

General Notes

- For information on using virtual machine templates in patch scans, asset scans, and patch deployments, see Roadmap of Tasks.
- The type of virtual machine template (server template, workstation template, etc.) does not matter, they are all supported by Ivanti Patch for Windows® Servers.
- Only virtual machine templates that are hosted on a VMware server are supported by Ivanti Patch for Windows® Servers. The templates are added to a machine group using the **Hosted Virtual Machines** tab. Virtual machine templates that reside on individual workstations are not supported.
- A unique icon () is used to identify virtual machine templates. You will see this icon when adding a template to a machine group and when viewing scan results in Scan View and in Machine View.
- As with anything that involves components on a network, errors can occur if connections go bad, if servers are shut down, if a template is modified while being accessed by Ivanti Patch for Windows® Servers, etc. In general, the templates should not be touched at any time during the scanning or patch deployment process.
- When you initiate a patch or an asset scan of a virtual machine template, Ivanti Patch for Windows® Servers will scan the template in its current state and will report the results the same way it does for virtual machines and physical machines.
- During a scan, a template will be accessed using the VMware server credentials. Any individual credentials supplied for the template are ignored.
- You should supply online credentials for any virtual machine template that will be included in a patch deployment process. During the patch deployment process the template is converted to a virtual machine and powered on -- Ivanti Patch for Windows® Servers will need the supplied credentials in order to access the online virtual machine.

Patch Deployments

- When deploying patches to a virtual machine template, the following VMware server permissions are required in order to manage snapshots and to perform the deployment:
  - VirtualMachine.State.CreateSnapshot
  - VirtualMachine.State.RemoveSnapshot
  - VirtualMachine.Provisioning.MarkAsTemplate

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- VirtualMachine.Provisioning.MarkAsVM

- When you initiate a patch deployment to a virtual machine template, Ivanti Patch for Windows® Servers will do the following:

1. Convert the virtual machine template to an offline virtual machine.
2. **(Optional)** Take a snapshot if the patch deployment template is configured to take a pre-deployment snapshot.
3. **(Optional)** Delete old snapshots if one of the snapshot thresholds defined on the patch deployment template is exceeded.
4. Push the patches to the offline virtual machine.
5. Reconfigure the following on the offline virtual machine:
   - Disable the network adaptor's**Connect at power on**option. This is done so that the machine is isolated from the network when the patch process is run.
   - If Sysprep is scheduled to run, disable it so it will not automatically configure the machine's operating system when the machine is first powered on.
6. Power on the virtual machine.
7. Install the patches.
8. Power down the virtual machine.
9. Reset the machine configuration to its original network connection and Sysprep settings.
10. **(Optional)** Take a snapshot if the patch deployment template is configured to take a post-deployment snapshot.
11. **(Optional)** Delete old snapshots if one of the snapshot thresholds defined on the patch deployment template is exceeded.
12. Convert the offline virtual machine back to a virtual machine template.

- The patch deployment template you use must not specify the use of a distribution server. The offline virtual machine will be disconnected from the network and unable to download the patches from the distribution server.
- The patch deployment template you use should not specify a pre-deploy reboot (the program will be unable to initiate the reboot because the machine will be offline) and it should always perform a post-deploy reboot (this is a "best practice" when deploying patches). For deployments to virtual machine templates it is recommended you use the **Virtual Machine Standard** deployment template.
- During a patch deployment, a virtual machine template that may normally be available only to an administrator will become visible to other users. This is because during the patch deployment process the template is temporarily converted to a virtual machine and powered on.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Roadmap of Tasks for Virtual Machines and Virtual Machine Templates



Show Me!

To view a video tutorial on this topic, click the video icon on the left.

Patch Tasks

Ivanti Patch for Windows® Servers can scan and deploy patches to online virtual machines, to offline virtual machines, and to virtual machine templates. You do this by performing the following tasks:

1. Create one or more machine groups that contain the virtual machines and virtual machine templates you want to scan and patch.

   See How to Add Virtual Machines.

2. Supply credentials for the virtual machines.

   When performing scans, the recommended best practice is to always supply credentials for the virtual machines and virtual machine templates. When performing patch deployments, credentials must be set at the machine, group, or default level. See Supplying Credentials for more details.

3. Use the machine group in a scan. See How to Initiate a Patch Scan for details.
4. Review the scan results. See Accessing Patch Scan Results for details.

   In the scan results, unique icons will distinguish an offline virtual machine () from a physical machine or an online virtual machine () and from a virtual machine template (). When viewing machines in Machine View the **Offline Scan** column in the top pane will indicate if a virtual machine was online or offline at the time of the scan.

5. (Optional) If you want to take snapshots of your hosted virtual machines and templates immediately before and/or immediately after the deployment process, make sure you specify this on the **Hosted VMs/Templates** tab of the deployment template you plan to use.
6. Deploy the desired patches to the desired virtual machines and virtual machine templates. See Deploying Patches to Virtual Machines for details.

   You may not know if a particular virtual machine is online or offline at the time you perform a deployment, and it typically doesn't matter. The following guidelines apply for patch deployments to virtual machines:

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- If a virtual machine is hosted on a server, the deployment can be successful regardless of whether the virtual machine is online or offline at the time of the deployment.
- If a virtual machine is defined in a machine group using the **Workstation Virtual Machines** tab, the deployment can be successful as long as the virtual machine is offline.
- If a virtual machine is defined in a machine group using the **Machine Name**, **Domain Name**, or **IP Address/Range** tab, the deployment can be successful as long as the virtual machine is online.

If a virtual machine is online the patch deployment is performed in the same manner as for a physical machine. Patch deployments to offline virtual machines and to virtual machine templates are performed by Ivanti Patch for Windows® Servers in a slightly different manner. See Deploying Patches to Virtual Machines for details.

7. Monitor the deployment activities. See Monitoring the Deployment for details.

Asset Management Tasks

Ivanti Patch for Windows® Servers can perform asset management scans of online virtual machines, of offline virtual machines, and of virtual machine templates. You do this by performing the following tasks:

1 Create one or more machine groups that contain the virtual machines and templates you want to scan.

See **How to Add Virtual Machines**.

2. Supply credentials for the virtual machines and virtual machine templates.

See Supplying Credentials for details.

3. Use the machine group in an asset scan. See How to Perform Asset Scans for details.
4. Review the asset scan results. See Viewing Asset Scan Results for details.

When viewing machines in Machine View the Offline Scan column in the top pane will indicate if a virtual machine was online or offline at the time of the scan.

Power Management Tasks

You can use Ivanti Patch for Windows® Servers to power on and off the virtual machines that reside on your ESXi hosts. For more information, see Performing Actions on Virtual Machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

What Sets Ivanti Patch for Windows® Servers Apart from the Others?

Features

Item	Description
Ease of use	Ivanti Patch for Windows® Servers can be installed and used to deploy missing patches within minutes; not days, weeks, or months.
Real-time patch validation	Ivanti Patch for Windows® Servers utilizes XML data files that are updated the moment a security patch is released.
Agentless and agent-based operation	Provides the ability to manage network machines directly from a console and to manage hard-to-reach and cloud-connected machines (such as roaming laptops) using agents.
Background (non-modal) tasking	Enables multiple tasks to run at the same time. Simultaneously perform patch and asset scans, download files, deploy patches, perform power management tasks, install agents, and keep on working.
Patch replacement	Only those patches that are necessary and applicable to the scanned platform are evaluated during the scan process. Unnecessary and replaced patches are not presented (although you can configure the program to do this if you want).
Dynamic product detection (DPD)	Provides the ability to support additional non-Microsoft products simply by updating the necessary XML files.
Virtual machine support	Operates exactly the same on both physical machines and on virtual machines that are online. Can perform patch assessment of offline virtual machines without powering them on. Missing patches are copied into the virtual image so when the offline image is powered on it immediately patches itself.

Security and Integrity

Item	Description

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Detailed Patch Analysis and Validation	File versions and registry keys are evaluated to aid in determining patch status. Solutions that rely solely on registry keys and/or minimum file versions are unable to differentiate between legitimate files and trojaned files, including patches that have been re-released by Microsoft.
External validation data	File data used to perform patch validation tests are obtained from a signed source independent of the machine being scanned.
Data file anti-spoofing protection	The XML patch data file is parsed only if obtained from a valid, specifically signed CAB file or SSL location.
Trojan protection	All digitally-signed vendor files are validated prior to patch deployment.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Scanning Engine Overview

The Ivanti Patch for Windows® Servers scan engine performs security patch assessment against a variety of Windows-based operating systems and products from Microsoft and other product vendors.

The Ivanti Patch for Windows® Servers engine uses an Extensible Markup Language (XML) file that contains information about which security hotfixes are available for each product. The XML file contains security bulletin name and title, and detailed data about product-specific security hotfixes, including:

- Files in each hotfix package and their file versions
- Registry changes that were applied by the hotfix installation package
- Information about which patches replace which other patches
- Related Microsoft Knowledge Base article numbers
- Cross references to the Common Vulnerabilities and Exposures (CVE) database hosted by Mitre.org (CVEID)

The XML patch data file, which is contained on the console in a secured file named **WindowsPatchData.zip**, is created and hosted by Ivanti.

When you run Ivanti Patch for Windows® Servers (without specifying advanced file input options), the program must download a copy of this XML file so that it can identify the hotfixes that are available for each product. The XML file is a digitally signed CAB file and is available on the Ivanti website. Ivanti Patch for Windows® Servers downloads the CAB file, verifies its digital signature, and then extracts the XML file to your local computer. Note that a CAB file is a compressed archive that is similar to a ZIP file.

After the XML file is extracted, Ivanti Patch for Windows® Servers scans your machine (or the selected machines) to determine the operating system, service packs, and programs that you are running. Ivanti Patch for Windows® Servers then identifies security patches that are available for your combination of installed software. Patches that are applicable to your machine but are not currently installed are displayed as **Missing Patch** in the resulting output. In the default configuration, Ivanti Patch for Windows® Servers output displays only those patches that are necessary to bring your machine up to date. Ivanti Patch for Windows® Servers recognizes roll-up packages and does not display those patches that are replaced by later patches.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Enumerating Machines in Domains

When scanning by domain name, Ivanti Patch for Windows® Servers does the following to enumerate the machines in the domain:

- The domain controller is contacted and its list of machine accounts is enumerated. Browse credentials defined within the machine group are used for this process. If browse credentials are not provided, the credentials of the user running the scan are used.

  You can reduce the number of machines that the program will attempt to connect to by enabling the **Use only the browse list** scan option.

- Machines are also enumerated from the network browse list which is the same list of machines seen on a per domain basis when viewing the network, or similar to 'net view /domain:domainname'. No special permissions are required to enumerate machine names this way as Ivanti Patch for Windows® Servers is using UDP port 137 (NetBIOS name service) to enumerate the browse list. If the scanning machine has just been connected to the network, it may take up to 15 minutes until the machine synchronizes with the browse master and for this list to become available to the scanning machine. The list of machines that are returned represent machines that are currently online or have been within the last 15 minutes. Machines that are 'hidden' via registry modifications won't appear as they don't propagate their machine names to the network browse list. If the scanning machine doesn't have access to the browse list, or the machines are behind filtering devices where the browse list isn't updated, etc. then no machines will appear.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Determining Patch Status

Ivanti Patch for Windows® Servers performs a detailed analysis of each scanned machine to accurately determine its patch status. Unlike other patch management systems, the Ivanti Patch for Windows® Servers engine goes far beyond the traditional patch detection mechanisms that rely solely on the presence of registry keys.

For Ivanti Patch for Windows® Servers to determine if a specific patch is or is not installed on a given computer, two items are typically evaluated:

- The registry keys that are installed by the patch
- The file versions for all files installed by the patch

Ivanti Patch for Windows® Servers compares file versions in the XML patch data file to the files versions on the computer that is being scanned. If any of the file versions on the scanned computer are less than those stored in the XML file, the associated security patch is identified as not installed and the results are displayed on the screen. Specific details about why a patch is considered not installed are also displayed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

File Version Analysis

In order for a system to 'pass' a given patch analysis for a patch that is applicable to the system, the file versions for all patch-related files must match what is stored in the XML patch data file.

- If the file version for a patch-related file is below what is expected (on the target system), the patch is considered not found, and both the file version found on the system and the file version expected (from the XML file) are displayed in the output with a 'Patch Missing' message.
- If the file version of any file on the system is greater than expected, both the existing and the expected file versions are displayed along with a warning message that the file on the system is more recent than expected. This may indicate the presence of a more recent non-security bulletin related hotfix, or the presence of a trojaned file.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Determining Patch Replacements

One of the benefits of Ivanti Patch for Windows® Servers is that it only shows you patches that are necessary for your machine to be up to date, and it doesn't show you earlier patches that have been replaced by later patches (although you can configure the program to do this if you want).

Many recent Microsoft security patches have been released as 'Cumulative Rollup' patches. Rollup patches include all the previously released security patches for the given product as well as including fixes for the most recently announced issues. A cumulative patch that completely encompasses an earlier patch is said to replace the earlier patch. In order for a patch to be replaced, all the files in the earlier patch must be included in the later patch, all file versions must be revved higher than those in the earlier patch (or the file versions must be the same as the earlier patch), and associated functional registry keys must be included in the replacement patch.

The XML patch data file contains information on each of the replaced patches. Ivanti Patch for Windows® Servers evaluates the patch replacement codes to identify patches that are applicable to each system being scanned. Particular attention is paid to replaced patches that span Service Pack applicability As an example:

- Patch A is applicable to Windows 7 Service Pack 1 (SP1)
- Patch B replaces Patch A and is applicable to both Windows 7 SP1 and SP2
- Patch C replaces Patch B and is applicable to Windows 7 SP2

Ivanti Patch for Windows® Servers correctly scans for the presence of Patch C on Windows 7 SP2 machines, and for Patch B on Windows 7 SP1 machines - even though Patch B is marked in the XML file as being replaced by Patch C.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Identifying Explicitly Installed Patches

In order to identify that a patch has been explicitly installed, several criteria must be met.

- The patch must include a registry key that gets written to the machine on which it will be installed.

  Some types of patches do not write registry keys to the system on which they're being installed. Since there is no explicit indication that the patch has been applied, it cannot be determined that the patch was specifically installed at any point in time. To ensure that these systems are up to date, run a scan against the system and ensure that there are no patches that appear as 'Patch Missing.'

  If Ivanti Patch for Windows® Servers deploys the patch, however, it will write its own registry key to the remote system. This data is encrypted to prevent tampering. So, even if the patch doesn't normally write a registry key during deployment (SQL Patches, Office patches, etc), Ivanti Patch for Windows® Servers will write a registry key that is then read by the scanner during the assessment phase. The application can read that all these patches are installed, what account was used to install the application, and when the patch was installed. This information is displayed on the patch details panel as well as a mouse over on 'Patch Found' text in the patch summary pane.
- The registry key must exist on the system being scanned.
- All the files in the patch (as defined by the XML file) that were written to the remote system must be equal to or greater than the file versions recorded in the XML file. If any of the file versions on the remote system are below what is expected, the patch is considered not installed even if the registry key is present.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Identifying Effectively Installed Patches

Ivanti Patch for Windows® Servers can also scan for 'effectively installed patches.' A common case is when you install a single patch that replaces other patches. In this circumstance, the patches that were not installed but that have been replaced by the newer patch are considered effectively installed since you have at least the expected file version or greater for each of the files. For example, suppose you install a new Windows machine and then install a patch that replaces 20 earlier patches. While you've only 'installed' one patch, you've effectively installed 20 other patches.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Patch Scanning Overview

Ivanti Patch for Windows® Servers allows you to perform a patch scan via a few simple mouse clicks. From one management console you can initiate a patch scan of a single machine or of many machines.

Scans Are Performed As Background Tasks

All patch scans are performed as background tasks using the services of the Operations Monitor. This means you can initiate a scan and then move on to other concurrent work within Ivanti Patch for Windows® Servers without having to wait for the scan to complete. This also means you can have multiple patch scans active at the same time.

Scanning Considerations

- Is there a practical limit to the number of scans you can have active at the same time?

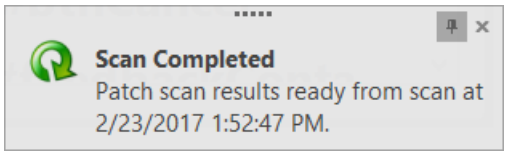
  Yes. It is dependent on the CPU and memory size of the console machine. It is also dependent on the number of other tasks currently active (for example, other patch downloads, patch deployments, etc.). While there is no exact answer, you'll know you've reached a practical limit if Ivanti Patch for Windows® Servers starts responding slowly.

- Is there a problem if the same machine is included in two or more concurrent scans?

  No. Multiple scanning tasks can be performed on a target machine at the same time.

- If I minimize the Operation Monitor window, how will I know when the scan is complete?

  A notification dialog box is displayed in the lower-right corner whenever a scan completes. The dialog box will be displayed for several seconds before slowly fading away. You can pin the dialog box in place by clicking the pin icon.

- Will I still be able to immediately view scan results?

  Yes. You can either click the **View results** link within the Operations Monitor or you can select the scan from within the Today's Items list of the **Patch Results** pane.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Patch Scanning Prerequisites

The following criteria must be met to ensure a successful patch scan:

When scanning your local (console) machine

- You must be an administrator on your local machine.
- Credentials must be provided for the local machine. See Supplying Credentials for details.
- The machine must be capable of obtaining the patch database XML file, either from a location on the Internet (via http or https) or from another specified location (either on the local machine or from a specified network location).
- The local machine's Workstation service must be started.

> The Server service is not required to be started on the local machine.

When scanning a remote machine, you must meet all the requirements for the local scan above, plus the following:

- You must have local administrative rights on the remote machine and be able to logon to this machine from the workstation performing the scan.
- Credentials must be provided for the target machines. See Supplying Credentials for details.
- The credentials you supply must have access to the control panel on the target machine. If control panel access is disabled through group policy, Ivanti Patch for Windows® Servers will be unable to connect to the target machine.
- File and Print Sharing must be enabled.
- The NetBIOS (tcp139) or Direct Host (tcp445) ports must be accessible on the remote machine.
- The remote machine must be running the Server service.

> The Workstation service is not required to be started on the remote machine.

- The remote machine must be running the Remote Registry service.

> The remote registry service is disabled by default on Windows Vista machines. You must enable the remote registry service (either manually or via group policy) before performing remote scans of Windows Vista machines.

- The %systemroot% share (usually C$ or similar) must be accessible on the remote machine.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- For machines using Windows operating systems that employ the use of User Account Control (this includes Windows Vista or later and Windows Server 2008 or later), you must either:
  - Join the machines to a domain and then perform the scan using domain administrator credentials, or
  - If you are not using the built-in Administrator account on the remote machines (and using that account is NOT recommended), you must disable User Account Control (UAC) remote restrictions on the machines. To do this:

1. Click **Start**, click **Run**, type **regedit**, and then press **Enter**.
2. Locate and then click the following registry subkey:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
3. If the **LocalAccountTokenFilterPolicy** registry entry does not exist, follow these steps:

   a. On the **Edit** menu, point to **New**, and then click **DWORD Value**.

   b. Type **LocalAccountTokenFilterPolicy** and then press **Enter**.
4. Right-click **LocalAccountTokenFilterPolicy** and then click **OK**.
5. In the **Value data** box, type **1**, and then click **OK**.
6. Exit Registry Editor.

   For more details on disabling UAC remote restrictions, see http://support.microsoft.com/kb/951016

Special note regarding Simple File Sharing

When Simple File Sharing is enabled, remote administration and remote registry editing does not work as expected from a remote computer and connections to administrative shares (such as C$) do not work because all remote users authenticate as *Guest*. Guest accounts do not have administrative privileges.

On Windows XP Professional or later operating systems, go to the following Microsoft Knowledge Base article to learn more about this feature and how to disable Simple File Sharing:

http://support.microsoft.com/default.aspx?scid=kb;en-us;304040

If you are running Windows XP Home Edition, Simple File Sharing cannot be disabled (Microsoft states that it is as designed) so remote scanning will not work on this operating system.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How to Initiate a Patch Scan

A patch scan can be initiated from the home page, from a machine group, from a favorite, or from Machine View or Scan View.

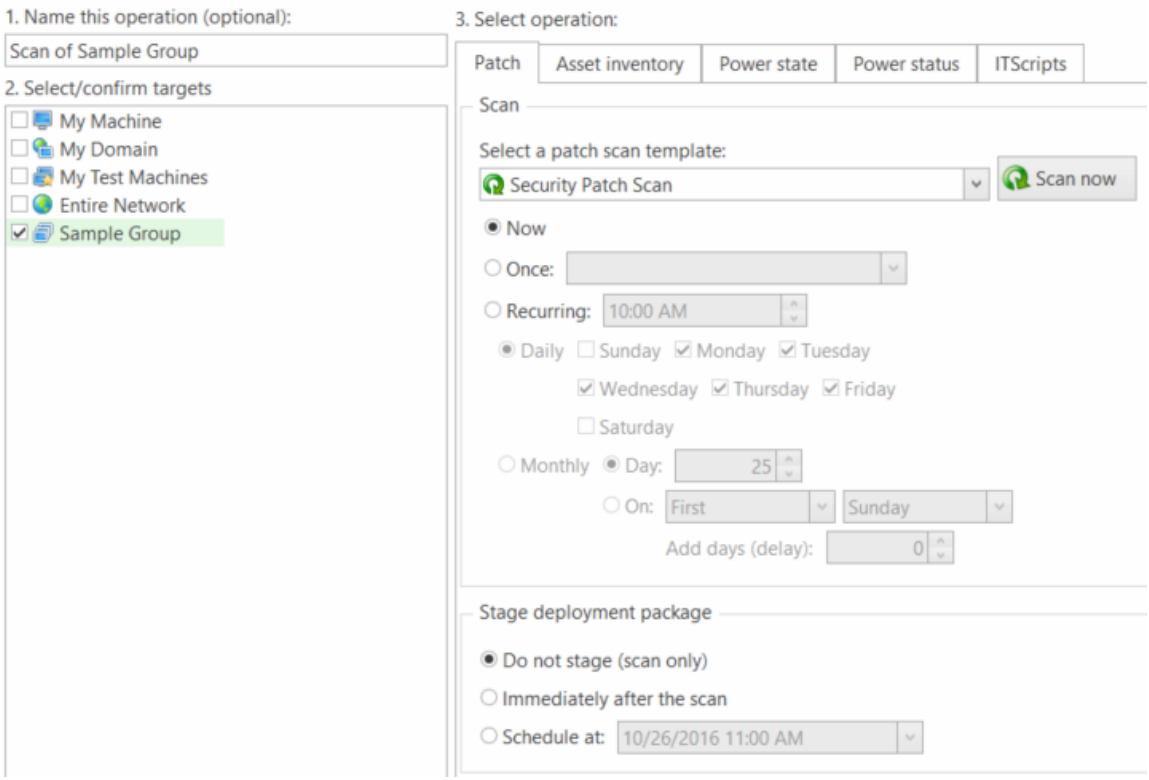
From the Home Page

You can use the home page to initiate a scan of any of the four pre-defined groups (**My Machine**, **My Domain**, **My Test Machines**, **Entire Network**) or of a custom machine group.

1. (Optional) Type a name for the operation you are about to perform (for example, *My machine scan mm/dd/yy*).

   A maximum of 100 characters can be used for the name.

2. Select the machine group you want to scan.



3. Select the template you want to use when performing the patch scan (Security Patch Scan, WUScan, or a custom patch scan template).
4. Choose when you want to perform the scan (**Now**, **Once**, or **Recurring**).
5. If you want to perform just a scan without automatically deploying any missing patches, choose **Do not stage (scan only)**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

For information on automatically staging and executing patch deployments, see Automatically Deploying Patches.

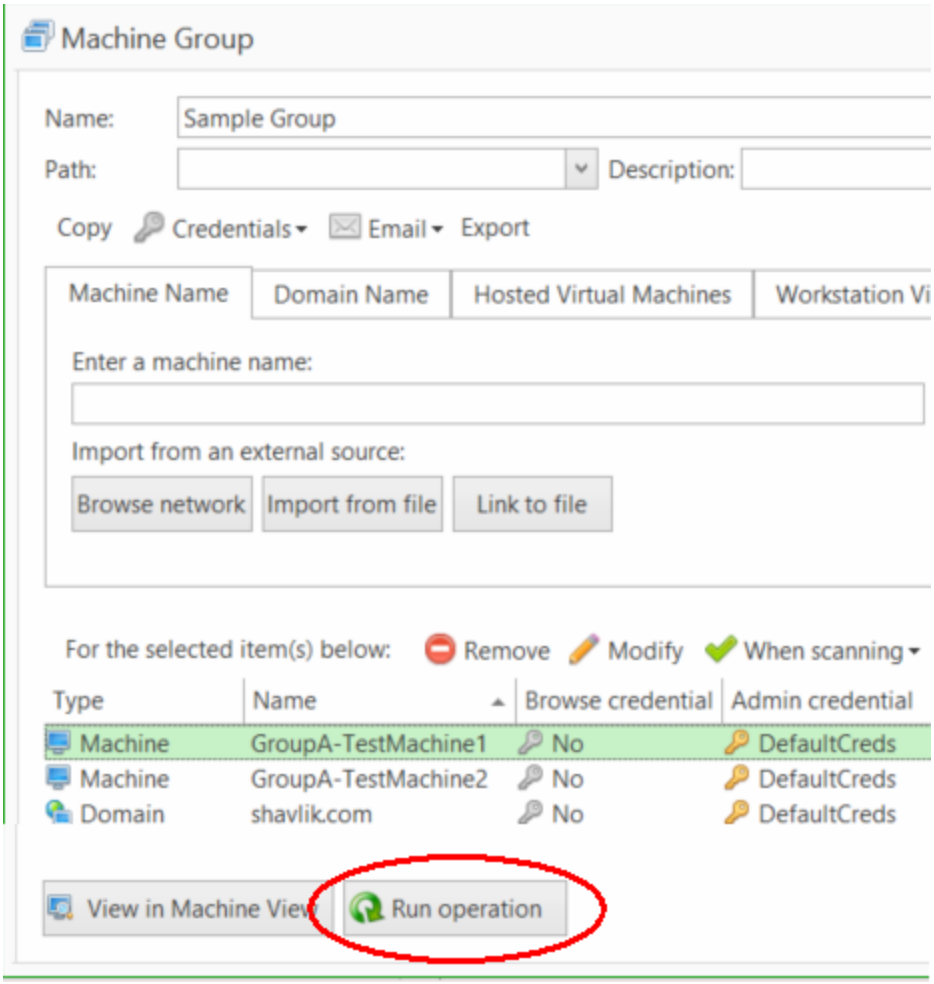
6. Click either **Scan Now** or **Schedule**.

   - **Scan now:** This is the button name if **Now** is your selected scheduling option. A scan of all machines in the machine group will begin immediately. The Operations Monitor is used to track the progress of the patch scan.
   - **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See Scheduling Patch Scans and Monitoring a Scheduled Patch Scan for more details.

From a Machine Group

1 In the **Machine Groups** list select the desired machine group.

2. Within the machine group dialog click **Run Operation**.



3. On the **Run Operation** dialog select when you want the scan to run and which patch scan template you want to use.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

4. If you want to perform just a scan without automatically deploying any missing patches, choose **Do not stage (scan only)**.

   For information on automatically staging and executing patch deployments, see Automatically Deploying Patches.

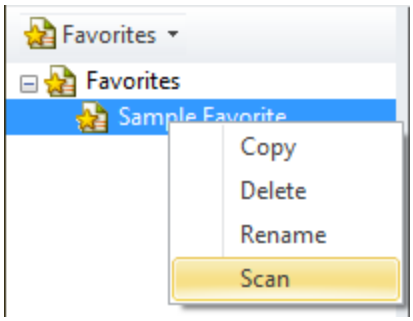
5. On the **Run Operation** dialog click either **Scan now** or **Schedule**.

   - **Scan now:** This is the button name if **Now** is your selected scheduling option. A scan of all machines in the machine group will begin immediately. The Operations Monitor is used to track the progress of the patch scan.
   - **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See Scheduling Patch Scans and Monitoring a Scheduled Patch Scan for more details.

From a Favorite

A favorite consists of one or more machine groups and one template. You select the machine groups you want to scan and then specify the template to use when performing the scan.

The quickest way to initiate a patch scan of a favorite is to right-click the favorite in the **Favorites** list and then select **Scan**. This will enable you to specify when to perform the scan but not how (the patch scan template specified in the favorite will always be used).



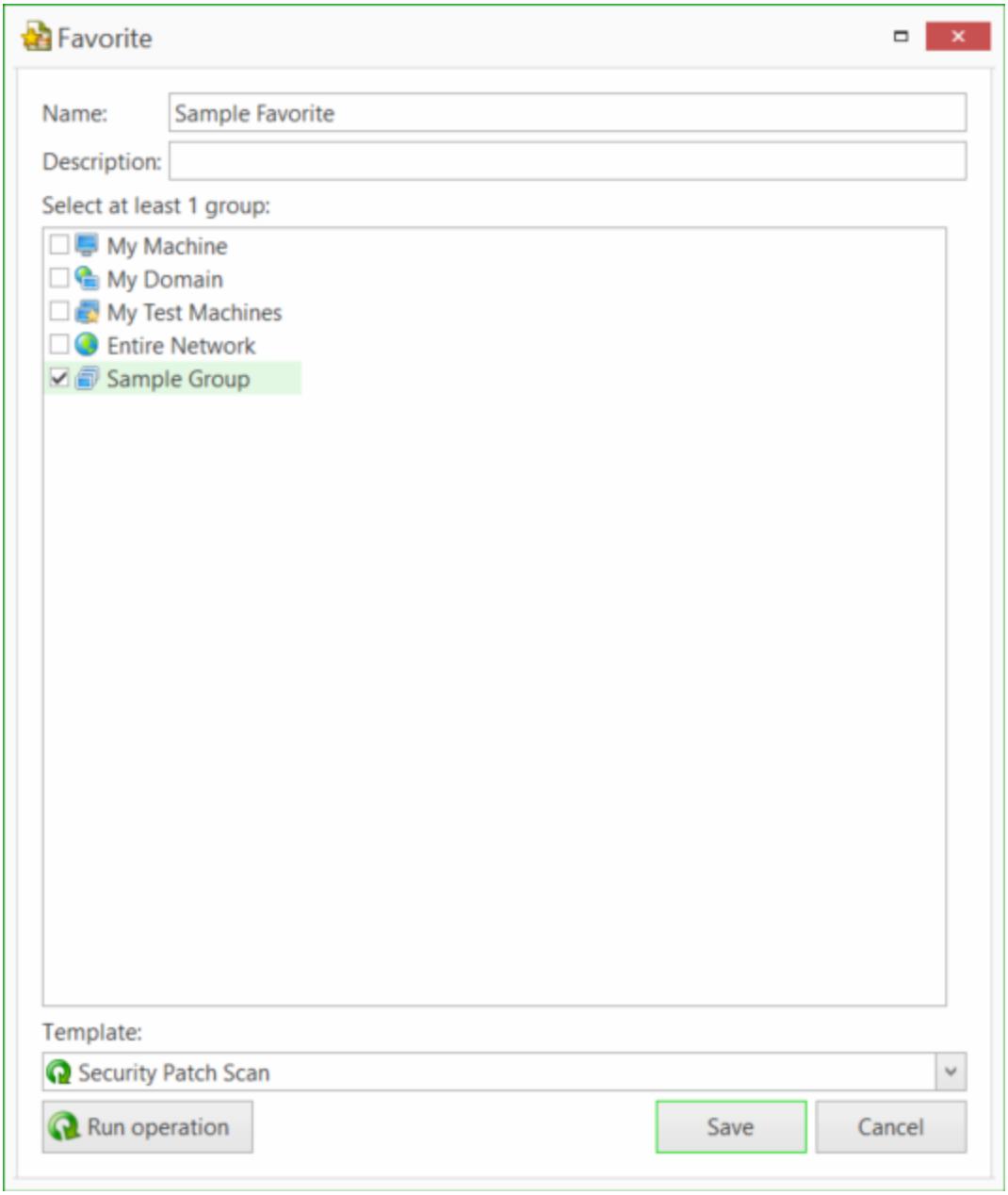
If you want to verify the configuration of the favorite before you initiate the scan you simply:

1 Select the desired favorite in the **Favorites** list.

   The **Favorite** dialog is displayed. It shows the current configuration of the favorite.

2. Verify the configuration and then click **Run Operation**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

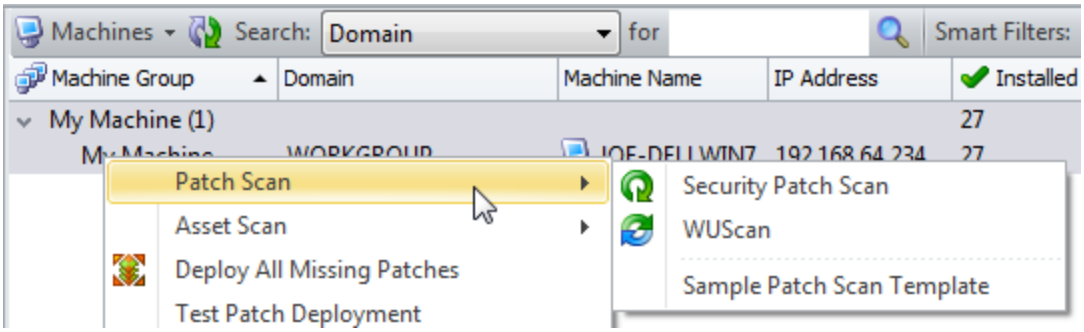


From Machine View or Scan View

1 Select one or more machines.

2. Right-click the machine(s) and then select the desired patch scan template.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



From the API

For information, see Using the API Feature.

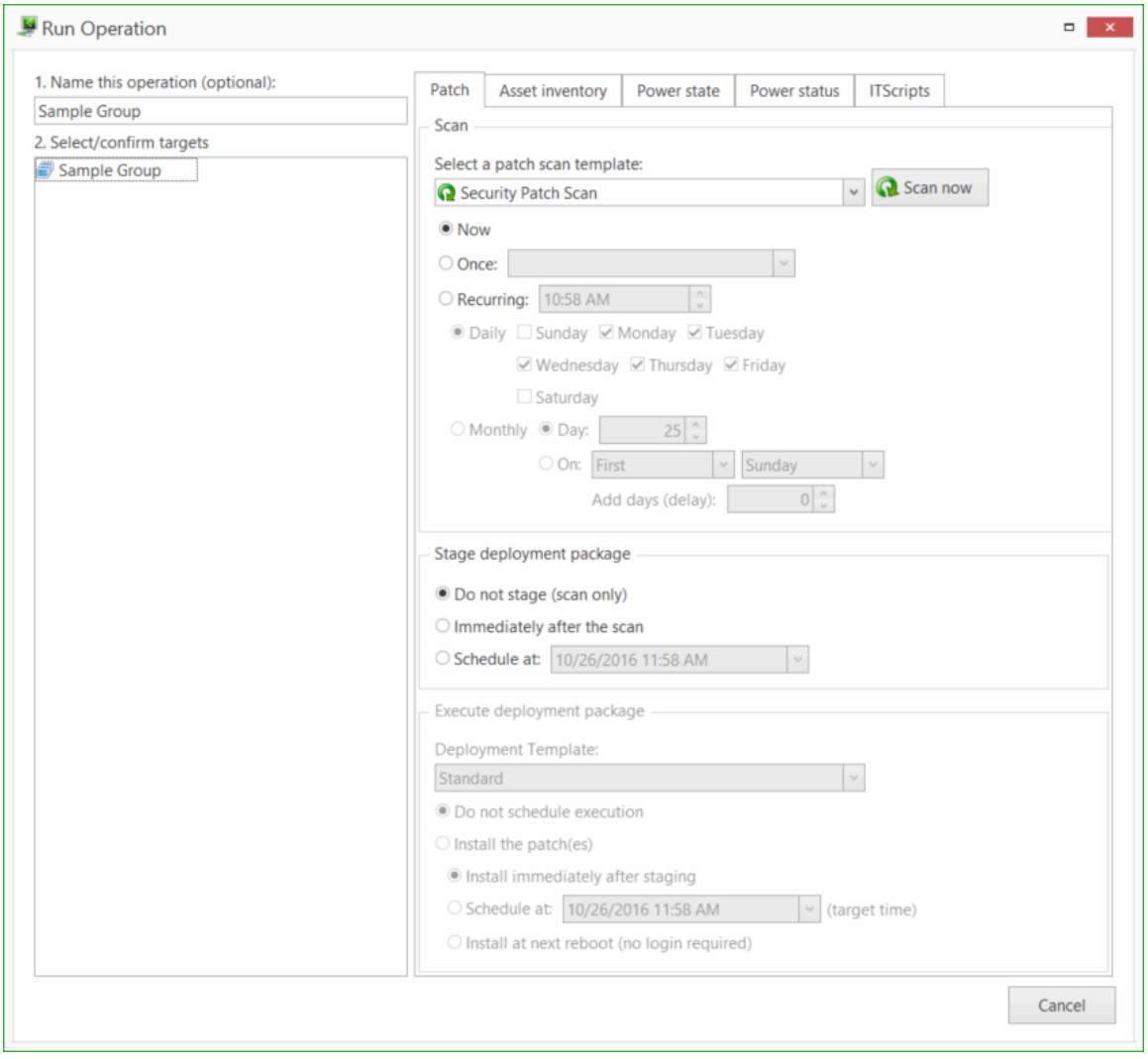
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Scheduling Patch Scans Using the Run Operation Dialog

This dialog may also be used to schedule asset operations , power tasks and ITScript operations.

When you initiate a patch operation from a machine group, from a favorite, or from Machine View, the **Run Operation** dialog is displayed. This dialog enables you to specify if the operation should run now or be scheduled for a future time or date. You can also specify if you want to automatically stage and deploy any missing patches detected by the scan.

Make sure you assign credentials for all machines involved in the scheduled scan.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

1. Name this operation	Enables you to provide a unique name for the operation. By default the name of the machine group or favorite used to initiate the operation will be used. The name is displayed in several locations: Scheduled Task Manager, Operations Monitor, the Results pane, the Scan View scan summary, and in Manage Items.
2. Select/confirm targets	This list is a reminder of the machine group(s) that will be affected by the operation. If the wrong group is listed, click **Cancel** and re-initiate the operation using the correct group.
Select a patch scan template	Select the template you want to use when performing the patch scan (Security Patch Scan, WUScan, or a custom patch scan template).
Select schedule	There are three scheduling options: • **Now** runs the operation as soon as the **Scan now** or **Run** button is clicked. • **Once** indicates that the operation will be run once at the day and time selected. • **Recurring** allows an administrator to regularly schedule operations at a specific time and using a specified recurrence pattern. For example, using this option, an operation could be run every night at midnight, or every Saturday at 9 PM, every weekday at 11 PM, or at any other user selected time and interval. You can also use the **Recurring** option to schedule an operation in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly patch scan to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by one day.
Stage deployment package	This area enables you to choose if you want to automatically stage a deployment package following the scan. • If you only want to perform a scan, choose **Do not stage (scan only)**. • If you want to automatically stage a deployment package for any patches that are detected as missing by the scan, choose either **Immediately after the scan** or **Schedule at**. The staging process includes creating the deployment package and copying the package to the target machine. For information on automatically staging and executing patch deployments, see Automatically Deploying Patches.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

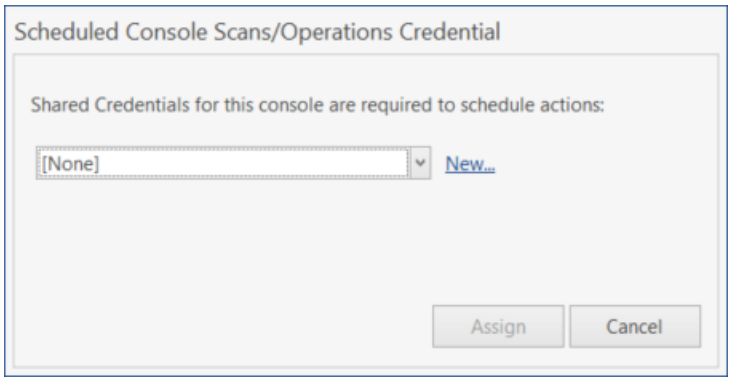
Execute deployment package	This area enables you to specify if and when a deployment package should be executed on a target machine. This area is not available if **Do not stage (scan only)** is selected. For more information, see Automatically Deploying Patches.

When the desired options are selected, click **Scan now** or **Run** (if **Now** is selected) or **Schedule** (if **Once** or **Recurring** is selected).

- **Scan now/Run:** The operation is initiated immediately and the **Operations Monitor** is displayed.
- **Schedule:** The scan operation is scheduled on the console machine. See Monitoring a Scheduled Patch Scan for details.

  If scheduled credentials are not currently assigned the **Scheduled Console Scans/Operations Credential** dialog is displayed. You must assign a shared credential to perform a schedule action. You can use the **Set scheduler credential** button on the **Scheduled Console Tasks** dialog to view and modify which credential is being used as the scheduler credential.

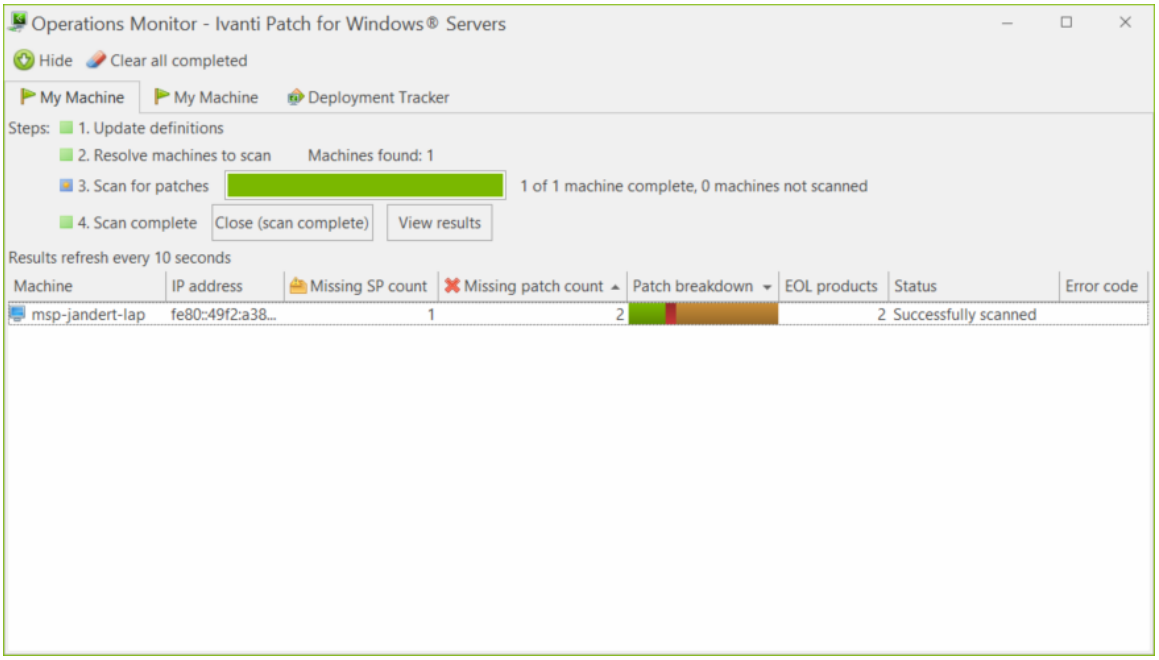
  The scheduled credentials are only used to schedule the operation on the console machine. The scheduled credentials are (typically) different from the machine-level credentials that are used to perform the actual operations on the target machines.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Monitoring a Patch Scan

The Operations Monitor is automatically displayed whenever a patch scan is initiated. It shows the steps involved in the patch scanning process and the progress of each step.



When the patch scan process is complete you can:

- View the patch scan results by clicking **View results**. The current patch scan tab will be removed from the Operations Monitor, the Operations Monitor will be closed, and the scan results will be displayed. See Accessing Patch Scan Results for details.
- Remove the current patch scan tab by clicking **Close (scan is complete)**. Any other tabs on the Operations Monitor will remain open.
- Minimize the Operations Monitor by clicking **Hide**. No tabs are removed from the Operations Monitor.
- Remove the current tab and all other tabs by clicking **Clear All Completed**.
- View summary information about each machine that was scanned. Right-click on a column heading and select **Column Chooser** to add or remove columns from the display.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Monitoring a Scheduled Patch Scan

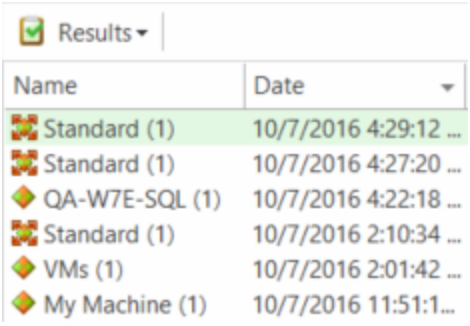
When you click **Schedule** on either the home page or the **Run Operation** dialog, a scheduled task is created on the console that will launch the scan at the appointed day and time. To view the scheduled task, select **Manage > Scheduled Console Tasks**.

The Scheduled Console Tasks Manager uses the services of the Microsoft Task Scheduler to schedule and initiate each task. If you prefer, you can view the tasks within the Microsoft Scheduler by accessing the **Task Scheduler** dialog on your Windows console machine and then expanding the **Task Schedule Library > LANDESK > Protect** tree.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Scan History

Even after a series of scans, all of the results of prior scans are just a click away. The scans are recorded in the **Results** list in the navigation bar.



Additionally, you can get a complete list of available prior scans by selecting **Manage > Items** from the main menu.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Patch Options Menu

Additional scanning options can be set using the **Tools** > **Options** menu. See Patch Options for details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About Patch Scan Templates

Ivanti Patch for Windows® Servers comes with two predefined patch scan templates: **Security Patch Scan** and **WUScan**. While these templates are good for most scanning activities, some administrators desire a higher level of flexibility when scanning machines. To this end, Ivanti Patch for Windows® Servers includes the ability to create any number of custom scan templates granting you the means to completely customize the way that machines are scanned.

Patch scan templates enable you to:

- Scan a smaller or larger number of machines simultaneously
- Customize what is actually scanned for or ignored
- Specify which, if any, filters are used (you can filter by product, patch, patch type, or vendor severity level)
- Configure automatic email notifications

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Predefined Patch Scan Templates

Security Patch Scan and **WUScan** are the predefined patch scanning templates provided with Ivanti Patch for Windows® Servers. The predefined templates cannot be modified. Both predefined templates do the following:

- Perform patch scans
- Use data from the patch data XML file
- Report on all installed and missing patches

The primary differences between the templates are:

- **Security Patch Scan:** Scans for missing and installed security patches. This is the default scan template.
- **WUScan:** Scans for missing and installed security patches and non-security patches.

If the predefined templates are not adequate for your needs, you can create a new scan template.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

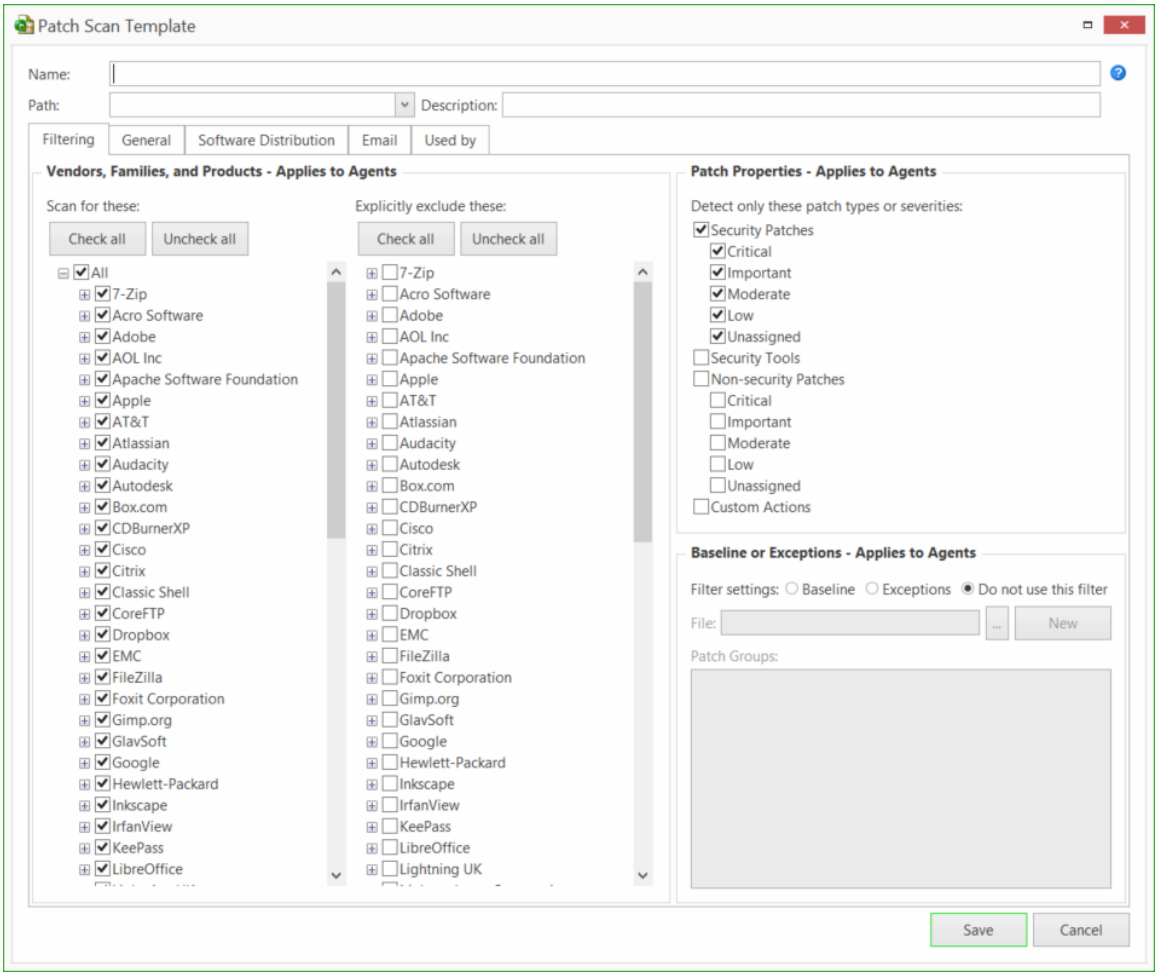
Creating or Editing a Patch Scan Template

To work with a patch scan template, do one of the following:

- To create a new scan template, click **New > Patch Scan Template**.
- To edit an existing scan template, in the **Patch Scan Templates** list in the navigation pane, click the patch scan template name.

This will display the **Patch Scan Template** dialog.

TIP: To speed the template creation process, copy an existing template that is similar to the one you want to create. The contents of the copied template will be populated in the new **Patch Scan Template** dialog and you can simply modify the appropriate items. You copy an existing template by right-clicking the template name in the **Patch Scan Templates** list and then selecting **Copy**.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

The Patch Scan Template dialog contains several tabs that collectively define the characteristics of a particular scan template.

Name	The name that you wish to assign to this scan template.
Path	This box is used to specify the folder path that this template will reside in within the **Patch Scan Templates** list in navigation pane. If you do not specify a path, the template will reside at the root level of the **My Patch Scan Templates** list. For more details, see Organizing Patch Scan Templates.
Description	A description of the template.
Filtering tab	There are three different filters available on this tab. • **Vendors, Families, and Products filter:** Scan for or exclude patches for the specified vendors, product families, and product versions. The items are presented in a hierarchical list. If you enable a check box at one level, all check boxes at lower levels are also enabled. If the same item is checked in both the **Scan for** and **Explicitly exclude** lists, the item will be excluded. TIP: If you want to exclude a small number of items, the recommendation is to include all items in the **Scan for** list and then use the **Explicitly exclude** list to exclude the desired items. This works because items in the **Explicitly exclude** list override items in the **Scan for** list. Another option is to use just the **Scan for** list and clear the check boxes of the items you want to exclude, but this is often more time consuming and prone to error. • **Patch Properties filter:** Specify the types of patches and the vendor severity level of those patches that should be included in the scan. The options are: • **Security Patches**: Security bulletin related patches. You can choose to scan for one or more specific severity levels. • **Critical:** Vulnerabilities that can be exploited by an unauthenticated remote attacker or vulnerabilities that break guest/host operating system isolation. The exploitation results in the compromise of confidentiality, integrity, availability user data, or processing resources without user interaction. Exploitation could be leveraged to propagate an Internet worm or execute arbitrary code between virtual machines and the host.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **Important:** Vulnerabilities whose exploitation results in the compromise of confidentiality, integrity, or availability of user data and processing resources. Such flaws could allow local users to gain privileges, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service.
- **Moderate:** Flaws where the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios could still lead to some compromise of the confidentiality, integrity, or availability of user data and processing resources. These are the types of vulnerabilities that could have had a critical impact or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations.
- **Low:** All other issues that have a security impact. Vulnerabilities where exploitation is believed to be extremely difficult, or where successful exploitation would have minimal impact.
- **Unassigned:** Security patches that have not been assigned a severity level.

- **Security Tools**: Updates for security tools such as Windows Defender and Windows Malicious Software Removal Tool. Also includes certificate updates and hotfixes for known security risks that are not yet fully supported by a security bulletin.
- **Non-security Patches**: Vendor patches that fix known software problems that are not security issues. You can choose to scan for one or more specific vendor severity levels. See **Security Patches** for a description of the available severity levels.
- **Custom Actions**: Enables you to perform custom actions even if you are already fully patched. It does this by scanning for a specific QNumber and patch (QSK2745, MSST-001) that will never be found. The process uses the temporary file *Nullpatch.exe*.

- **Baseline or Exceptions filter:** Use this filter to define either a baseline set of patches that should be included or a set of patches that should be excluded.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **Baseline:** Specify a patch list and/or one or more patch groups that collectively represent a baseline set of patches. The baseline is often determined by your corporate security policy and is considered the minimum set of patches that should be installed on your machines. The baseline is considered dynamic because, even though you only define it once on the template, you can continually update the patch list as new patches are made available. For an example of how you might use a baseline filter, see Implementing an Unattended Console Configuration.

  The **Vendors, Families, and Products** filter and the **Patch Properties** filter are unavailable when **Baseline** is selected. The **Software distribution** check box on the **Software Distribution** tab will also be ignored.

- **Exceptions:** Specify a patch list and/or one or more patch groups that contain patches that you always want to be excluded. The **Vendors, Families, and Products** filter and the **Patch Properties** filter will be applied first, and then the patches defined here will be excluded.

  Be careful when using the **Exceptions** filter. If you exclude a patch that replaces another patch, the program will now scan for the replaced patch. This is done on purpose to avoid any unintentional vulnerabilities. If the intended consequence of excluding a patch is to not automatically deploy it or the related patches, then all the patches in the chain of replaced patches must also be excluded.

- **Do not use this filter:** Disables this filter.

- **File:** Specify a text file that contains the list of patches you want to use as your baseline or that you want to exclude. To create a text file, click New. The text file must contain just the QNumbers associated with each patch, one entry per line. For an example text file, see Implementing an Unattended Console Configuration.

- **Patch group(s):** Specify one or more patch groups that contain the patches you want to use as your baseline or that you want to exclude.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

General tab	• **Scan For:** During the scanning process, you can choose to scan for just missing patches or for both missing and installed patches. When scanning for both missing and installed patches, you can include effectively installed patches in the results. These are patches that replace other patches. See Effectively Installed Patches and Determining Patch Replacements for more information. The following option applies only to the console, not to agents that may also be using this template. • **Global Thread Pool Override:** Specify if you want to override the **Global thread pool** setting on the **Tools > Options > Patch** dialog. You should only do this if you want to temporarily perform some bandwidth testing with your patch scans. The value you specify in the **Restrict scan to maximum number of threads** box defines the maximum number of machines that can be simultaneously scanned during one patch scan. The value specified is the actual limit; it is not multiplied by the number of logical CPUs on the console machine as is done on the **Tools > Options > Patch** dialog. You should clear the box when you have finished your testing.
Software Distribution tab	This tab enables you to specify if you want to scan for free third-party products that can be deployed by Ivanti Patch for Windows® Servers. If you enable the **Software distribution** check box, the available third-party products will be included in the **Patch Missing** list of the scan results. Use the vertical scroll bar to view the complete list of third-party products supported by Ivanti Patch for Windows® Servers. The products that will be displayed are those that are available for the operating system being used on the scanned machine. If you want to include or exclude reporting on a particular product, specify that product in the **Vendors, Families, and Products** filter on the **Filtering** tab.
Email tab	This tab applies only to agentless scans initiated from the console; it does not apply to agents that may also be using this template. This tab enables you to specify which reports should be automatically sent and to whom the reports should get sent. The specified reports will be sent when a scan using this template is completed. There are many different reports that can get sent. To understand what a particular report contains, click on the report in the list and view its description immediately below the list. To specify which reports should be automatically sent and to whom they should be sent:

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

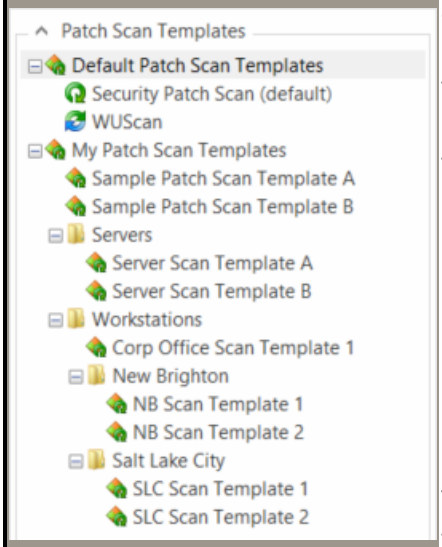
	New templates must be saved before you can perform these steps. 1. Select a report in the **Reports** list. 2. In the **Report Recipients** list, select the groups and/or individuals you want to email the report to. 3. Repeat Step 1 and Step 2 for each report you want to be automatically sent. 4. When finished, click **Save**.
Used by tab	This tab shows you the Favorites and agent policies that are currently using this scan template. This is important to know if you are considering modifying the template, as it tells you what other areas of the program are affected.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Organizing Patch Scan Templates

If you create many patch scan templates, you should consider organizing the templates into logical folders. Doing so will enable you to quickly locate and manage your templates. You can create as many folders and sub-folders as needed within the **My Patch Scan Templates** list in the navigation pane. For example, you might choose to organize your patch scan templates based on the type of machines that will be scanned, by location, by the vendors and products that will be scanned, etc.

Sample Organizational Scheme



To create a new folder, in the **Patch Scan Template** dialog, type a folder path into the **Path** box. You can specify as many folder levels as needed by using a backslash (\) to separate the levels in the name. The folder will be created when you save the template. If you do not specify a path, the template will be contained at the root level of the **My Patch Scan Templates** list.

Folder path examples:

- \Servers
- \Workstations
- \Workstations\Location A
- \Workstations\Location B

To assign a template to a different folder, do one of the following:

A patch scan template can only belong to one folder.

- In the **Patch Scan Template** dialog, type a new folder path into the **Path** box
- In the navigation pane, click and drag the template to a different folder
- Right-click the template and select **Edit path**.

To assign a folder and its contents to a different folder:

- Click and drag the folder to another existing folder.

The folder you move becomes a sub-folder.
To delete a folder, do one of the following:

- Change or remove the folder name in the **Path** box of all patch scan templates contained in that folder
- Click and drag the templates to a different folder

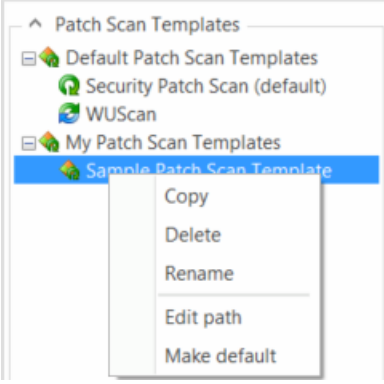
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• Delete all templates contained in the folder path The folder will be automatically deleted when the last template is removed from the folder.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Managing a Patch Scan Template

Custom patch scan templates are contained in the **My Patch Scan Templates** list in the navigation pane. You can edit an existing template by clicking the template name. You can also right-click a template and perform a number of different actions.



Copy	Enables you to create a new template by using the existing template as a base. The name of the new template will be 'Copy of { selected template name }'. Change the name and the other template characteristics as desired.
Delete	Deletes the current template. You cannot delete a template that is currently being used by an agent policy.
Rename	Enables you to change the name of the patch scan template. Be careful if you rename a template that is currently being used by an agent policy.
Edit path	Enables you to change which folder the template resides in within the navigation pane.
Make default	Sets the selected patch template as the default template.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Specifying a Default Patch Scan Template

To specify which patch scan template Ivanti Patch for Windows® Servers should use as the default, you can do one of the following:

- In the **Patch Scan Templates** list, right-click the template name and select **Make default**.
- Select **Tools > Options > Patch** and specify the default scan template in the **Default Patch Scan Template** box.

When you have identified a default template, the word **(default)** will be appended to the template name. The default template will be used for all one-click scanning operations on the home page.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About Patch View

Patch View is an extremely powerful and flexible tool. It is used to create custom patch groups that enable you to scan for a particular set of patches. Patch View also enables you to display detailed information about every product patch contained in the XML patch data file. It organizes the information so it is displayed in one comprehensive view, regardless of when the patches were released.

With Patch View you can:

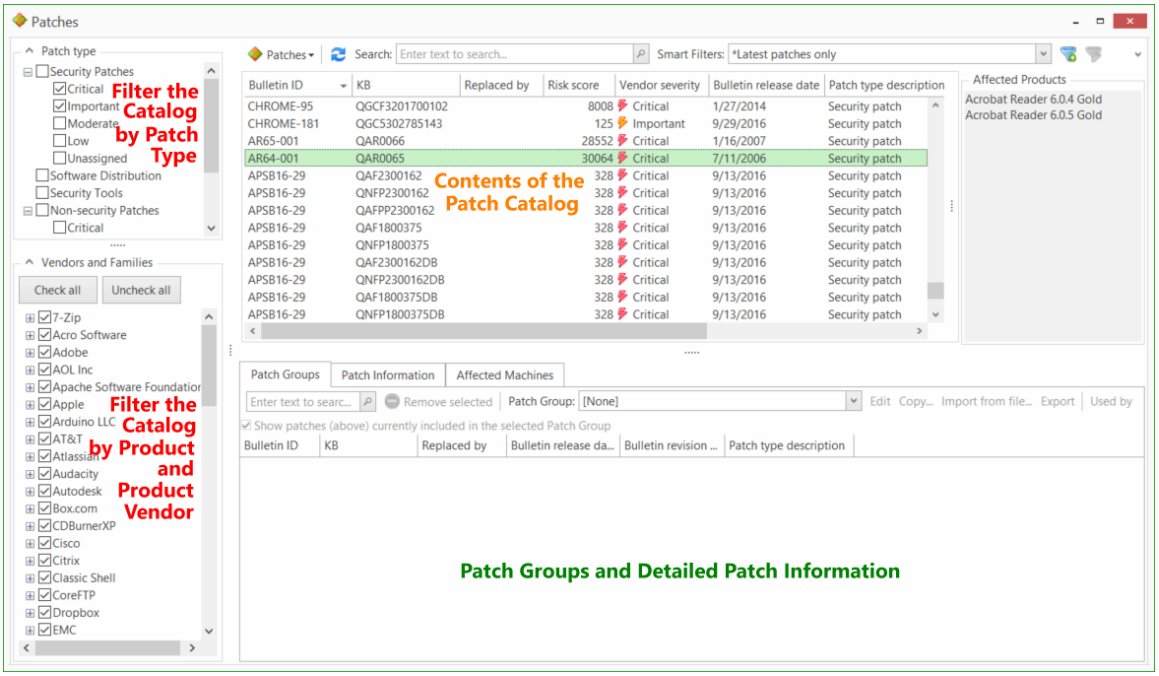
- Create and maintain patch groups
- Quickly and easily display the list of products supported and the associated patches with each product
- Display detailed information about any patch
- Filter the information and drill down into the table for a more detailed analysis
- Search for specific patches or patch components
- Perform actions on each patch
- Quickly determine which machines have a selected patch installed or are missing a selected patch

Patch View is accessed by selecting **View > Patches** or by creating a new patch group (**New > Patch Group**).

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Navigating Patch View

Patch View consists of several different panes. Each pane displays unique information and provides unique functionality.



- The two left-hand panes are used to filter the content in the patch catalog. They dictate what patch content is displayed in the top pane.
  - Filtering by Patch Type
  - Filtering by Product Vendor
- The top pane displays all patches in the patch catalog that are not filtered out by the two left-hand panes. You can apply additional filters, you can view information about individual patches and you can add patches to new or existing patch groups.
  - Searching Patch View
  - Filtering the Top Pane
  - Performing Actions on Patches
  - Customizing the Column Headers
- The bottom pane displays the contents of any patch groups that you have defined. It also displays detailed information about the patch selected in the top pane.
  - Creating and Editing Patch Groups

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- Viewing Patch Details
- Viewing Machines Affected by a Selected Patch
- Customizing the Column Headers

The top and bottom panes are interrelated in that the information presented in the bottom pane is dependent on what is selected in the top pane. This "top down" approach means you use the top pane to view high-level information and the bottom pane to drill down to more detailed information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Filtering Patch View by Patch Type

If nothing is selected in this filter, then nothing will be filtered out of the patch catalog and all patch types will be included in the top pane.

This filter is used to specify the types of patches, and the vendor severity levels of those patches, that should be displayed in the top pane. The options are:

- **Security Patches**: Security bulletin related patches. You can choose to include one or more specific severity levels. If a bulletin has multiple QNumbers with different severity levels, the most severe level will be shown. The specific states of each QNumber can be viewed by selecting the affected products in the **Patch Information** tab.
    - **Critical:** Vulnerabilities that can be exploited by an unauthenticated remote attacker or vulnerabilities that break guest/host operating system isolation. The exploitation results in the compromise of confidentiality, integrity, availability user data, or processing resources without user interaction. Exploitation could be leveraged to propagate an Internet worm or execute arbitrary code between virtual machines and the host.
    - **Important:** Vulnerabilities whose exploitation results in the compromise of confidentiality, integrity, or availability of user data and processing resources. Such flaws could allow local users to gain privileges, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service.
    - **Moderate:** Flaws where the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios could still lead to some compromise of the confidentiality, integrity, or availability of user data and processing resources. These are the types of vulnerabilities that could have had a critical impact or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations.
    - **Low:** All other issues that have a security impact. Vulnerabilities where exploitation is believed to be extremely difficult, or where successful exploitation would have minimal impact.
    - **Unassigned:** Security patches that have not been assigned a severity level.
- **Software Distribution**: Free third-party products that can be deployed by Ivanti Patch for Windows® Servers
- **Security Tools**: Updates for security tools such as Windows Defender and Windows Malicious Software Removal Tool. Also includes certificate updates and hotfixes for known security risks that are not yet fully supported by a security bulletin.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **Non-security Patches**: Vendor patches that fix known software problems that are not security issues. You can choose to include one or more specific vendor severity levels. See **Security Patches** for a description of the available severity levels.
- **Custom Actions**: Displays the null patch (MSST-001) that is used when performing a custom action.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Filtering Patch View by Product Vendor

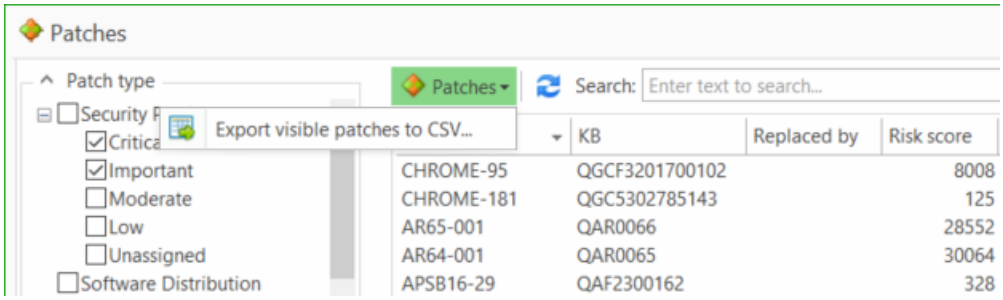
If nothing is selected in this filter, then nothing will be filtered out of the patch catalog and all vendors and products will be included in the top pane.

This filter is used to specify the product vendors that should be displayed in the top pane. You can expand each vendor tree to select individual products from a vendor.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Exporting Patches

The **Patches** menu enables you to export information about the patches contained in the top pane to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program.



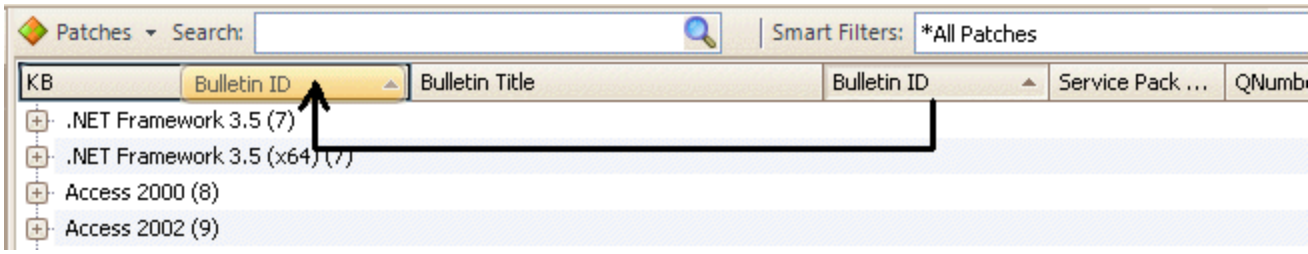
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Customizing the Patch View Column Headers

You can easily customize the way information is displayed within Patch View.

- You can reorder the columns by clicking and dragging the column headers to new locations.

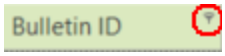
  For example, if you want Bulletin ID information to be displayed in the first column of the top pane, simply click on the Bulletin ID icon and drag it to the first column.



> TIP: When reordering columns, the column header you are moving will always be placed in front of the column you drag it to.

- You can apply filters to one or more column headers.

  Hover over a column header and then click the filter icon located in the upper-right corner. For example:

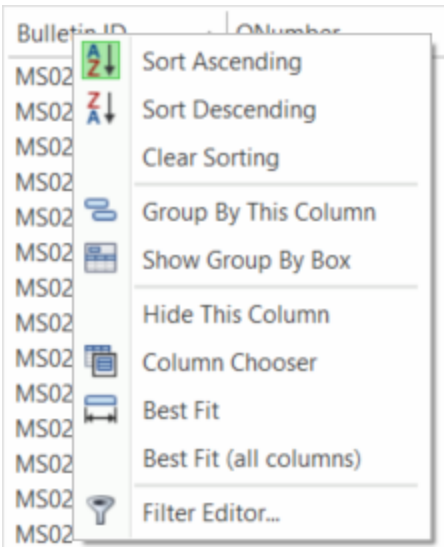


  Use the filter menu to select which of the values currently contained in the column should be displayed. When you apply a column filter, the filter definition will be displayed beneath the pane. You can use this to confirm which column filters have been applied to the current display, and you can edit the filter. For example:



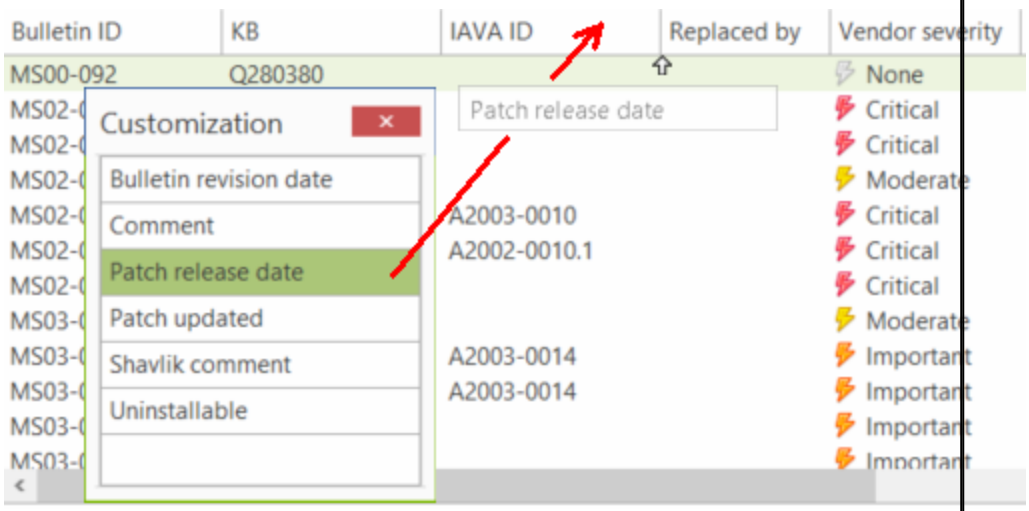
- You can right-click within a column header and perform a number of additional actions.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Sort Ascending	Sorts the selected column in ascending order. The table will be sorted first using the information in the first column and then by the column you selected.
Sort Descending	Sorts the selected column in descending order. The table will be sorted first using the information in the first column and then by the column you selected.
Clear Sorting	Clears the ascending or descending sorting criteria currently set for a column.
Group By This Column	Groups the table using the data in the selected column. It does this by moving the data into expandable lists that are located in the body of the grid. One expandable list will be created for each possible column value. If you perform this action on any subsequent columns, that data will be presented as nested groups at increasingly lower levels within the expandable lists. If **Show Group By Box** is enabled, this will also create a "Group By" box in the area immediately above the column headers. TIP: To turn off the **Group By This Column** feature and revert to the original view: Enable **Show Group By Box**, drag the Group By boxes back to the column header and then right-click in the column header and select **Hide Group By Box**.
Show Group By Box / Hide Group By Box	Displays or hides an area immediately above the column headers that contains "Group By" boxes. One "Group By" box will be displayed for each column header for which **Group By This Column** is currently enabled. You can also drag column headers to and from this area.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	The table will be grouped according to the data in the box. If there are two or more boxes then the grouping will be nested, with the left-most box presented at the highest level, the second box presented at the second level, etc.
Hide This Column	Removes the column from the table. You can add the column back to the table using the **Column Chooser**.
Column Chooser	Enables you to add and remove information from Patch View. When you select **Column Chooser** the **Customization** dialog is displayed. This dialog is used to store the columns you don't currently want displayed within the table. Simply click and drag the desired column headers from the table to the **Customization** dialog. For example, if you decide you want to add the **Patch release date** column to the table, simply drag that column header from the **Customization** dialog to the table.  If you decide you want an item back in the table, simply click and drag it from the Customization dialog back to the table.
Best Fit	Resize the width of the selected column so that the header text is displayed in the optimal amount of space.
Best Fit (all columns)	Resize the width of all columns in the table so that the header text is displayed in the optimal amount of space.
Filter Editor	The **Filter Editor** dialog will show any filters that are currently active in the column headers. You can use the editor to modify the existing filter criteria and to build new criteria using the available filter conditions and logical operators.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

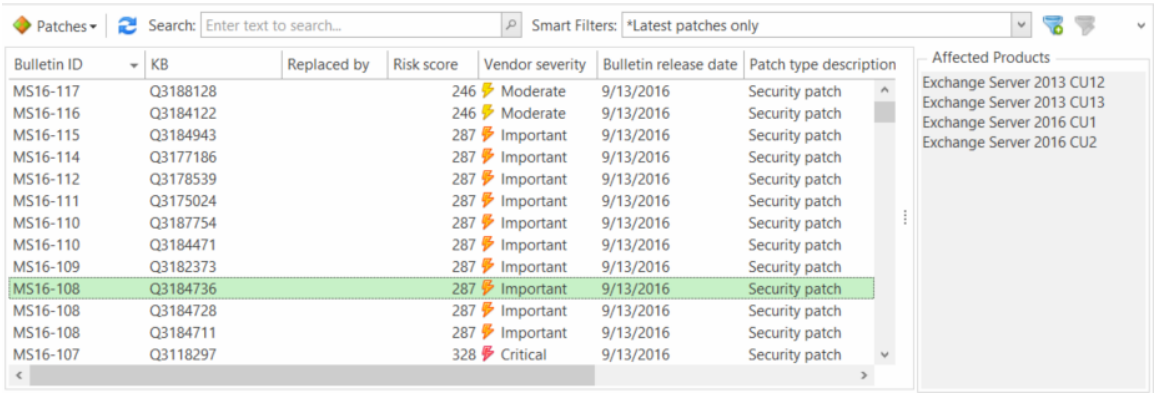
Understanding the Top Pane

The top pane in Patch View displays a table containing detailed information about each patch in the XML patch catalog. Click on a column heading to sort the table by that information. You can also specify what information is presented by right-clicking the table heading and selecting or clearing the available items.

By default the table is ordered by Bulletin ID. If you select a patch, information about that patch is displayed on the **Patch Information** tab of the bottom pane. Products affected by the selected patch are displayed in the **Affected Products** table that is located on the right side of the top pane.

No information is displayed on the **Patch Information** tab if you select a service pack (represented by SP1, SP2, etc. in the **KB** column). In addition, most products contain a unique entry whose **Service Pack Name** and **KB** are both **Gold**. These entries represent the "out of the box" base installation of a product, they contain no downloaded files, and are therefore neither a patch nor a service pack.

By default, service packs are not displayed in Patch View. To view service packs, select **Tools > Options** and on the **Display** tab enable the **Show Service Packs in View > Patches** check box.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Searching Patch View

You can easily search for specific patches contained in the top pane. All searches are performed using the Search tool.



To initiate a search you simply click in the Search box and then type the text you want to find. Only those patches matching the search criteria are displayed; all other patches are hidden.

Tips for Using the Search Tool

- The Search tool works only on the information currently visible in the top pane.
- If a Smart Filter is applied, only patches matching BOTH the search criteria and the smart filter criteria are displayed.
- All partial matches are displayed. For example, if you search for patches that contain the text *acrobat*, any patch with "acrobat" in its name will be considered a match (e.g. Acrobat Distiller, Acrobat Reader, etc.).
- A semicolon (;) can be used to concatenate multiple search terms into one search string. For example, specifying "chrome;firefox" will return all items containing either of the two terms.
- The use of wildcards in the Search tool is not allowed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Filtering Patch View

Information displayed in the top pane can easily be filtered to narrow the focus to only those patches of interest. One way to do this is by using the Smart Filter.



The Smart Filter initially contains several default filters. Default filters are identified by a leading asterisk. Default filters cannot be modified or deleted.

Another option is to apply filters to individual columns. For more information, see Customizing the Column Headers.

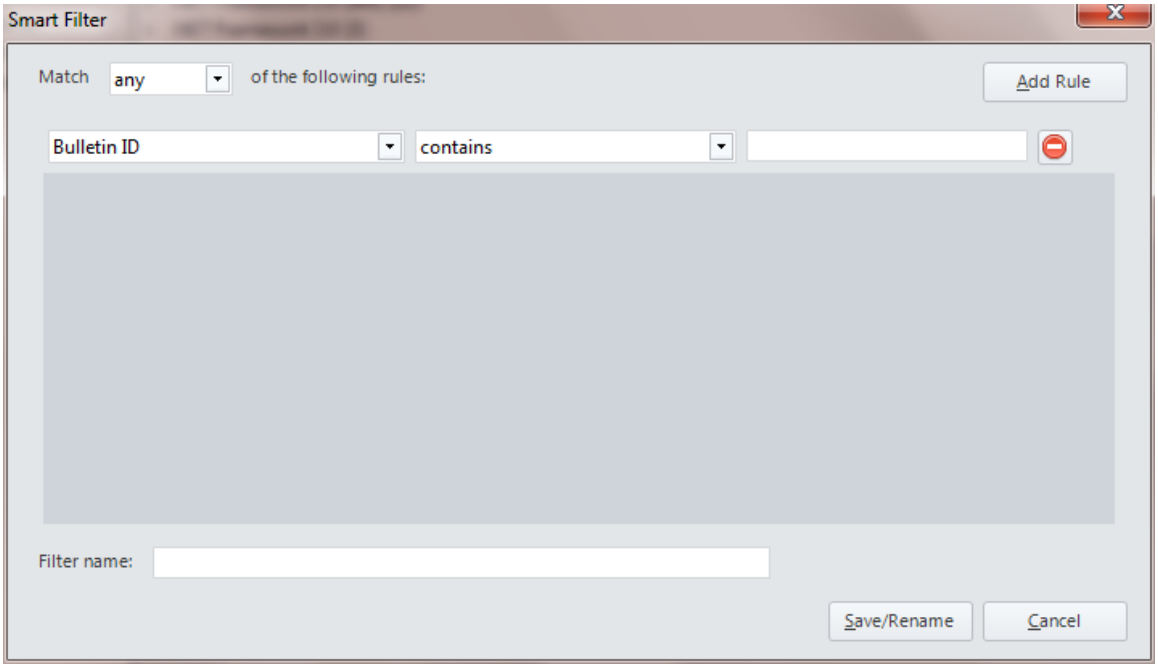
Custom Filters

You can create your own custom filters. This is a powerful tool that enables you to specify exactly which patches you want displayed in Patch View. Each custom filter is comprised of one or more rules. You can define as many rules in a filter as needed.

To create a new filter:

1. Click **New Smart Filter**.

   The **Smart Filter** dialog is displayed.



2. Specify which rules in the filter must be matched.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **All**: Only those patches that match all the rules in the filter will be displayed.
- **Any**: Patches that match at least one rule in the filter will be displayed.

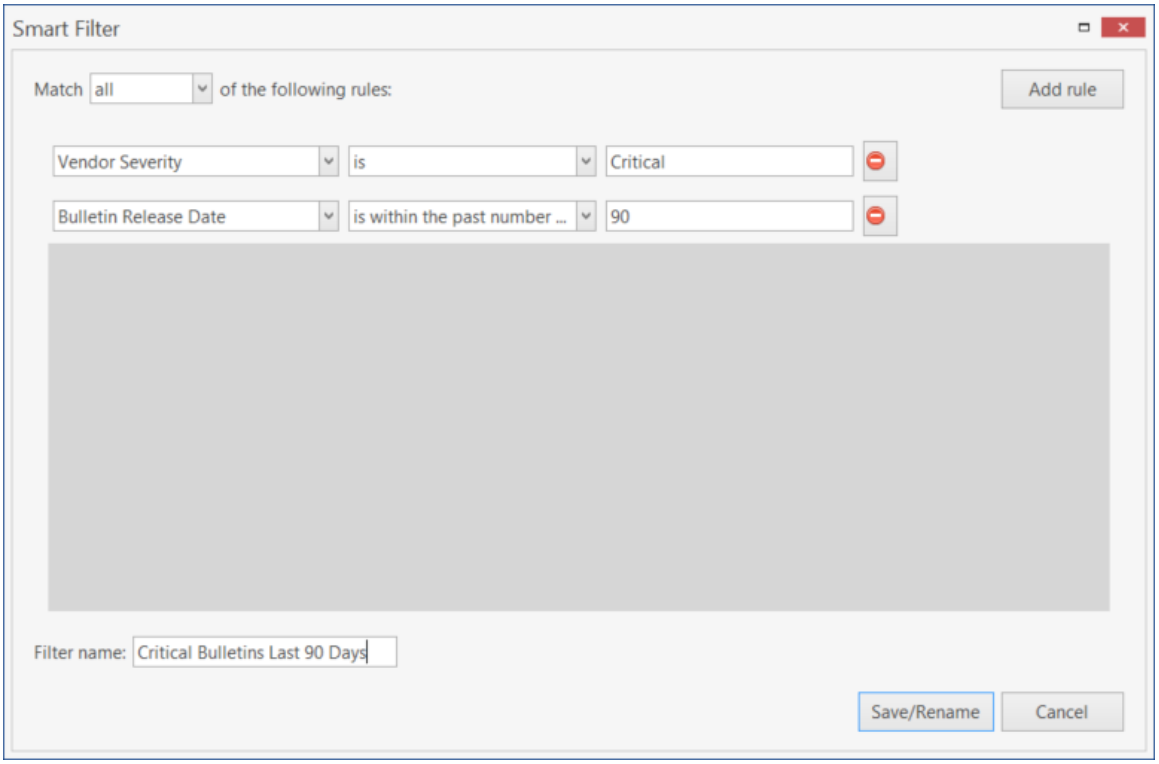
3. Define one or more rules.

   To define a rule, select an option in each of the first two logic boxes and then type the criteria in the third box. To add another rule simply click **Add Rule**.

4. Type a name for the filter.
5. When you are finished defining your custom filter, click **Save/Rename**.

Example

Assume you want to see a list of all critical bulletins that were released within the past 90 days. You simply create a filter similar to the following:

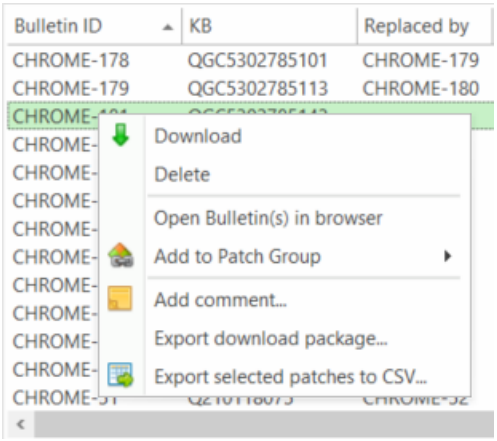


Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing Actions on Patches

Right-Click Menu

You can right-click on any patch or service pack in the top pane of Patch View and perform a number of different actions.



Download	Enables you to download the selected patches or service packs to the patch download directory. For more information on the download process, see Downloading Patches and Service Packs. The **Download** command is only available if the patch can be downloaded automatically. For more information see the description of the **Download method** column.
Delete	Enables you to delete the selected patches from the patch download directory. If the selected patches have never been downloaded, this command will be unavailable.
Open Bulletin(s) in Browser	Enables you to display, within your default Web browser, vendor information about the selected patch bulletin.
Add to Patch Group	Enables you to add the selected patches to a new or existing patch group. See Creating and Editing a Patch Group for more information.
Add Comment	Enables you to provide a comment about the patch.
Export download package	Export the location of the download packages for the selected patches to a Comma Separated Values (CSV) file.
Export selected patches to CSV	Export information about the selected patches to a CSV file. The CSV file can then be used within a spreadsheet program.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Keyboard Shortcuts

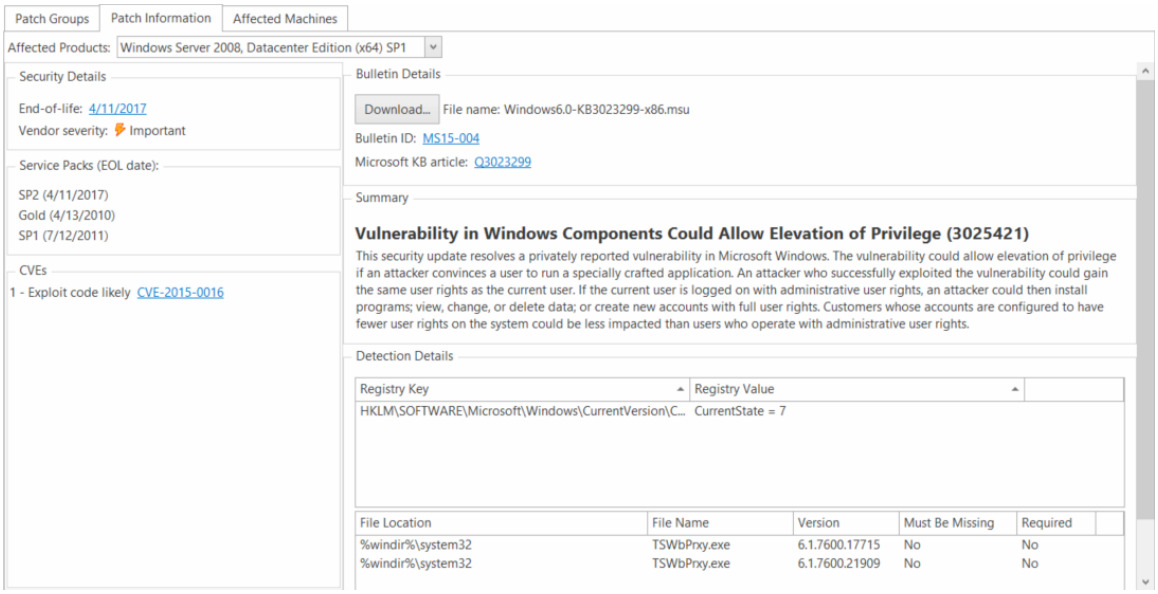
The following keyboard shortcuts are available:

- **Ctrl+A**: Selects all patches.
- **CTRL+click**: Multiple patches can be selected by holding down the CTRL key while selecting patches.
- **SHIFT+click**: A contiguous group of patches can be selected by holding down the SHIFT key while selecting the starting and ending patches in the list.
- **SHIFT+PAGE UP**: Selects a range of patches from the one currently selected to the top of the display. Each time you press **Page Up** an additional range of patches is added to the selection.
- **SHIFT+PAGE DOWN**: Selects a range of patches from the one currently selected to the bottom of the display. Each time you press **Page Dn** an additional range of patches is added to the selection.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Patch Details

The **Patch Information** tab in the bottom pane displays detailed information about the patch, service pack, or informational item selected in the top pane. Detailed information will not be displayed if multiple patch items are selected in the top pane.



Affected Products	For patches that affect multiple products, this box enables you to select a specific product and then view how the patch relates to that product.
End-of-life	Indicates the End Of Life date for the patch. You can click the link to view additional information.
Replaced by	If shown, indicates that the patch is replaced by another more recent patch.
Vendor Severity	Ivanti assigns one of four severity levels based on its perceived threat of the vulnerability related to the patch. (Red) Ivanti has deemed the problem associated with this patch to be **Critical** in nature. (Orange) Ivanti considers the problem related to this patch **Important** to correct.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	 (Yellow) The related vulnerability is of **Moderate** severity.  (Brown) While it poses a security risk, Ivanti deems that risk to be **Low**.
Service Packs (EOL date)	If shown, indicates that the patch is contained in one or more service packs. Also indicates the End Of Life (EOL) date for the service pack.
CVE number	Provides a cross reference to the Common Vulnerabilities and Exposures (CVE) database hosted by Mitre.org (CVEID).
Download	Enables you to download the patch to the patch download directory. When you click this button the **Patch Download Status** dialog is displayed. Use this dialog to select which language version of the patch you want to download. On the dialog, if the download icon is grayed out () it indicates the patch has not yet been downloaded. If the icon is green () it indicates the patch has already been downloaded and verified.
Bulletin ID	Provides a link to the Microsoft Security Bulletin article that describes the threat addressed by this patch.
Microsoft Knowledge Base Article	Provides a link to the associated Knowledge Base article that provide more information about the flaw.
Summary	Provides a concise description of the threat addressed by this patch. It identifies the product that is affected by this patch and describes how the product is vulnerable.
Comments	If shown, provides comments from Ivanti about this patch.
Registry Key table	Identifies the registry key information used to determine whether the product in question exists on the target machines. This table can be sorted by clicking within a column header.
File Location table	Shows the file criteria used for determining whether or not a patch is installed. This table can be sorted by clicking within a column header.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Machines Affected by a Selected Patch

The **AffectedMachines** tab in the bottom pane displays which of your managed machines are affected by the patch that is selected in the top pane. The listed machines will be in one of two lists:

- **Missing:** These machines are vulnerable to the threat corrected by the patch.
- **Installed:** These machines already contain the selected patch.

Managed machines that are not listed are not affected by the selected patch.



The **Affected Machines** table can be sorted and customized. See Customizing The Patch View Column Headers for more information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About Patch Groups

Ivanti Patch for Windows® Servers provides the ability to use a patch group to scan for a particular set of patches.

Example 1: Suppose Company A has a patch approval process under which they've certified four patches as being mandatory for their organization. They want to scan just for those four patches, receive compliance reports, and then be able to patch for those specific items. By creating a patch group, they can then scan for only those selected patches.

Example 2: Suppose you identify a certain patch as being critical for your organization. You can create a patch group with just this patch. When you create the group, you can browse patches from the list and select a product and service pack and then a patch. Ivanti Patch for Windows® Servers will scan for all instances of that QNumber, not just for the product and SP that you select. You can perform a scan using the patch group and a scan will be done just for the selected patch.

When scanning for the specified patches, the program will reference the **Tools > Options >Patch >Use replacement patches** setting to determine if patches that have been replaced should be included in the scan results.

When Ivanti Patch for Windows® Servers uses a patch group to scan for selected patches, it always scans for and reports on the status of all service packs.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating and Editing a Patch Group

You can create a new patch group or modify an existing group.

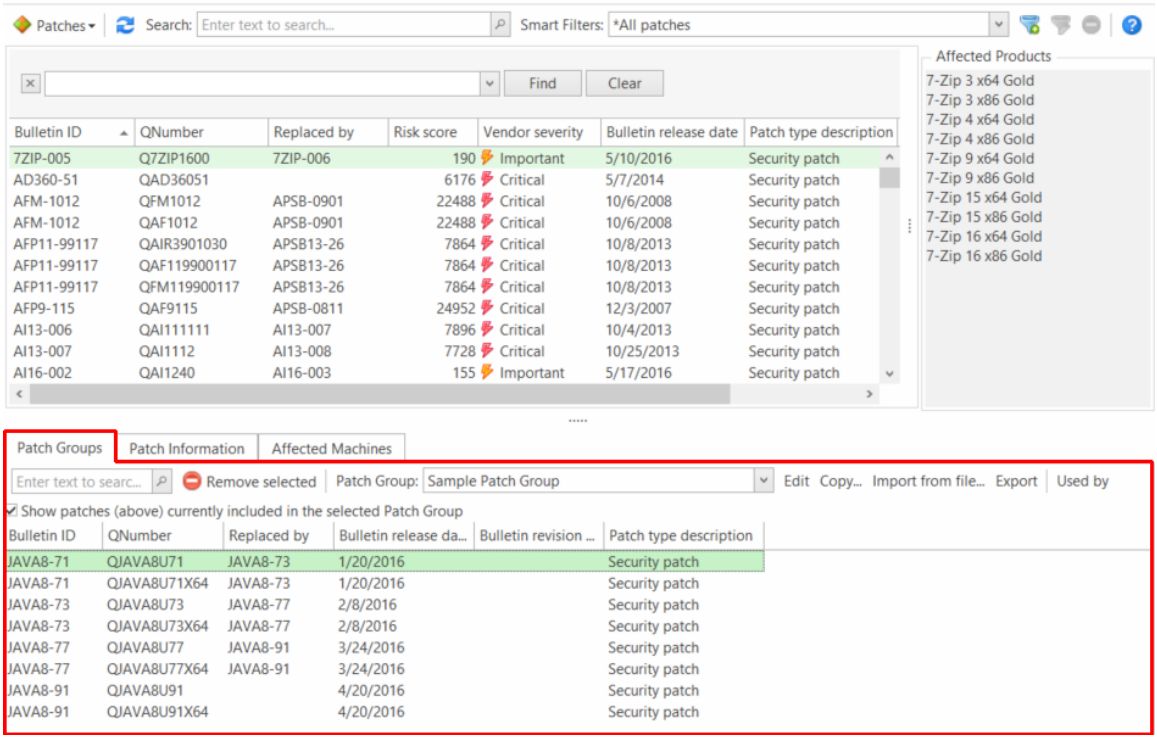
- To create a new patch group, click **New > Patch Group**.

  In the **New Patch Group** dialog, type a name that you would like to assign to this patch group, add a comment that describes the purpose of the group, and then click **Save**.

- To edit an existing patch group, in the **Patch Groups** list, click the patch group name.

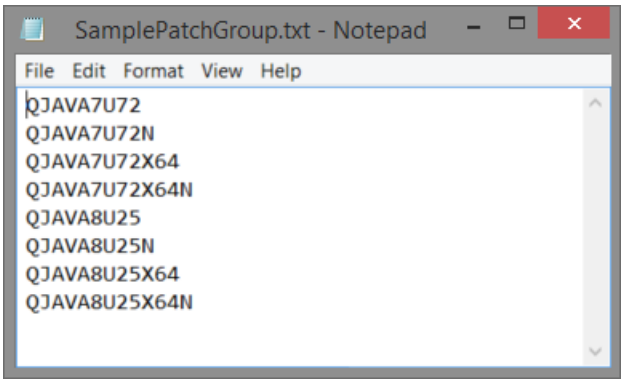
Be careful when editing an existing patch group. Any modifications you make will affect any scan template that references the patch group. Also, if you edit and save a patch group that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console.

The patch group will be displayed on the **Patch Groups** tab in the bottom pane of the **Patches** dialog (also known as Patch View). If this is a new patch group, the group will be empty.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing Actions on Patch Groups

How to add one or more patches to a patch group	There are several ways to add one or more patches to a patch group. You cannot add service packs to a patch group. You can, however, define separate service pack groups for use with agents. • In the top pane, right-click on the desired patch or patches, select **Add to patch group** and then choose a patch group name. For information on filtering the patches contained in the top pane, see Filtering Patch View by Patch Type, Filtering Patch View by Product Vendor, and Filtering Patch View. • You can import a list of patches from a text file. The text file might have been created from another patch group that you have previously exported, or it might be a file that you created manually using a program such as Notepad. The text file must contain just the KB numbers associated with each patch, one entry per line.  • You can also add to a patch group from Machine View or Scan View. Select the desired patches and then use the right-click menu to create a new patch group or to add to an existing patch group.
Search	Enables you to search for specific patches contained in a patch group. To initiate a search you simply click in the **Search** box and then type the text you want to find. Only those patches matching the search criteria are displayed; all other patches are hidden. Here are some tips for using the Search tool: • The Search tool works only on the information currently visible in the bottom pane. • All partial matches are displayed. • The use of wildcards in the Search tool is not allowed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

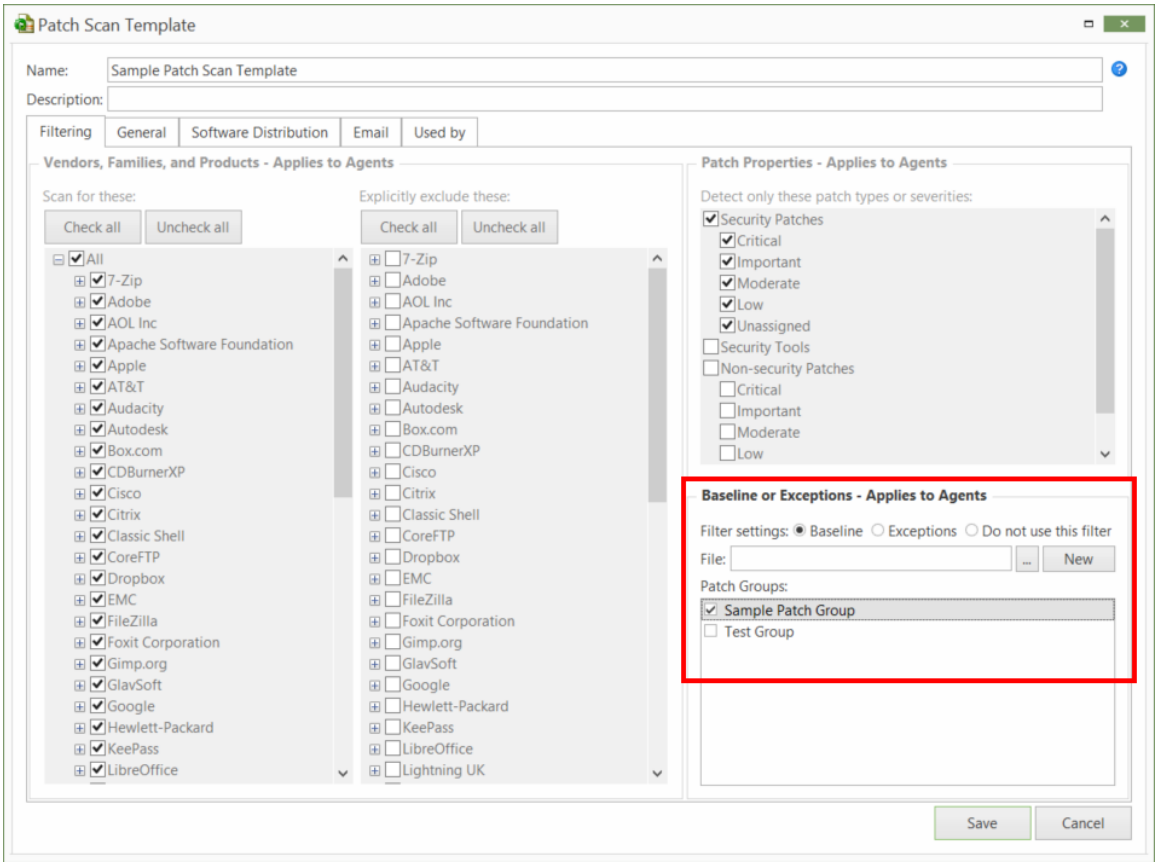
Remove selected	To remove one or more patches from the patch group, select the desired patches and then click **Remove selected**.
Patch group	Use this box to select the desired patch group.
Edit	Enables you to edit the name and description of the patch group.
Copy	Makes a copy of the patch group. Type a new name for the group and then click **Save**.
Import from file	You can import a list of patches from a previously created text file. For more information, see the section above titled **How to add one or more patches to a patch group**.
Export	Exports the selected patch group to a text file. This file can be imported into another patch group on the same console or on a different console.
Used By	This button shows you the patch scan templates and agent policies that are currently using this patch group. This is important to know if you are considering modifying the group, as it tells you what other areas of the program are affected.
Show patches (above) currently included in the selected Patch Group	If enabled, patches contained in the selected patch group will also be displayed in the Patch View list in the top pane. If you prefer not to view the same patches in both the Patch View list and the patch group list, then disable this check box.
How to delete a patch group	Patch groups can be deleted from the **Patch Groups** list using the right-click menu.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Using a Patch Group

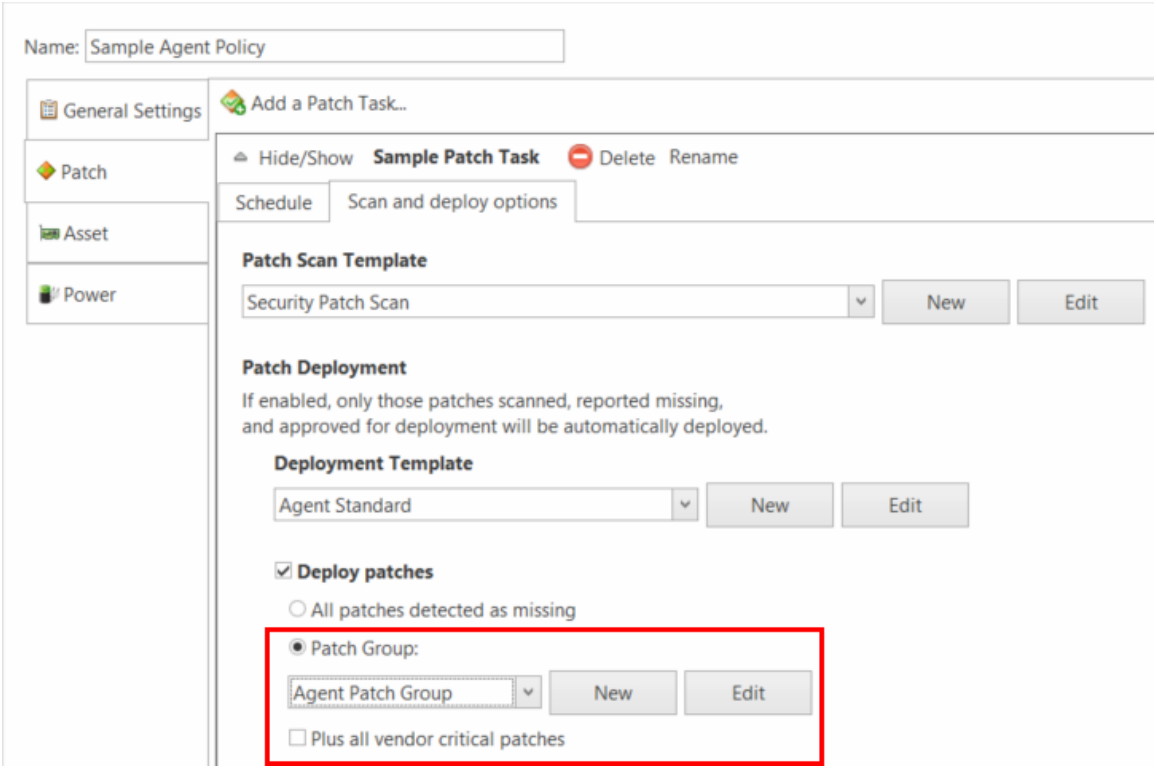
To use a patch group in a custom scan template:

1. In the **My Patch Scan Templates** list, click the desired custom patch scan template.
2. In the scan template, on the **Filtering** tab, select either **Baseline** or **Exceptions**.
3. In the **Patch Groups** box, select the patch group(s) that contain the patches you want to use as your baseline or that you want to exclude.



A patch group can also be used in an agent policy.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About Third-Party Applications

Ivanti Patch for Windows® Servers can scan for and deploy a number of free third-party applications, including:

- RealNetworks RealPlayer
- Mozilla Firefox
- Adobe Reader
- Apple QuickTime
- And more ...

To do this you simply scan your machines to identify the machines that are missing the third-party applications and then deploy the desired application(s) to the machines you specify. See How to Scan for Third-Party Applications and Deploying Third-Party Applications for more details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

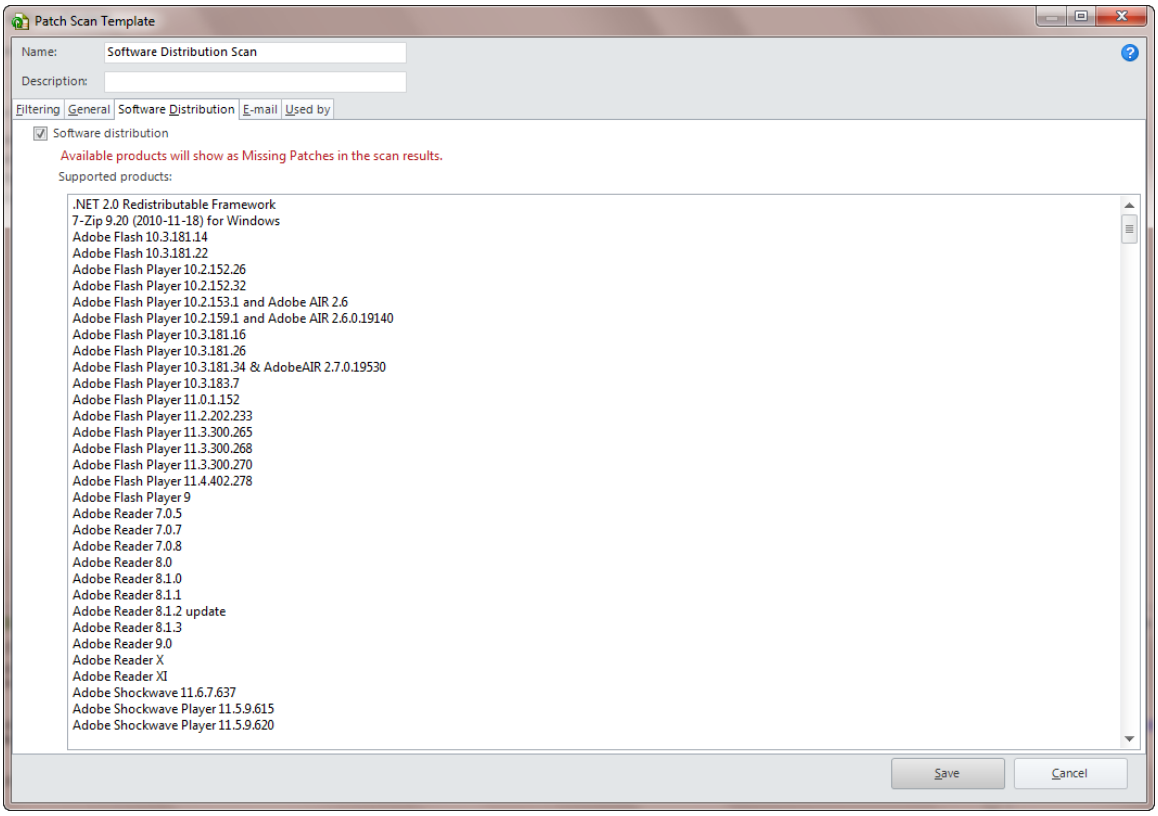
How to Scan for Third-Party Applications

This topic describes how to scan for third-party applications that you want to install on your target machines.

1. From the main menu click **New > Patch Scan Template**.

   The **Patch Scan Template** dialog appears.

2. In the **Name** box, type a name for this custom scan (for example, Software Distribution Scan).



3. On the **Software Distribution** tab, enable the **Software distribution** check box.
4. Click **Save**.
5. Initiate a scan using this new scan template.

   For example, you might click on the desired group in the **Machine Group** pane, select the new custom scan template in the **Scan with** box, and then click **Begin Scan**.

6. When the scan is complete, see Deploying Third-Party Applications for information on installing the applications.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

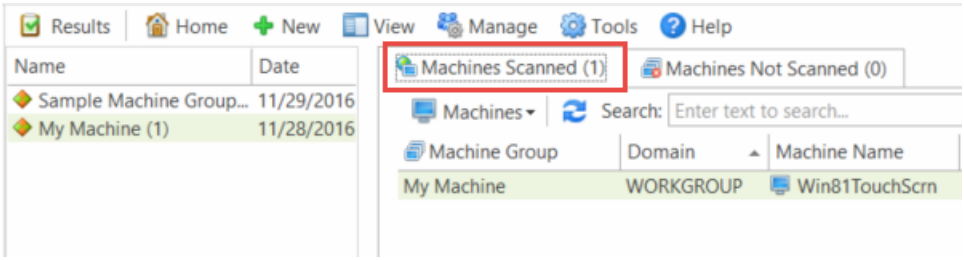
Accessing Patch Scan Results (Scan View)

Patch scan results are available immediately following a successful scan by clicking the **View results** link on the **Operations Monitor** dialog (see Monitoring a Patch Scan). The scan results are also available when you select a previous scan from the **Results** list in the navigation pane.

If scan results are not displayed it could be because the program's background services do not have the proper credentials to use when making a connection to the database. For more information see Performing a New Installation.

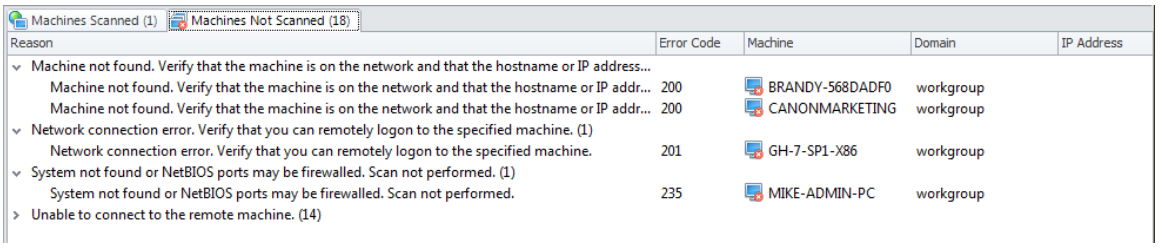
Machines Scanned

Machines that were successfully scanned will be included on the **Machines Scanned** tab. For information on understanding and using your patch scan results, see Navigating the Scan View Grid.



Machines Not Scanned

Any machines that the program was unable to scan will be contained on the **Machines Not Scanned** tab. There may be several reasons why a particular machine was not scanned. Error codes are provided that explain the reason for a particular failure. The error codes are described in greater detail in the knowledge base located here: http://community.shavlik.com/docs/DOC-2159.



TIP: You can generate a **Machines Not Scanned** report that will contain additional information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

You can right-click on a machine and perform a number of different actions. See Performing Actions on Machines for more details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Navigating the Scan View Grid

Patch scan results are presented in a Scan View grid that contains three separate panes. Each pane displays unique information and provides unique functionality. The panes are interrelated in that the information presented in a lower pane is dependent on what is selected in the pane directly above it. This "top down" approach means you use the top pane to view high-level information and the two lower panes to drill down to more detailed information.

While the two are extremely similar in look and feel, Scan View is different than Machine View. Scan View represents a point in time (the date and time the scan was performed) for the machines specified in the scan. Machine View, however, displays the most current information for all machines that have ever been scanned.

- The top pane displays all machines that were either successfully or unsuccessfully scanned. See the following topics for information on using the top pane:
  - Searching for Machines
  - Filtering Info in the Top Pane
  - Performing Actions on Machines
- The middle pane displays patch information about the machine(s) selected in the top pane. See the following topics for information on using the middle pane:
  - Viewing Scan Result Patch Summaries
  - Performing Actions on Patches
- The bottom pane displays detailed information about the patch selected in the middle pane. See the following topics for information on using the bottom pane:
  - Viewing Patch Details
  - Viewing Machines Affected by a Selected Patch

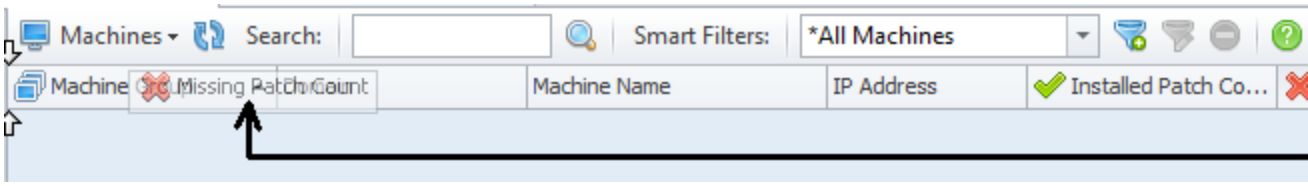
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Customizing the Column Headers

You can easily customize the way information is displayed within any of the panes in Machine View or Scan View.

- You can reorder the columns by clicking and dragging the column headers to new locations.

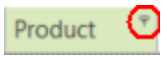
  For example, if you want missing patch information to be displayed in the first column of the top pane, simply click on the **Missing Patch Count** icon and drag it to the first column.



  TIP: When reordering columns, the column header you are moving will always be placed in front of the column you drag it to.

- You can apply filters to one or more column headers.

  Hover over a column header and then click the filter icon located in the upper-right corner. For example:

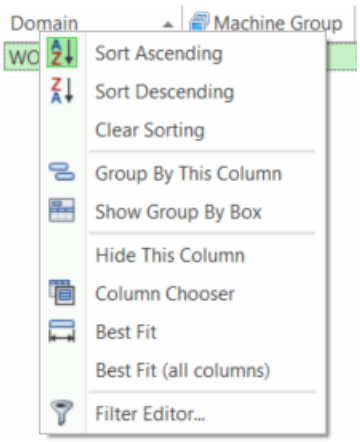


  Use the filter menu to select which of the values currently contained in the column should be displayed. When you apply a column filter, the filter definition will be displayed beneath the pane. You can use this to confirm which column filters have been applied to the current display, and you can edit the filter. For example:



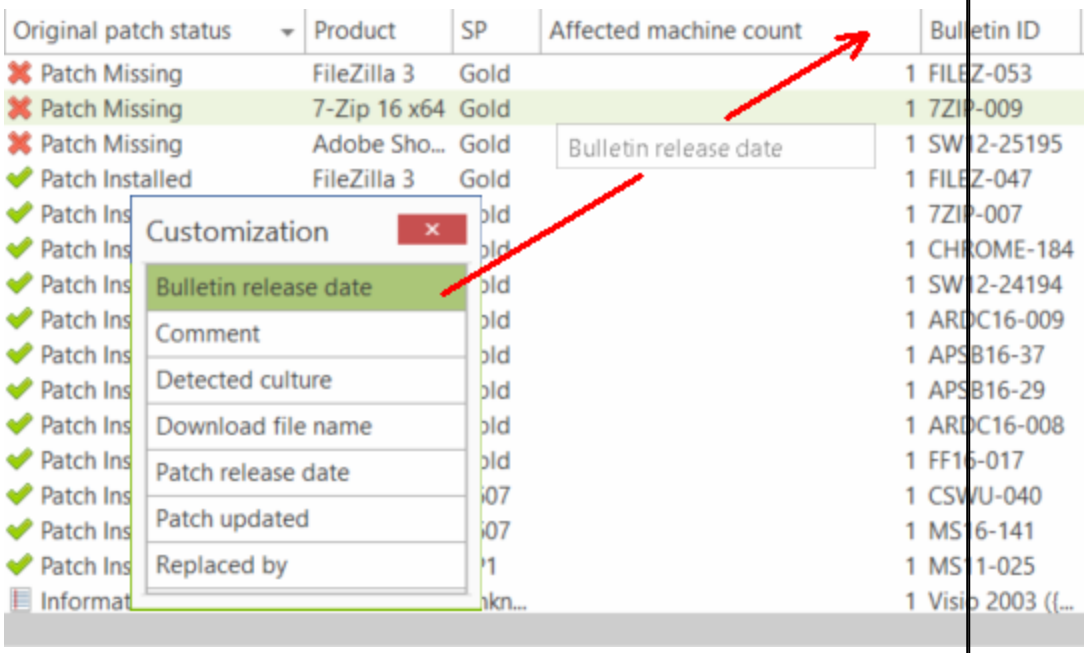
- You can right-click within a column header and perform a number of additional actions.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Sort Ascending	Sorts the selected column in ascending order.
Sort Descending	Sorts the selected column in descending order.
Clear Sorting	Clears the ascending or descending sorting criteria currently set for a column.
Group By This Column	Groups the table using the data in the selected column. It does this by moving the data into expandable lists that are located in the body of the grid. One expandable list will be created for each possible column value. If you perform this action on any subsequent columns, that data will be presented as nested groups at increasingly lower levels within the expandable lists. If **Show Group By Box** is enabled, this will also create a "Group By" box in the area immediately above the column headers. TIP: To turn off the **Group By This Column** feature and revert to the original view: Enable **Show Group By Box**, drag the Group By boxes back to the column header and then right-click in the column header and select **Hide Group By Box**.
Show Group By Box / Hide Group By Box	Displays or hides an area immediately above the column headers that contains "Group By" boxes. One "Group By" box will be displayed for each column header for which **Group By This Column** is currently enabled. You can also drag column headers to and from this area.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

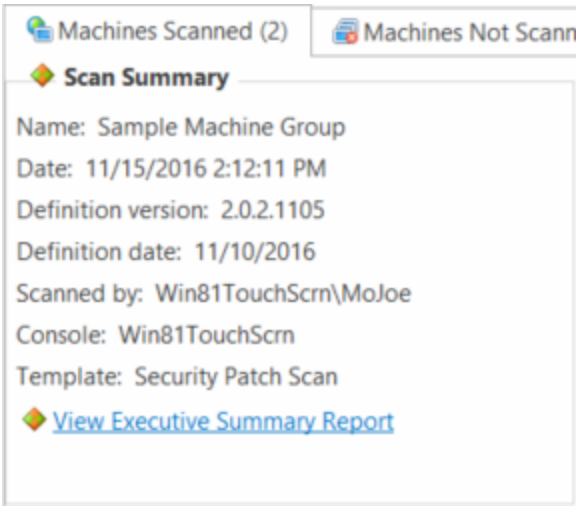
	The table will be grouped according to the data in the box. If there are two or more boxes then the grouping will be nested, with the left-most box presented at the highest level, the second box presented at the second level, etc.
Hide This Column	Removes the column from the table. You can add the column back to the table using the **Column Chooser**.
Column Chooser	Enables you to add and hide information within a pane. When you select **Column Chooser** the **Customization** dialog is displayed. This dialog is used to store the columns you don't currently want displayed within the pane. Simply click and drag the desired column headers from the table to the Customization dialog. For example, if you decide you want to add the Bulletin release date column to the table, simply drag that column header from the Customization dialog to the table. For example, if you decide you don't want Language and Last Scan Template information displayed in the table, simply drag those column headers into the Customization dialog.  If you decide you want an item back in the table, simply click and drag it from the Customization dialog back to the table.
Best Fit	Resize the width of the selected column so that the header text is displayed in the optimal amount of space.
Best Fit (all columns)	Resize the width of all columns in the table so that the header text is displayed in the optimal amount of space.
File Editor	The **Filter Editor** dialog will show any filters that are currently active in the column headers. You can use the editor to modify the existing filter criteria and to build new criteria using the available filter conditions and logical operators.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

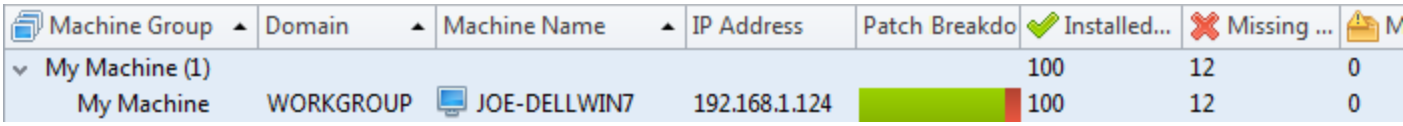
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Scan View Scan Summary

The left side of the top pane contains a Scan Summary sub-pane. This pane provides summary information about the scan. The pane can be collapsed to provide more room in the top pane.



The top pane in the scan summary also displays a table containing detailed information about each machine that was scanned. Click on a column heading to sort the table by that information. You can also specify what information is presented by right-clicking the table heading and selecting or clearing the available items.



, , or	Indicates whether the computer is a physical machine or an online virtual machine ( ), an offline virtual machine ( ), or a virtual machine template ( ).
Machine Group	The machine group that was scanned and that contains the selected machine.
Domain	The domain of the scanned machine.
Machine Name	The machine name.
IP Address	The IP address of the scanned machine.
Virtual Server	The name of the server that is hosting the virtual machine. This column does not apply to physical machines.

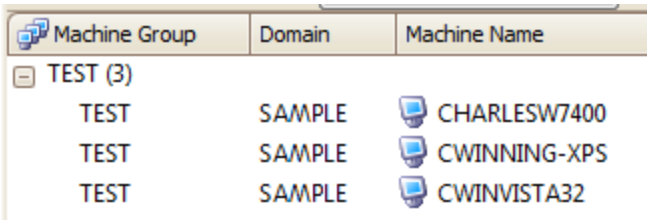
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

VM Name	The name of the virtual machine. This column does not apply to physical machines.
Path	The full path name of the hosted virtual machine. This column does not apply to physical machines.
Patch Breakdown	A visual representation of the percentage of installed patches (green) vs. missing patches (red) and missing service packs (yellow). If you choose to sort this column, the sort value for each machine is computed as follows: number of missing patches + (number of missing service packs * 10).
Installed Patch Count	The total number of patches installed on the scanned machine.
Missing Patch Count	The total number of patches missing on the scanned machine.
Missing Service Pack Count	The total number of service packs missing on the scanned machine.
EOL Products	The number of software products on the machine that have been designated as at End-of-Life by their vendor.
Operating System With Service Pack	The operating system and service pack level being used on the scanned machine. If the operating system is shown in red it indicates that it has reached its end-of-life (EOL) phase and the vendor will limit support for the product.
Operating System Language	The operating system language being used on the scanned machine.
Assigned Credentials	The credentials used when authenticating Ivanti Patch for Windows® Servers to the machine.
Last Scan Template	The template that was used to scan the machine.
Machine Criticality	The criticality level assigned to this machine.
Custom	Any custom notes that describe unique properties about the machine.

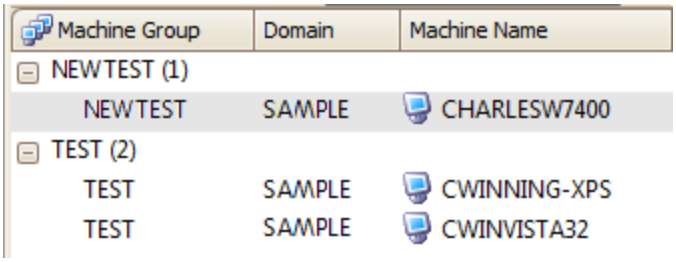
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Machine Group Information is Dynamic

The machine group information that is displayed is based on the machine group used to perform the most recent action on each machine. So it is possible for the machine group information to change. For example, if you perform a scan of a group containing three machines, the information displayed will be similar to the following:



If you then re-scan the first machine from a different machine group, the refreshed display will reflect this change:



The first machine is no longer listed with its original group because the most recent scan of the machine was initiated from a different machine group.

When agents check in with the console they will be listed with the machine group from which they were last scanned from the console.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Searching for Machines in the Top Pane

You can easily search for machines contained in the top pane. All searches are performed using the Search tool.



To initiate a search you type the machine name you want to find and then press **Enter** or click the search icon (). Only those machines matching the search criteria are displayed; all other machines are hidden.

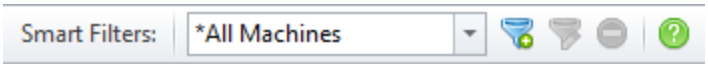
Tips for Using the Search Tool

- The Search tool works only on the information currently visible in the top pane.
- If a Smart Filter is applied, only items matching BOTH the search criteria and the smart filter criteria are displayed.
- All partial matches are displayed. For example, if you search for items named *Test*, any item with "test" in its name will be considered a match (e.g. TestMachine1, Contest, etc.).
- A semicolon (;) can be used to concatenate multiple search terms into one search string. For example, specifying "server;workstation" will return all items containing either of the two terms.
- The use of wildcards in the Search tool is not allowed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Using Smart Filter

Information displayed in the list can be easily filtered to narrow the focus to only those machines of interest. One way to do this is by using the Smart Filter.



The Smart Filter contains several default filters. You can also define your own custom filters.

Another option is to apply filters to individual columns. For more information, see Customizing the Column Headers.

Default Filters

The default filters are identified by a leading asterisk. Default filters cannot be modified or deleted. The default filters include the following:

- ***All Machines**: All machines are displayed, including servers and workstations.
- ***Servers**: Only servers are displayed.
- ***Workstations**: Only workstations are displayed.
- ***Today**: Only those machines that have been scanned within the last 24 hours are displayed.
- ***Last 7 Days**: Only those machines that have been scanned within the last seven days are displayed.
- ***Last 14 Days**: Only those machines that have been scanned within the last 14 days are displayed.
- ***Last 30 Days**: Only those machines that have been scanned within the last 30 days are displayed.
- ***Last 60 Days**: Only those machines that have been scanned within the last 60 days are displayed.
- ***Last 90 Days**: Only those machines that have been scanned within the last 90 days are displayed.
- ***Missing at least 1 patch**: Only those machines that are missing at least one patch are displayed.
- ***Has an Agent Policy**: Only those machines that have Ivanti Patch for Windows® Servers Agent installed are displayed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- ***Does not have an Agent Policy**: Only those machines that do not have Ivanti Patch for Windows® Servers Agent installed are displayed.

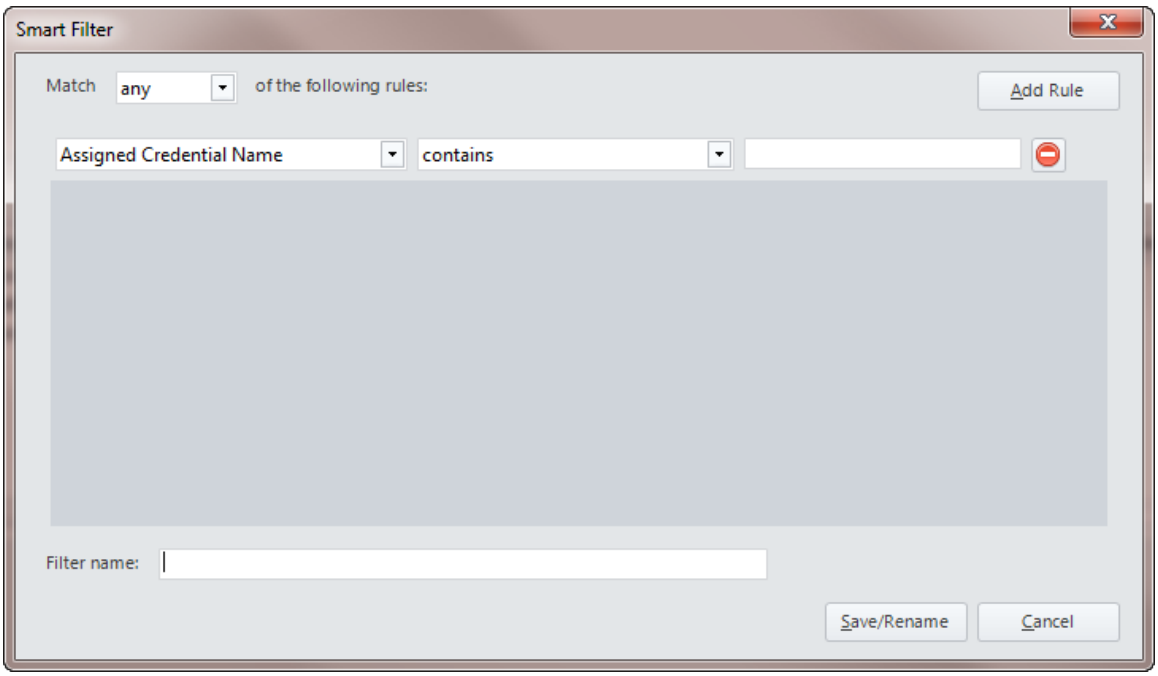
Custom Filters

You can create your own custom filters. This is a powerful tool that enables you to specify exactly which machines you want displayed in the top pane. Each custom filter is comprised of one or more rules. You can define as many rules in a filter as needed.

To create a new filter:

1. Click the Create a New Smart Filter icon ( ).

   The **Smart Filter** dialog is displayed.



2. Specify which rules in the filter must be matched.
   - **All**: Only those machines that match all the rules in the filter will be displayed.
   - **Any**: Machines that match at least one rule in the filter will be displayed.
3. Define one or more rules.

   To define a rule, select an option in each of the first two logic boxes and then type the criteria in the third box. To add another rule simply click **Add Rule**.

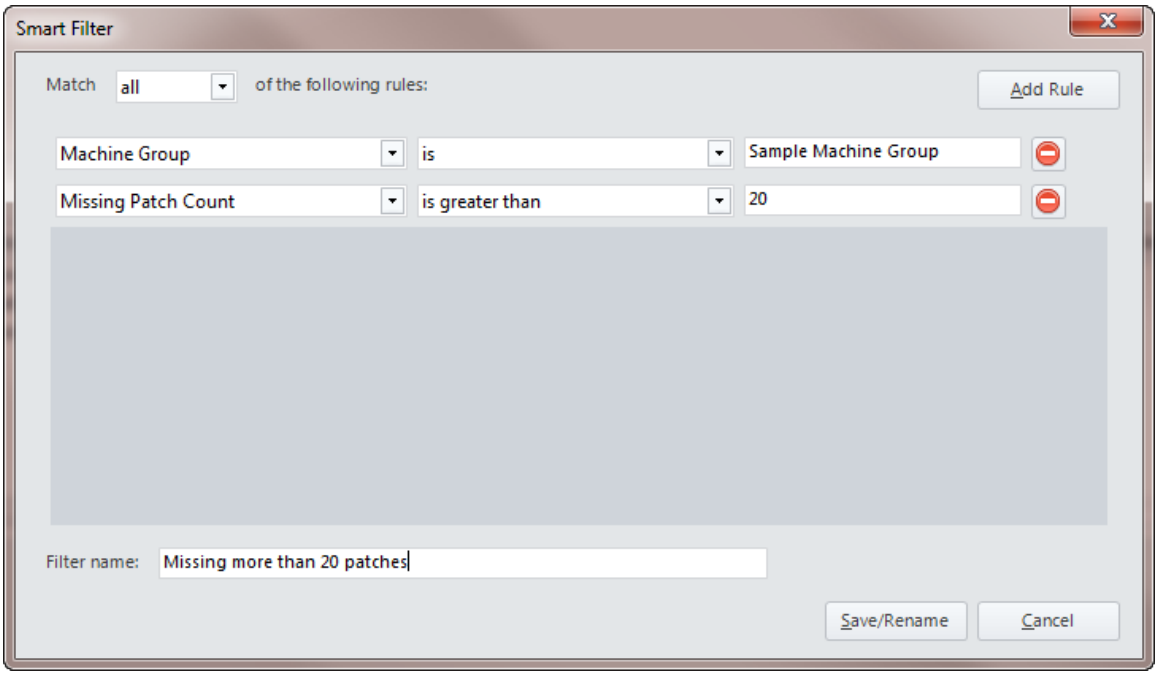
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

If you define a rule that does not make sense (for example, "Machine Name is greater than 3") the rule will simply be ignored.

4. Type a name for the filter.
5. When you are finished defining your custom filter, click **Save/Rename**.

Example

Assume you want to see which machines in a particular machine group are missing more than 20 patches. You simply create a filter similar to the following:

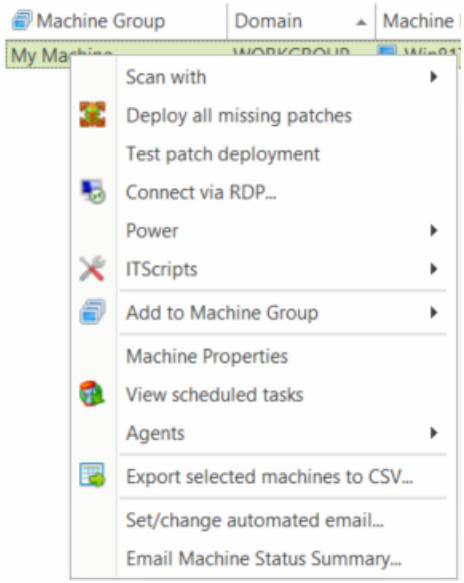


Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing Actions on Machines

Right-Click Menu

You can right-click on any machine in the top pane and perform a number of different actions. For example:



Scan With	Enables you to initiate a patch scan of the selected machines using any of the available patch scan templates.
Deploy All Missing Patches	Enables you to deploy (install) all patches currently missing on the selected machine. See Deploying All Missing Patches to a Machine for more information.
Test Patch Deployment	Enables you to perform a test deployment to the selected machines. This is especially useful for patch deployments you want to schedule for a later time. Testing the deployment allows you to correct any potential problems in a deployment and make it less likely that a deployment will fail. See the Operations Monitor for more information.
Connect via RDP	Enables you to make a Remote Desktop connection to the selected machine. See How to Initiate a Remote Desktop Connection for more details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Power	Enables you to modify the power state of the selected machines. You can immediately restart, shut down, or awaken the machines, or you can use a power state template to schedule a reboot of the machines and leave them in a particular state (fully powered on, in sleep mode, in hibernate mode, or powered off). See How to Initiate Power Management Tasks for more information. You can immediately restart or shut down the machine(s).
ITScripts	Enables you to either open a Windows PowerShell™ prompt or select and execute an approved script. See How to Execute a Script for details.
Add to Machine Group	Enables you to add the selected machines to a new machine group or to an existing machine group. See Creating A New Machine Group for more information. IMPORTANT! Machines you add to the machine group are automatically assigned the associated machine credentials. If no machine credentials are available, no credentials will be assigned and the default credentials will be used in any subsequent scans. If the default credentials are not valid for the machines, and if the account credentials of the person currently logged on to the program are also not valid for the machines, scans of the machines you just added to the group will fail. To prevent scanning errors, always supply credentials for machines you add to a machine group. See Supplying Credentials for more information.
Machine Properties	Enables you to view and edit machine properties. See Managing Individual Machine Properties for more information.
View scheduled tasks	Enables you to view the Scheduled Remote Tasks Manager, which gives you a single location from which to monitor the power tasks and patch deployment tasks currently scheduled on this machine.
Agents	Enables you to: • Install an agent, assign a different policy to the agent,or uninstall an agent. • Send a number of different commands to the selected agents. The commands apply only to machines that already have agents installed, that are online, and that are configured to be listening agents. See the Send command description for detailed information about the available commands.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **(Machine View only)** Initiate any of the tasks currently defined within the selected agents. When you select a task a confirmation dialog is displayed. If you choose to continue, the task is immediately started on the agent machines. See Creating a New Agent Policy for information on the types of tasks that may be available.
Export selected machines to CSV	Export information about the selected machines to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program. This can also be accomplished using the **Machines > Export visible machines to CSV** menu.
Set/Change automated email	This option is only available if you have enabled the email feature and defined an SMTP server. It enables you to set or change the automated report settings for this machine. Changes you make here will override email settings you specified on the **Manage Machine Properties** dialog.
Email Machine Status Summary	This option is only available if you have enabled the email feature and defined an SMTP server. It enables you to send a **Machine Status Summary** report to one or more recipients.

Keyboard Shortcuts

The following keyboard shortcuts are available:

- **Ctrl+A**: Selects all machines.
- **CTRL+click**: Multiple machines can be selected by holding down the CTRL key while selecting machines.
- **SHIFT+click**: A contiguous group of machines can be selected by holding down the SHIFT key while selecting the starting and ending machines in the list.
- **SHIFT+PAGE UP**: Selects a range of machines from the one currently selected to the top of the table.
- **SHIFT+PAGE DOWN**: Selects a range of machines from the one currently selected to the bottom of the table.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

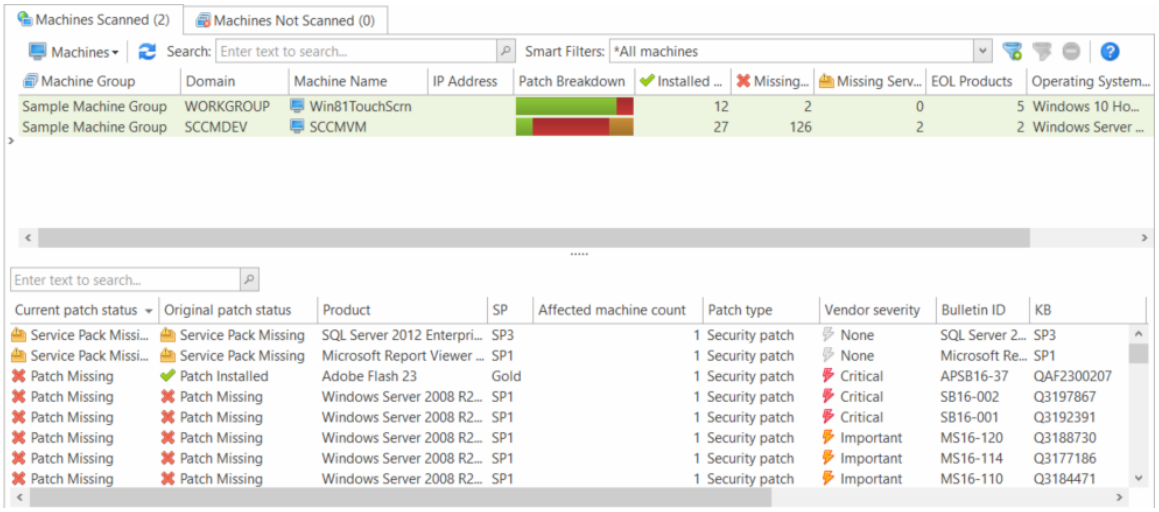
Viewing Patch Summaries in Scan View

The middle pane displays general patch information about the machine(s) selected in the top pane. If multiple machines are selected in the top pane, this pane will display patch information for all selected machines. For example, if you select two domains in the top pane, summary information about all the machines in both domains will be displayed. The **Affected Machine Count** column indicates how many of the selected machines are affected by a specific patch or service pack.

The values for the **Installed Patch Count** and **Missing Patch Count** columns in the top pane may not always match the values shown in the middle pane. This is because the top pane counts every patch on every machine, while the middle pane counts only unique patches and ignores duplicates.

If you refresh Scan View during or after a patch deployment, the **Current Patch Status** column will reflect the new patch status. For example, in the following figure, the Adobe Flash 23 patch that was originally detected as missing is now being reported as installed.

You can customize the way information is displayed within this pane. See Customizing the Column Headers for information.

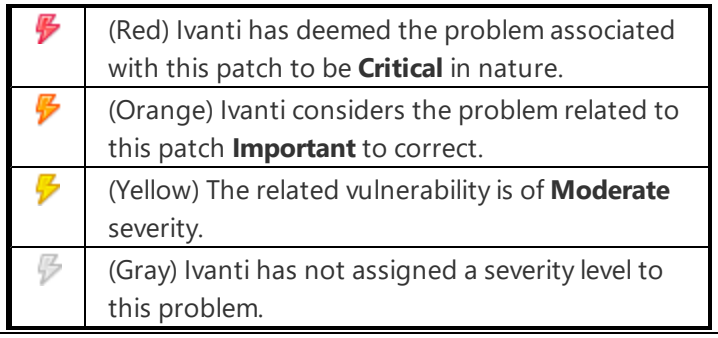


Current patch status	The current status of the patch. This may be different from the status of the patch when the scan was originally performed. (For example, the patch may have been deployed since the scan was originally performed.)
Original patch status	Indicates the patch status at the time the patch scan was performed.
Product	The software product affected by this patch.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

SP	The service pack level of the patch. For original patches the level will be Gold.
Affected machine count	Indicates the number of machines that are missing the patch. This number only applies to those machines that are selected in the top pane.
Patch type	Indicates the patch type. The possible types are: • **Non-security Patches:** The set of patches supported by Microsoft Software Update Services • **Security Patches:** Security bulletin-related patches • **Security Tools:** Patches for the malware tool provided by Microsoft • **Software Distribution:** Free third-party products that can be deployed by Ivanti Patch for Windows® Servers
Bulletin ID	Identifies the Microsoft Security Bulletin article that describes the threat addressed by the patch.
Bulletin title	The descriptive title of the Microsoft Security Bulletin article that describes the threat addressed by the patch.
Download method	Indicates if the patch can be downloaded automatically by the program or if it must be downloaded manually. There may be a number of different reasons why a patch cannot be automatically downloadable. For example, you may have a patch that was created for a proprietary software program, or you may receive patches for a program that is no longer officially supported by the vendor. If the value in this column is **Automatic**, it means that Ivanti Patch for Windows® Servers can download the patch automatically. If the value is **Acquire from vendor** or some other value, it means that you must manually download the patch on your own and then move it into the patch download directory. Once the patch is there it can be deployed using the normal deployment process.
KB	The knowledge base number used to identify the Microsoft-based patch.
IAVA ID	This column is available only if you have a Government Edition of Ivanti Patch for Windows® Servers.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

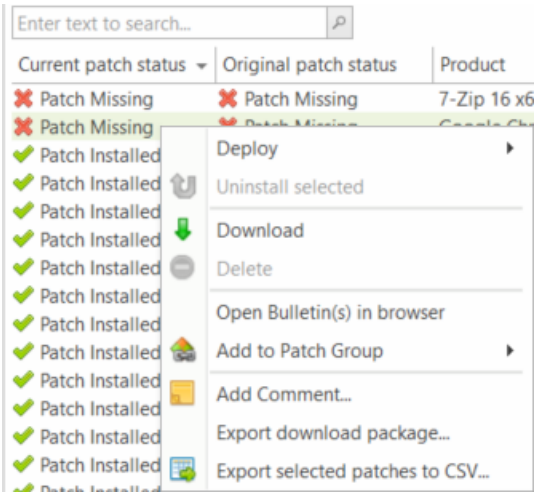
	The number used to identify patches in the Information Assurance Vulnerability Alert (IAVA) XML file compiled by the U.S. Government.
Vendor severity	One of four severity levels assigned by Ivanti based on the perceived threat of the vulnerability related to the patch.  (Red) Ivanti has deemed the problem associated with this patch to be **Critical** in nature. (Orange) Ivanti considers the problem related to this patch **Important** to correct. (Yellow) The related vulnerability is of **Moderate** severity. (Gray) Ivanti has not assigned a severity level to this problem.
Uninstallable	Indicates if the patch can be uninstalled. Uninstalling a patch restores a machine to its original state before the patch was deployed. Patches must be uninstalled in the reverse order in which they were installed.
Downloaded	Indicates if the patch has been downloaded to the patch download directory.
EOL	The number of software products on the machine that have been designated as at End-of-Life by their vendor.
Bulletin release date	The original publication date of the security bulletin that identifies the vulnerability.
Comment	A user-supplied comment about the patch.
Detected culture	The local form of the operating system language detected on the target machine.
Download file name	The file name used by Ivanti Patch for Windows® Servers when downloading and deploying the patch. The name may include a three letter identifier that specifies the operating system language supported by the patch.
Patch release date	The date the patch was originally published.
Patch updated	The date an updated version of the patch was published.
Replaced by	The bulletin ID that identifies a more recent update for the vulnerability.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing Actions on Patches

You can easily search for patches contained in the middle pane. All searches are performed using the Search tool. To initiate a search you type the alphanumeric characters that you want to find and then press **Enter** or click the search icon ( ). Only those patches matching the search criteria are displayed; all other patches are hidden. For tips on using the Search tool, see Searching for Machines.

In addition, you can right-click on any patch in the middle pane and perform a number of different actions. For example:



Deploy	Enables you to deploy (install) patches or service packs currently missing on the machine(s) selected in the top pane. See Deploying One or More Patches to a Machine for more information.
Uninstall Selected	Enables you to uninstall (rollback) the selected patch. See How to Uninstall Patches for more information.
Download	Enables you to download to the patch download directory the selected patches or service packs. See Downloading Patches for more information. The **Download** command is only available if the patch can be downloaded automatically. For more information see the description of the **Download method** column.
Delete	Enables you to delete selected patches from the patch download directory.
Open Bulletin(s) in Browser	Displays the related Microsoft security bulletin within a Web browser.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Add to Patch Group	Enables you to add the selected patch(es) to an existing patch group or to a new patch group. See Creating and Editing a Patch Group for more information.
Add Comment	Enables you to add your own specific comment about the patch.
Export download package	Export the download links for the selected patches to a Comma Separated Values (CSV) file. This is especially useful for a console that is in a disconnected environment. The CSV file can be used by a connected machine to download the patches and the patches can then be copied into the disconnected console's patch directory. A File Downloader PowerShell script is available to assist with the file download process; contact the Support group for more details.
Export selected patches to CSV	Export information about the selected patches to a CSV file. The CSV file can then be used by a spreadsheet program.

Keyboard Shortcuts

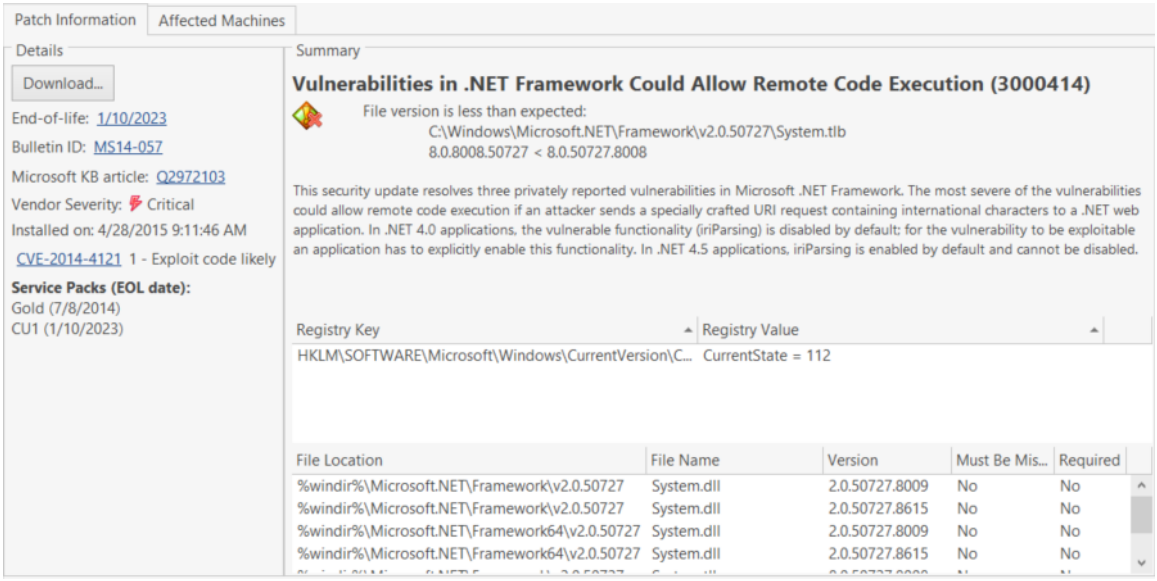
The following keyboard shortcuts are available:

- **Ctrl+A**: Selects all patches.
- **CTRL+click**: Multiple patches can be selected by holding down the CTRL key while selecting patches.
- **SHIFT+click**: A contiguous group of patches can be selected by holding down the SHIFT key while selecting the starting and ending patches in the list.
- **SHIFT+PAGE UP**: Selects a range of patches from the one currently selected to the top of the table.
- **SHIFT+PAGE DOWN**: Selects a range of patches from the one currently selected to the bottom of the table.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Patch Information

The **Patch Information** tab in the bottom pane displays detailed information about the patch, service pack, or informational item selected in the middle pane. Detailed information will not be displayed if multiple patch items are selected in the middle pane.



Download	Enables you to download the patch to the patch download directory. When you click this button the **Patch Download Status** dialog is displayed. Use this dialog to select which language version of the patch you want to download. On the dialog, if the download icon is grayed out ( ) it indicates the patch has not yet been downloaded. If the icon is green ( ) it indicates the patch has already been downloaded and verified.
End-of-life	Indicates the End of Life date for the patch. You can click the link to view additional information.
Bulletin ID	Provides a link to the Microsoft Security Bulletin article that describes the threat addressed by this patch.
Replaced by	If shown, indicates that the patch is replaced by another more recent patch.
Microsoft Knowledge Base Article	Provides a link to the associated Knowledge Base article that provide more information about the flaw.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Vendor Severity	Ivanti assigns one of four severity levels based on its perceived threat of the vulnerability related to the patch.  (Red) Ivanti has deemed the problem associated with this patch to be **Critical** in nature.  (Orange) Ivanti considers the problem related to this patch **Important** to correct.  (Yellow) The related vulnerability is of **Moderate** severity.  (Gray) While it poses a security risk, Ivanti deems that risk to be **Low**.
Service Packs (EOL date)	If shown, indicates that the patch is contained in one or more service packs. Also indicates the End Of Life (EOL) date for the service pack.
Description	Identifies the product that is affected by this patch, and describes how the product is vulnerable.
Summary	Provides a concise description of the threat addressed by this patch.
Comments	If shown, provides comments from Ivanti about this patch.
Registry Key table	Identifies the registry key information used to determine whether the product in question exists on the target machines. This table can be sorted by clicking within a column header.
File Location table	Shows the file criteria used for determining whether or not a patch is installed. This table can be sorted by clicking within a column header.

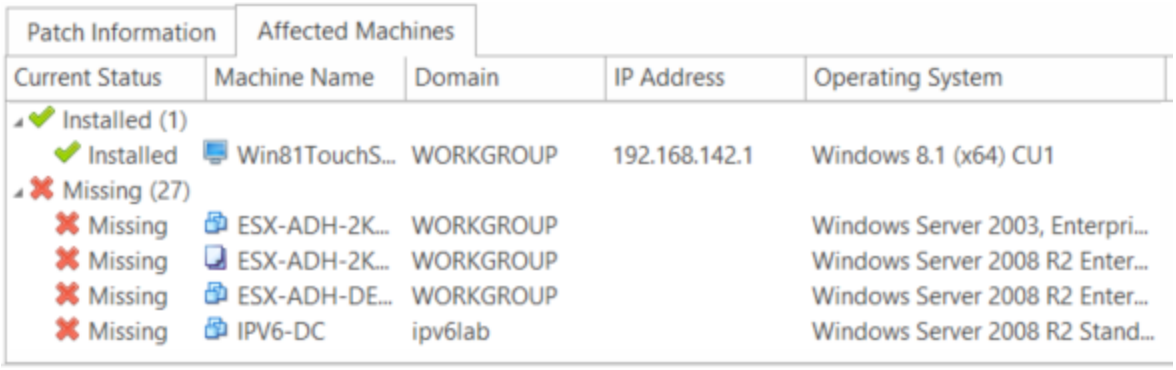
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Machines Affected by a Selected Patch

The **Affected Machines** tab in the bottom pane displays which of your selected scanned machines are affected by the patch that is selected in the middle pane. The listed machines will be in one of two lists:

- **Missing:** These machines are vulnerable to the threat corrected by the patch.
- **Installed:** These machines already contain the selected patch.

Managed machines that are not listed are not affected by the selected patch.



The **Affected Machines** table can be sorted and customized. See Customizing the Patch View Column Headers for more information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Downloading Patches and Service Packs

Ivanti Patch for Windows® Servers automatically downloads necessary patches as part of the deployment process, removing the need to manually download them in advance. If needed, however, Ivanti Patch for Windows® Servers also provides the ability to manually download patches to the patch download directory prior to deployment. There are multiple ways to download patch files.

To download a single patch

- From the middle pane of Scan View, right-click the patch and choose **Download**.
- From the bottom pane of Scan View, on the **Patch Information** tab click **Download**.
- From within the bottom pane of Machine View, on the **Patch Information** tab click **Download**.
- From within the bottom pane of Patch View, on the **Patch Information** tab click **Download**.

To download multiple patches

- From within the middle pane of Scan View, right-click the selected patches and choose **Download**.
- From within the middle pane of Machine View, right-click the selected patches and choose **Download**.
- From within the top pane of Patch View, right-click the selected patches and choose **Download**.

To download service packs

- From within the middle pane of Scan View, right-click a service pack and choose **Download**.
- From within the middle pane of Machine View, right-click a service pack and choose **Download**.

Tips

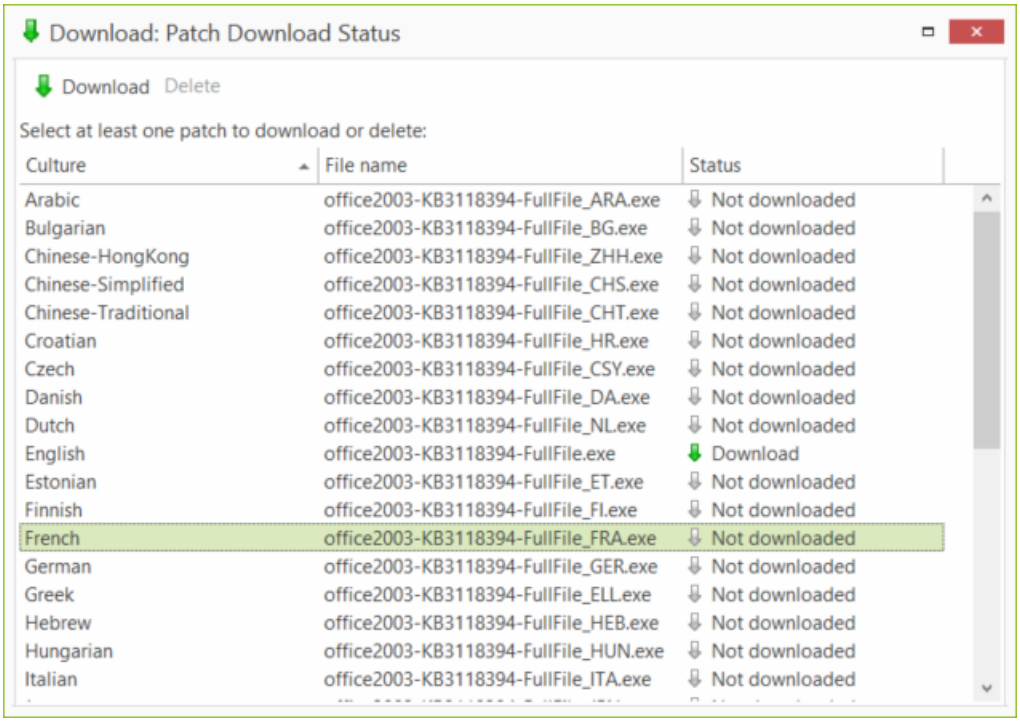
- If you have trouble downloading a patch, try clearing your browser cache files before attempting another download.
- For information about downloading any custom patches you may have created, please see Overview of the Custom XML Process.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How to Download Different Language Versions of a Patch

When you initiate a download by right-clicking one or more patches, Ivanti Patch for Windows® Servers will immediately begin the download process. The program will automatically detect the operating system languages used on your managed machines and then download only those language versions of the patch file that are needed. In many cases, all that is needed is a single universal patch package file that can be used by all languages. If you do not have managed machines that require a particular patch, the program will use the **Patch View download status indicator language** option as the default.

If you initiate the patch download from the **Patch Information** tab in Scan View, Machine View or Patch View, you will have the opportunity to manually select the individual files you want to download. Simply select the desired language versions and then click **Download**.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Patch Downloads Are Performed As Background Tasks

All patch downloads are performed as background tasks, regardless of how they are initiated. In other words, the download is launched as its own separate Windows task. This means you can initiate a patch download and then move on to other work within Ivanti Patch for Windows® Servers without having to wait for the download to complete. This also means you can have multiple patch downloads active at the same time.

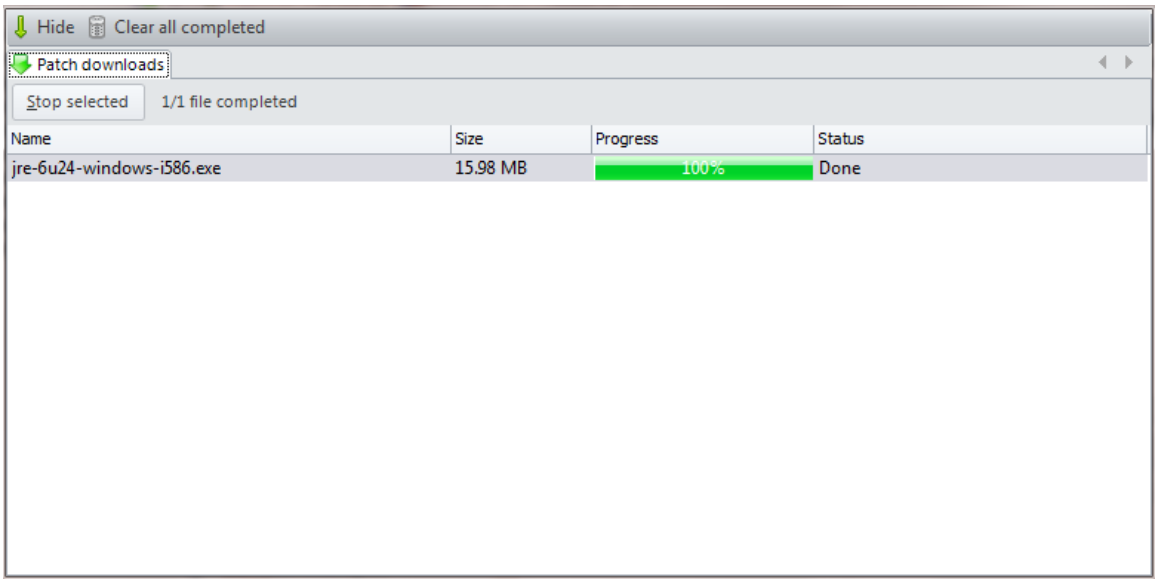
Download Considerations

- Is there a practical limit to the number of patch downloads you can have active at the same time?

  Yes. It is dependent on the CPU and memory size of the console machine. It is also dependent on the number of other tasks currently active (for example, other patch scans, patch deployments, etc.). While there is no exact answer, you'll know you've reached a practical limit if Ivanti Patch for Windows® Servers starts responding slowly.

- How will I know when a download completes?

  The **Operations Monitor** will display the status of the patch download.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Patch Deployment Overview

Ivanti Patch for Windows® Servers allows local and remote patch deployment via a few simple mouse clicks. From one management console you can deploy missing patches and service packs to a single machine or to many machines.

Service packs should be applied before all patches. For this reason Ivanti Patch for Windows® Servers will not allow you to deploy service packs and patches in the same deployment.

Patch Deployments Are Performed As Background Tasks

All patch deployments are performed as background tasks, regardless of how they are initiated. In other words, the deployment is launched as its own separate Windows task. This means you can initiate a patch deployment and then move on to other concurrent work within Ivanti Patch for Windows® Servers without having to wait for the deployment to complete. This also means you can have multiple patch deployments active at the same time.

Deployment Considerations

- Is there a practical limit to the number of deployments you can have active at the same time?

  Yes. It is dependent on the CPU and memory size of the console machine. It is also dependent on the number of other tasks currently active (for example, other patch downloads, patch deployments, etc.). While there is no exact answer, you'll know you've reached a practical limit if Ivanti Patch for Windows® Servers starts responding slowly.

- Is there a problem if the same machine is included in two or more concurrent deployments?

  You should avoid concurrent deployments to the same machine. Exactly what will happen is dependent on a number of issues. The second deployment may overwrite the patch files already deployed, it may fail if the files are currently in use by the first deployment, or it may fail if the first deployment reboots the machine while the second deployment is still in progress.

- How will I know when a deployment is complete?

  The **Operations Monitor** will display the status of the patch deployment. From the Ivanti Patch for Windows® Servers console's perspective, the deployment is complete when all necessary files have been copied to the target machine and the deployment is scheduled.

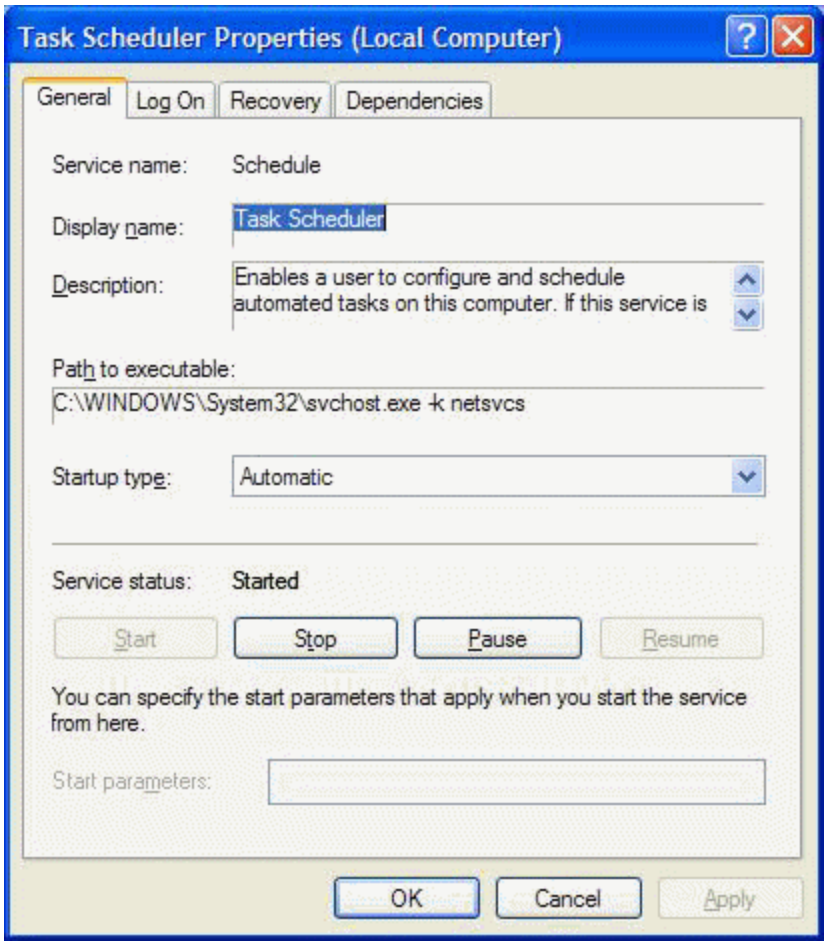
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Patch Deployment Prerequisites

In addition to the scanning prerequisites, the following are required in order to successfully deploy patches to target machines:

- The Windows Update service must not be disabled; rather, it must be set to either **Manual** or **Automatic** in order to successfully deploy patches. In addition, the Windows Update setting on each target machine (**Control Panel > System and Security > Windows Update > Change settings**) should be set to **Never check for updates**.
- The machine credentials that you supply are used to provide access to the remote machine and to push the necessary patch deployment files. See Credential Precedence for information on what occurs if machine credentials are not supplied. The actual deployment, however, will be run under the remote machine's Local System account.
- A scheduler is required on the machines being patched to ensure a successful deployment. If you are not using the default IvantiScriptLogic Scheduler (see Scheduling Options), you will need to enable the Windows Task Scheduler on the machines being patched. On most Windows machines you can access the Task Scheduler by selecting **Start > Administrative Tools > Services** and then right-clicking **Task Scheduler**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Patch Deployment Security

Ivanti Patch for Windows® Servers takes the security of patch deployment very seriously. To that end, each patch undergoes up to three signature validation checks and is stored in a location on the remote machine with tight security permissions. If any of the signature checks fail, the patch will not be deployed.

During deployment, when a patch is copied to a remote system, the copy is not initiated unless the patch is signed. This is to prevent someone from tampering with the copy of the patch stored in the patch download directory. Before a patch is pushed out, it is always checked for a valid signature to ensure you are getting a legitimate patch.

Once the patch is copied to the deployment target it might sit for a period of time for a scheduled deployment. To prevent someone from tampering with the patch, the signature is checked again before deploying on that machine. Additionally, the patch directory that Ivanti Patch for Windows® Servers creates on the remote machine has permissions set to LOCALSYSTEM and Local Administrators only so other users will not be able to modify, add or remove files from the deployment directory.

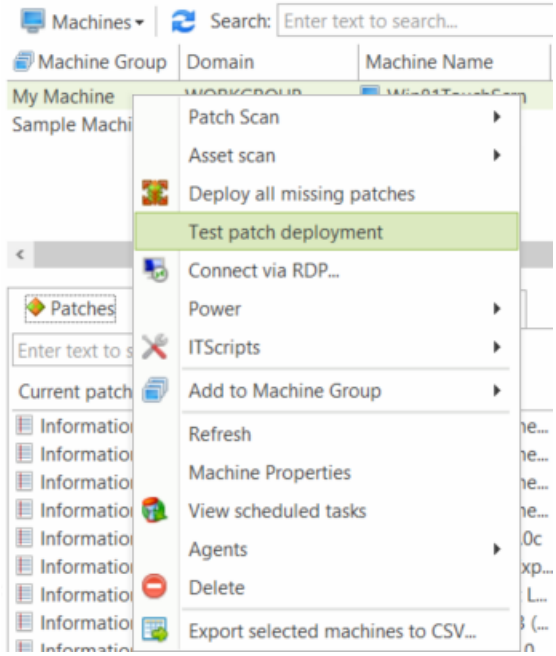
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Testing the Deployment

Ivanti Patch for Windows® Servers includes the ability to perform a test deployment to one or more machines. This is especially useful if you intend to schedule a patch deployment for a later time. Testing the deployment allows you to correct any potential problems in a deployment and make it less likely that a deployment will fail.

How to Perform a Test Deployment

You perform a test deployment from Machine View or Scan View. Simply right-click the machine, machine group, or domain you want to test and then select **Test Patch Deployment**.



The test is conducted using a non-security patch named TEST-PATCH. The patch does not modify the state of the target machine. The test will exercise all of the actions in the deployment process, including:

- Testing for available deployment seats
- Verifying port requirements and the availability of a secure connection
- Downloading and copying files to the target machine
- Verifying patch signatures
- Scheduling the patch task
- Executing the deployment package
- Delivering status messages

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Test deployment results are reported in the Operations Monitor. Status messages are provided for each major step in the process. The results are also reported on the Manage Items dialog.

A test deploy may fail for a number of different reasons. For example, if the workstation or scheduling services are not started in a particular machine, Ivanti Patch for Windows® Servers cannot deploy patches to it and a test deploy will return a failing result. If a test does fail you can click the available link for information on why the test failed.

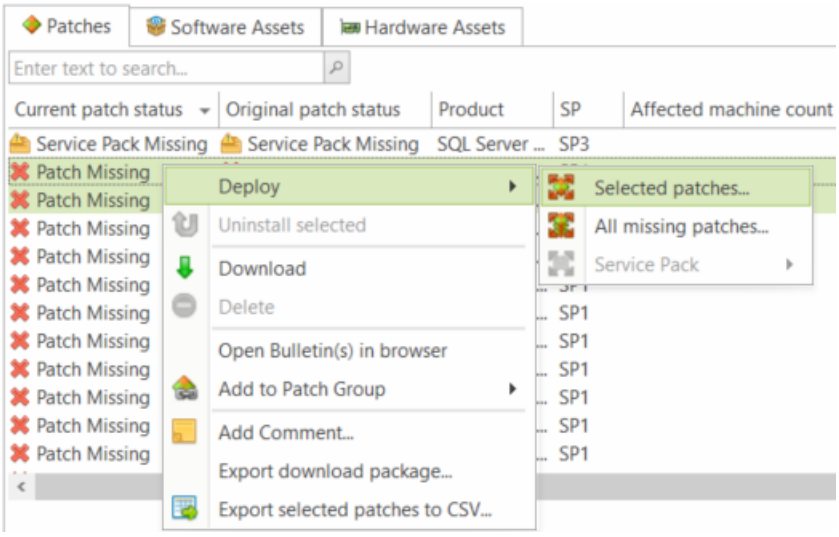
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deploying One or More Patches to a Machine

1. In the middle pane of Scan View or Machine View, select the patches that you would like to deploy to the selected machine.

   Multiple patches can be selected by holding down the CTRL key while selecting patches. A contiguous group of patches can be selected by holding down the SHIFT key while selecting the starting and ending patch in the list.

2. Right-click one of the patches that are to be deployed and select **Deploy > Selected Patches** from the shortcut menu.



   This will launch the Deployment Configuration dialog.

If default credentials are not currently assigned the **Default Credentials** dialog is displayed. If you choose not to assign default credentials by clicking **Cancel**, then the deployment may fail for any machine that does not contain assigned credentials.

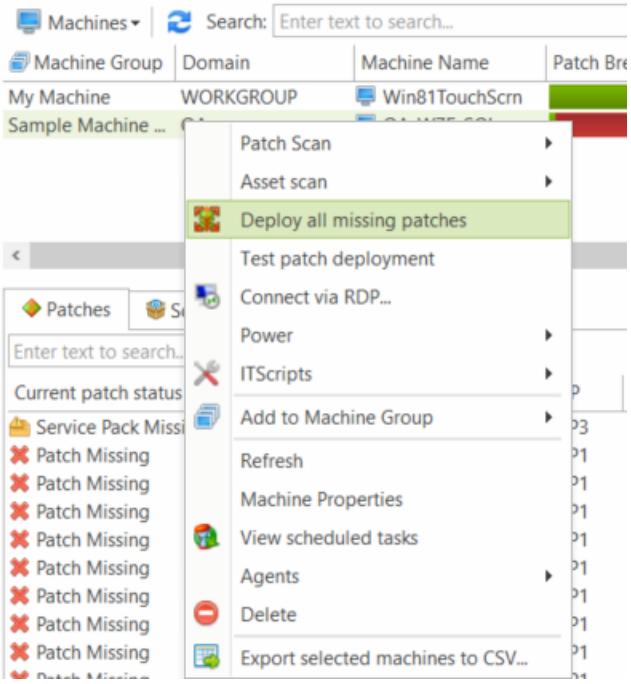
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deploying All Missing Patches to a Machine

You can easily deploy all patches that are missing from a machine. There are a couple of ways to do this within Ivanti Patch for Windows® Servers.

From the Top Pane of Machine View or Scan View

1. In the top pane of Machine View or Scan View, select the desired machine.
2. Right-click the machine and select **Deploy All Missing Patches**.



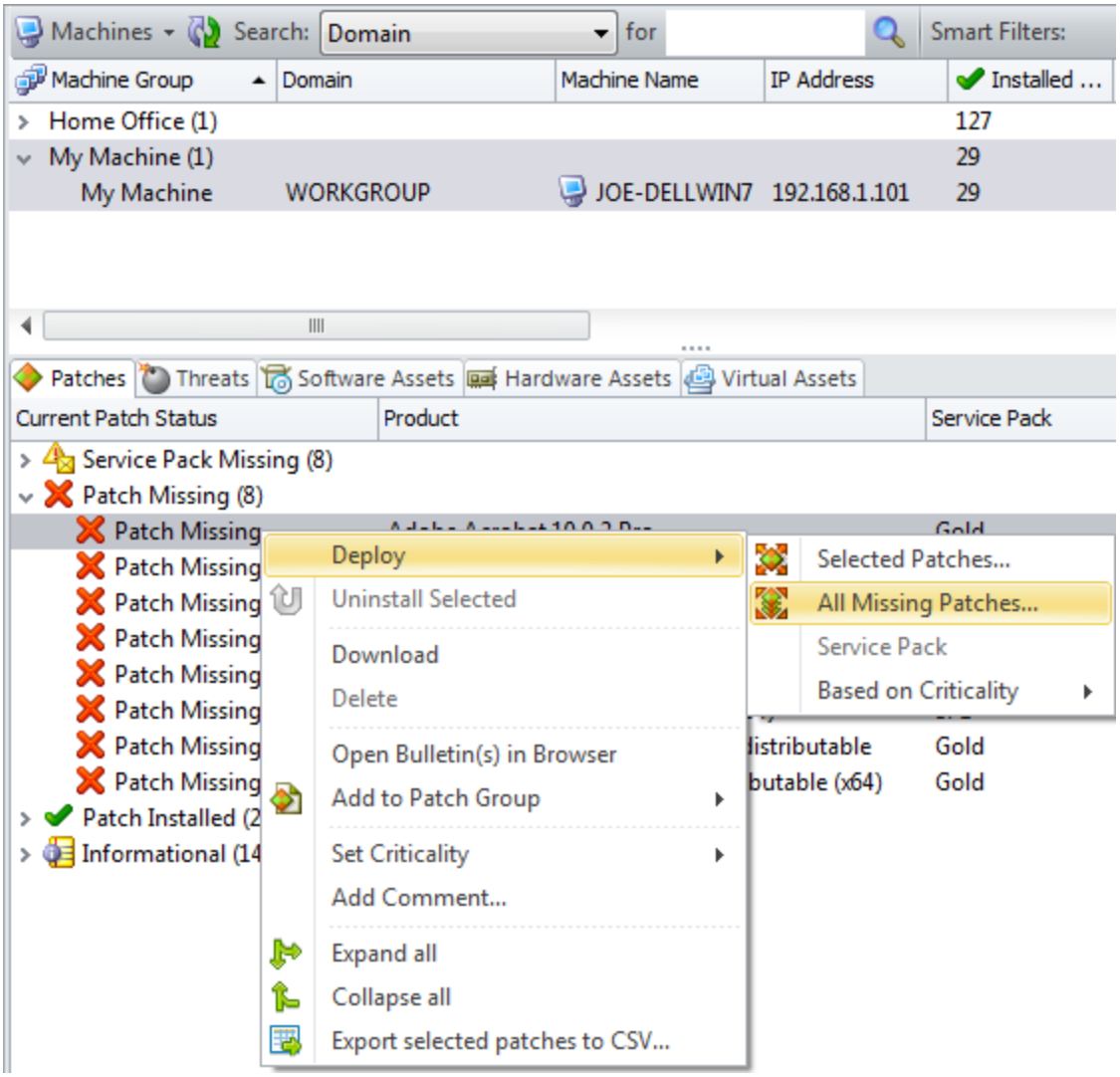
This will launch the Deployment Configuration dialog.

If default credentials are not currently assigned the **Assign Credentials** dialog is displayed. If you choose not to assign default credentials by clicking **Cancel**, then the deployment may fail for any machine that does not contain assigned credentials.

From the Middle Pane of Machine View or Scan View

1 In the top pane of Machine View or Scan View, select the desired machine.
2. In the middle pane, right-click a missing patch and select **Deploy > All Missing Patches**.

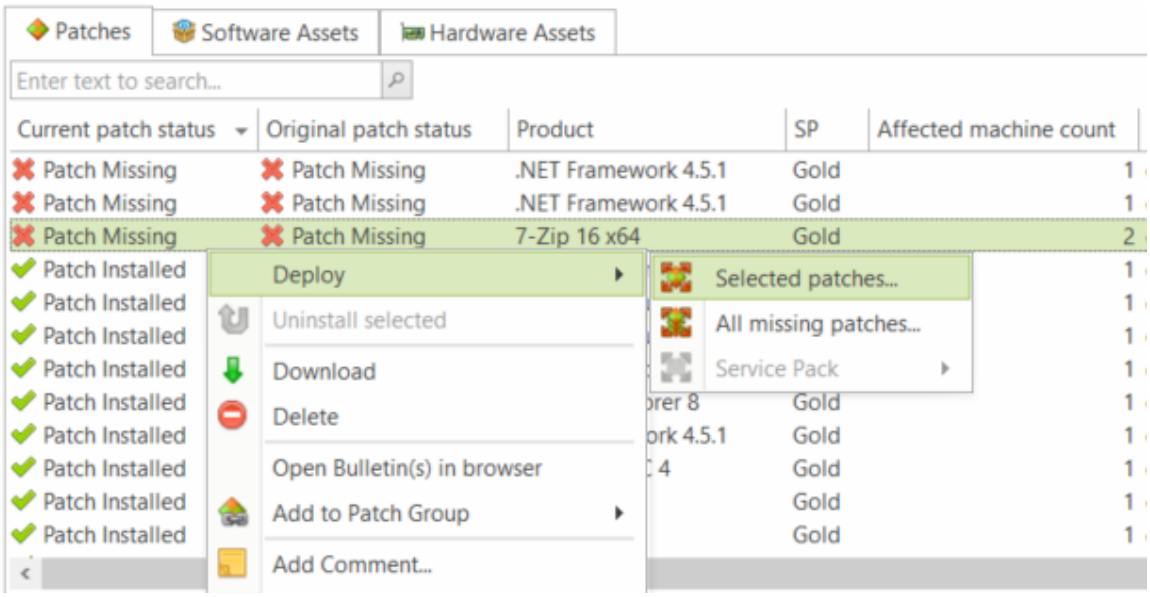
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deploying Patches to Multiple Machines

You can deploy patches to multiple machines using Machine View or Scan View. In the top section select the machines that are missing the patch, and then in the middle section right-click the patch and select **Deploy > Selected Patches**. You can also select multiple patches in the middle section and it will deploy them to all machines selected in the top section that are missing them.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

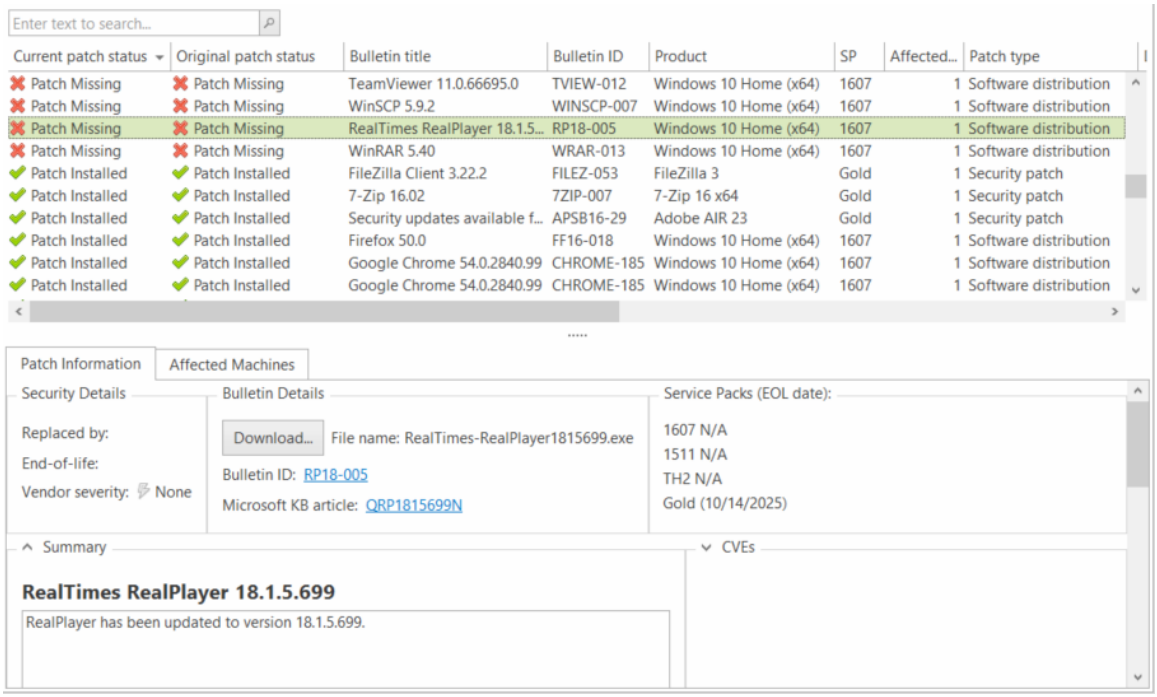
Deploying Third-Party Applications

Click here for information on how to scan for third-party applications.

You deploy (install) third-party applications to selected machines in the exact same manner that you deploy missing patches to selected machines. Ivanti Patch for Windows® Servers will treat the missing application exactly like a missing patch and will simply install the application on the selected machines. Here's an example showing how to deploy a third-party application from Scan View. The procedure is very similar using Machine View.

1. Select the third-party application you want to deploy.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.





2. Right-click the selected application and select **Deploy > Selected Patches**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deploying Patches to Virtual Machines and to Virtual Machine Templates

The method for initiating a patch deployment is the same regardless of whether you are deploying to a physical machine, an online virtual machine, an offline virtual machine, or a virtual machine template. It's what happens after you initiate the deployment, however, that is slightly different for virtual machines and for virtual machine templates.

For deployments to virtual machines that are hosted on a server it is recommended you use the **Virtual Machine Standard** deployment template. Also, in all cases, during deployment the virtual network will need to remain connected.

IMMEDIATE PATCH DEPLOYMENTS

Also applies to **Install at next reboot** patch deployments performed on offline hosted virtual machines.

When you perform an immediate deployment to a physical machine, an online workstation virtual machine, or an offline workstation virtual machine, the files required for the deployment are copied to the target machine immediately and the deployment is scheduled to occur immediately using the scheduler on the target machine. The patch installation is performed on the target machines and the console is not actively involved. If the machine is in a different power state from when it was last scanned, the deployment will fail.

When you perform an immediate deployment to a virtual machine that is hosted on a server, the entire deployment process occurs on the Ivanti Patch for Windows® Servers console machine. The console determines the online/offline status of the hosted virtual machines and the console service is actively involved during the patch installation. This allows the console service to modify the state of the hosted virtual machines during the deployment.

The following table summarizes what happens at the time you perform an immediate deployment based on where the virtual machines are defined within the machine group.

Machine Group Tab Used to Define the Virtual Machine	Target Machine is Online	Target Machine is Offline
Machine Name, Domain Name, IP Address/Range, Organizational Unit	Push files and initiate deployment immediately.	Fail

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Workstation Virtual Machines	Fail	Push files and schedule on target; deployment will occur the next time the virtual machine is brought online.
Hosted Virtual Machines	Push files and initiate deployment immediately. The process is the same as a physical machine except that snapshots will be taken and deleted as directed by the deployment template.	*See steps below. VMware tools must be installed on the virtual machine in order for the deployment to be successful.

*During deployment to an offline hosted virtual machine or an offline virtual machine template, the following steps occur:

1. **[Conditional: Templates Only]** Convert the virtual machine template to an offline virtual machine.
2. **(Optional)** Take a snapshot if the deployment template is configured to take a pre-deployment snapshot.
3. **(Optional)** Delete old snapshots if one of the snapshot thresholds defined on the patch deployment template is exceeded.
4. Copy the patches to the offline virtual machine.
5. Reconfigure the following on the offline virtual machine:
   - Disable the network adaptor's **Connect at power on** option. This is done so that the machine is isolated from the network when the patch process is run.
   - Disable Sysprep so it will not automatically configure the machine's operating system when the machine is first powered on.
6. Power on the virtual machine.
7. Install the patches.
8. Power down the virtual machine.
9. Reset the machine configuration to its original network connection and Sysprep settings.
10. **(Optional)** Take a snapshot if the deployment template is configured to take a post-deployment snapshot.
11. **(Optional)** Delete old snapshots if one of the snapshot thresholds defined on the patch deployment template is exceeded.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

12. **[Conditional: Template Only]** Convert the offline virtual machine back to a virtual machine template.

SCHEDULED PATCH DEPLOYMENTS

Also applies to **Install at next reboot** patch deployments performed on online hosted virtual machines and offline workstation virtual machines.

When you schedule a deployment to a physical machine, an online workstation virtual machine, or an offline workstation virtual machine, the files required for the deployment are copied to the target machine immediately and the deployment is scheduled using the scheduler on the target machine. The patch installation is performed on the target machines and the console is not actively involved. At the time of the actual deployment, if the machine is in a different power state from when it was last scanned, the deployment will fail.

When you schedule a deployment to a virtual machine that is hosted on a server, the entire deployment process is scheduled to occur on the Ivanti Patch for Windows® Servers console machine using the scheduler on the console. The online/offline status of the hosted virtual machines is determined at the scheduled time, and the console is actively involved at the time the patches are installed. This allows the console to modify the state of the hosted virtual machines during the deployment.

The following table summarizes what happens at the time you schedule a deployment based on where the virtual machines are defined within the machine group.

Machine Group Tab Used to Define the Virtual Machine	Target Machine is Online When Scheduled	Target Machine is Offline When Scheduled
Machine Name, Domain Name, IP Address/Range, Organizational Unit	Push files to the target and schedule the deployment on the target. The deployment will occur the next time both of the following are true: • The machine is online • The scheduled time has passed	Fail

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Workstation Virtual Machines	Fail	Push files to the target and schedule the deployment on the target. The deployment will occur the next time both these are true: • The machine is online • The scheduled time has passed
Hosted Virtual Machines	Schedule the deployment on the console. At the scheduled time (or, for **Install at next reboot** deployments, when the machine is restarted), treat as an immediate deployment. See **Hosted Virtual Machines** in the previous table.	

If the scheduled deployment contains a mix of hosted virtual machines and other types of machines, the machines are separated into two groups. The deployment of the hosted virtual machines is scheduled to occur on the console at the scheduled time. For all machines other than hosted virtual machines, the files are copied to the target machines immediately and the deployment is scheduled to occur using the scheduler on the target machine.

CREDENTIAL AND POWER STATE REQUIREMENTS FOR A SUCCESSFUL DEPLOYMENT

Keep in mind that, from Ivanti Patch for Windows® Servers's point of view, the definition of a successful deployment depends on where the virtual machine is located. A successful deployment to a hosted virtual machine means the machine is fully patched, while a successful deployment to a workstation-based virtual machine means the patches have been pushed to the offline virtual machine.

When performing the deployment, the program will attempt to authenticate to the target machine using the credentials defined in the **Manage Machine Properties** dialog. If the credential is invalid the deployment will fail. For workstation-based virtual machines, if the power state of the machine has changed since the scan, the deployment will fail.

For more information, see Power State and Credential Requirements for VMs.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deploying Service Packs

This describes the process for deploying service packs to agentless machines. For information on deploying service packs to agent-based machines, see Using a Service Pack Group.

Service pack deployments are handled differently than patch deployments. Since Microsoft recommends that a service pack be applied before all patches, Ivanti Patch for Windows® Servers will not allow you to deploy service packs and patches in the same deployment. It is because of this behavior that when you select **Deploy > All Missing Patches**, it literally means to deploy all missing patches; no service packs will be included with this operation.

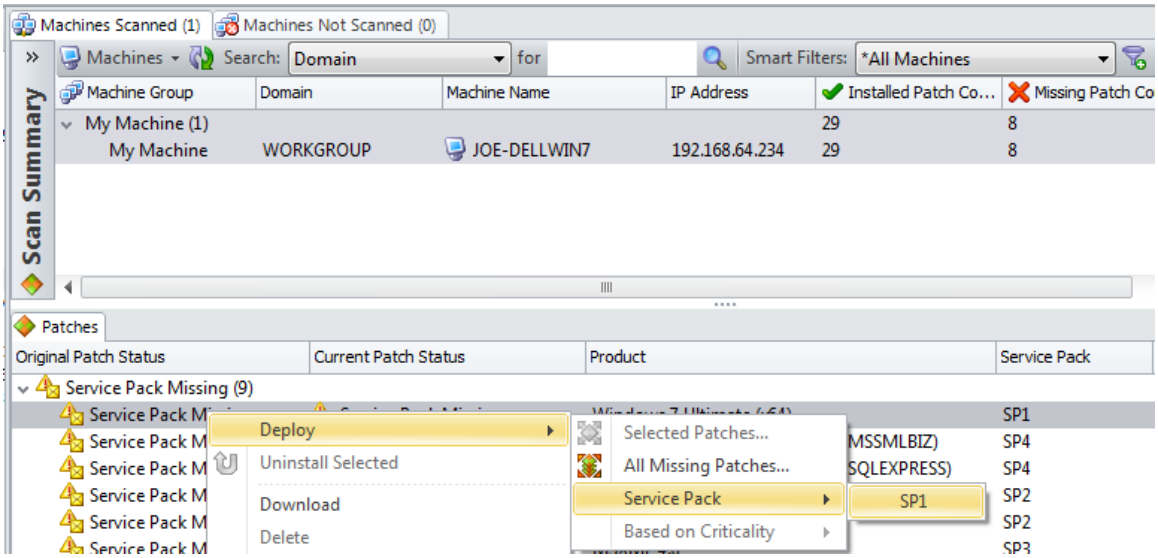
To deploy a service pack:

1. In the top pane select a machine.
2. In the middle pane, right-click the desired service pack and then select **Deploy > Service Pack > specific service pack (SP1, SP2, etc.)**.

In general, deploying the latest service pack will automatically include any previous service packs. Sometimes, however, a previous service pack is a prerequisite for a later service pack. In this case the program will only let you deploy the prerequisite service pack.

In some cases you may want to deploy a service pack that is not the latest version. This may be necessary if your organization has not approved the latest service pack or if the latest service pack is not inclusive (does not include previous service packs).

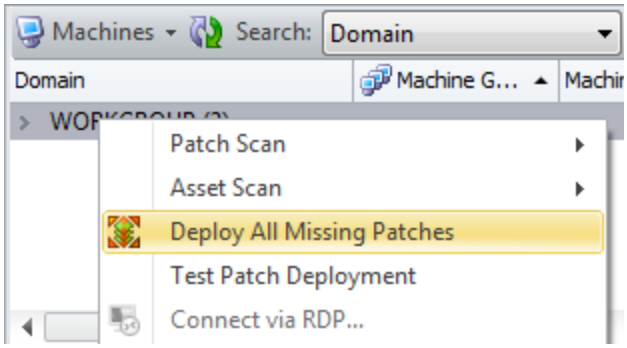
The following figure illustrates the deployment procedure from within Scan View. Service packs can also be deployed in a similar manner from within Machine View.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deploying Patches to All Members of a Domain

Patches can be deployed to all members of a single domain. From within Scan View or Machine View, group the display by domain by sliding the **Domain** column to the first column. You can then deploy to the machines in the domain using the right-click **Deploy All Missing Patches** menu.

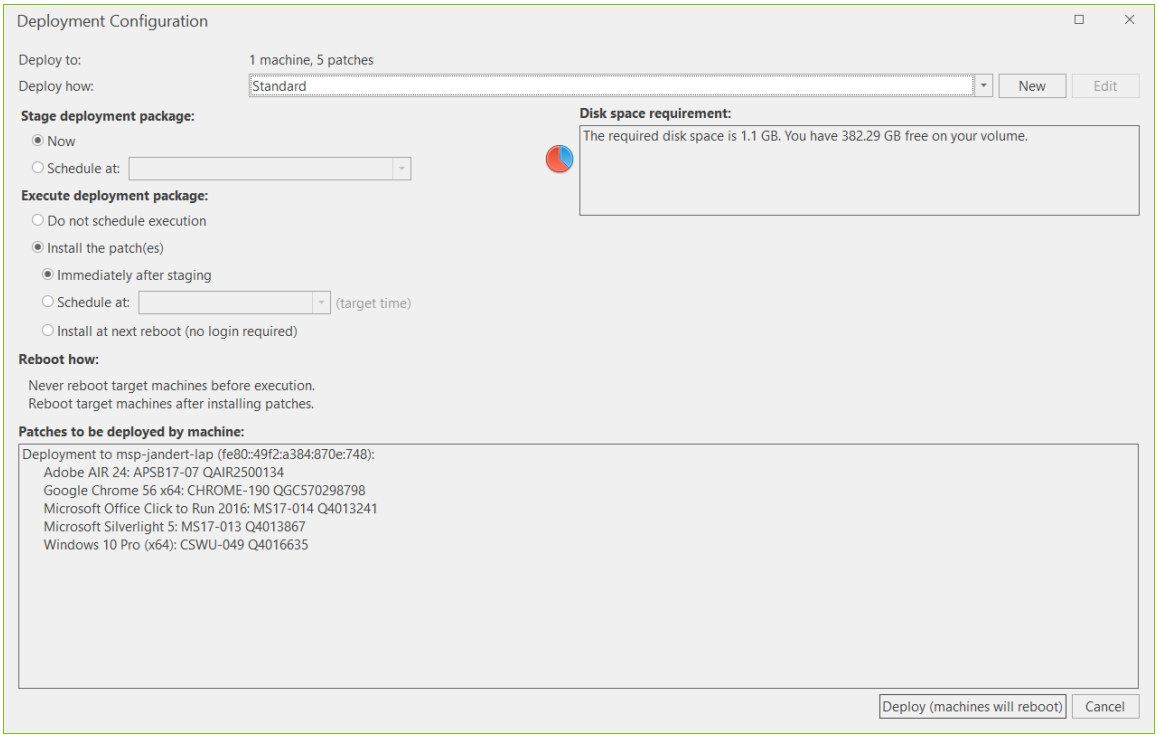


This will launch the Deployment Configuration window.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Scheduling and Configuring a Deployment

When a patch deployment is initiated the **Deployment Configuration** dialog is displayed. This dialog enables you to specify exactly when and how the patches will be deployed.



Deploy To	Indicates how many patches are being deployed and to how many machines.
Deploy How	Specify the deployment template you want to use. There are two buttons associated with this field: • **New**: Enables you to create a new deployment template. • **Edit**: Enables you to permanently modify the selected deployment template. The default templates (**Agent Standard**, **Standard**, and **Virtual Machine Standard**) cannot be modified. Clicking **Edit** lets you view but not change the default templates.
Disk space requirement	Provides status information about the patches that will be deployed.
Stage deployment package	Specify when you want the patches to be staged. The staging steps include creating the deployment package and copying the package to the target machine. Your options are:

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **Now**: The staging process will begin right after you click **Deploy**. • **Schedule at**: Enables you to choose the date and time at which the staging process will occur.
Execute deployment package	Specify when you want to deploy the staged patches. Your options are: • **Do not schedule execution**: Choose this option if you do not want Ivanti Patch for Windows® Servers to deploy the staged patches. You might choose this option if you want to manually start the patch installation at the remote machines at a later time. You have two options for deploying the patches after they are copied to the target machines: • Deploy from the console: Initiate the deployment using any of the standard methods. The deployment process will be faster than normal because the patch files have already been downloaded and copied to the target machines. • Deploy from the remote machine: On the remote machine, go to the *C:/Windows/ProPatches/Staged/<timestamp>/* directory and execute the batch file named **InstallPatches-#.bat**. • **Install the patch(es):** There are three options for installing patches. • **Immediately after staging:** The staged patches are installed immediately on the target machine. • **Schedule at:** The staged patches are installed on the target machine at the time of your choosing. • **Install at next reboot (no login required)**: The staged patch files will not begin until the next time the target machine is restarted. Offline hosted virtual machines are the exception, for them the deployment process will begin immediately. For more details see **Deploying Patches to Virtual Machines**.
Reboot How	Displays the current reboot instructions defined by the selected template.
Patches to be deployed by machine	Expands the dialog to display detailed information about the machines and the patches selected for deployment.
Deploy	When you are ready to deploy your patches using the selected deployment options, click this button. If the target machines will reboot as part of the deployment process, the button name will change to **Deploy (machines will reboot)**; this serves as a reminder about the upcoming reboots.

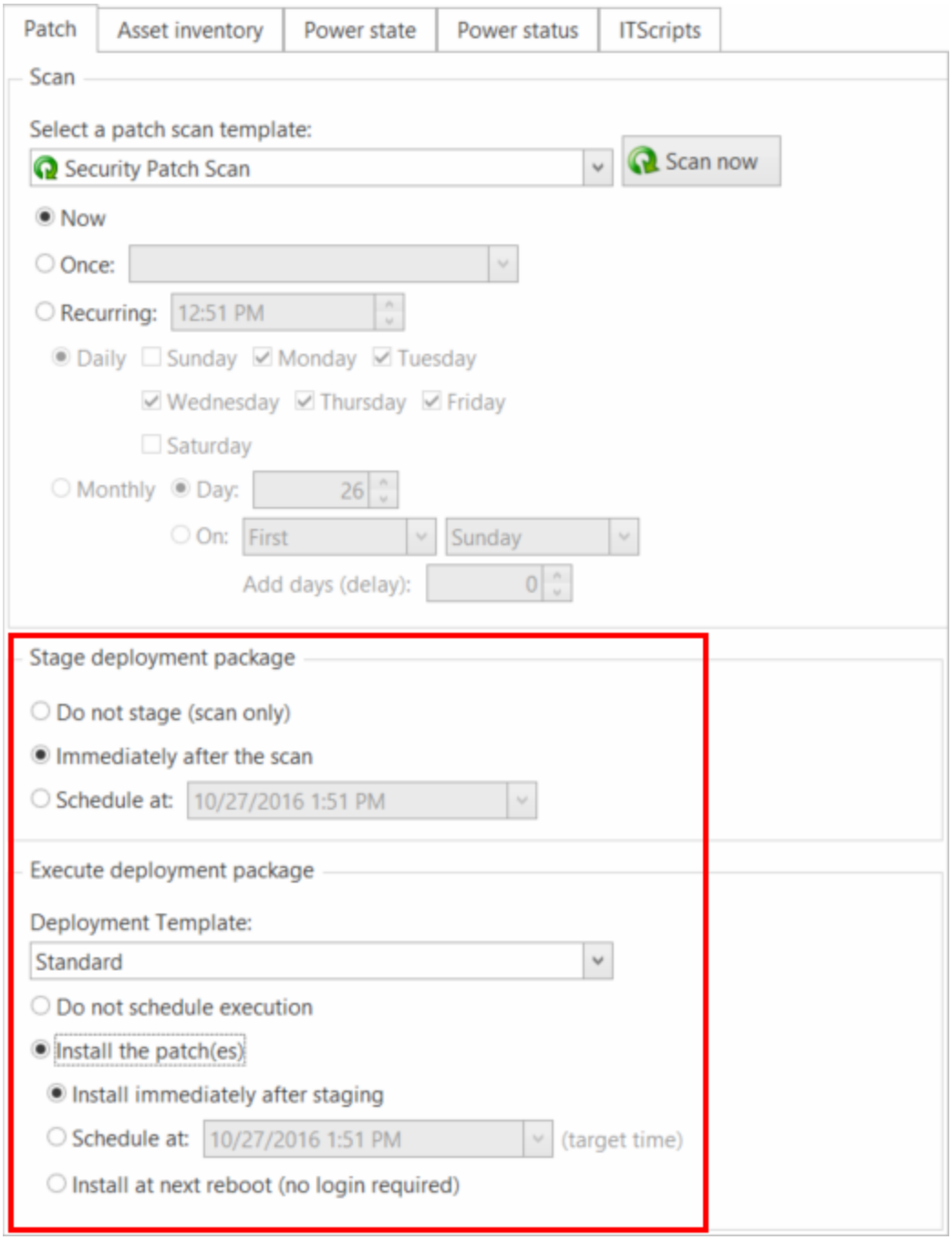
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Automatically Deploying Patches

Ivanti Patch for Windows® Servers can be configured to automatically deploy all missing patches to machines after a scan is performed. When performing domain scans, this can be especially useful as it provides a one-step update. The automatic deployment is performed by enabling the proper deployment package options on either the home page or the Run Operation dialog.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Here is how you configure Ivanti Patch for Windows® Servers to automatically deploy missing patches following a scan:

- Choose one of the following stage deployment package options:
  - **Immediately after the scan**: The staging process will begin immediately after the scan is complete. The staging steps include creating the deployment package and copying the package to the target machine.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **Schedule at**: Enables you to choose the date and time at which the staging process will occur. It is not necessary for the machine that performed the scan to be available at the scheduled deployment time.

- Choose a deployment template to use during the patch deployment.
- Choose one of the following **Install the patch(es)** options:
  - **Install immediately after staging:** The staged patches are installed immediately on the target machine.
  - **Schedule at:** The staged patches are installed on the target machine at the time of your choosing.
  - **Install at next reboot (no login required)**: The staged patch files will not begin until the next time the target machine is restarted.

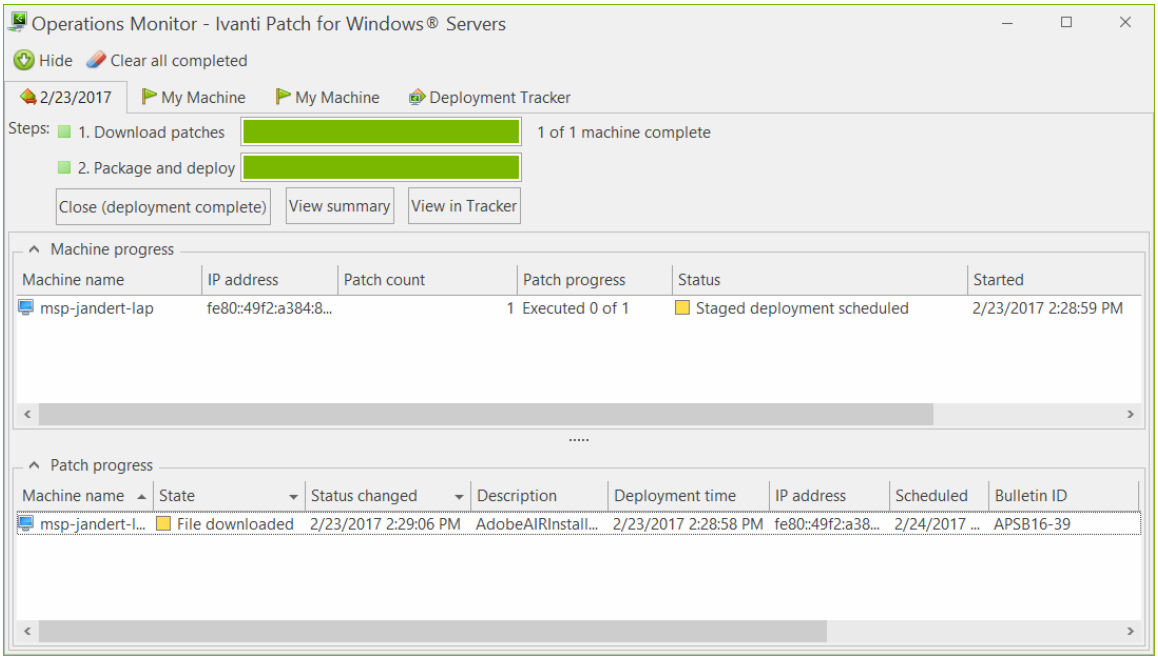


Offline hosted virtual machines are the exception, for them the deployment process will begin immediately. For more details see **Deploying Patches to Virtual Machines**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Monitoring the Deployment

The Operations Monitor is used to track the status of each patch deployment. It is displayed automatically and it provides progress information about each step in the deployment process. You can expand the list in the **Patch progress** table to view deployment information on individual patches. You can also sort the tables by dragging a column to the first position.



Scheduled patch deployments can be managed using the Scheduled Remote Tasks Manager.

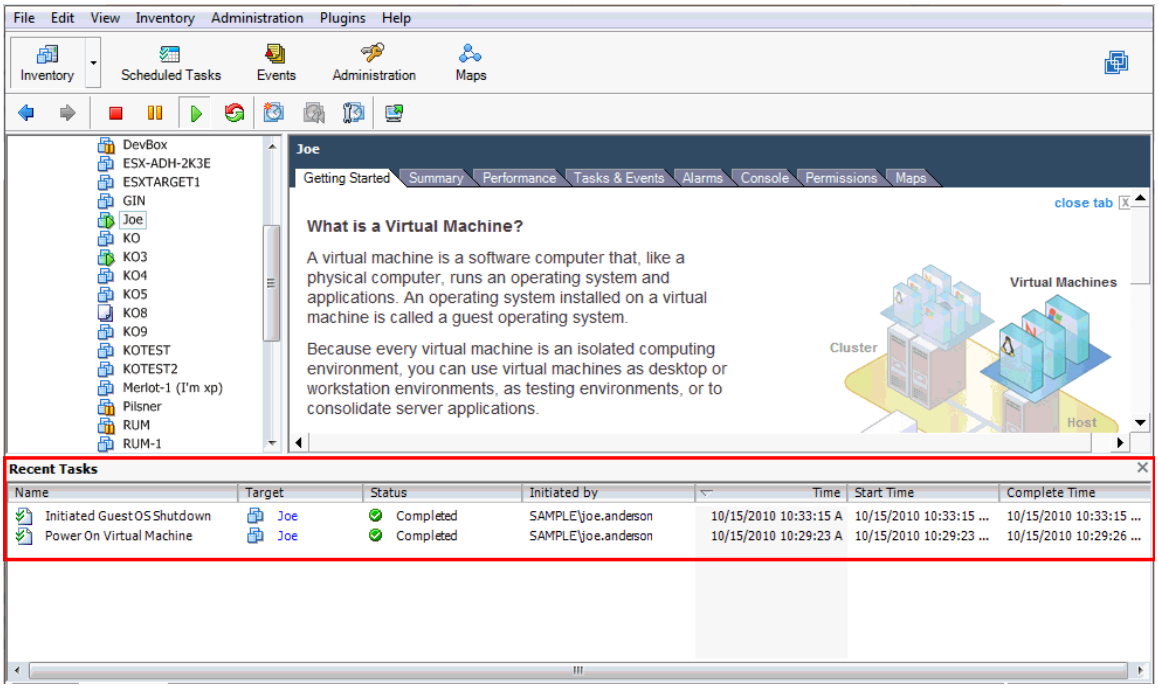
Active patch deployments can be monitored using the Deployment Tracker.

Completed patch deployments can be reviewed by selecting the deployment in the **Results** list. See Viewing Deployment Results for details.

Tips for Monitoring Patch Deployments to Virtual Machines

- When using Deployment Tracker, if you notice that a server task has failed for a virtual machine (for example, taking a snapshot or re-enabling the network), you can complete the task using your client software.
- In addition to using the tracking tools provided by Ivanti Patch for Windows® Servers, for virtual machines that are hosted on a server you can also use your client software to monitor the patch deployment progress. For example:

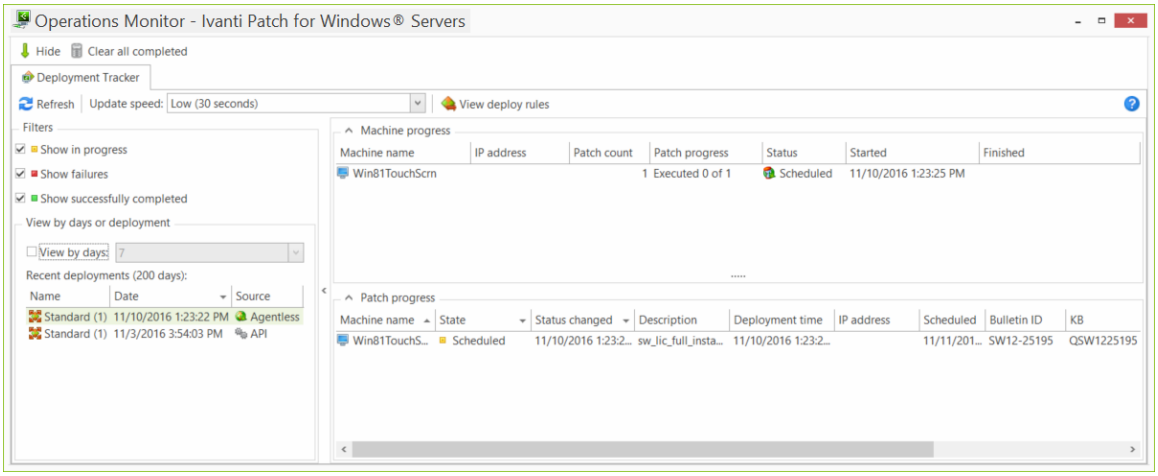
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Deployment Results

If you select a deployment from the **Results** list in the navigation pane, details about the deployment are displayed on the **Deployment Tracker** tab within the Operations Monitor. The top pane displays a list of the machines involved in the deployment and shows how many patches each machine received. The lower pane provides information about how the patches were deployed. For more information, see About the Deployment Tracker Dialog.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Canceling a Deployment

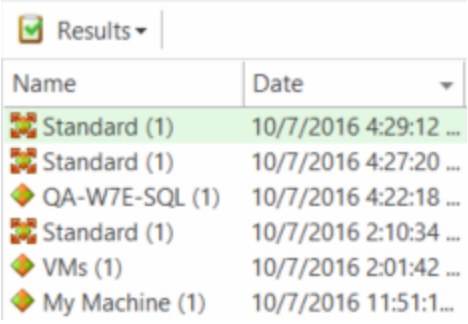
There are several ways to cancel a patch deployment.

- Immediately following the initiation of a patch deployment, the Operations Monitor appears and displays the status of the steps in the deployment preparation process. You can use the **Stop deployment** button to cancel any deployment that is still in the preparation stage.
- After the Operations Monitor shows that the deployment preparation process is complete, you can right-click on a scheduled job in either Operations Monitor or Deployment Tracker and select **Cancel deployment**. You can cancel scheduled deployments on multiple machines at one time.
- You can use the Scheduled Remote Tasks Manager to delete any patch deployment tasks currently scheduled on any of the machines in your network. Simply right-click the task(s) and select **Delete**.
- You can select a deployment in the **Results** list of the navigation pane and use the right-click menu to cancel the deployment.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deployment History

Even after a series of deployments, all of the results of prior deployments are just a click away. The deployment results are recorded in the **Results** list in the navigation pane. In addition to deployments, the **Results** list also maintains a list of recent scans. The number of items shown in this list is configurable using **Tools > Options > Display > Recent Items**.



Additionally, you can get a complete list of available prior deployments by choosing **Manage > Items**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About Deployment Templates

When deploying patches to a machine, Ivanti Patch for Windows® Servers allows you to specify a number of different options such as whether the deployment target should be restarted after deployment, how fast the patches should be copied to the remote machine, whether reports should be sent, and much more.

Ivanti Patch for Windows® Servers provides three predefined deployment templates:

- The **Agent Standard** deployment template is designed to be used with agents. It will perform a post-patch deployment reboot only when needed.
- The **Standard** deployment template is designed to be used with agentless deployments initiated by the console. It will always perform a post-patch deployment reboot.
- The **Virtual Machine Standard** deployment template is designed for use with virtual machines. It will take a pre-deployment snapshot of any virtual machine that is hosted on a server, and it will delete old snapshots that are more than four days old.

If you wish to create your own unique deployment template, see Creating a Deployment Template.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating or Editing a Deployment Template

To work with a patch deployment template, do one of the following:

- To create a new deployment template, click **New > Deployment Template**.
- To edit an existing deployment template, in the **My Deployment Templates** list in the navigation pane, click the deployment template name.

TIP: To speed the template creation process, copy an existing template that is similar to the one you want to create. The contents of the copied template will be populated in the new **Deployment Template** dialog and you can simply modify the appropriate items. You copy an existing template by right-clicking it in the **Deployment Templates** pane and then selecting **Copy**.

The **Deployment Template** dialog contains several tabs that collectively define the characteristics of a particular deployment template. The tabs are:

- General tab
- Pre-Deploy Reboot tab
- Post-Deploy Reboot tab
- Email tab
- Custom Actions tab
- Distribution Servers tab
- Hosted VMs/Templates tab
- Used By tab

The dialog also contains **Name**, **Path** and **Description** boxes that apply to the entire template.

Name	The name you wish to assign to this deployment template.
Path	This box is used to specify the folder path that this template will reside in within the **My Deployment Templates** list in navigation pane. If you do not specify a path, the template will at the root level of the **My Deployment Templates** list. For more details, see Organizing Patch Deployment Templates.
Description	A comment that describes the purpose of this deployment template.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

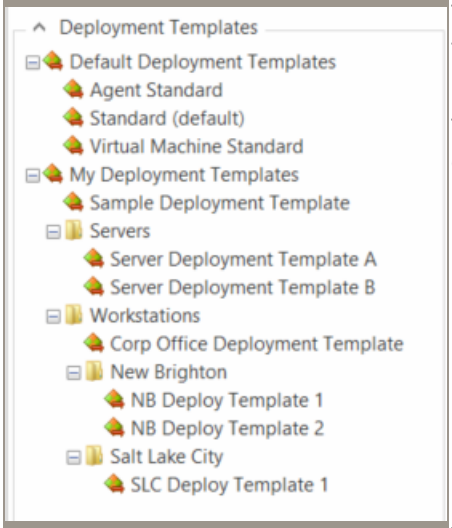
Once you have made your selections for this deployment template, click the **Save** button and then the **Close** button to save the template. Click the **Cancel** button and then the **Close** button to close the window without making any changes. Certain types of changes will require you to save the deployment template earlier in the process.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Organizing Patch Deployment Templates

If you create many patch deployment templates, you should consider organizing the templates into logical folders. Doing so will enable you to quickly locate and manage your templates. You can create as many folders and sub-folders as needed within the **My Deployment Templates** list in the navigation pane. For example, you might choose to organize your deployment templates based on the reboot requirements, by location, etc.

Sample Organizational Scheme



To create a new folder, in the **Deployment Template** dialog, type a folder path into the **Path** box. You can specify as many folder levels as needed by using a backslash (\) to separate the levels in the name. The folder will be created when you save the template. If you do not specify a path, the template will be contained at the root level of the **My Deployment Templates** list.

Folder path examples:

- \Servers
- \Workstations
- \Workstations\Location A
- \Workstations\Location B

To assign a template to a different folder, do one of the following:

A deployment template can only belong to one folder.

- In the **Deployment Template** dialog, type a new folder path into the **Path** box
- In the navigation pane, click and drag the template to a different folder
- Right-click the template and select **Edit path**.

To assign a folder and its contents to a different folder:

- Click and drag the folder to another existing folder.

The folder you move becomes a sub-folder.
To delete a folder, do one of the following:

- Change or remove the folder name in the **Path** box of all patch scan templates contained in that folder
- Click and drag the templates to a different folder

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

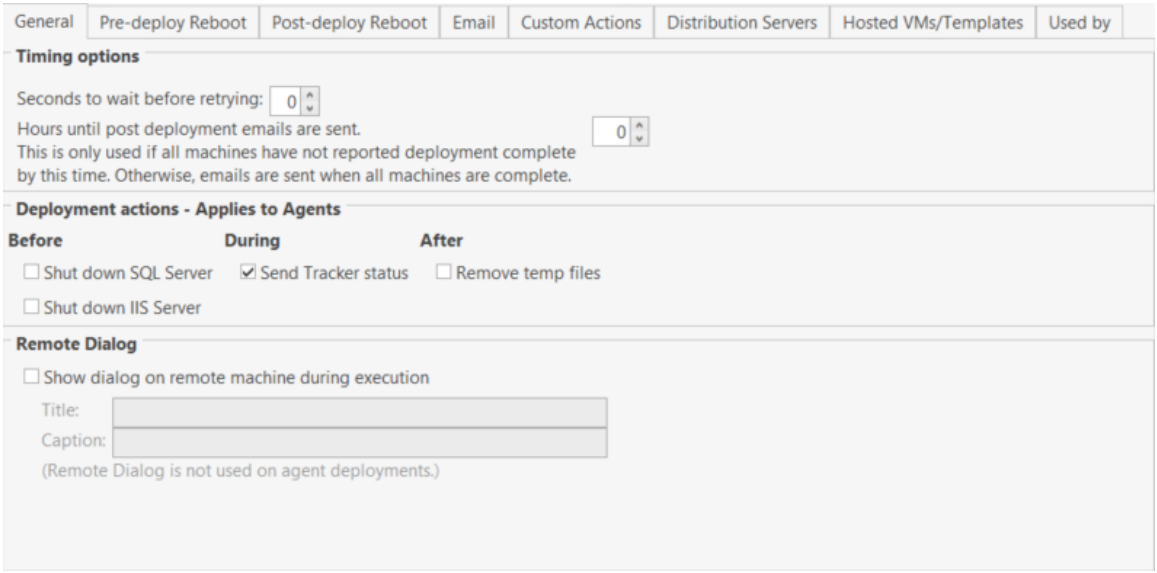


- Delete all templates contained in the folder path

The folder will be automatically deleted when the last template is removed from the folder.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deployment Template: General Tab



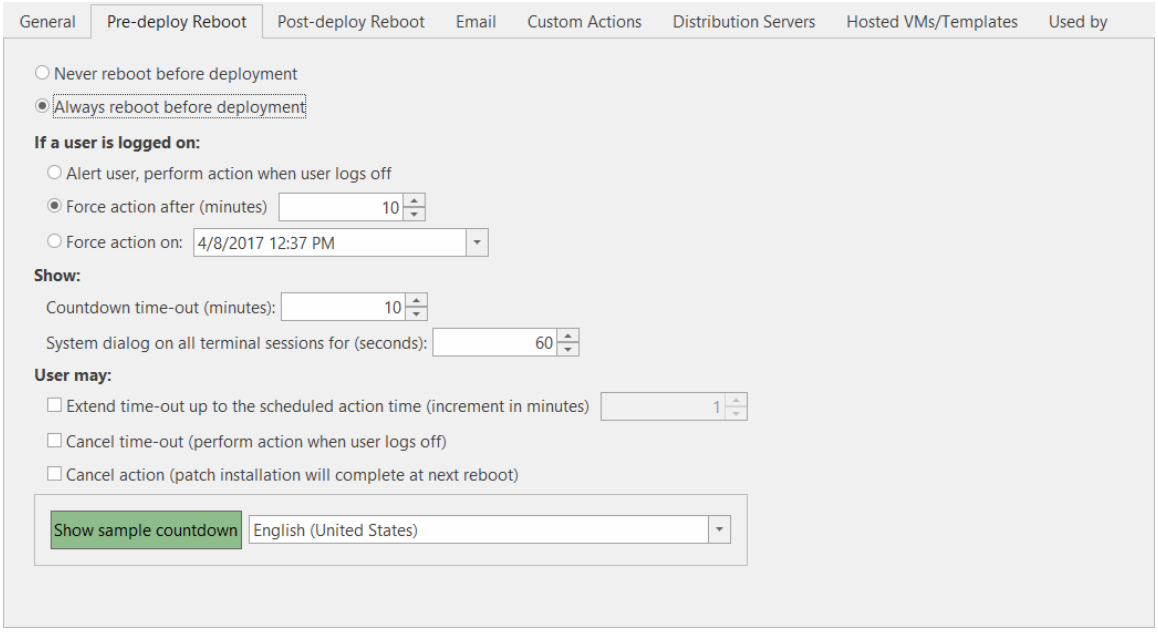
Seconds to wait before retrying	If a patch copy fails, you can specify how long to wait between retries. Valid values are from 0 to 100 seconds.
Hours until post deployment emails are sent	Enables you to specify how long to wait for patches to be successfully deployed before sending any automatic email messages. This field forces the email messages to be sent even if the console cannot determine that all the machine deployments completed because Deployment Tracker is not enabled or because a network connection is lost.
Deployment Actions	There are a number of options that can be selected to take place before, during and after patch deployment. **Before** You can choose to shut down the SQL Server and the IIS Server. These services will be automatically shut down when an SQL or IIS patch (respectively) is applied to a remote machine regardless of this setting. Use this setting to shut down these services when installing OS or similar hotfixes, particularly if you are planning to reboot the machine after installation. **During** During the deployment, you can elect not to send Deployment Tracker status messages from the machines being patched. For example, clearing the **Send Tracker status** check box makes sense if the machines will not be attached to the network when the patch installation takes place.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	After After the scan is complete, you can choose to remove the temporary patch files that were copied during the deployment process.
Remote Dialog	The Remote Dialog functions are not supported by Ivanti Patch for Windows® Servers Agent. **Show dialog on remote machine during execution:** If this check box is enabled, then if a user is logged on at the target machine at the scheduled deployment time, a dialog box will be displayed to the user when the deployment begins. **Title:** Type the text you want to appear in the dialog box title. **Caption:** Type the text you want to appear in the dialog box caption.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

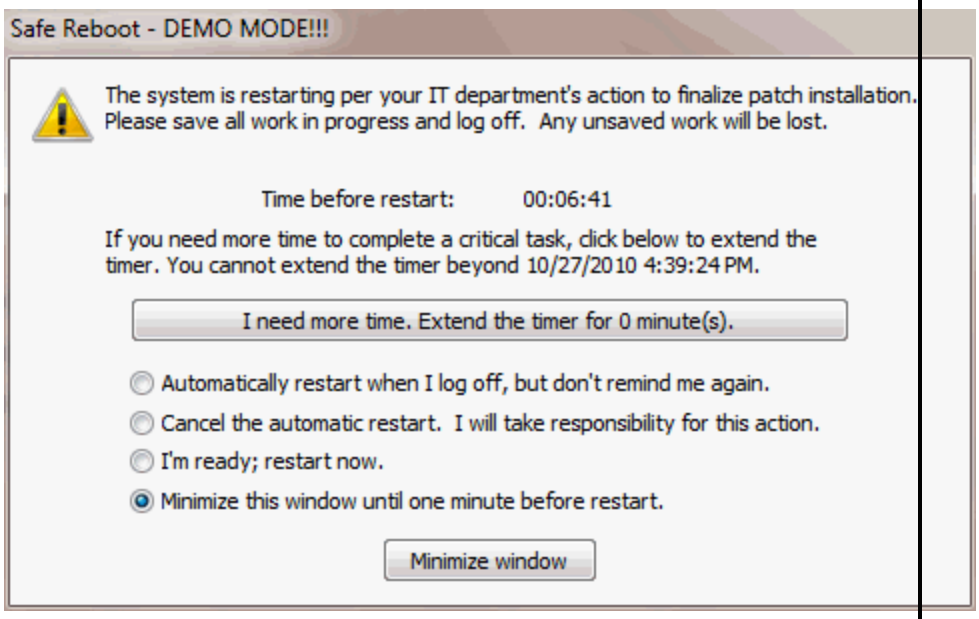
Deployment Template: Pre-Deploy Reboot Tab



Never reboot before deployment	This SafeReboot™ capability specifies that it is unnecessary to reboot each machine before the patches are deployed. The remaining options on this tab will be disabled.
Always reboot before deployment	This SafeReboot™ capability specifies that each machine should be reboot before the patches are deployed. It is considered a *best practice* to reboot machines before installing significant new software, especially for large software changes such as operating system service packs.
User Interaction	If you elect to reboot the machines, you can then specify the amount of warning that a logged-on user will receive and you can choose the degree of control the user will have over the reboot process. You can: • Alert the user that a restart will occur when they log off. • Elect to force a restart after a number of minutes have passed. • Elect to force a restart at a specific date and time.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

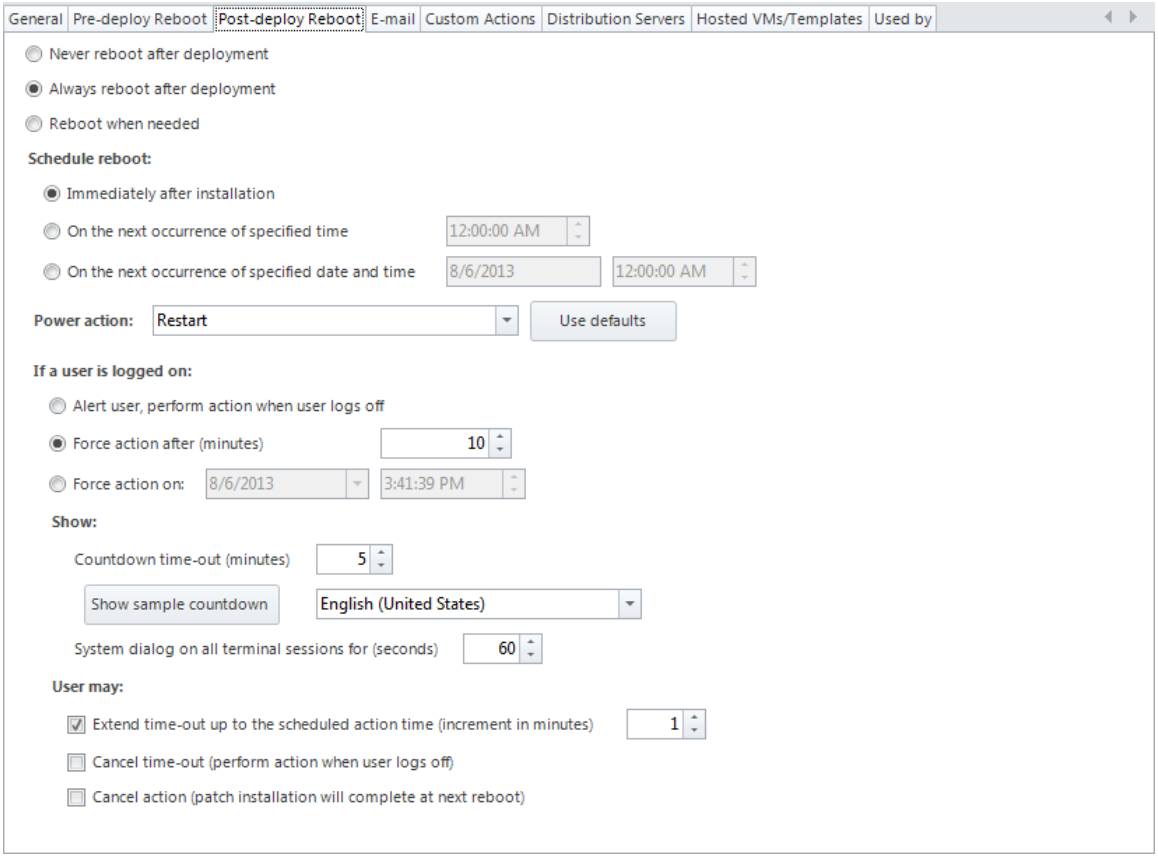
- Show a countdown dialog on the user's machine in advance of the restart. To preview the dialog box that the user will see, click **Show sample countdown**. The language box to the right can be used to preview this dialog in different languages.



- Select the duration to display the standard Windows shutdown message when the shutdown sequence is initiated.
- Allow the user to extend the time-out countdown up to a specified maximum. The maximum can be specified as either a duration or as a specific latest time that the restart will occur.
- Allow the user to cancel the time-out. If a time-out is cancelled the patches will not be deployed until the user logs off or manually restarts the machine.
- Allow the user to cancel the restart. The patches will not be installed until the machine is restarted.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deployment Template: Post-Deploy Reboot Tab

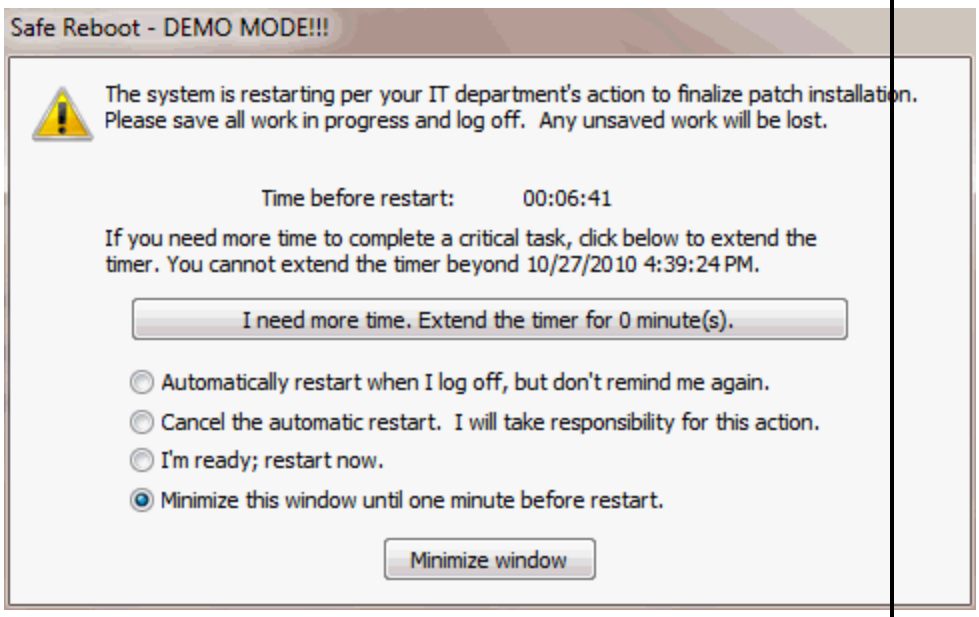


Never reboot after deployment	This SafeReboot™ capability specifies that it is unnecessary to reboot each machine after the patches are deployed. The remaining options on this tab will be disabled. As a rule, you should only enable this option when you are deploying patches that you know do not require a reboot.
Always reboot after deployment	This SafeReboot™ capability specifies that each machine should be reboot after the patches are deployed. This is the safest option when deploying patches as most patches require a reboot in order to complete, but there may be times when machines are rebooted unnecessarily.
Reboot when needed	This SafeReboot™ capability specifies that Ivanti Patch for Windows® Servers will determine whether or not a reboot of each machine is required.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Schedule reboot	If you elect to reboot the machines, you can specify when the reboot should occur. You can: • Reboot the machines immediately after installation • Reboot at a specific time • Reboot at a specific date and time If a target machine is rebooted before a scheduled reboot occurs, the scheduled reboot is no longer necessary and will be cancelled.
Power action	You can specify what state you want to leave the machines after the reboot. • **Restart:** The machines are restarted and left in a powered on state. • **Restart, then sleep if possible:** The machines are restarted and then put into a sleep state. There is a two minute delay between the completion of the restart and the time the machines are put into the sleep state. The Microsoft Scheduler is used on each target machine to initiate the sleep state following the restart. For more detailed information about sleep state, see Sleep and Hibernation Notes. • **Restart, then hibernate if possible:** The machines are restarted and then put into a hibernation state. There is a two minute delay between the completion of the restart and the time the machines are put into the hibernate state. The Microsoft Scheduler is used on each target machine to initiate the hibernation state following the restart. If a target machine is not configured to allow hibernation, the program will instead attempt to put the machine into a sleep state after the restart. If the machine cannot be put into a sleep state no action will occur. For more detailed information about hibernate state, see Sleep and Hibernation Notes. • **Restart, then shut down:** The machines are restarted and then powered off. There is a two minute delay between the completion of the restart and the time the machines are shut down. This option is useful if you want to perform a reboot in order to complete a maintenance task but then want the machines to be shut down. The Microsoft Scheduler is used on each target machine to initiate the shutdown following the restart. • **Shut down only, do not restart:** The machines are powered off. This option is also useful if you simply want to make sure non-critical machines are turned off each night or over a weekend, saving energy.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	For more information about the power management capabilities of Ivanti Patch for Windows® Servers, see Power Management Overview.
Use defaults	This button is tied to the **Restart and power action** box. When you click **Use defaults**, all remaining options on the dialog will be changed to the values recommended for use with the currently selected **Restart and power action**.
If a user is logged on	If you elect to restart the machines, you can specify the amount of warning that a logged-on user will receive and you can choose the degree of control the user will have over the restart process. You can: • Alert the user that a restart will occur when they log off. • Elect to force a restart after a number of minutes have passed. • Elect to force a restart at a specific date and time. • Show a countdown dialog on the user's machine in advance of the restart. To preview the dialog box that the user will see, click **Show sample countdown**. The language box to the right can be used to preview this dialog in different languages.  • Select the duration to display the standard Windows shutdown message when the shutdown sequence is initiated. • Allow the user to extend the time-out countdown up to a specified maximum. The maximum can be specified as either a duration or as a specific latest time that the restart will occur.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

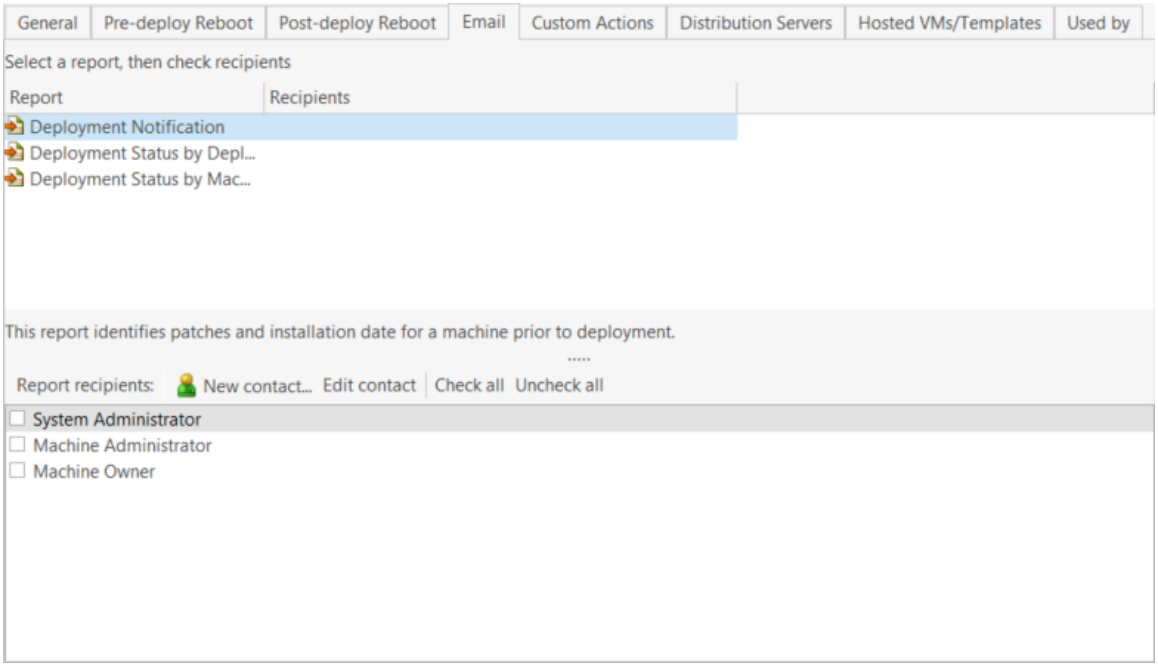
	• Allow the user to cancel the time-out. If a time-out is cancelled the patches will not be deployed until the user logs off or manually restarts the machine. • Allow the user to cancel the restart. The patches will not be installed until the machine is restarted.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deployment Template: Email Tab

This tab applies only to agentless deployments initiated from the console; it does not apply to agents that may also be using this template.

This tab enables you to specify which reports should be automatically sent and to whom the reports should get sent. The specified reports will be sent for each deployment that uses this template.



Available Reports	There are three different deployment reports that can get sent: • **Deployment Notification**: This report is sent after the deployment is successfully scheduled. It identifies the patches that will be deployed and the date and time of the pending installation. • **Deployment Status by Deployment**: This report is sent after the deployment is complete and verified or after the maximum time specified on the General tab. The report provides general status information about the deployment. • **Deployment Status by Machine**: This report is sent after the deployment is complete and verified or after the maximum time specified on the General tab. The report identifies each machine included in the deployment and indicates if the patch deployment on each machine was successful or unsuccessful.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Report Recipients	Lists the contacts you want to receive a particular report. The contacts listed are those contained in the address book. You can add new contacts or edit contact information by clicking the **New Contact** and **Edit** buttons, respectively.

To specify which reports should be automatically sent and to whom they should be sent:

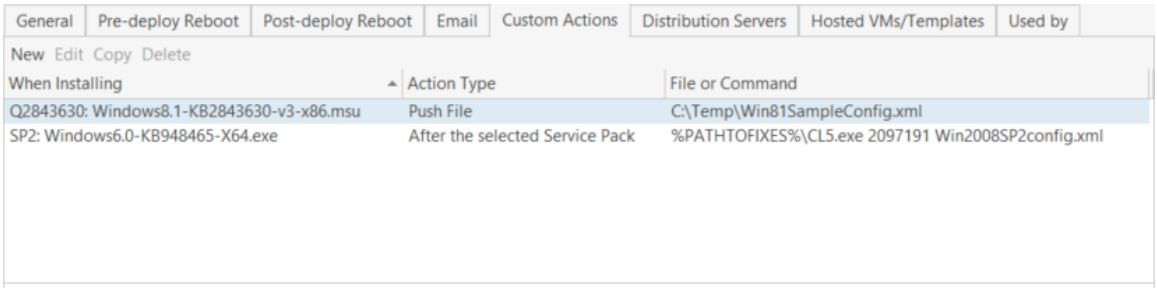
1. Select a report in the **Available Reports** list.
2. In the **Report Recipients** list, select the groups and/or individuals you want to email the report to.

   You can select all and clear all recipient check boxes using the **Check All** and **Uncheck All** buttons, respectively. The selections you make are added as report recipients in the **Available Reports** list.
3. Repeat Step 1 and Step 2 for each report you want to be automatically sent.
4. When finished, click **Save**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

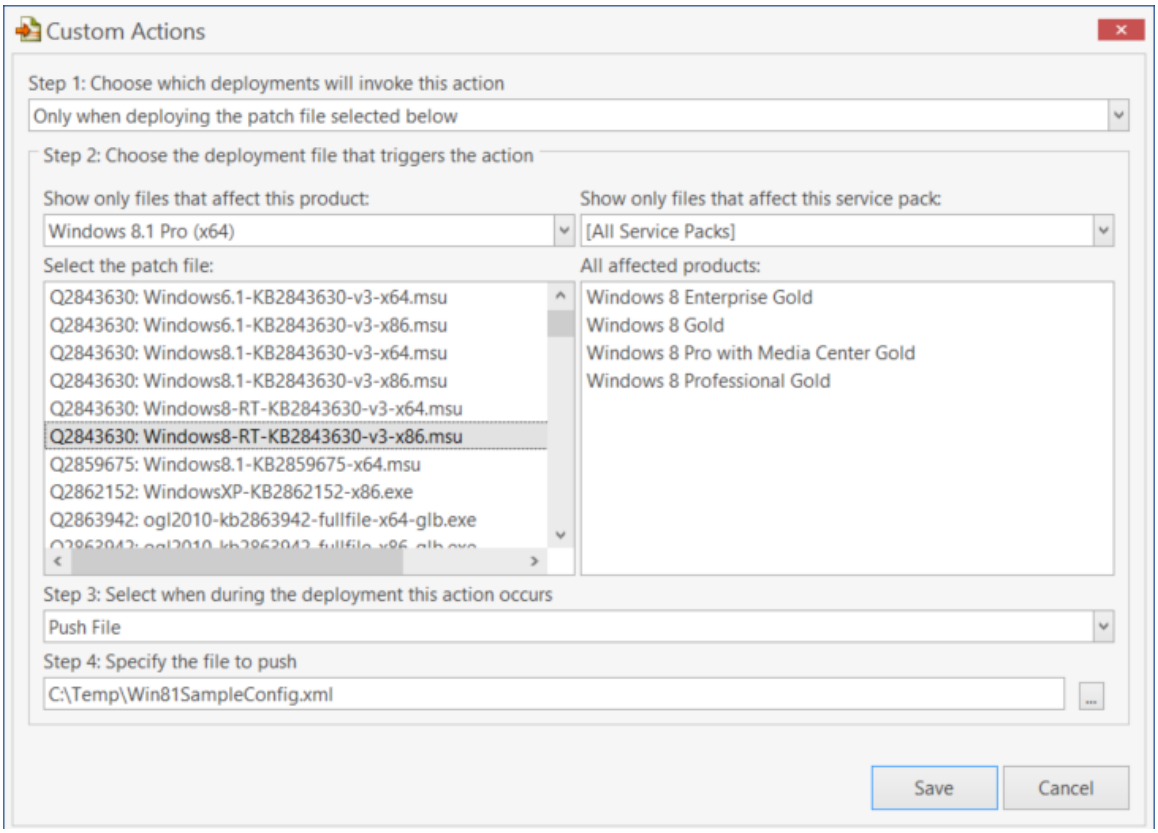
Deployment Template: Custom Actions Tab

The functions on this tab are not supported by Ivanti Patch for Windows® Servers Agent.



This tab gives you the ability to push custom files to the machines being patched, and to program customized commands that will be executed during patch deployment. A custom action may include executing a specific command or invoking a custom batch file at specified time(s) during the deployment process. You can specify custom files and actions that occur during every deployment that uses the template, or only for those deployments that install a specific patch or service pack.

To program a new action, click **New** and the **Custom Action** dialog appears.



Step 1: Specify what patch deployment action will trigger the command.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **All deployments using this template:** Allows you to perform actions such as custom logging.
- **Only when deploying the patch/service pack selected below:** Allows you to perform actions only when pushing a specific patch or service pack to a target machine using this deployment template.

Step 2: If in Step 1 you indicate that only the deployment of specific patches or service packs will trigger the command, specify those files here.

Step 3: Specify when during the patch deployment process the command will be triggered. The choices are:

- **Push File** (pushes a custom batch file or custom executable file to the target machines as part of the deployment)
- **Before any patches** are installed
- **Before each patch** or **Before the selected patch/service pack** is installed
- **After each patch** or **After the selected patch/service pack** is installed
- **After all patches** are installed (but before reboot)
- **After reboot**

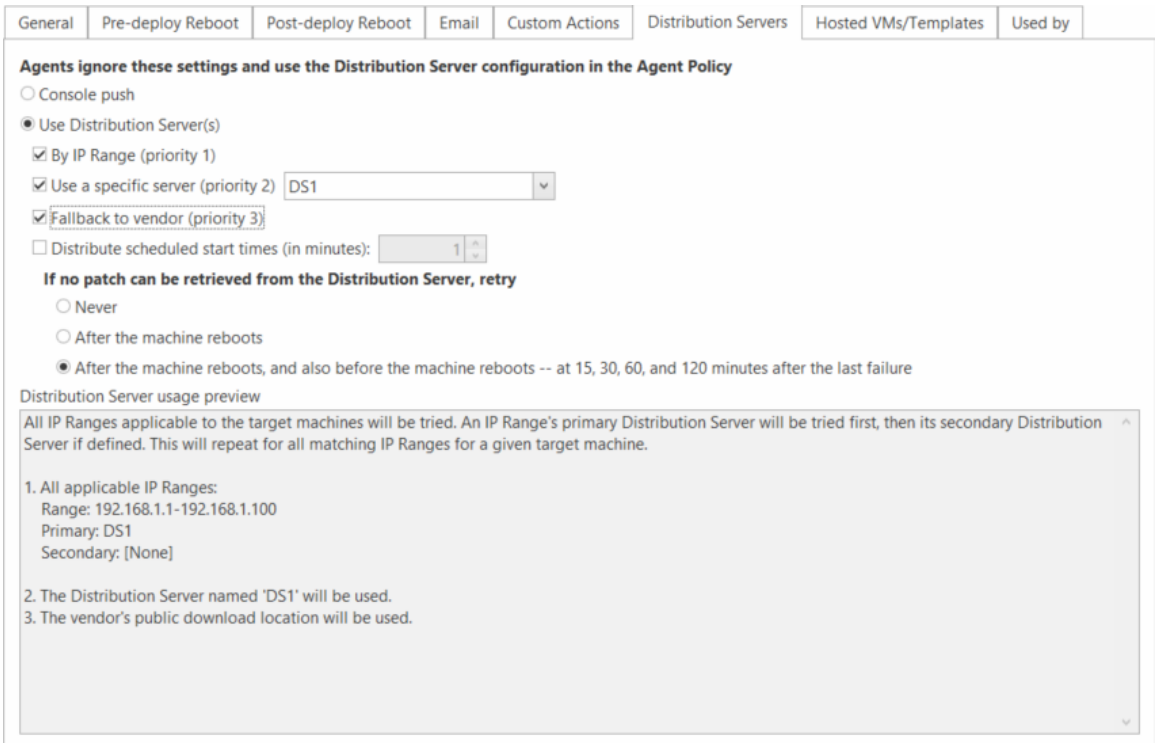
Step 4: Specify the file to push or the command to execute. The command will be inserted into the patch installation batch file at the point(s) specified in Step 3. If Step 3 specifies **Push File** then the specified file will be copied to the target machines and put in the C:\Windows\ProPatches directory. The base folder location can be changed using the **Patch drive path** option on the **Machine Properties** dialog. You can reference the file in other custom actions by specifying **%PATHTOFIXES%file_name**.

Example 1: If you push the file **myFile.exe**, you can execute that file with the following custom command: **%PATHTOFIXES%myFile.exe**.

Example 2: If you push the batch file **myCommands.bat** to the target machines, you can invoke the batch file at the appropriate point in the deployment with the following custom command: **call%PATHTOFIXES%myCommands.bat**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deployment Template: Distribution Servers Tab



Console push	If enabled, indicates that a distribution server will not be used and the console will serve as the source for all patches.
Use Distribution Server(s)	If enabled, indicates that a distribution server will serve as the source for all patches during deployments that use this template. The three check boxes that immediately follow are used to determine which distribution server to use, if any. The program will search for an available distribution server using only those options that you enable, and the search will be performed in the listed order (priority 1, priority 2 and priority 3). If you enable **Use Distribution Server(s)** but do not specify at least one of the three source options, the deployment will fail. See Configuring Distribution Servers and Assigning IP Addresses to Servers for information on configuring the distribution servers.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	When patches are deployed via distribution servers, patches are not pushed to the target machines. Rather, the target machines will download the patches from one or more distribution servers. Patches must be copied from the console's patch download directory to the servers before they will be available for deployment. See Synchronizing Servers for information on copying patches to your distribution servers.
By IP Range (priority 1)	If enabled, indicates that the distribution server to use will be determined by the IP address of each target machine. In order for this to work you must have previously defined one or more IP ranges and assigned the ranges to a primary distribution server and to a backup server.
Use a specific server (priority 2)	If desired, specify a specific distribution server to use if the primary and backup distribution servers defined by the **By IP Range** option are unavailable. If the **By IP Range** option is not enabled, the server specified here will become the default server.
Fallback to vendor (priority 3)	If the distribution servers identified by the first two options are not available, enabling this check box will allow the machine being patched to try to download the patch from the patch vendor's website. This option does not apply to custom patches because custom patches do not contain download URLs. Custom patches must be either pushed to the target machines from the console's patch download directory or pulled by the target machines from a distribution server.
Distribute scheduled start times (in minutes)	If you are deploying patches to a large number of machines at the same time, all the machines will begin to download the patches from the distribution server at approximately the same time. If you enable this option, the start times for the machines will be randomly distributed over the interval that you specify. This can help to reduce the peak network load.
If no patch can be retrieved from the Distribution Server, retry	If no patches can be obtained from the distribution server at the scheduled deployment time, you can specify how often you want to attempt a retry. If at least one patch is successfully downloaded, the deployment will resume without a retry, even if one or more patches are not successfully downloaded. • **Never:** A retry will not be attempted and the deployment will fail. • **After the machine is rebooted:** A retry will be attempted each time the target machine is rebooted, for up to three reboots. If the download process is still failing after three reboots, the deployment will fail.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **After the machine reboots, and also before the machine reboots -- at 15, 30, 60, and 120 minutes after the last failure:** A retry will be attempted at 15, 30, 60, and 120 minute intervals after the initial failure, and again when the target machine is rebooted. Retries are also attempted after two subsequent reboots. If the download process is still failing after three reboots, the deployment will fail.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deployment Template: Hosted VMs/Templates Tab

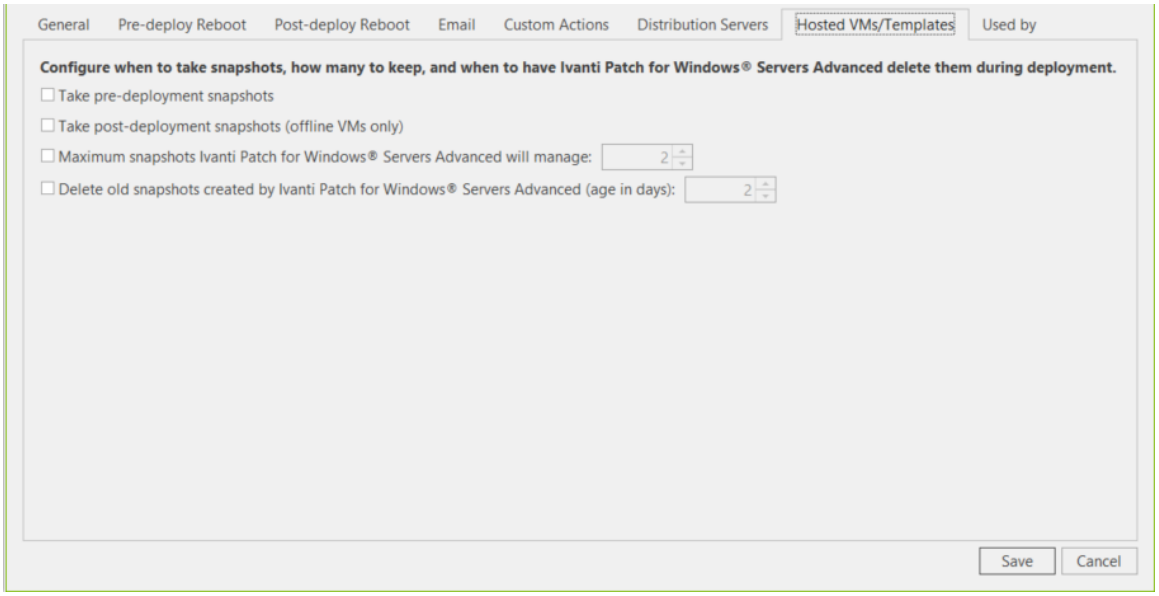
This tab allows you to remove old snapshots during the patch deployment process. If you want to schedule the removal of old virtual machine snapshots without having to perform a deployment, see Scheduled Snapshot Maintenance.

This tab only applies if you have virtual machines in your network that are hosted on one or more VMware servers. It enables you to specify if snapshots will be taken of the hosted virtual machines (or of hosted virtual machine templates) immediately before and/or immediately after patches are deployed to the virtual machines. This tab does not apply to virtual machines that reside on workstations.

What is a virtual machine snapshot? A snapshot captures the state, configuration, and disk data of a virtual machine at a given time. Snapshots are useful for storing states that an administrator or user might want to return to at some point in the future.

Complete snapshots are taken of offline virtual machines and of virtual machine templates. If a virtual machine is online at the time of the patch deployment the memory state will not be included in the snapshot—this will quicken the process and reduce the amount of time that the online virtual machine is affected.

There are reasons why you may choose to NOT take a snapshot. You may have a limited amount of disk space, or you may have performance concerns. Taking a snapshot reduces the performance of the virtual machine while the snapshot is being created.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

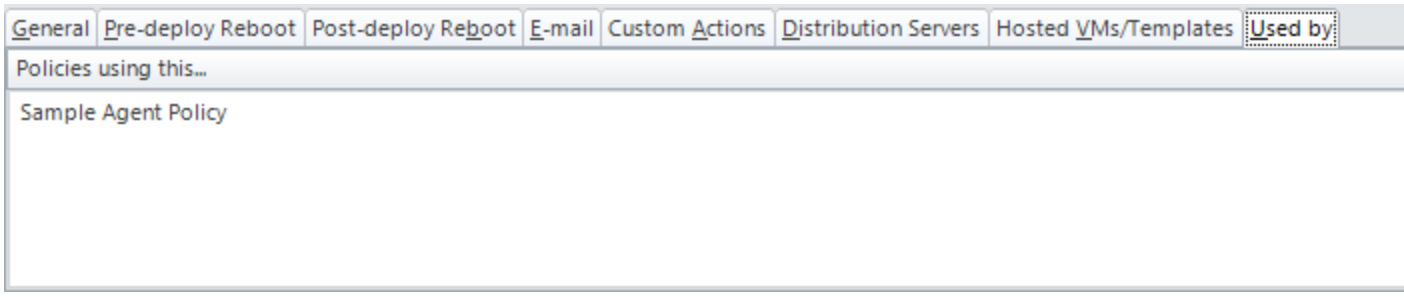
Take pre-deployment snapshots	If enabled, indicates that Ivanti Patch for Windows® Servers will take a snapshot of the hosted virtual machine or the hosted virtual machine template before deploying missing patches or service packs. Taking a snapshot of the environment is a good precaution to take in the event there is a problem with the deployment or if at some point you simply want to revert to the original environment.
Take post-deployment snapshots	If enabled, indicates that Ivanti Patch for Windows® Servers will take a snapshot of the offline virtual machine or virtual machine template after deploying missing patches or service packs. Taking a post-deployment snapshot of the environment is a good idea in the event there is a problem down the road and you want to revert to a time immediately following the patch deployment.
Maximum snapshots Ivanti Patch for Windows® Servers will manage	If enabled, indicates the maximum number of snapshots that will be maintained for each offline virtual machine or virtual machine template. Only snapshots created by Ivanti Patch for Windows® Servers are counted. If the threshold is exceeded the oldest snapshot is deleted. The threshold is checked each time a new pre-deployment or post-deployment snapshot is made. Snapshots are saved to disk and require a certain amount of storage space. It is important to limit the number of snapshots to avoid needless consumption of storage space.
Delete old snapshots created by Ivanti Patch for Windows® Servers (age in days)	If enabled, indicates the number of days a snapshot created by Ivanti Patch for Windows® Servers will be allowed to exist. Snapshots older than the specified number of days are automatically deleted. The threshold is checked each time a new pre-deployment or post-deployment snapshot is made.

You can choose to manage snapshot retention both by the number of snapshots and by the snapshot age. In this case, when a pre- or post-deployment snapshot is requested, all snapshots created by Ivanti Patch for Windows® Servers that are older than the specified number of days are deleted. If the number of remaining snapshots still exceeds the maximum number specified, the oldest of those will be deleted until only the maximum number specified remain.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deployment Template: Used By Tab

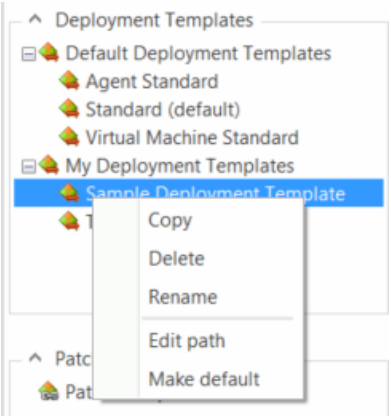
This tab shows you the agent policies that are currently using this deployment template. This is important to know if you are considering modifying the deployment template, as it tells you what other areas of the program are affected.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Managing a Deployment Template

Custom deployment templates are contained within the **My Deployment Templates** list in the navigation pane. You can edit an existing deployment template by clicking the template name. You can also right-click a template and perform a number of different actions.



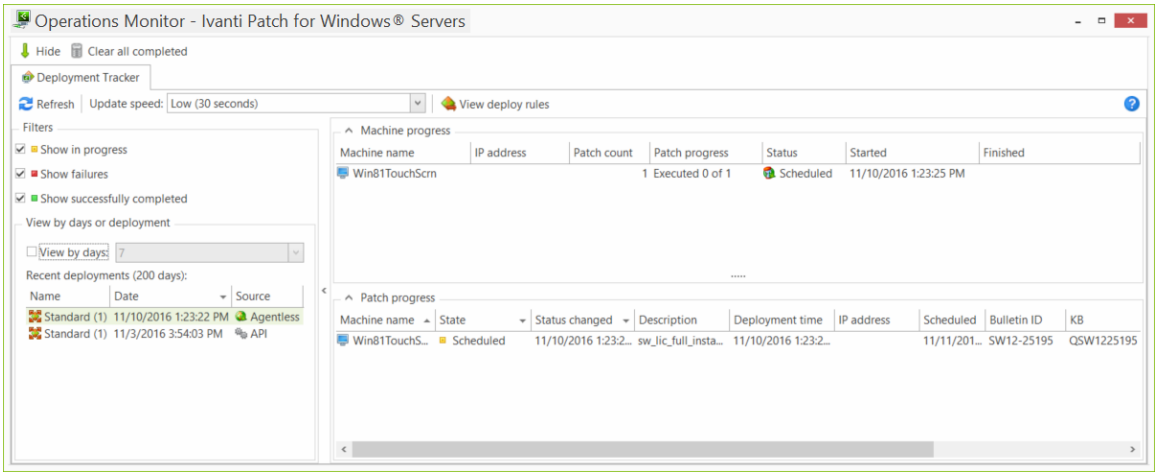
Copy	Copies the selected template. The name of the new template will be 'Copy of { selected template name }'. Change the name and the other template characteristics as desired.
Delete	Deletes the current template. You cannot delete a template that is currently being used by an agent policy.
Rename	Enables you to change the name of the deployment template. Be careful if you rename a template that is currently being used by an agent policy.
Edit path	Enables you to change which folder the template resides in within the navigation pane.
Make Default	Selecting this option will use the currently selected template as the default.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About the Deployment Tracker

Ivanti Patch for Windows® Servers includes a feature called the Ivanti Patch for Windows® Servers Deployment Tracker. This feature enables you to monitor the status of patch deployment tasks currently in progress. Deployment Tracker utilizes the Ivanti Patch for Windows® Servers Patch Service, which is a component of the Ivanti Patch for Windows® Servers Console Service. This service receives status messages from the target machines that are being patched. The service is installed and started during the Ivanti Patch for Windows® Servers installation and it listens on the same port as the other console services (TCP port 3121). If this service is stopped, then Deployment Tracker will not be able to provide updated state information.

To start Deployment Tracker, select **View > Deployment Tracker**. For information on how to use the dialog, see About the Deployment Tracker Dialog.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About the Deployment Tracker Dialog

The Deployment Tracker dialog provides at-a-glance information pertaining to patch deployment status. The information is displayed in two lists in the right pane. The **Machine progress** list shows the status of deployments on a machine basis and the **Patch progress** list shows the status of each individual patch that is scheduled for deployment.

You can view the current state of a deployment in either list. The states of a successful patch deployment are:

- Copied to machine
- Scheduled
- Executing
- Executed (pending reboot)
- Pending rescan
- Successfully installed

You can use the buttons, boxes and check boxes in the dialog to specify what deployment information is displayed in the dialog.

- **Refresh:** Refreshes the content in the dialog.
- **Update speed:** Specifies how often you want the patch deployment information within Deployment Tracker to be updated. Each update request causes the console to access the database and then report the information within Deployment Tracker. You may want to specify a slower update speed if you find that your database is being overtaxed by frequent update requests.
- **View deploy rules:** Shows the patch deployment template rules that were used when scheduling the deployment. This button is not available if the **View by days** check box is enabled.
- **Show in progress:** Shows the patch deployments that have not yet completed installation. If the status remains yellow, it could be an indication that the remote machine cannot communicate back to the Deployment Tracker.
- **Show failures:** Shows patch deployments that didn't fully take and that require more research. The Operations Monitor may provide additional information if one of the main steps in the deployment process failed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

One of the more common reasons for seeing a "Failed" item in Deployment Tracker is because a patch that requires a reboot to complete was deployed but 'Never Reboot' was specified in the deployment template. If you receive a "Failed" status in Deployment Tracker, check the Patch Details for the patch in question to see if a reboot is required to complete the installation of this patch.

- **Show successfully completed:** Shows the deployment tasks that have been successfully implemented.
- **View by days or deployment:** Use this area to specify whether you want to view all of the deployments that have occurred over the last specified number of days or view just a specific deployment.
  - **View by days:** If this check box is enabled, it means that you can specify how many days' worth of deployments to show in the right pane.
  - **Recent deployments:** This area is only available if the **View by days** check box is not enabled. It enables you to select which specific patch deployment you want to see information about in the right pane. When using this area, you can only select one deployment at a time. The patch deployments that are available for selection is defined by the **Tools > Options > Display > Recent items** box.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Canceling a Task

You can use Deployment Tracker to cancel either an incomplete deployment task or a staged deployment that has been scheduled but not yet performed. To cancel a deployment task, right-click on the scheduled job and then select **Cancel deployment**.

You can also cancel deployments using the Scheduled Remote Tasks Manager. See Canceling a Deployment for details.

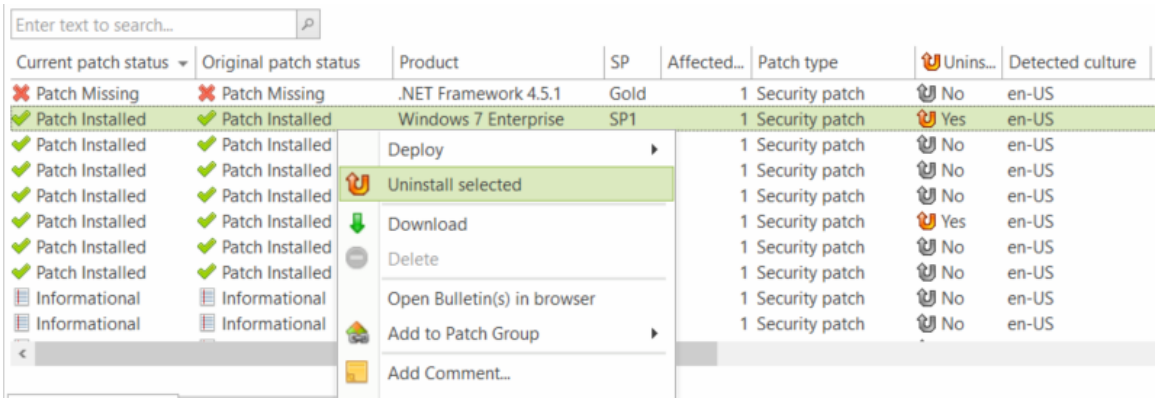
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Uninstalling Patches

Ivanti Patch for Windows® Servers provides the ability to uninstall selected patches. Not all patches can be uninstalled; only patches identified by the rollback icon  can be uninstalled. Uninstalling or "rolling back" patches restores a machine to its original state before the patch was deployed. Patches must be rolled back in the reverse order in which they were installed.

You can uninstall one or more patches from Scan View, Machine View, or Patch View.

1. In the top pane, select the desired machine(s).
2. In the middle pane, select the desired patch(es).
3. Right-click the patch(es) and then select **Uninstall Selected**.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Overview of the Custom Patch XML Process



Show Me!

To view a video tutorial on this topic, click the video icon on the left.

CAUTION! Creating and using custom patch XML files should only be attempted by experienced administrators. Creating and deploying inaccurate custom patches may have seriously adverse effects on the performance of the programs in use at your organization.

Ivanti Patch for Windows® Servers provides the ability to scan for and deploy patches not supported in the primary XML patch data file. It does this by allowing you to create your own custom patch XML files that contain the information about the additional patches and products you want to support. Ivanti Patch for Windows® Servers will then combine your custom XML files with the primary XML patch data file and use that modified file when performing scans and deployments.

Within each custom XML file you can define multiple custom products, bulletins, and patches.

- Custom product: A product not currently supported by the primary XML patch data file. For example, you might have a product that was developed strictly for use within your organization.
- Custom bulletin: Used to announce and describe a security update. A custom XML file can contain multiple bulletins, and each bulletin can contain multiple patches. Some of the information typically included in a bulletin includes a summary, known issues, a list of all affected software, and a link to the security update (patch) file. Of course, in this case the patch is contained in the same XML file as the bulletin.
- Custom patch: A software update that is not currently supported by the primary XML patch data file. A custom patch can be applied to either an existing product or to a custom product. For example, you might receive a special private patch from a vendor, you might create your own patch to a vendor's product, or you might create a patch for your own custom product.

One major difference between a regular patch and a custom patch is that you cannot download a custom patch to the patch download directory in advance of a deployment. Rather, you must make the patch available by manually copying the patch to all expected locations (typically to the console as well as any distribution servers).

If you are using agents to deploy custom patches, be certain you enable the **Use Server by IP Range** check box on the deployment template used by the agents. Custom patches cannot be downloaded from a vendor and the agents must therefore be able to download the custom patches from one or more distribution servers. See Deployment Template: Distribution Servers Tab for more information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating a New Custom XML File

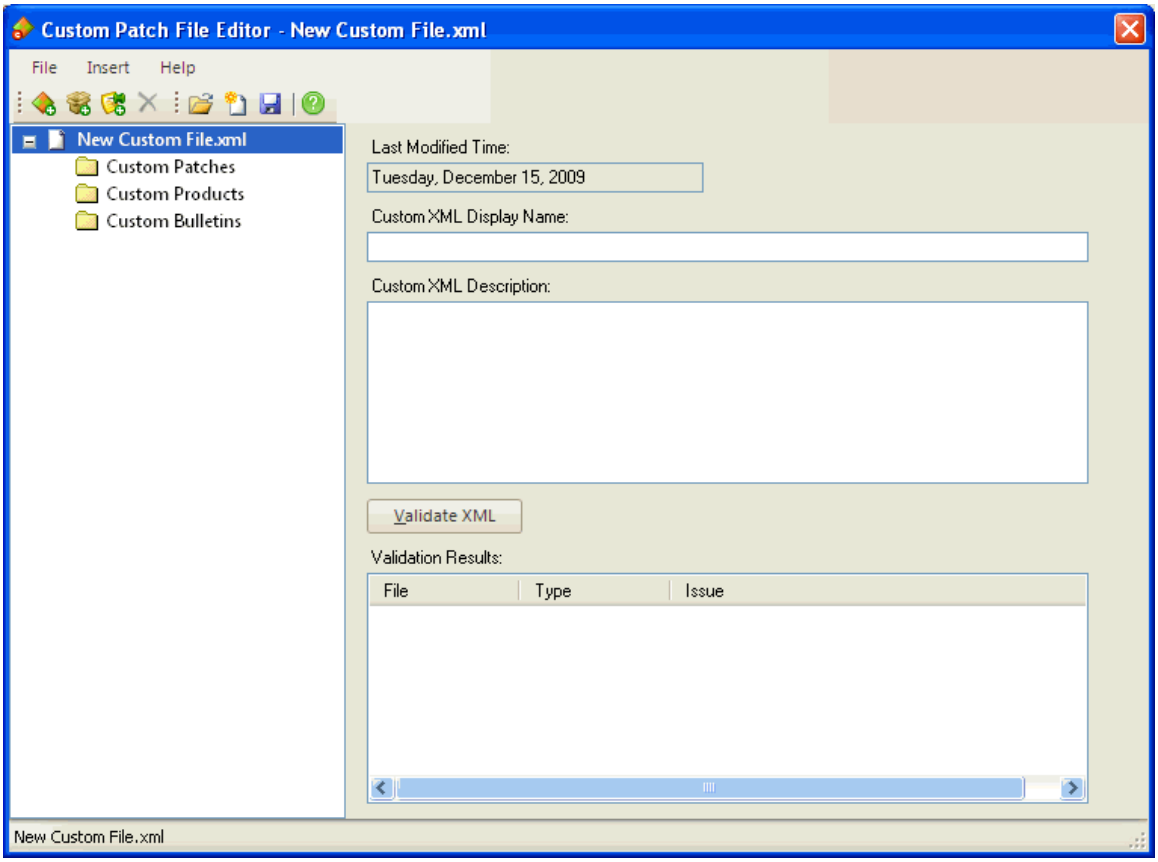
To create a customized XML file you use the **Custom Patch File Editor**.

1. Access the Custom Patch File Editor by selecting **Tools > Custom Patch Editor**.

   The **Custom Patch File Editor** dialog is displayed.

2. Create a new custom XML file by selecting **File > New** or by clicking the **Create a new custom XML file** link in the right-hand pane.

   The **New Custom File** dialog is displayed.



3. Save the new custom XML file by selecting **File > Save As** and then specifying the name and location of the file.

   You can give the file any unique name you want. The file can be saved anywhere you want, but a logical location is the program's **DataFiles** folder.

   The **DataFiles** folder is located here: **C:\ProgramData\LANDESK\Shavlik Protect\Console\DataFilesC:\ProgramData\ScriptLogic Corporation\Patch Authority Ultimate\Console\DataFiles**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

This is the directory used to store all the other XML files used by the program.

4. Use the fields in the right-hand pane to define the file characteristics.

Last Modified Time	This read-only field indicates the last time the custom XML file was changed.
Custom XML Display Name	Type a unique name for the file.
Custom XML Description	Type a description that explains the purpose of the file.
Validate XML	To verify that the XML file is properly formed and valid, click this button. You should validate the XML file anytime you make modifications to the XML file. Be sure to save the file before performing the validation to ensure that you are validating the most current file.
Validation Results	Displays the results of the most recent validation check.

5. Define the bulletins, products, and patches you want included in this custom XML file.

What order to define items in a custom XML file

If creating a patch for a new product:	Then create the items in this order: 1 Create the new custom product. 2. Create a new bulletin, or tie the patch to an existing bulletin. 3. Create the new patch.
If creating a patch for an existing product:	Then create the items in this order: 1 Create a new bulletin, or tie the patch to an existing bulletin. 2. Create the new patch.

For details, see the following topics:

- Creating a Custom Product
- Creating a Custom Bulletin
- Creating a Custom Patch

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating a Custom Product

Your organization may use a custom or "home-grown" software product. In order for Ivanti Patch for Windows® Servers to be able to scan for and patch that product it must be able to detect the product. Creating a custom product provides the registry key information needed for Ivanti Patch for Windows® Servers to determine whether the custom product exists on the machines it is scanning.

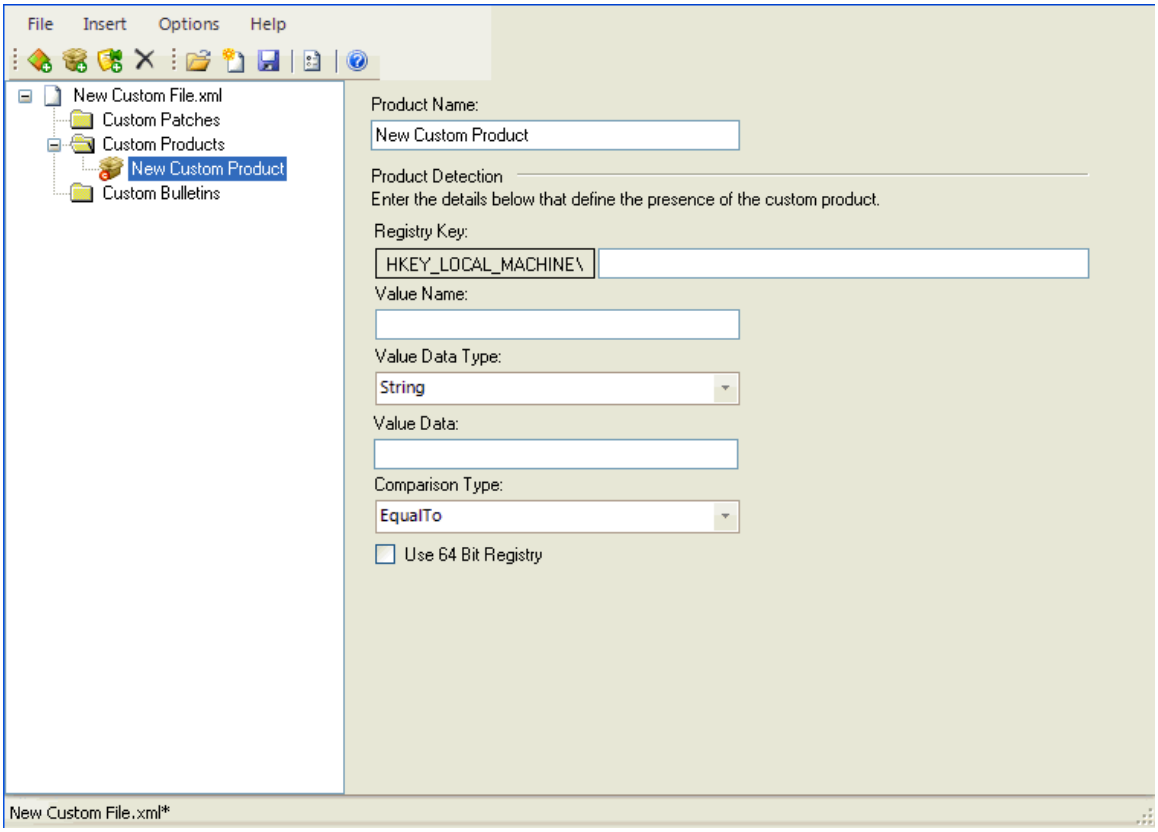
If you have multiple versions of a custom product you must define a unique custom product for each version. For example, assume you currently support both the original version as well as an updated version of a custom CRM product. Within the Custom Patch File Editor you must create a separate custom product for each version.

TIP: After importing a new custom XML file, you can use Patch View to verify the custom product is contained in the updated XML patch data file.

1. To create a custom product, within Custom Patch File Editor select **Insert > Add Product** or click the **Add Product** toolbar icon ( ).
2. Select **New Custom Product** beneath the **Custom Products** folder.

   The new custom product is selected and the product characteristics are displayed in the right pane. For example:

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



3. Use the options in the right-hand pane to define the new product.

> To get the most current registry information we recommend using the Microsoft Registry Editor (regedit), a tool for viewing settings in your system registry. You can copy the required information from this tool to the appropriate fields in this dialog.

Product Name	Provide a unique name for the product. The name cannot match a product name already defined to Ivanti Patch for Windows® Servers. Once this custom product is defined and saved, the name you provide here will be added to the **Available Products** list that is used during the patch creation process. See the **Targeting** tab section in Patch Scan Information Tab for more information.
Registry Key	You can only specify keys that are relative to the HKEY_LOCAL_MACHINE hive. The easiest and most accurate way to populate this box is to display the desired key from within the Microsoft Registry Editor, copy the key name and then paste the name into this box. The HKEY_LOCAL_MACHINE portion of the name will likely be repeated so you'll need to remove that portion of the name from the box.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Value Name	The name of the specific registry key.
Value Data Type	There are two options: • **String:** Specifies that the data must be a string. • **DWORD:** Specifies that the data must be a number.
Value Data	The expected value of the registry key. You can find this value by locating the key within the Microsoft Registry Editor and then looking in the Data column.
Comparison Type	This specifies the test criteria you want to use when determining if a product exists on a scanned machine. While there are many different options here, they can basically be broken down into two categories: Comparisons to value data: The first six options all relate to the value data you specified for the registry key. • **EqualTo:** The check passes if the registry value is equal to the reference data • **NotEqual:** The check passes if the registry value is not equal to the reference data • **LessThan:** The check passes if the registry value is less than the reference data • **LessThanOrEqual:** The check passes if the registry value is less than or equal to the reference data • **GreaterThan:** The check passes if the registry value is greater than the reference data • **GreaterThanOrEqual:** The check passes if the registry value is greater than or equal to the reference data • **Exist or not exists:** The last two options (**Exists**, **NotExists**) have nothing to do with the value data but instead simply test whether the registry key itself exists. In either category, if the comparison test passes Ivanti Patch for Windows® Servers will consider the product installed.
Use 64 Bit Registry	Enable this check box if the registry key is in the 64-bit part of the registry on a 64-bit operating system.

4. When complete, save and then validate the XML file (see Saving and Validating Your Changes).

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

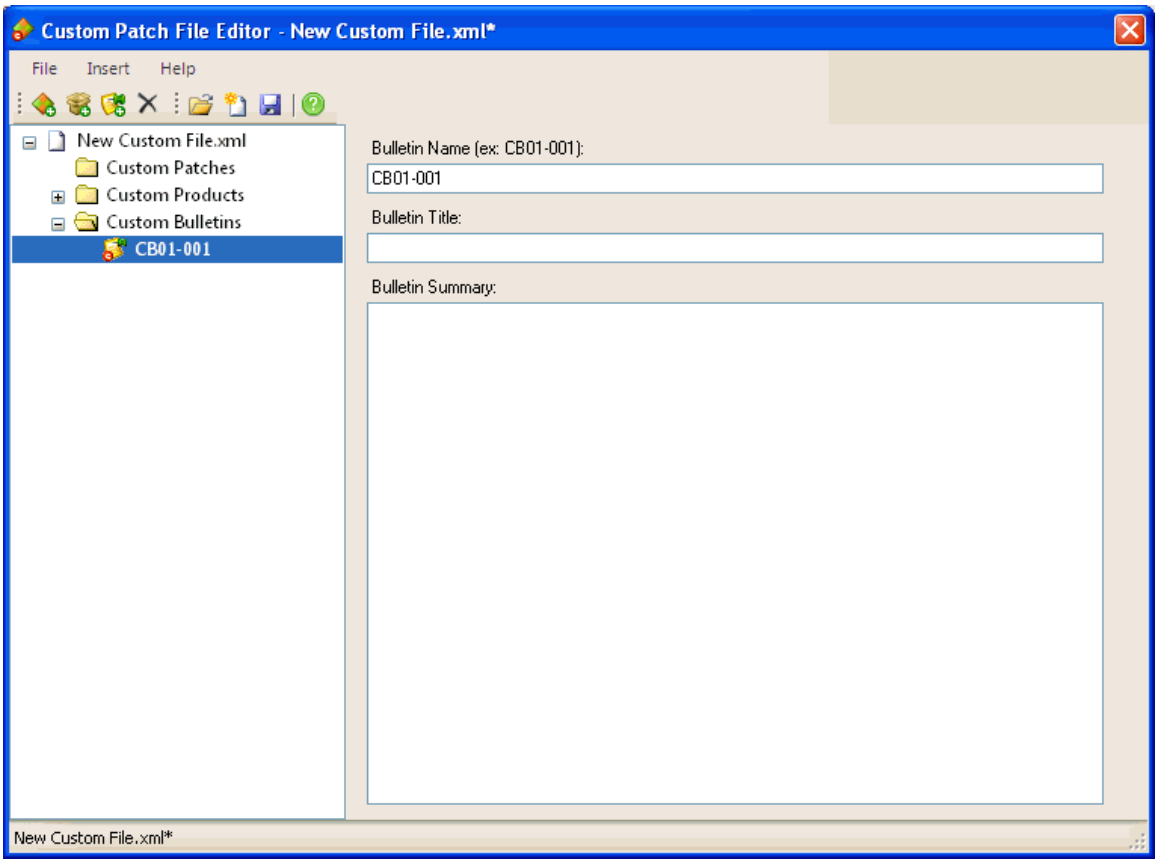
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating a Custom Bulletin

A security bulletin provides a summary describing why a custom product or patch is being created. Many times a bulletin will describe a particular software vulnerability that is being addressed by a patch. You must apply a new custom patch to a bulletin, so if you are not tying a patch to an existing bulletin then you must create a new bulletin.

1. To create a custom bulletin, within Custom Patch File Editor select **Insert > Add Bulletin** or click the **Add Bulletin** toolbar icon ( ).

   The new custom bulletin is selected and the bulletin characteristics are displayed in the right pane.



2. Use the options in the right-hand pane to define the new bulletin.

Bulletin Name	Type a unique name for the bulletin. The name cannot match a bulletin name already defined to the program.
Bulletin Title	Type a short description of the bulletin.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Bulletin Summary	Type a detailed summary that describes the purpose of the bulletin and any related patches and products.

3. When complete, save and then validate the XML file (see Saving and Validating Your Changes).

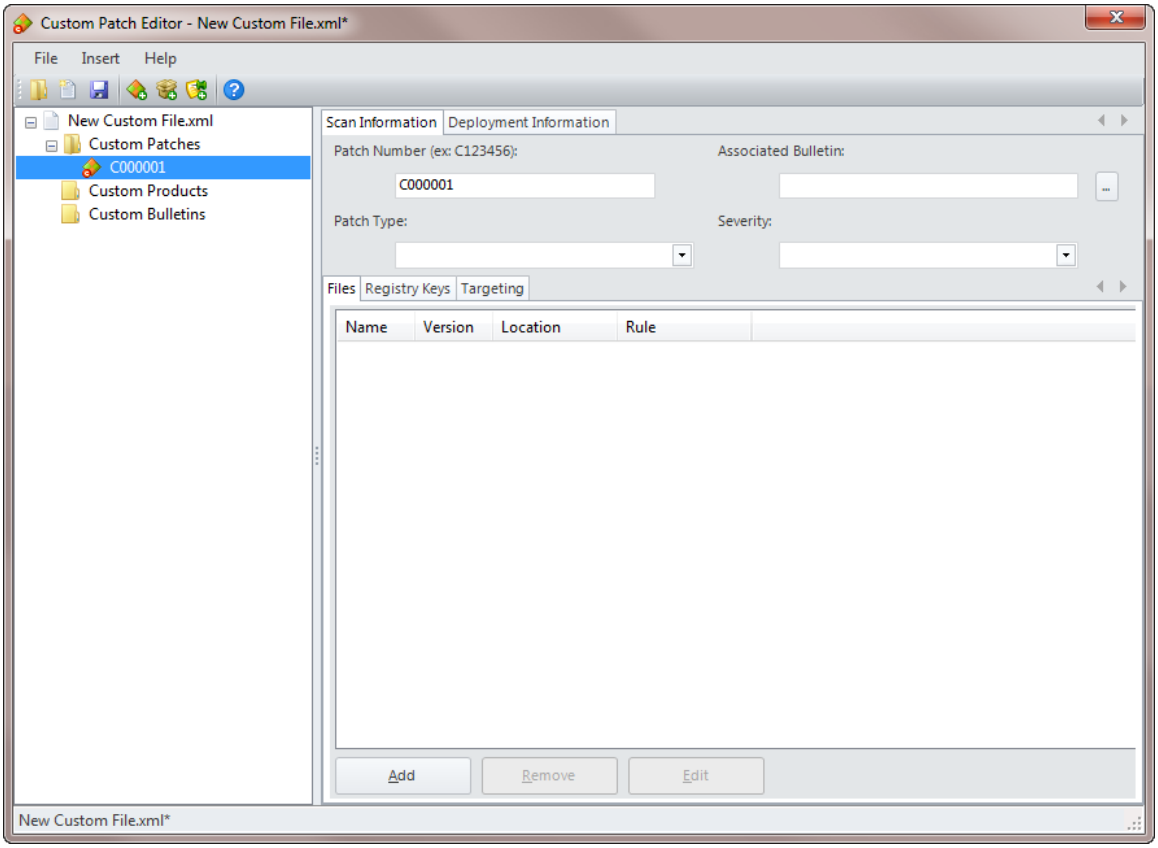
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating a Custom Patch

The Custom Patch File Editor is not used to create the actual patch file. The patch itself is provided by a vendor (e.g. Microsoft) or is created by your organization. When you create a custom patch within the Custom Patch File Editor you are simply defining how to detect if the patch is missing from target machines and how to deploy the patch.

1. To create a custom patch, within Custom Patch File Editor select **Insert > Add Patch** or click the **Add Patch** toolbar icon ( ).

   The new custom patch is selected and the patch characteristics are displayed in the right pane.



2. Use the options in the right-hand pane to create the new patch.

   Two major tabs are used in the right-hand pane. For detailed information about the options on these two tabs please refer to the following topics:

   - Scan Information Tab
   - Deployment Information Tab

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

IMPORTANT! You should avoid creating a custom patch that requires user interaction. This is because this is no guarantee how the patch installation process will react if there is no response to a user prompt. The most likely scenario is that it will wait a number of hours before eventually timing out. Use command line switches if necessary.

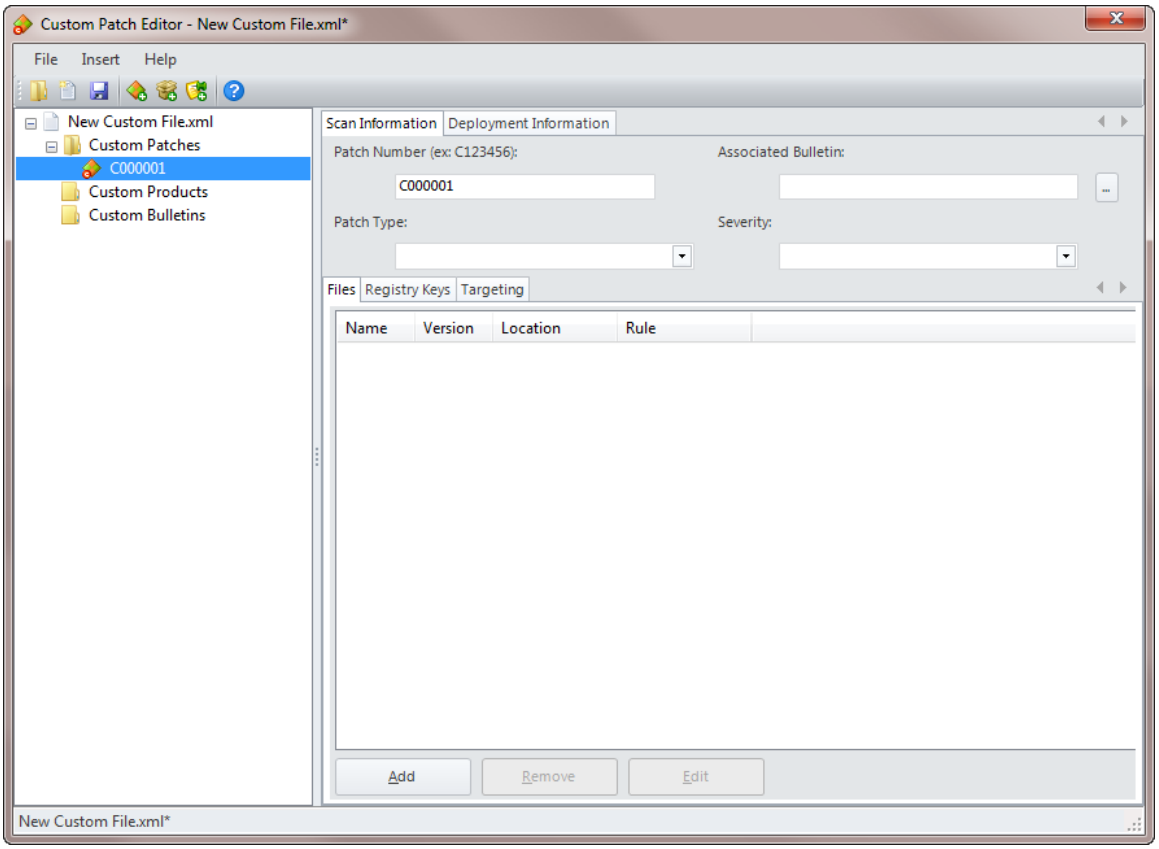
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Scan Information Tab

When creating a custom patch, two major tabs are used in the right-hand pane. This topic describes the options and sub-tabs contained on the **Scan Information** tab.

This tab contains two sub-tabs that enable you to specify criteria for determining whether or not a patch is installed. You must use your own discretion in determining whether to specify detection criteria on the **Files** tab, the **Registry Keys** tab, or both. If your requirements are that a specific file version and a specific registry key value must both be detected in order to declare that the patch is installed, then by all means do it. The recommendation, however, is to keep things as simple as possible. If detecting an old file version is criteria enough to determine that a patch is required, you probably don't need to also specify registry key information (and vice versa).

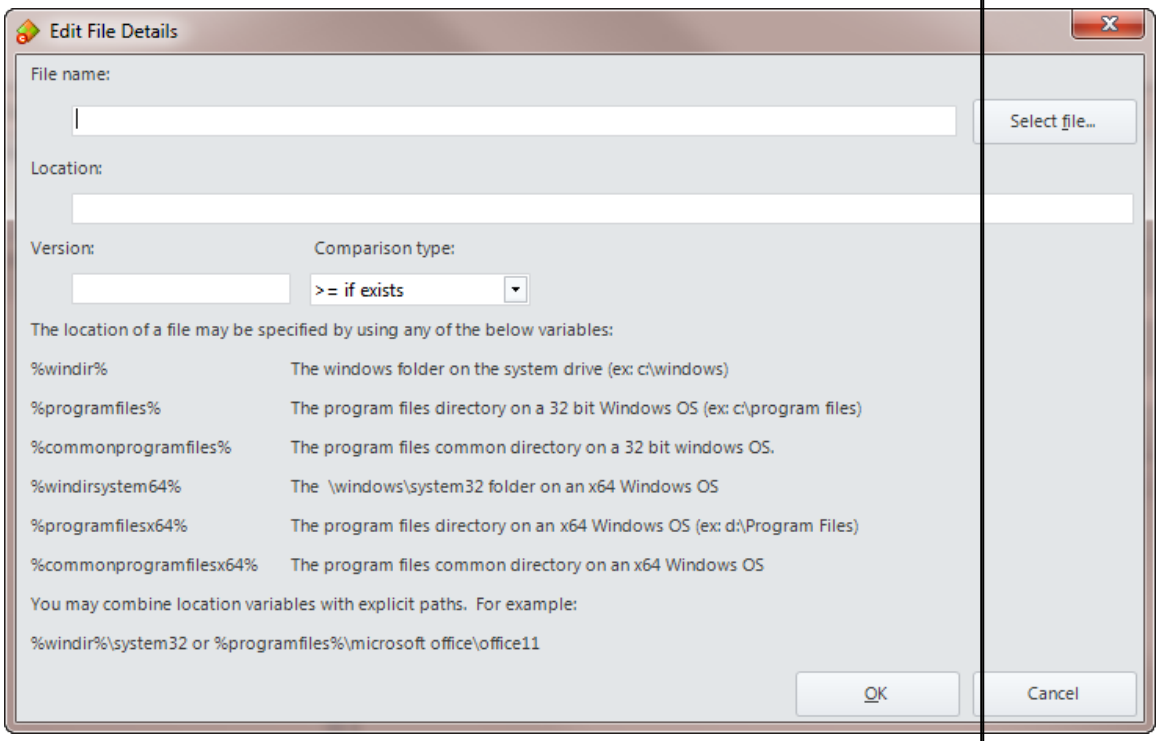
If you do not specify registry key information, patches that were not installed by Ivanti Patch for Windows® Servers will be reported as *Effectively Installed*. In order for Ivanti Patch for Windows® Servers to display a patch as Effectively Installed you must use a scan template that scans for both missing and installed patches. See Creating a New Patch Scan Template for more information.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Patch Number	An identifying number for this patch. You can follow whatever numbering convention you want when defining the patch number. The only rule is that the number must be no more than 10 alphanumeric characters. Although it is not mandatory for the number to be unique, in almost all cases it makes sense to make it unique. Only in extremely rare cases is it advisable to assign the same patch number to two or more patches. The patch number specified here will be the number shown within the Ivanti Patch for Windows® Servers interface when referring to the patch. It is also the identifier used by such things as patch groups when specifying which patches belong to a certain group. As a point of reference, the patch number is akin to the knowledge base number (or QNumber) used to identify patches in the Microsoft world. By default the first patch in the custom XML file is C000001. This number is automatically incremented for each new patch.
Associated Bulletin	You must associate each patch with an existing bulletin. The bulletin can be one that you created or one that was issued by another vendor. To see the list of all available bulletins, click the **Browse** button (···). In the dialog that appears, select the desired bulletin and then click **OK**.
Patch Type	Specify the types of patch you are creating. • **Security Patches:** Security bulletin related patches. This is the default setting. • **Non-security Patches:** The set of patches supported by Microsoft Software Update Services (driver updates not supported). • **Security Tools:** Patches for the malware tool provided by Microsoft. • **Software Distribution:** Free third-party applications that can be deployed by Ivanti Patch for Windows® Servers. • **Custom Actions:** Enables you to perform custom actions even if you are already fully patched. It does this by scanning for a specific QNumber and patch (QSK2745, MSST-001) that will never be found. The process uses the temporary file Nullpatch.exe.
Severity	Assign one of the following four severity levels based on the perceived threat of the vulnerability related to the patch. • **Critical:** The problem or issue associated with the patch is deemed critical in nature. • **Important:** The problem or issue associated with the patch is deemed important to fix.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **Moderate:** The problem or issue associated with the patch is of moderate severity. • **Low:** While the problem or issue is real, the security risk or capability is deemed to be low.
Files tab	One of the ways to determine if a patch should be installed is to check the version number of the affected file on the machines being scanned. The **Files** tab is used to specify the file version information. If you also specify criteria on the **Registry Keys** tab, the tests on that tab must also be satisfied in order for the patch to be installed. • **Add:** To add a new file definition, click this button. • **Remove:** To remove an existing file definition, click this button. • **Edit:** To edit an existing file definition, click this button. After clicking **Add** or **Edit**, the **Edit File Details** dialog is displayed.  • **Filename:** The name of the portable executable format file affected by the patch. For most instances the file will therefore be either an .exe or a .dll file. The file must contain version information for this check to be correct.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **Select File:** Use this button to browse the local computer or network for the file affected by the patch. When you use this button to find the file, the program will use information about the file you select to also populate the Location and Version boxes. For this reason you will typically use this button when defining the Filename box.
- **Location:** Specify the location of the affected .exe or .dll file. You must provide the full directory path when specifying the location. If this box was automatically populated by the Select File button, you may need to edit the path if the location represents the position of the file on the local machine and is not representative of where it will be located on all other machines.
- **Version:** Specify the version number of the affected .exe or .dll file.
- **Comparison Type:** This specifies the test criteria you want to use when determining if a scanned machine needs this patch. The two available options have very similar names so be careful when making your selection.
  - **If the file exists, its file version must be equal to or greater than the specified version:** The only way to fail this test is if the file exists on the scanned machined but its version number is less than the number specified in the Version box. If the file does not exist on the scanned machine then the patch does not apply.
  - **The file must exist and its file version must be equal to or greater than the specified version:** There are two ways to fail this test. (1) If the file does not exist on the scanned machine then the test fails and the patch is required. (2) If the file does exist but its version number is less than the number specified in the Version box then the test fails and the patch is required.
- **File Location Parameters:** Shows the parameters that can be used when specifying a file location. Rather than specifying one hard coded location that may not apply to every machine in your organization, you can use parameters to specify variable locations. For example, if you want to specify the Windows folder but the folder may be located at C:\Windows, D:\Windows, or C:\WinNT on the different machines in your organization, you can accommodate all options by using the %windir% parameter. You can use a parameter within a location path and you can use multiple parameters within a path.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

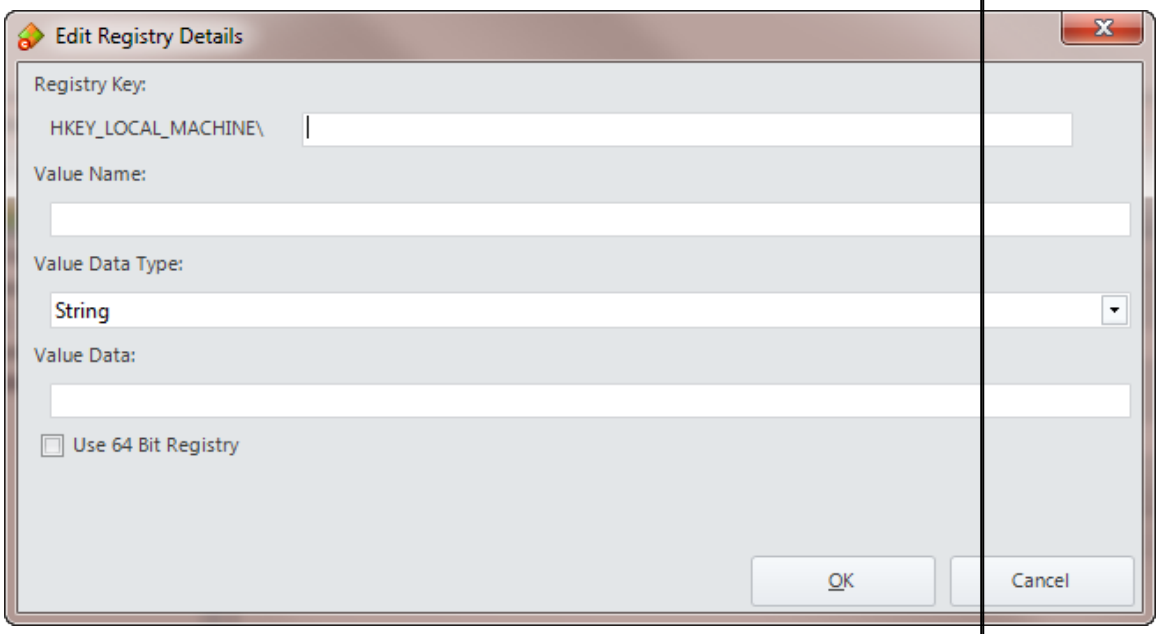
Registry Keys tab

Another way to determine if a patch should be installed is to check for the data defined on certain registry keys on the machines being scanned. The **Registry Keys** tab is used to specify the registry information. If the scanned machine satisfies the criteria specified here then the patch will be applied.

If you also specify criteria on the **Files** tab, the tests on that tab must also be satisfied in order for the patch to be installed.

- **Add:** To add new registry key information, click this button.
- **Remove:** To remove existing registry key information, click this button.
- **Edit:** To edit existing registry key information, click this button.

After clicking **Add** or **Edit**, the **Edit Registry Details** dialog is displayed.



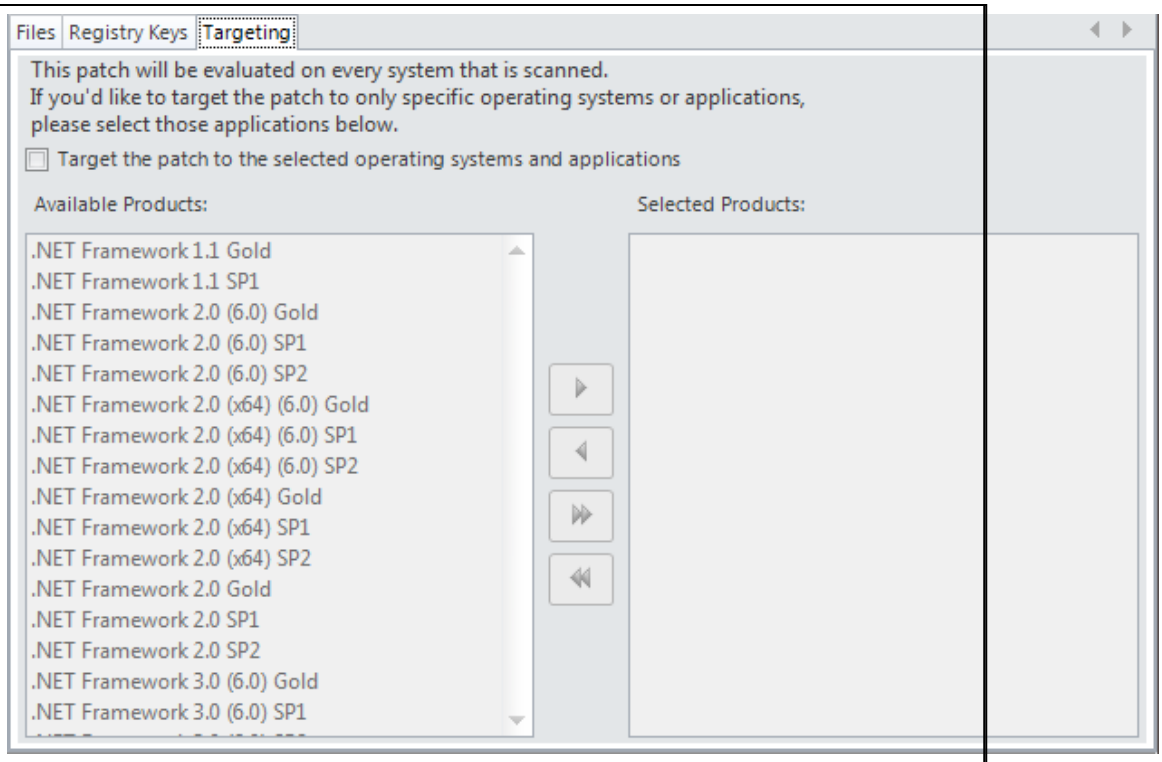
To get the most current registry information we recommend using the Microsoft Registry Editor (regedit), a tool for viewing settings in your system registry. You can copy the required information from this tool to the appropriate fields in the **Edit Registry Details** dialog.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **Registry Key:** You can only specify keys that are relative to the HKEY_LOCAL_MACHINE hive. The easiest and most accurate way to populate this box is to display the desired key from within the Microsoft Registry Editor, copy the key name and then paste the name into this box. The HKEY_LOCAL_MACHINE portion of the name will likely be repeated so you'll need to remove that portion of the name from the box.
	• **Value Name:** The name of the specific registry key.
	• **Value Data Type:**
	  • **String:** Specifies that the data must be a string.
	  • **DWord:** Specifies that the data must be a number.
	• **Value Data:** The expected value of the registry key. You can find this value by locating the key within the Microsoft Registry Editor and then looking in the Data column.
	• **Use 64 Bit Registry:** Enable this check box if the registry key is in the 64-bit part of the registry of a 64-bit architecture.

Targeting tab	This tab enables you to specify which products apply to this patch. By default all available operating systems will be evaluated. You can greatly speed the evaluation process if you can narrow the list of products. Targeting the patch to a limited number of products can be a real time saver during the scan process as it eliminates the scanning of unnecessary products. **Said Another Way:** If you do not specify any products in the **Selected Products** list, the patch will be associated with all available operating systems. The program will scan for the patch regardless of what is installed on the target machines. This can be useful if you want to perform a mass distribution of the patch, but it can also be quite time consuming. If you specify one or more products in the **Selected Products** list, the patch will be associated with only those products and not with any unspecified operating systems. TIP: After importing a new custom XML file, you can use Patch View to verify the custom patch is associated with the correct product(s).

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



To narrow the list of products:

1. Enable the **Target the patch to the selected operating systems and applications** check box.
2. In the **Available Products** list, select the desired product and move it to the **Selected Products** list.

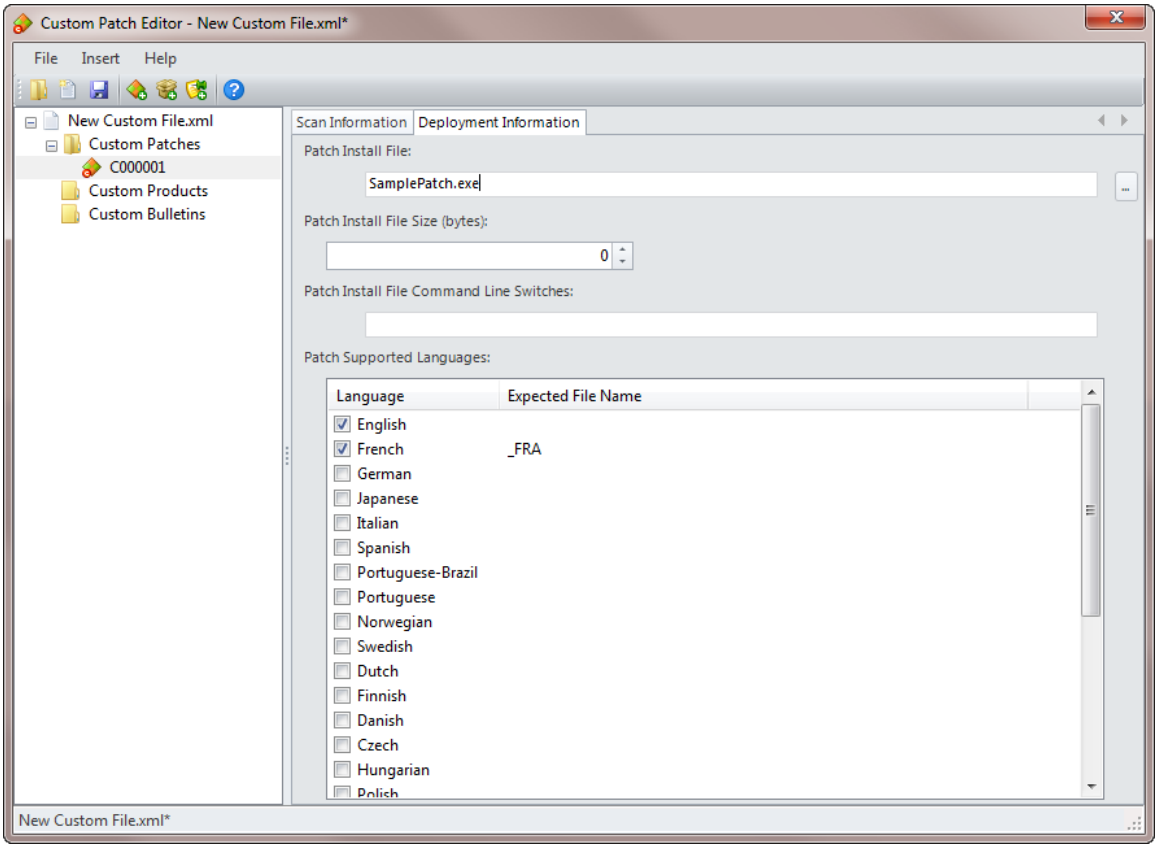
   The **Available Products** list contains all products currently defined in the XML patch data file plus any new custom products you may have defined using the **Custom Patch File Editor**.
3. Repeat Step 2 for each product that applies to this patch.

When complete, save and then validate the XML file (see Saving and Validating Your Changes).

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deployment Information Tab

When creating a custom patch, two major tabs are used in the right-hand pane. This topic describes the options contained on the **Deployment Information** tab.



Patch Install File	Batch files (.bat and .cmd file formats) are not supported by the custom patch process and must not be used as a patch install file. This is the patch file that will be used when the conditions specified on the **Scan Information** tab are met. Specify just the file name here and not the full path name to the patch install file. This file is typically supplied by the vendor of the product you are patching. You can use the browse button to locate and select this file. Doing so will automatically populate the **Patch Install File Size** box.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	IMPORTANT! The actual file used in the patch process may have several different names and you must manually copy the files to every location the patch file is expected to reside, including the console and possibly one or more distribution servers. See the description of the **Patch Supported Languages** option for more information.
Patch Install File Size (bytes)	Specifies the size of the patch install file. This box is automatically filled in when you use the **Browse** button to select the **Patch Install File**. Providing the file size enables the program to accurately determine the progress during the installation process.
Patch Install File Command Line Switches	Specify any command line switches you want to use during the installation of the patch. For example, you might want a silent install (/quiet), you might want to dictate that the target machines are not restarted (/norestart), etc.
Patch Supported Languages	Enable the check boxes for the operating system languages you want to support with this custom patch. There are two reasons for doing this: • It tells the program which languages are supported by the patch. • It tells you what identifying text should be added to the end of the patch file name. IMPORTANT! You must make as many copies of the file as is needed using the appropriate names and then make those files available everywhere the patch file is expected to reside. **Example 1:** Assume your vendor supplied two versions of the same patch, one for English language systems named *SamplePatchENGLISH.exe* and one for French language systems named *SamplePatchFRENCH.exe*. You must add the text shown in the **Expected File Name** column to the end of the associated patch file. In this example the updated file names would be *SamplePatchENGLISH.exe* and *SamplePatchFRENCH_FRA.exe*. (The English language patch does not require the suffix, although *SamplePatchENGLISH_ENU.exe* would also work.) You then place copies of each file in the console's patch download directory and on the appropriate distribution servers.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	Example 2: Assume your vendor supplied a patch file named *SamplePatch.exe* and that file supports English, French, and German language systems. You must make three copies of the file, rename them by adding the text shown in the **Expected File Name** column to the end of each file name, and then place copies of each file on the appropriate distribution servers. In this example the file names would be *SamplePatch.exe*, *SamplePatch_FRA.exe*, and *SamplePatch_GER.exe*.

When complete, save and then validate the XML file (see Saving and Validating Your Changes).

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Saving and Validating Your Changes

Anytime you create a new custom XML file or make changes to an existing custom XML file, you should save your changes and then perform a validation. The validation ensures that the custom XML is properly formed and will interact correctly with Ivanti Patch for Windows® Servers's primary patch XML file.

You should always save the custom XML file before performing the validation. If you don't save the file the validation will be performed on the previously saved version of the file.

To validate a custom XML file:

1. Save the file by selecting **File > Save**.
2. In the left-hand pane select the topmost folder.

   This folder specifies the location of the custom XML file.
3. In the right-hand pane click **Validate XML**.

   The results are displayed in the **Validation Results** section at the bottom of the right-hand pane. If an error is detected you must correct that error before attempting to use the custom XML file.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Changing a Custom XML File

If you make changes to an existing custom XML file, you must use the **Edit Custom Patch Collection** dialog to remove the old version of the custom XML file and then re-import the updated file. If you just save the file without removing and then re-importing it, the program will continue to use the old version of the file.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Specifying Which Custom XML Files to Use

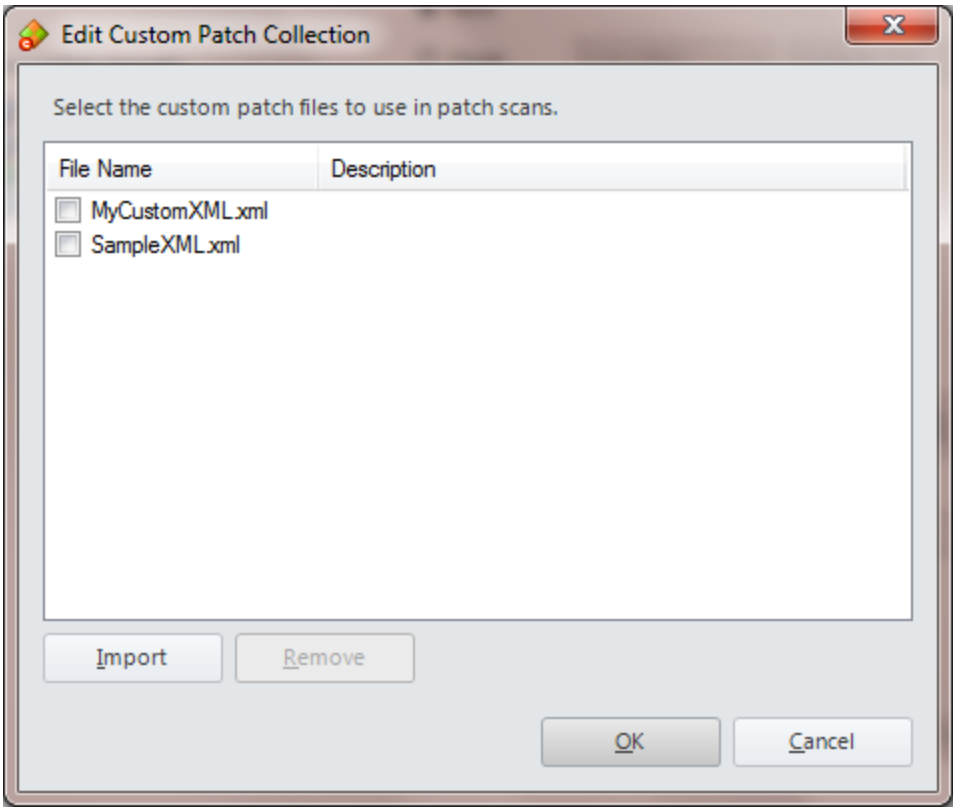
Ivanti Patch for Windows® Servers enables you to create many different custom XML files. However, you may not want to use all your custom XML files all the time. For this reason Ivanti Patch for Windows® Servers also enables you to specify which of your custom XML files (if any) that you want to use in your scans and deployments.

For information on creating custom XML files, see Creating A New Custom XML File.

To specify the custom XML files that will be used in your scans and deployments:

1. From the Ivanti Patch for Windows® Servers menu select **Manage > Custom Patches**.

   The **Edit Custom Patch Collection** dialog is displayed. It contains a list of custom XML files you have previously imported into the dialog.



2. (Optional) If you have created additional custom XML files that are not currently in the list, you can add them to the list by clicking **Import**.

   Navigate to the custom XML file you want to add and then click **Open**. The new XML file is added to the list. Repeat this step for each new custom XML file you want to add to the list.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

IMPORTANT! Any custom XML file that has been changed since it was initially imported must be removed and then re-imported. If you just re-import a changed file without first removing it, the program will continue to use the old version of the file.

3. Enable the check boxes for the custom XML files you wish to include in your patch scans and deployments.

   The XML files included in all future scans and deployments will be the standard XML patch file plus any of the custom XML files enabled here. The available XML files are called your *collection*; the custom XML files currently enabled for use is called your *active collection*.

4. Click **OK**.

   Ivanti Patch for Windows® Servers will perform a validation process to ensure that all the selected custom XML files and the primary XML patch file can be successfully combined. Although you should have already validated each individual custom XML file, Ivanti Patch for Windows® Servers must make sure that the files collectively are okay. For example, if you inadvertently used the same name for two different custom products in two different custom XML files, the validation process will catch this.

   If an error occurs during the validation process the custom XML files will not be used. You must correct the problem and try again.

Removing a Custom XML File

To remove a custom XML file that has been previously combined with the primary XML file:

1 On the **Edit Custom Patch Collection** dialog, clear the check box of the custom XML file you no longer want to use.

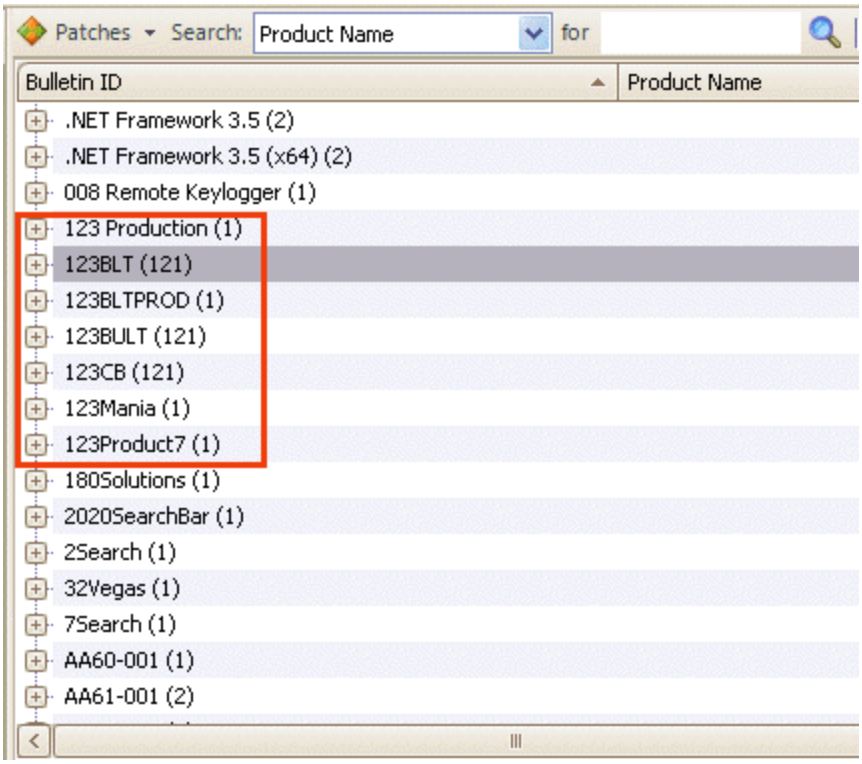
2. Click **OK**.

Only those custom XML files still enabled will be included in the validation process and used with the primary XML file.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

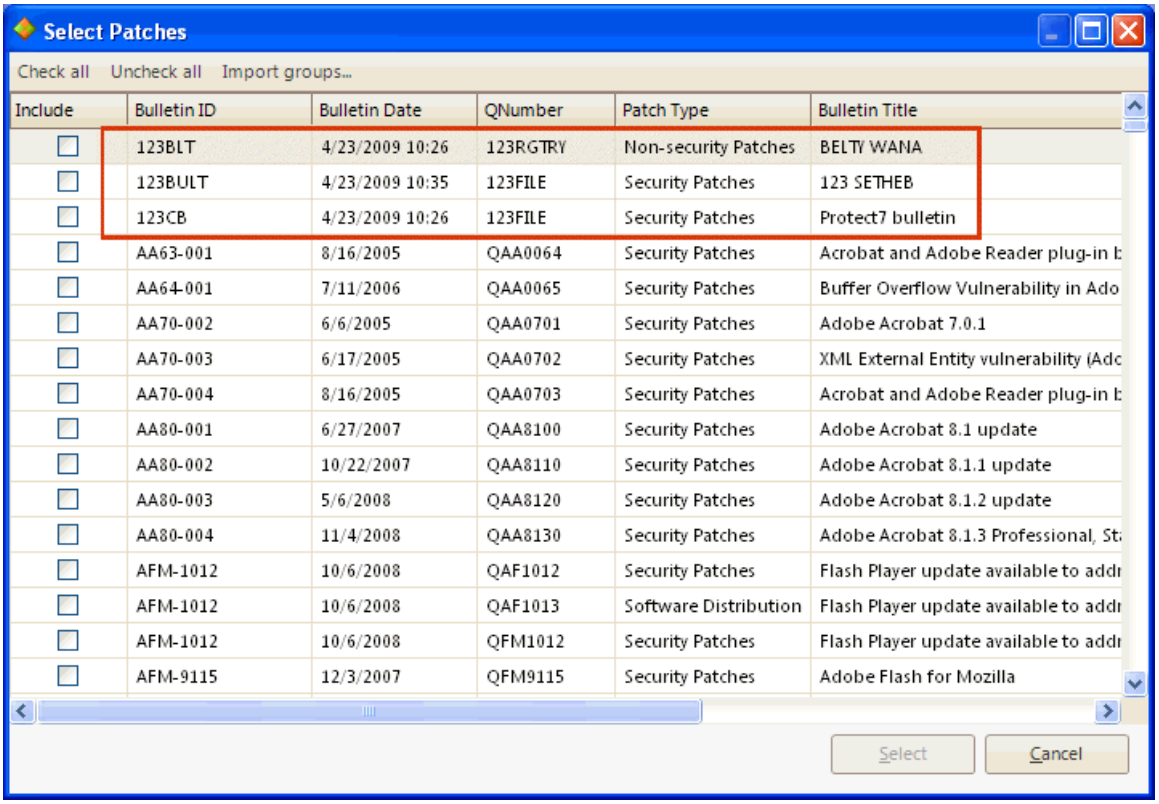
Viewing Custom Patches and Products

Once a custom XML file is used within a scan, the custom products and patches defined within the custom XML file will be displayed in Patch View.



They will also be displayed when adding patches to a patch group.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Be careful though. Just because a custom product or patch is displayed in Patch View or in a patch group doesn't guarantee it is still being used in scans and deployments. It only indicates that the custom product or patch was at some point included in a scan or deployment. If you remove a custom XML file from the list of active custom XML files (see Specifying Which Custom XML Files to Use), the products and patches within that custom XML file will not be used in subsequent scans and deployments. A custom XML file must be active in order to be used.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Asset Inventory Overview

If you want to perform a virtual asset scan for the properties of your vCenter Servers, ESXi hypervisors and virtual machines, see the Virtual Inventory feature.

The asset inventory function enables you to track your software and hardware assets. Performing an asset scan enables you to thoroughly and dynamically discover and catalog your IT assets. You will uncover software applications you didn't know were installed and discover physical machines you didn't even know you had. By eliminating these blind spots, you can quickly close the gaps in your security and policy compliance. By consolidating hardware and software asset information in one location, you have all relevant information about your assets at your fingertips, enabling you to make informed decisions with confidence and accuracy.

The function works by performing scans to detect and categorize the software and hardware contained on your machines. Detailed information about your software and hardware assets is available immediately following a scan.

You also have the ability to create reports that can be used to track your asset inventory over time. For example, you might create a scheduled scan of your domain that automatically generates and sends usage reports to your IT personnel. So in addition to providing you with visibility and understanding of the IT assets in your network, the asset inventory function is also a great record keeping tool for use in audits.

Asset scans can be performed in either an agentless or an agent-based fashion. This section describes the agentless process. For information on performing agent-based asset scans, see Creating and Configuring an Asset Task.

How-To Information

For information on how to perform asset inventory tasks, see:

- Creating a New Asset Scan Template
- How to Initiate an Asset Scan
- Monitoring an Asset Scan
- Viewing Asset Scan Results

Software Asset Scan Information

Scans for the software components contained on one or more machines. You can perform this scan on physical machines, online virtual machines, offline virtual machines, and virtual machine templates.

This scan helps you answer the following important questions:

- What software is on the machines in my network?

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- Where are the software resources located?
- How many do I own?
- How many different versions of a software program are in use?
- How long ago were the programs installed?
- Are there software programs that shouldn't be on my network? (For example: iTunes, shareware programs, etc.)

Hardware Asset Scan Information

Scans for the hardware components contained on one or more machines. You can perform this scan on physical machines and online virtual machines. Offline virtual machines and virtual machine templates are ignored by this scan.

This scan helps you answer the following important questions:

- What hardware components are on my scanned machines?
- How many do I own?
- How much memory is on each machine?
- What type of processors are on my machines?
- What services are running on my machines?
- What services have failed to start on my machines?

Ivanti Patch for Windows® Servers's Advantages Over Other Asset Tools

With Ivanti Patch for Windows® Servers, all the machine information you want is consolidated nicely in one location. With most tools you must spend a lot of time and energy clicking around in different tables to locate the information you want. In order to present it in an organized fashion you need to copy the information from multiple sources and then paste it into a text or spreadsheet program. With Ivanti Patch for Windows® Servers's asset inventory feature, all the information is readily available in one location and is easily groupable and sortable.

The machine information is also easily distributable. The reporting feature enables you to generate several different reports that contain a considerable amount of information. The reports can be printed or they can be exported to a number of different electronic formats, enabling you save them to disk, view them with the program of your choice, or email them to others.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Asset Management Scan Requirements

Before attempting an asset scan, please confirm that you meet the following requirements:

- The Windows Management Instrumentation (WMI) service must be enabled and accessible on the target machines.
- TCP port 135 must be configured on your organization's firewall to allow the WMI protocol.
- Credentials must be provided for the target machines. You cannot perform scans using your current logon credentials. See Supplying Credentials for details.
- For target machines using Windows operating systems that employ the use of User Account Control (this includes Windows Vista or later and Windows Server 2008 or later), you must either:
  - Join the machines to a domain and then perform the scan using domain administrator credentials, or
  - If you are not using the built-in Administrator account on the target machines (and using that account is NOT recommended), you must disable User Account Control (UAC) remote restrictions on the machines. To do this:

1. Click **Start**, click **Run**, type **regedit**, and then press **Enter**.
2. Locate and then click the following registry subkey:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
3. If the **LocalAccountTokenFilterPolicy** registry entry does not exist, follow these steps:

   a. On the **Edit** menu, point to **New**, and then click **DWORD Value**.

   b. Type **LocalAccountTokenFilterPolicy** and then press **Enter**.
4. Right-click **LocalAccountTokenFilterPolicy** and then click **OK**.
5. In the **Value data** box, type **1**, and then click **OK**.
6. Exit Registry Editor.

For more details on disabling UAC remote restrictions, see http://support.microsoft.com/kb/951016

Windows Firewall Requirements for Hardware Asset Scans

Ivanti Patch for Windows® Servers scans for hardware assets using WMI in semisynchronous mode. This means the firewall policy only requires DCOM connections from the console machine to the target machines. Asynchronous mode, which would require reverse connections back to the console, are not used.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

To scan hardware assets of a machine with Windows Firewall running, you must set that machine's firewall to allow remote administration. You can configure the firewall via group policy or local command. The local command is:

```
netsh firewall set service RemoteAdmin enable
```

If you are unfamiliar with Windows Firewall administration, the following links may help:

http://support.microsoft.com/kb/875605

http://msdn.microsoft.com/en-us/library/aa389286(VS.85).aspx

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Asset Scans are Performed as Background Tasks

All asset scans are performed as background tasks using the services of the Operations Monitor. This means you can initiate a scan and then move on to other concurrent work within Ivanti Patch for Windows® Servers without having to wait for the scan to complete. This also means you can have multiple asset scans active at the same time.

Scanning Considerations

- Is there a practical limit to the number of scans you can have active at the same time?

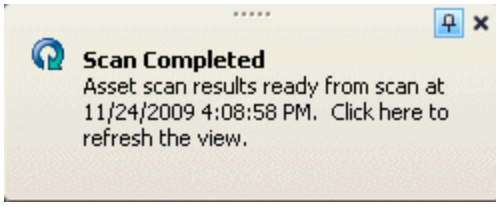
  Yes. It is dependent on the CPU and memory size of the console machine. It is also dependent on the number of other tasks currently active (for example, other patch downloads, patch deployments, etc.). While there is no exact answer, you'll know you've reached a practical limit if Ivanti Patch for Windows® Servers starts responding slowly.

- Is there a problem if the same machine is included in two or more concurrent scans?

  No. Multiple scanning tasks can be performed on a target machine at the same time.

- If I minimize the Operation Monitor window, how will I know when the scan is complete?

  A notification dialog box is displayed in the lower-right corner whenever a scan completes. The dialog box will be displayed for several seconds before slowly fading away. You can pin the dialog box in place by clicking the pin icon.

- Will I still be able to immediately view scan results?

  Scan results are viewed from within Machine View. See Viewing Asset Scan Results for details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

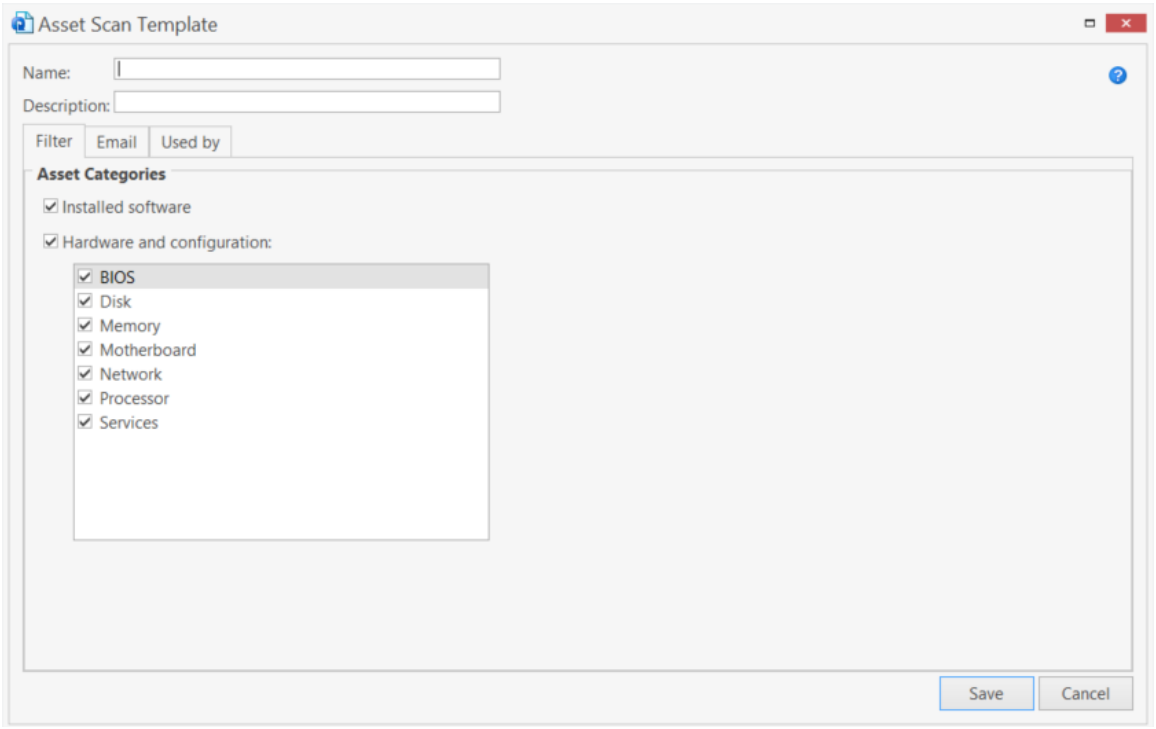
Creating a New Asset Scan Template

Ivanti Patch for Windows® Servers comes with one predefined asset scan template, named **Full Asset Scan**. This template cannot be modified. It will:

- Perform a software asset scan
- Perform a hardware asset scan of all hardware components except services

While this template is fine for most scanning activities, you may desire a higher level of flexibility when scanning machines. To this end, Ivanti Patch for Windows® Servers includes the ability to create any number of custom asset scan templates.

To create a new asset scan template, from the main menu select **New > Asset Scan Template**. This will display the **Asset Scan Template** dialog.



The **Asset Scan Template** dialog contains three tabs that collectively define the characteristics of the scan template.

Name	The name that you wish to assign to this scan template.
Description	A description of the template.
Filtering tab	There are three different types of asset scans that can be performed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **Installed Software:** To scan for the software components contained on a physical machine, an online virtual machine, or an offline virtual machine, enable this check box. • **Hardware and Configuration:** To scan for the hardware components contained on a physical machine or an online virtual machine, enable this check box. Offline virtual machines are ignored by this scan. You can elect to scan for information on a number of different hardware components, including: • BIOS • Disk • Memory • Motherboard • Network • Processor • Services
Email tab	This tab applies only to agentless scans initiated from the console; it does not apply to agents that may also be using this template. This tab enables you to specify which reports should be automatically sent and to whom the reports should get sent. The specified reports will be sent when a scan using this template is completed. There are many different reports that can get sent. To understand what a particular report contains, click on the report in the list and view its description immediately above the list. To specify which reports should be automatically sent and to whom they should be sent: New templates must be saved before you can perform these steps. 1. Select a report in the **Reports** list. 2. In the **Report Recipients** list, select the groups and/or individuals you want to email the report to. 3. Repeat Step 1 and Step 2 for each report you want to be automatically sent. 4. When finished, click **Save**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Used By tab	This tab shows you the Favorites and the agent policies that are currently using this asset scan template. This is important to know if you are considering modifying the template, as it tells you what other areas of the program are affected.

To save the template click **Save**. To close the dialog without saving the changes **Cancel.**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How to Initiate an Asset Scan

An asset scan can be initiated from the home page, from a machine group, from a favorite, or from Machine View.

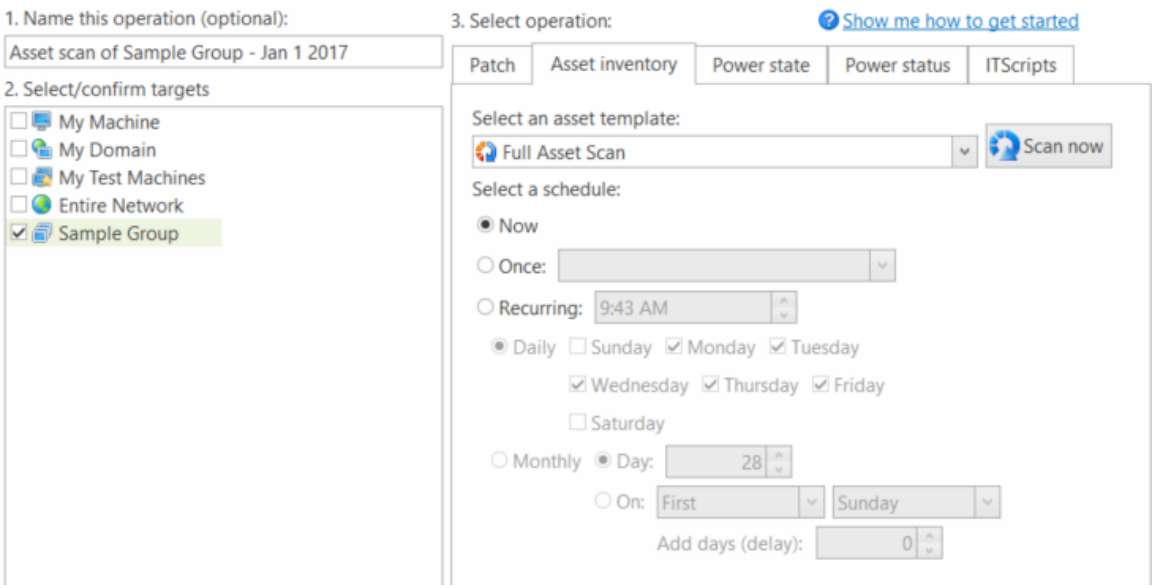
FROM THE HOME PAGE

You can use the home page to initiate a scan of any of the four pre-defined groups (**My Machine**, **My Domain**, **My Test Machines**, **Entire Network**) or of a custom machine group.

1. Type a name for the operation you are about to perform.

   At a minimum the name should indicate what you are scanning and when it is being scanned (for example, *Machine group name mm/dd/yy*). You may wish to include other identifiers such as the scan template being used, if it is a regularly scheduled scan or an out of band task, etc. A maximum of 100 characters can be used for the name.

2. Select the machine group you want to scan.



3. On the **Asset inventory** tab, select the template you want to use when performing the asset scan (Full Asset Scan or a custom asset scan template).
4. Choose when you want to perform the scan (**Now**, **Once**, or **Recurring**).
5. Click either **Scan now** or **Schedule**.

   - **Scan now:** This is the button name if **Now** is your selected scheduling option. A scan of all machines in the machine group will begin immediately. The Operations Monitor is used to track the progress of the asset scan.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

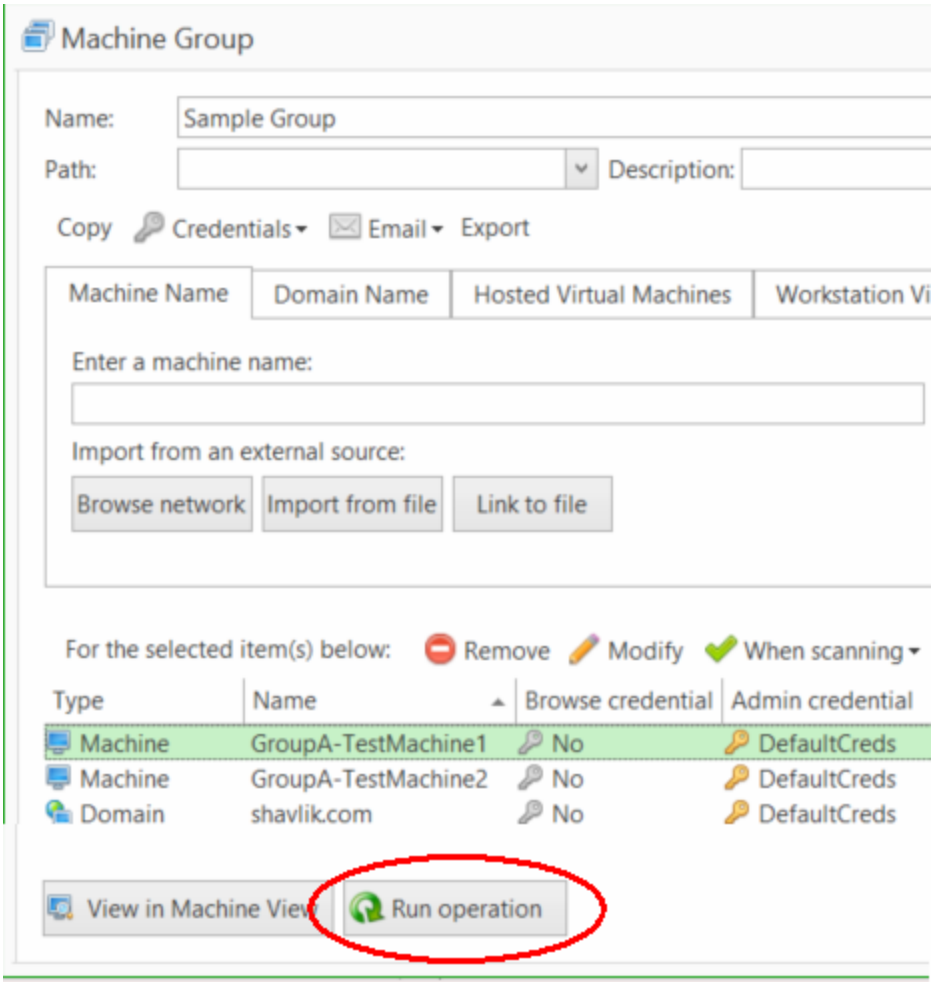
- **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See Scheduling Asset Scans and Monitoring a Scheduled Asset Scan for more details.

You can review the results of the asset scan using Machine View.

FROM A MACHINE GROUP

1 In the **Machine Groups** pane select the desired machine group.

2. Within the machine group dialog click **Run Operation**.



3. On the **Run Operation** dialog select when you want the asset inventory scan to run and which asset scan template you want to use.

4. On the **Run Operation** dialog click either **Scan now** or **Schedule**.

- **Scan now:** This is the button name if **Now** is your selected scheduling option. A scan of all machines in the machine group will begin immediately. The Operations Monitor is used to track the progress of the asset scan.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

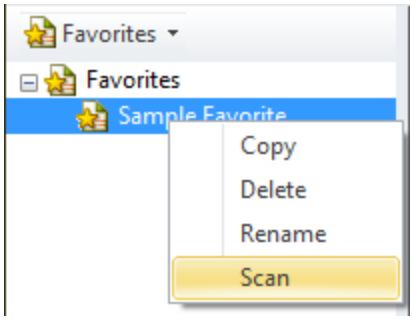
- **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See Scheduling Asset Scans and Monitoring a Scheduled Asset Scan for more details.

You can review the results of the asset scan using Machine View.

FROM A FAVORITE

A favorite consists of one or more machine groups and one template. You select the machine groups you want to scan and then specify how the machines should be scanned. A favorite is typically used to initiate a scheduled scan.

One way to initiate an asset scan of a favorite is to right-click the favorite in the **Favorites** list and then select **Scan**. This will enable you to specify when to perform the scan but not how (the asset scan template previously configured for use with this favorite will always be used).



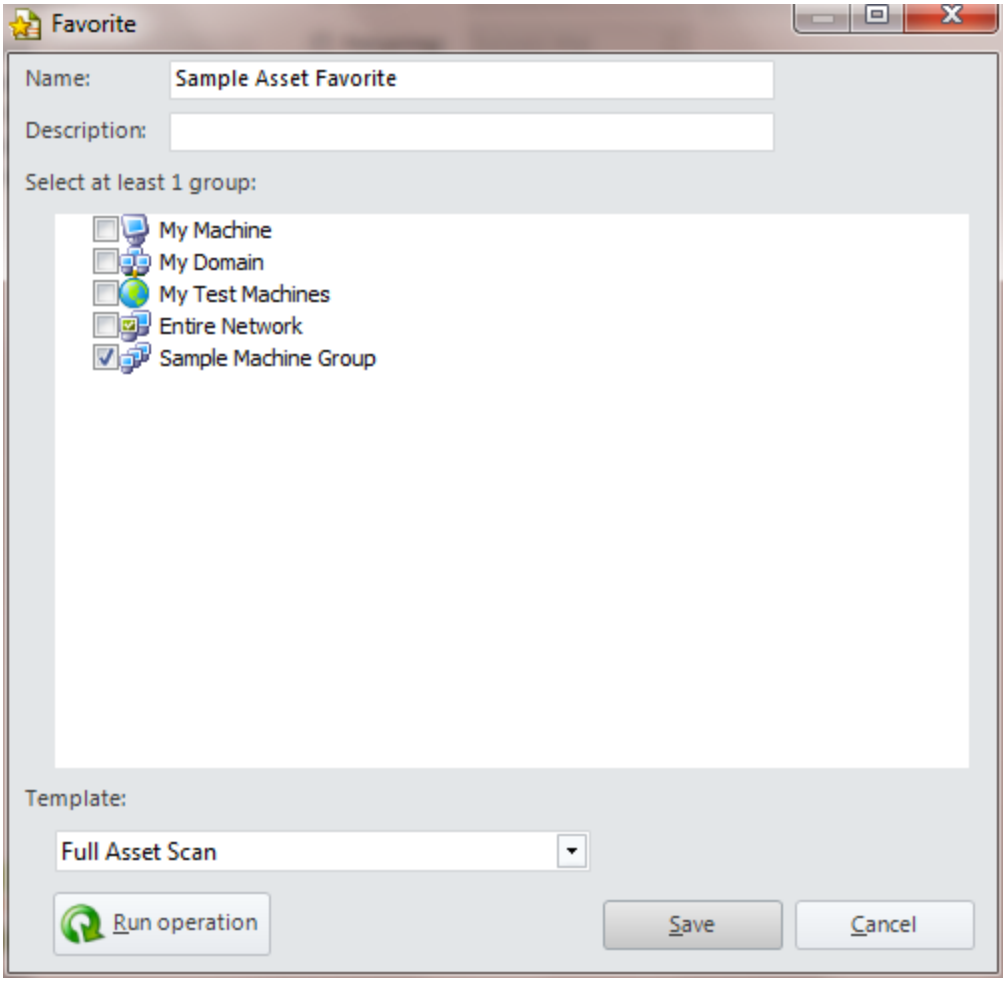
If you want to verify and/or change the configuration of the favorite before you initiate the scan you simply:

1 Select the desired favorite in the **Favorites** list.

The **Favorite** dialog is displayed. It shows the current configuration of the favorite.

2. Review the configuration, make any desired changes, and then click **Run Operation**.

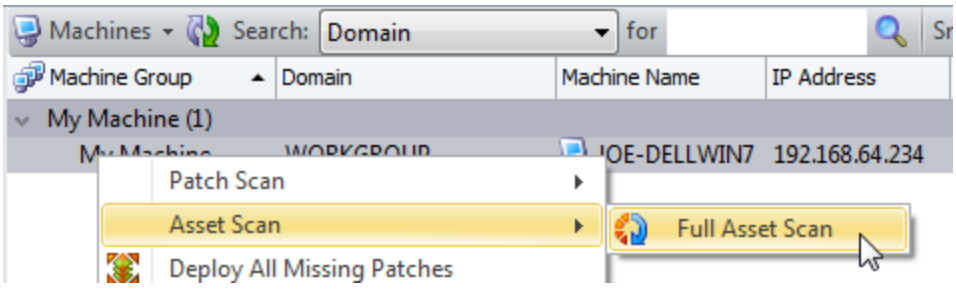
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



FROM MACHINE VIEW

1 Select one or more machines.

2. Right-click the machine(s) and then select the desired asset scan template.

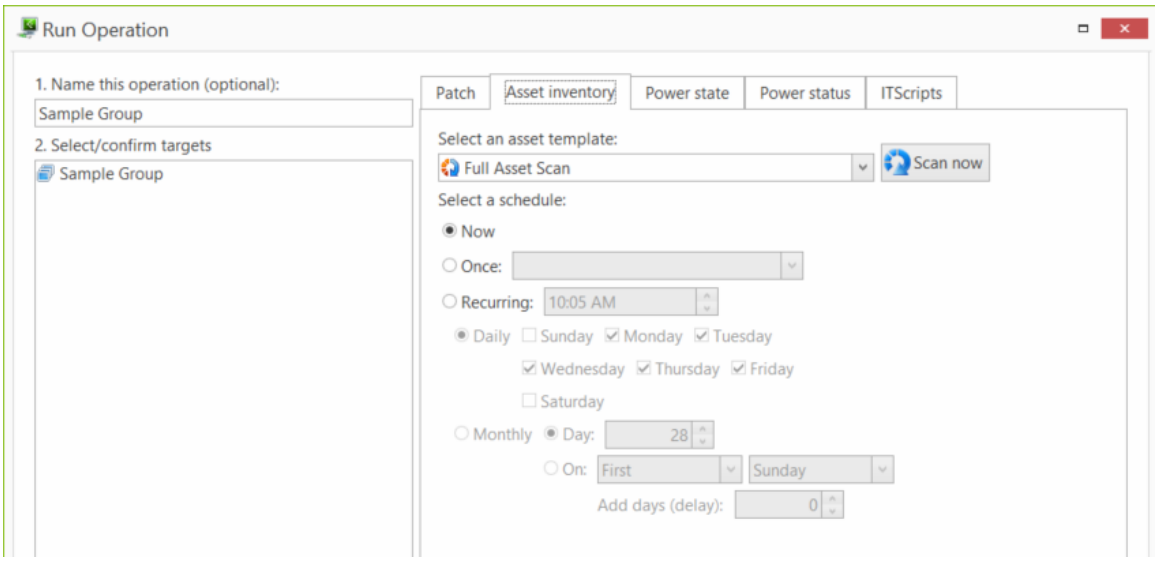


Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Scheduling Asset Scans Using the Run Operation Dialog

When you initiate an asset operation from a machine group or from a Favorite the **Run Operation** dialog is displayed. This dialog enables you to specify if the operation should run now or be scheduled for a future time or date.

Make sure you assign credentials for all machines involved in the scheduled scan.



Name this operation (optional)	Enables you to provide a unique name for the operation. By default the name of the machine group or favorite used to initiate the operation will be used. The name is displayed in the Results pane.
Select/confirm targets	This list is a reminder of the machine group(s) that will be affected by the operation. If the wrong group is listed, click **Cancel** and re-initiate the operation using the correct group.
Select an asset template	Enables you to select the asset scan template you want to use when performing the operation.
Select schedule	There are three scheduling options: • **Now** runs the operation as soon as the **Scan now** or **Run** button is clicked. • **Once** indicates that the operation will be run once at the day and time selected.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **Recurring** allows an administrator to regularly schedule operations at a specific time and using a specified recurrence pattern. For example, using this option, an operation could be run every night at midnight, or every Saturday at 9 PM, every weekday at 11 PM, or at any other user selected time and interval. You can also use the **Recurring** option to schedule an operation in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly asset scan to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by one day.

When the desired options are selected, click **Scan now** or **Run** (if **Now** is selected) or **Schedule** (if **Once** or **Recurring** is selected).

- **Scan now/Run:** The operation is initiated immediately and the **Operations Monitor** is displayed.
- **Schedule:** The scan operation is scheduled on the console machine. See Monitoring an Asset Scan for details.

  If scheduled credentials are not currently assigned the **Scheduled Console Scans/Operations Credential** dialog is displayed. You must assign a shared credential to perform a schedule action. You can use the **Set scheduler credential** button on the **Scheduled Console Tasks** dialog to view and modify which credential is being used as the scheduler credential.

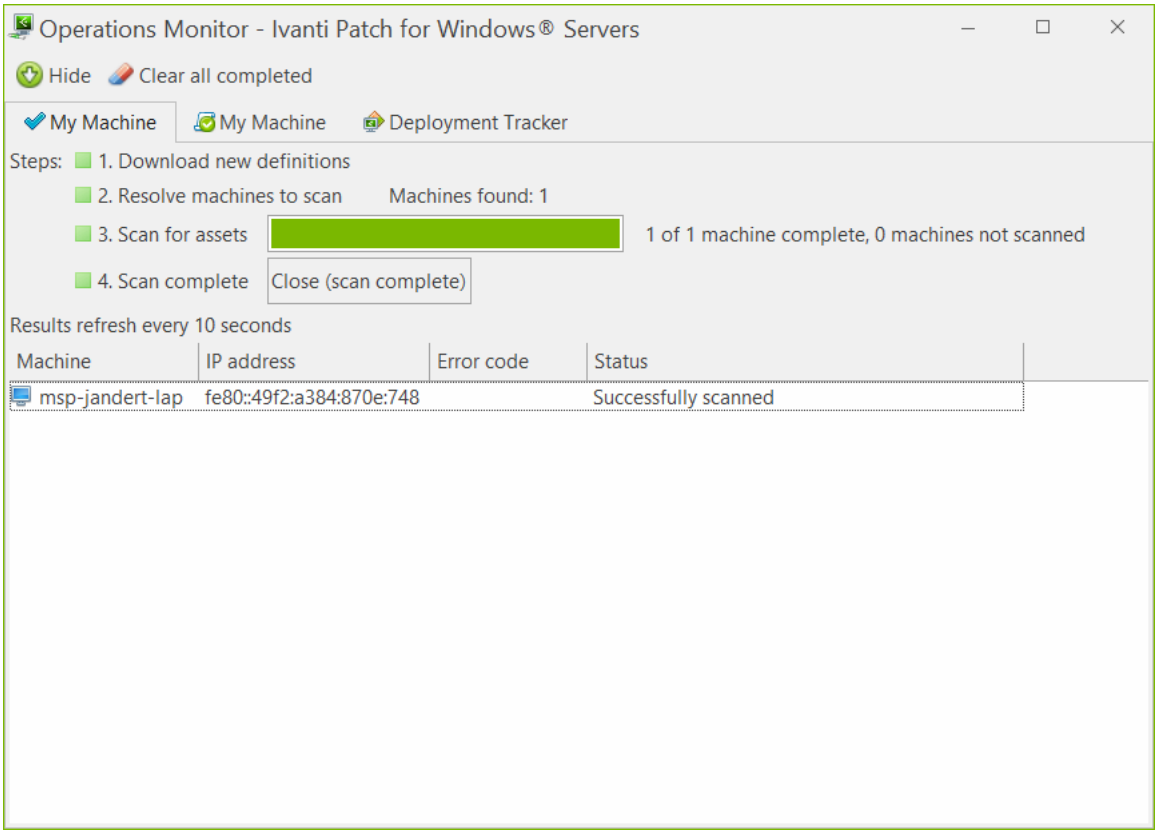
  

  The scheduled credentials are only used to schedule the operation on the console machine. The scheduled credentials are (typically) different from the machine-level credentials that are used to perform the actual operations on the target machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Monitoring an Asset Scan

The Operations Monitor is automatically displayed whenever an agentless asset scan is initiated. It shows the steps involved in the asset scanning process and the progress of each step.



Using the Operations Monitor you can:

- Cancel the asset scan by clicking **Cancel scan**.
- Remove the current asset scan tab by clicking **Close (scan complete)**. Any other tabs on the Operations Monitor will remain open.
- Close the Operations Monitor by clicking **Hide**. No tabs are removed from the Operations Monitor. Select **View > Operations Monitor** to reopen the window.
- Remove the current tab and all other tabs with completed tasks by clicking **Clear All Completed**.
- View summary information about each machine that was scanned. Right-click on a column heading and select **Column Chooser** to add or remove columns from the display.

To view the results of the scan, see Viewing Asset Scan Results.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Monitoring a Scheduled Asset Scan

When you click **Schedule** on either the home page or the **Run Operation** dialog, a scheduled task is created on the console that will launch the scan at the appointed day and time. To view the scheduled task, select **Manage > Scheduled Console Tasks**.

The Scheduled Console Tasks Manager uses the services of the Microsoft Task Scheduler to schedule and initiate each task. If you prefer, you can view the tasks within the Microsoft Scheduler by accessing the **Task Scheduler** dialog on your Windows console machine and then expanding the **Task Schedule Library > LANDESK > Protect** tree.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Asset Scan Results

Asset scan results are available within Machine View. See the following for details:

- Viewing Software Asset Summaries
- Viewing Hardware Asset Summaries

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Power Management Overview

Power management (including Wake-on-LAN) requires either a Ivanti Patch for Windows® Servers Advance license or a separately purchased add-on license key.

The power management function enables you to control the power state of the physical machines and the online virtual machines in your organization. The primary reasons for using power management are to:

- Prepare your machines for maintenance tasks
- Reduce power consumption and noise
- Reduce operating costs
- Prolong battery life

You can shut down, restart, or wake up machines either immediately or on a scheduled basis. You also have the ability to put machines into a sleep or hibernate state.

TIP: If you want to perform power tasks on offline virtual machines that reside on an ESXi Hypervisor, you can do so using the Virtual Inventory feature.

How-To Information

For information on how to perform power management tasks, see:

- Creating and Editing a Power State Template
- How to Initiate Power Management Tasks
- Monitoring a Power Task
- Initiating and Monitoring a Power Status Scan
- Viewing Power Status Scan Results

Extremely Flexible Implementation Options

Ivanti Patch for Windows® Servers provides a number of ways for you to implement the power management options.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **Immediate Shutdowns or Restarts With No User Warning:**You can immediately shut down or restart one or more connected machines from Machine View or Scan View by using a right-click command. The machines must be in a fully powered on state in order to accept the shutdown or restart command. These immediate actions will typically be used for maintenance purposes when you cannot wait for machines to be shut down or restarted. When performing an immediate restart of a machine it will always be returned to a fully powered on state. For more information, see Shutdown Implementation Notes and Restart Implementation Notes.

- **Scheduled Shutdowns or Restarts With A User Warning:** You can shut down or restart one or more connected machines by using a power state template. The advantage of using a power state template is that it gives you the option to provide a warning to any active users of the machines. It also enables you to schedule the action to happen immediately or at some time in the future.

  Scheduled shutdowns and restarts are typically used for reducing power or turning off machines at night, over weekends, or on holidays. This can be used to fulfill a corporate "green" initiative by saving power when machines are not being used. The machines must initially be in a fully powered on state in order for the scheduled job to be performed.

- **Initiate sleep or hibernate state with or without a prior restart:** A power state template can be used to put machines into a sleep state or a hibernate state. You can choose to perform the action with or without a prior restart of the target machines. As with all jobs initiated using a power state template, you can schedule the job to run now or at some time in the future. For more information, see Sleep and Hibernation Implementation Notes.

- **Immediate or scheduled Wake-on-LAN:** The Wake-on-LAN (WoL) feature is used to return machines to a fully powered on state. This is performed from Machine View or Scan View by using a right-click command. Any connected machine that is sleeping, hibernating, or powered off (but with power available to the network card) can be awakened by a WoL request. One typical reason for using WoL is to turn on machines that have been powered off overnight or over a long holiday weekend, making the machines ready for use for the coming work day. Another reason may be to power on machines prior to performing maintenance tasks such as console-based patch or asset scans. Machines that are sleeping, hibernating, or powered off cannot be scanned, so using the WoL feature ensures that your maintenance tasks will be performed on schedule.

  The Wake-on-LAN request can be issued immediately, or it can be scheduled to occur at a specific time. It's like scheduling a wakeup call for each machine. For more information on WoL, see Wake-on-LAN Implementation Notes.

  Machines that are sleeping, hibernating, or powered off cannot be restarted or awakened using a power state template, they must be awakened using the WoL feature.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Agentless vs. Agent-based

Power management tasks can be performed using either an agentless or an agent-based method. This section describes the agentless method. For information on performing agent-based power tasks, see Creating and Configuring a Power Task.



An agentless power state task will push a small number of files from the console to each target machine. If a large number of machines are involved it may affect the performance of your network.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Power Management Requirements

Before performing a power management task, please confirm that you meet the following requirements.

General Requirements

- Power management tasks performed from machine groups will be successful on physical machines and online virtual machines, but not on offline virtual machines
- A power management license key is required for all power tasks (you must have either Ivanti Patch for Windows® Servers Advanced or Ivanti Patch for Windows® Servers Standard + a separately purchased add-on license key)
- In order for power state changes to be made to a target machine, a user must be logged on to the machine or the local security policy **Interactive logon: Do not require CTRL+ALT+DEL** must be disabled.
- When initiating a power management action, the program will attempt to authenticate to the target machines using a variety of credentials and will do so using the following strategy:

1. If one or more of the following are available, try to authenticate using the credential with the highest precedence, where the precedence order is as follows:

    a. Any managed machine credentials (if initiating the action from Machine View or Scan View) or machine group credentials (if initiating the action from a machine group or favorite)

    b. Default credentials (used if the machine credentials are missing)

2. If the credential used above does not work, the Integrated Windows Authentication credentials (the credentials of the person currently logged on to the program) will be used.

    If neither of these credentials work then the action will fail.

Sleep and Hibernate Requirements

In order to put a machine in or take a machine out of a sleep or hibernate state, its operating system must be configured to allow the operation.

Wake-on-LAN (WoL) Requirements

Hardware Requirements

- WoL tasks must be performed on physical machines, not on virtual machines

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- WoL must be enabled in the BIOS of the target machines. See your hardware vendor's product documentation for details.
- Target machines must have either a wired or a wireless Network Interface Card (NIC) that supports WoL. See your hardware vendor's product documentation for details.
- The target machines can be in sleep, hibernate, or powered off states.
- The network cards on the target machines must have power available (either electric or battery).
- Any intervening routers may need to be configured to forward subnet-directed broadcasts. See your hardware vendor's product documentation for details on configuring your routers.

  Whether you need to configure your routers depends on where your target machines are located. If all the target machines are located on the same subnet as the console then your routers do not need to be reconfigured. If some of your target machines are behind one or more routers and thus on different subnets, then the intervening routers must be configured to forward subnet-directed broadcasts on UDP port 9.

Software Requirements

- A hardware asset scan of each target machine must be performed prior to initiating a WoL request. The scan is needed in order to obtain the MAC address of each target machine. When configuring the hardware asset scan make sure the **Network** option is selected.
- Each target machine's operating system must be configured to allow WoL.
- Outbound UDP port 9 must be open on the console machine.

Power Status Scan Requirements

A power status scan can be performed on physical machines, online virtual machines, and offline virtual machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating and Editing a Power State Template

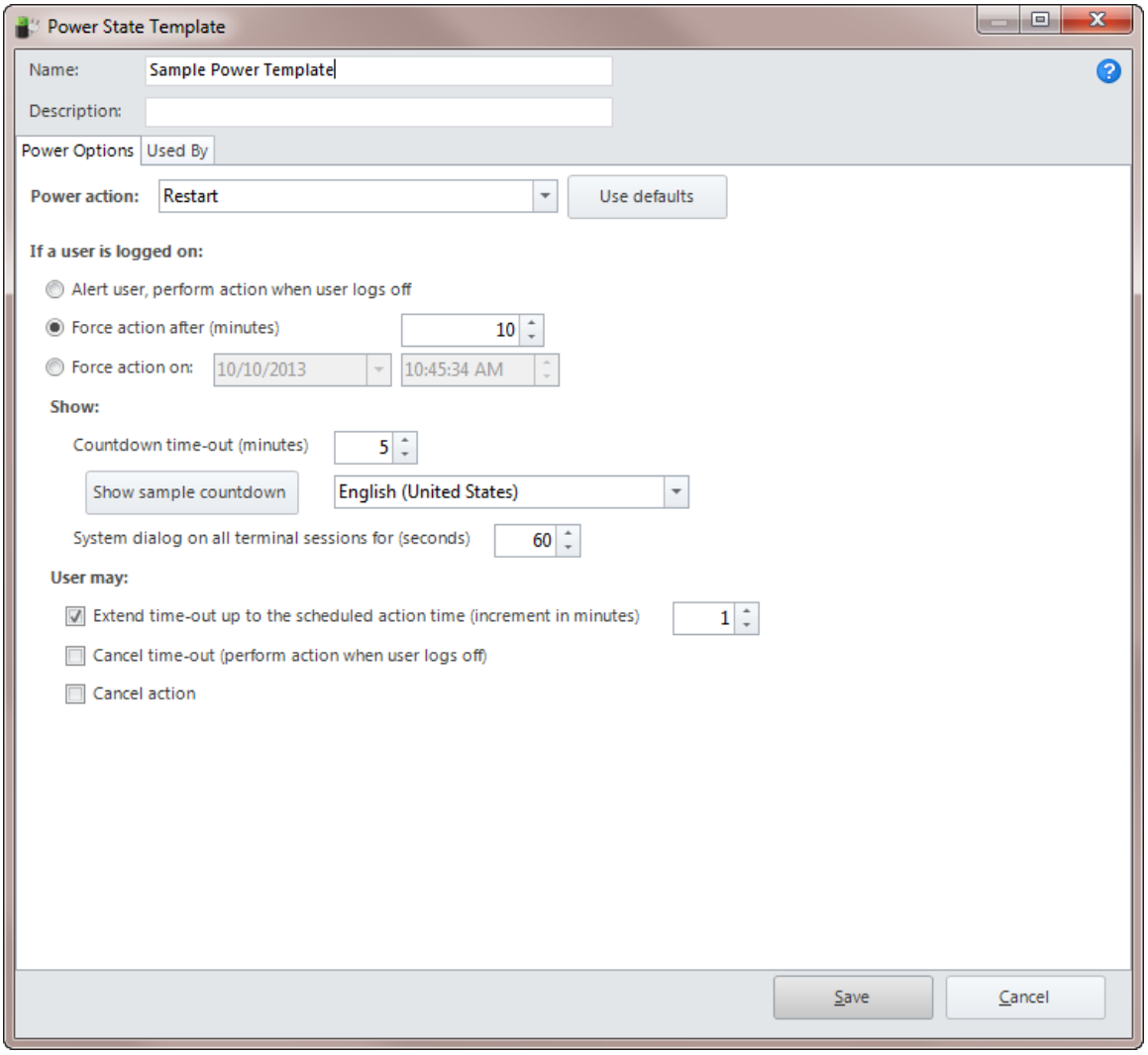
Ivanti Patch for Windows® Servers comes with one predefined power state template, named **Standard Power**. This template cannot be modified. It will:

- Initiate an immediate restart of all machines
- Enable a logged on user to extend the reboot in one minute increments up to 10 minutes
- Bring the machines back online after the reboot

While the Standard template is fine for many instances, you may want to utilize some of the more advanced features, such as the ability to leave the machines in a reduced power or powered off state. To this end, Ivanti Patch for Windows® Servers enables you to create any number of custom power state templates.

To create a new power state template, from the main menu select **New > Power State Template**. The **Power State Template** dialog will appear.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



The **Power State Template** dialog contains two tabs that collectively define the characteristics of the template.

Name	The name that you wish to assign to this power state template.
Description	A description of the template.
Restart and power action	You can specify if a restart should occur and what power state you want to leave the machines. • **Sleep if possible:** The machines are put into a sleep state directly without a restart. This is a low power state that eliminates power to all unneeded areas of a machine. For more detailed information about sleep state, see Sleep and Hibernation Notes.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **Hibernate, otherwise try sleep:** The machines are put into a hibernation state without a restart. This is very similar to sleep state, with the difference being that the machine's RAM is copied to a storage areas (such as a hard drive) before hibernation state is initiated. This enables an end user to very quickly restart the machine, restore the previous state, and resume working.

  If a target machine is not configured to allow hibernation, the program will instead attempt to put the machine into a sleep state. If the machine cannot be put into a sleep state no action will occur. For more detailed information about hibernate state, see Sleep and Hibernation Notes.

- **Shut down:** The machines are powered off. This option is also useful if you simply want to make sure non-critical machines are turned off each night or over a weekend, saving energy.

- **Restart:** The machines are restarted and left in a powered on state.

- **Restart, then sleep if possible:** The machines are restarted and then put into a sleep state. There is a two minute delay between the completion of the restart and the time the machines are put into the sleep state. The Microsoft Scheduler is used on each target machine to initiate the sleep state following the restart.

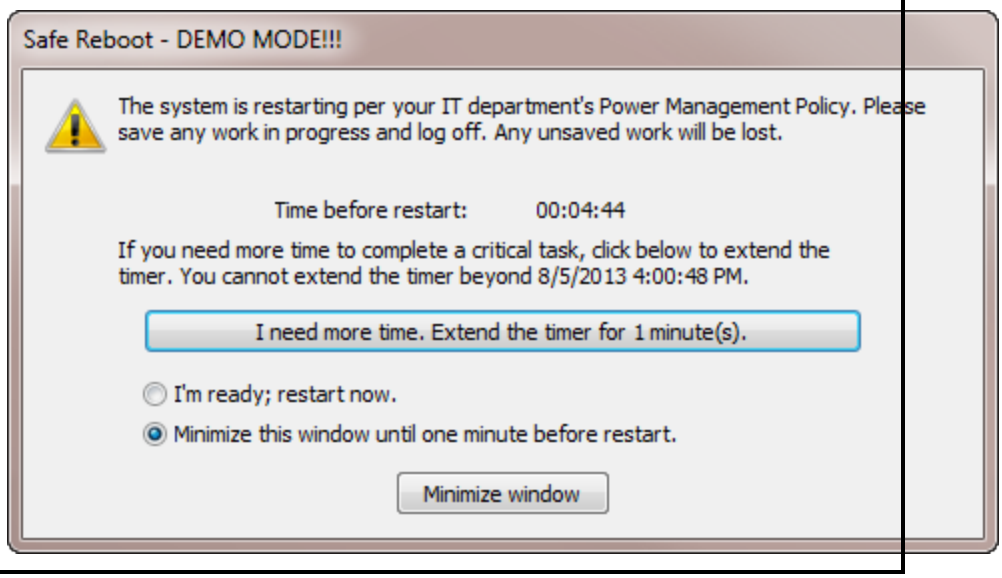
- **Restart, then hibernate if possible:** The machines are restarted and then put into a hibernation state. There is a two minute delay between the completion of the restart and the time the machines are put into the hibernate state. The Microsoft Scheduler is used on each target machine to initiate the hibernate state following the restart.

  If a target machine is not configured to allow hibernation, the program will instead attempt to put the machine into a sleep state after the restart. If the machine cannot be put into a sleep state no action will occur. For more detailed information about hibernate state, see Sleep and Hibernation Notes.

- **Restart, then shut down:** The machines are restarted and then powered off. This option enables you to provide a warning to any active users about the pending restart. There is a two minute delay between the completion of the restart and the time the machines are shut down. This option is useful if you want to perform a reboot in order to complete a maintenance task but then want the machines to be shut down. The Microsoft Scheduler is used on each target machine to initiate the shutdown following the restart.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	IMPORTANT! The **Restart, then shut down** option will not work correctly on Windows XP target machines that do not require users to press Ctrl+Alt+Del before logging on (see http://support.microsoft.com/kb/816938). On these machines the shutdown will not occur until after a user logs in. You can remedy this by using the Local Security Policy editor on each Windows XP machine to disable the **Do not require CTRL+ALT+DEL** security option. Keep in mind that for domain-joined machines the group policy may override the local policy.
Use defaults	This button is tied to the **Restart and power action** box. When you click **Use defaults**, all remaining options on the dialog will be changed to the values recommended for use with the currently selected **Restart and power action**.
If a user is logged on	If you elect to restart or shut down the machines, you can specify the amount of warning that a logged-on user will receive and you can choose the degree of control the user will have over the process. You can: • Alert the user that a restart (or shutdown) will occur when they log off. • Elect to force a reboot (or shutdown) after a number of minutes have passed. • Elect to force a reboot (or shutdown) at a specific date and time. • Show a time-out countdown on the user's machine in advance of the reboot (or shutdown) with a specified initial time-out value. To preview the dialog box that the user will see, click **Show Sample Countdown**. The language box to the right can be used to preview this dialog in different languages.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• Select the duration to display the standard Windows shutdown message when the shutdown sequence is initiated. • Allow the user to extend the time-out countdown up to a specified maximum. • Allow the user to cancel the time-out. If a time-out is cancelled the machine will be restarted after the user logs off or manually reboots the machine. • Allow the user to cancel the restart.
Used By tab	This tab shows you the Favorites and the agent policies that are currently using this power state template. This is important to know if you are considering modifying the template, as it tells you what other areas of the program are affected.

To save the template click **Save**. To close the dialog without saving the changes **Cancel.**

To use a power state template, see How to Initiate Management Tasks.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How to Initiate Power Management Tasks

There are a number of power management tasks that you can perform on the machines in your organization, including:

- Restart now
- Shut down now
- Send a Wake-on-LAN request (immediate or scheduled)
- Determine the current power state by performing a power status scan
- Modify the power state using a power state template (immediate or scheduled)

Power management tasks can be initiated from several different areas of the interface.

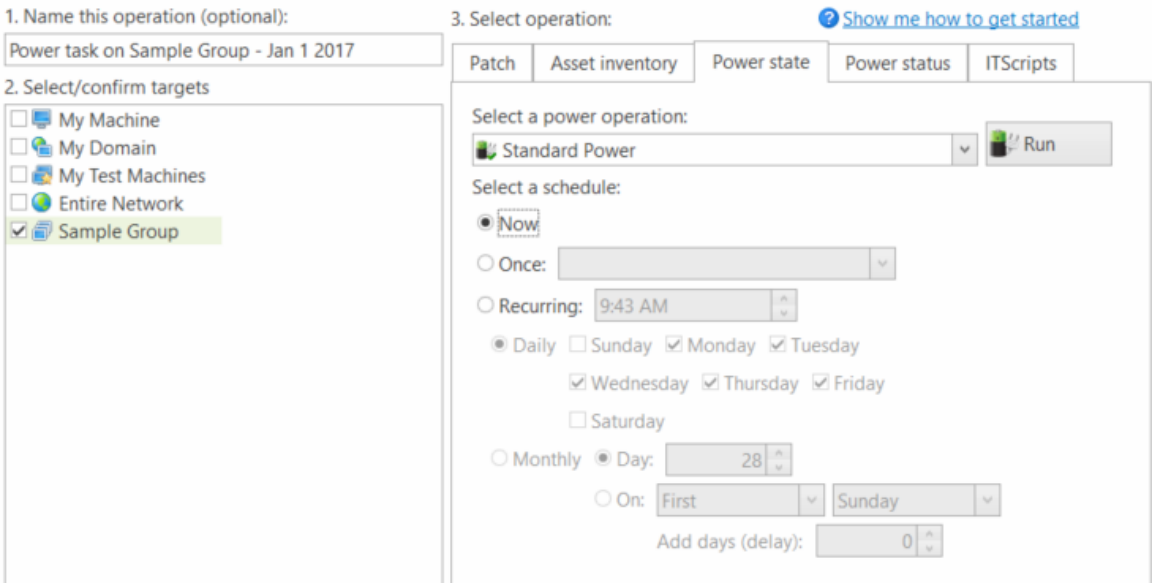
FROM THE HOME PAGE

You can use the home page to initiate a power task on any of the four pre-defined groups (**My Machine**, **My Domain**, **My Test Machines**, **Entire Network**) or of a custom machine group.

1. Type a name for the operation you are about to perform.

   At a minimum the name should indicate which machines will be affected and when the power task will be run (for example, *Machine group name mm/dd/yy*). You may wish to include other identifiers such as the power state template being used, if it is a regularly scheduled task or an out of band task, etc. A maximum of 100 characters can be used for the name.

2. Select the desired machine group.



3. Choose either the **Power state** tab or the **Power status** tab.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

The **Power state** tab is used if you want to modify the power state of your machines and the **Power status** tab is used if you want to determine the current power state of your machines.

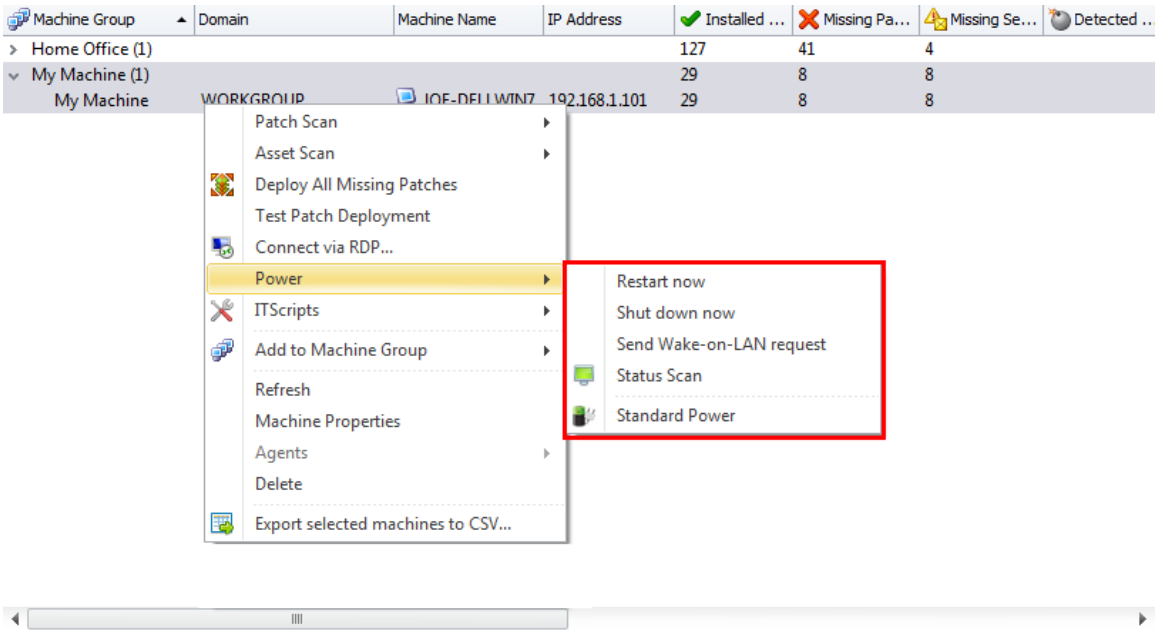
4. (Conditional) If you choose the Power state tab, select the power task you want to perform (either the **Standard Power** template or a custom power state template).
5. Choose when you want to perform the power task (**Now**, **Once**, or **Recurring**).
6. Click either **Run/Scan now** or **Schedule**.

   - **Run/Scan now:** When **Now** is the scheduling option, the button name will be either **Run** (if a power template is selected) or **Scan now** (if **Power Status Scan** is selected). The power task will begin immediately on all machines in the machine group. The Operations Monitor is used to track the progress of the power task.
   - **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See Scheduling Power Tasks and Monitoring a Scheduled Power Task for more details.

FROM MACHINE VIEW OR SCAN VIEW

You can initiate a number of different power management tasks from within Machine View or Scan View by using right-click commands.

1 Select one or more machines.
2. Right-click the machine(s) and then select either a power management command or the desired power state template.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

The first two power management commands enable you to immediately restart or shut down the selected machines. The **Send Wake-on-LAN request** can be sent to the selected machines immediately or it can be scheduled for a later date and time. The **Status Scan** command initiates a power status scan of the selected machines. Finally, a power state template can be used to put the selected machines into a particular state (powered on, in sleep mode, in hibernate mode, or powered off).

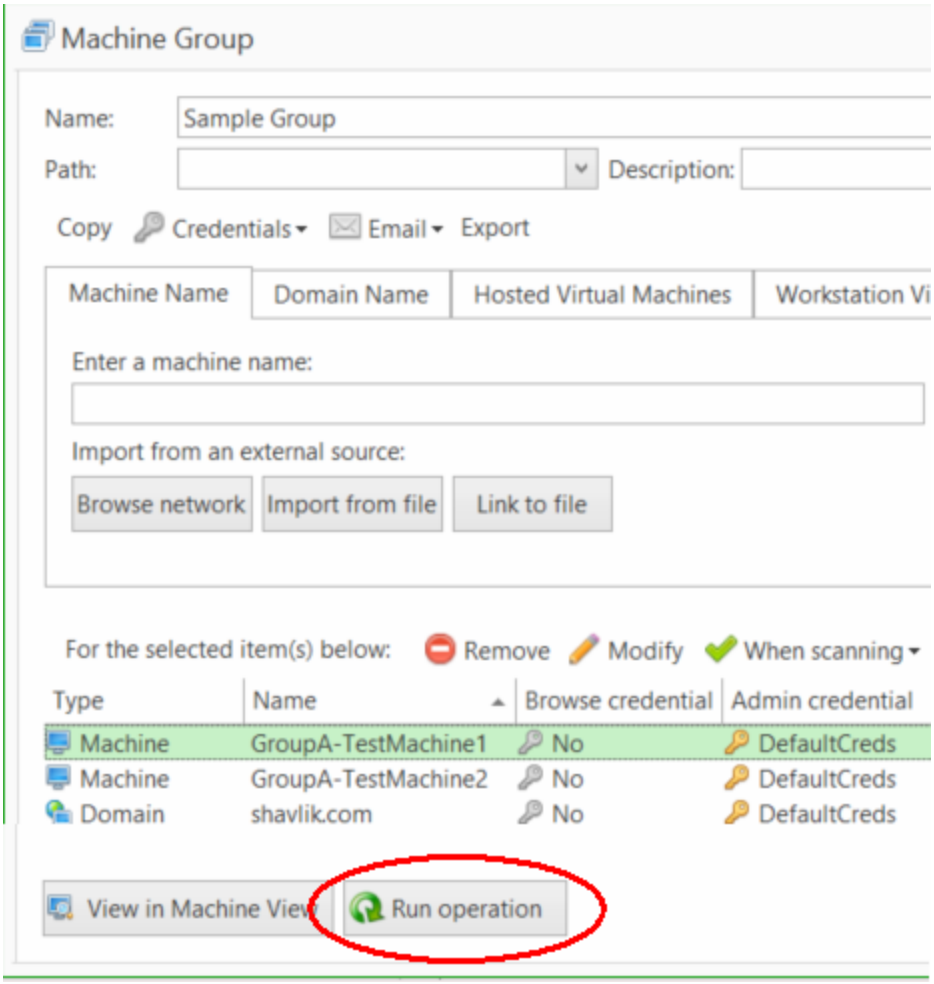
For more specifics please see the following:

- Scheduling Power Management Tasks
- Restart Implementation Notes
- Shutdown Implementation Notes
- Wake-on-LAN Implementation Notes
- Sleep and Hibernation Implementation Notes
- Monitoring a Power Status Scan

FROM A MACHINE GROUP

1 In the **Machine Groups** pane select the desired machine group.
2. Within the machine group dialog click **Run Operation**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



3. On the **Run Operation** dialog select when you want the power state or power status task to run.
4. On the **Run Operation** dialog click either **Run/Scan now** or **Schedule**.
    - **Run/Scan now:** When **Now** is the scheduling option, the button name will be either **Run** (if a power template is selected) or **Scan now** (if **Power Status Scan** is selected). The power task will begin immediately on all machines in the machine group. The Operations Monitor is used to track the progress of the power task.
    - **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See Scheduling Power Tasks and Monitoring a Scheduled Power Task for more details.

What state the machines are left in following a restart is dependent on how the power template is configured.

FROM WITHIN A FAVORITE

You can schedule one or more machine groups for a shutdown or a restart by using a power state

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

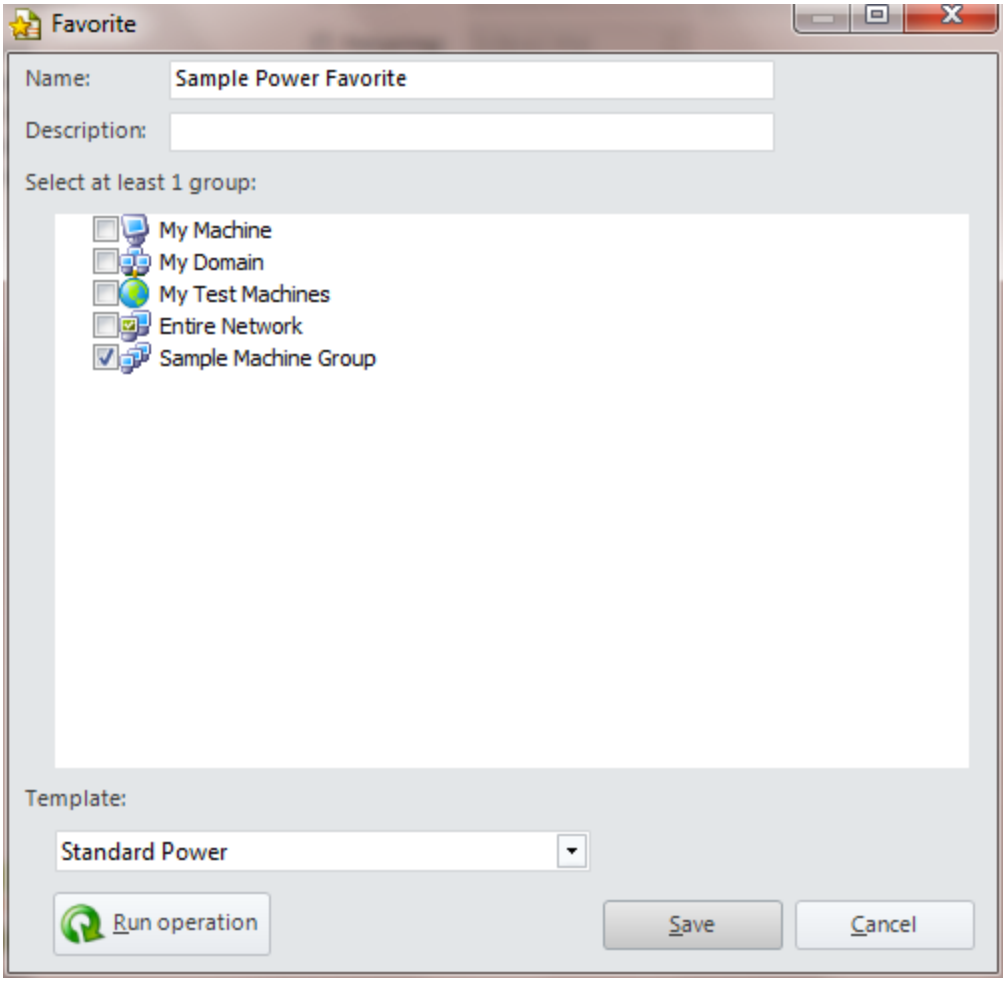
template.

1 In the **Favorites** pane select the desired favorite.

2. In the **Favorite** dialog select the desired machine group(s).

3. In the **Template** box select the desired power state template.

   See Creating and Editing a Power State Template for information on creating your own unique power state templates.



4. Click **Run operation**.

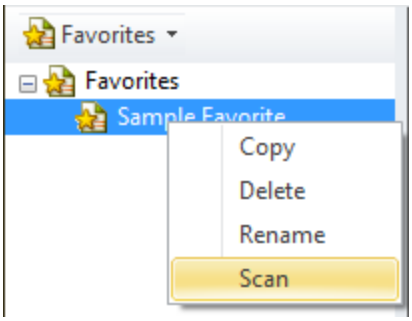
The **Run Operation** dialog is displayed, enabling you to schedule the power state job to run now or at some time in the future. What state the machines are left in following a restart is dependent on how the power template is configured.

BY RIGHT-CLICKING A FAVORITE

With this method the favorite must already specify the power state template to use.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

1 In the **Favorites** pane, right-click the desired favorite.



2. Select **Scan**.

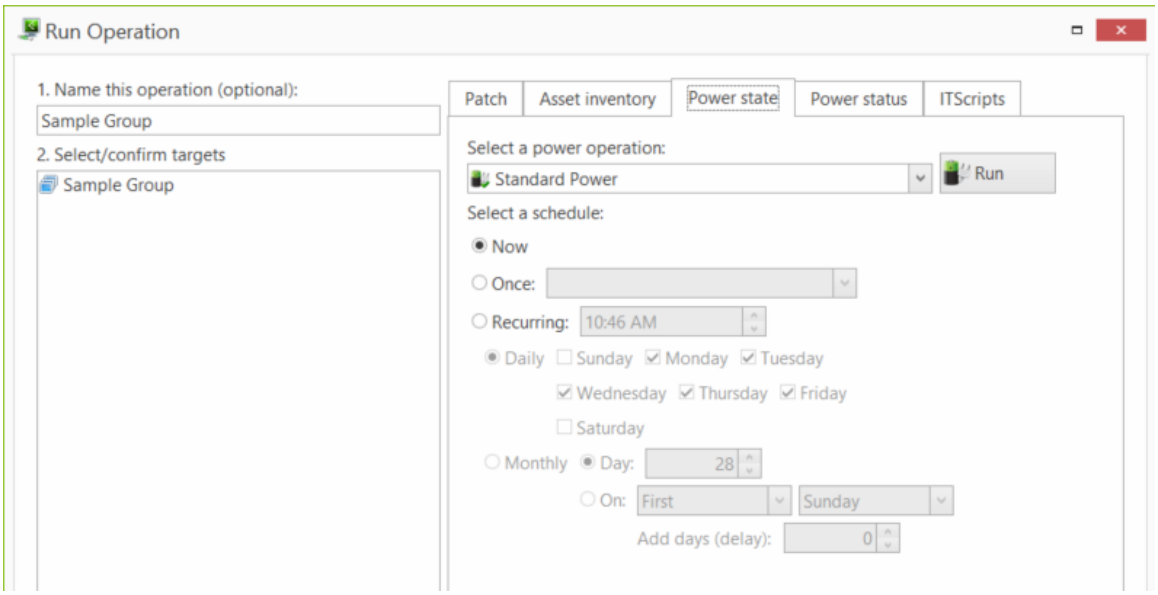
Ivanti Patch for Windows® Servers will not actually scan the machines; rather, it will launch a **Run Operation** dialog that enables you to schedule the power state job to run now or at some time in the future. What state the machines are left in following a restart is dependent on how the power template used by this favorite is configured.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Scheduling Power Management Tasks Using the Run Operation Dialog

When you initiate a task from a machine group or from a Favorite, or when you initiate a Wake-on-LAN request, the **Run Operation** dialog is displayed. You can use the dialog to schedule the power task immediately or at some point in the future.

Make sure the proper credentials are available for all machines involved in the scheduled task.



Name this operation (optional)	Enables you to provide a unique name for the operation. By default the name of the machine group or favorite used to initiate the operation will be used. The name is displayed in the Results pane.
Select/confirm targets	This list is a reminder of the machine group(s) that will be affected by the operation. If the wrong group is listed, click**Cancel**and re-initiate the operation using the correct group.
Select a power operation	Enables you to select the power state template you want to use when performing the operation.
Select a schedule	There are three scheduling options: • **Now** runs the operation as soon as the **Scan now** or **Run** button is clicked. • **Once** indicates that the operation will be run once at the day and time selected.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **Recurring** allows an administrator to regularly schedule operations at a specific time and using a specified recurrence pattern. For example, using this option, an operation could be run every night at midnight, or every Saturday at 9 PM, every weekday at 11 PM, or at any other user selected time and interval. You can also use the **Recurring** option to schedule a power status scan in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly power status scan to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by one day. The **Add delay (days)** option is not available for other power state operations.

When the desired options are selected, click **Scan now** or **Run** (if **Now** is selected) or **Schedule** (if **Once** or **Recurring** is selected).

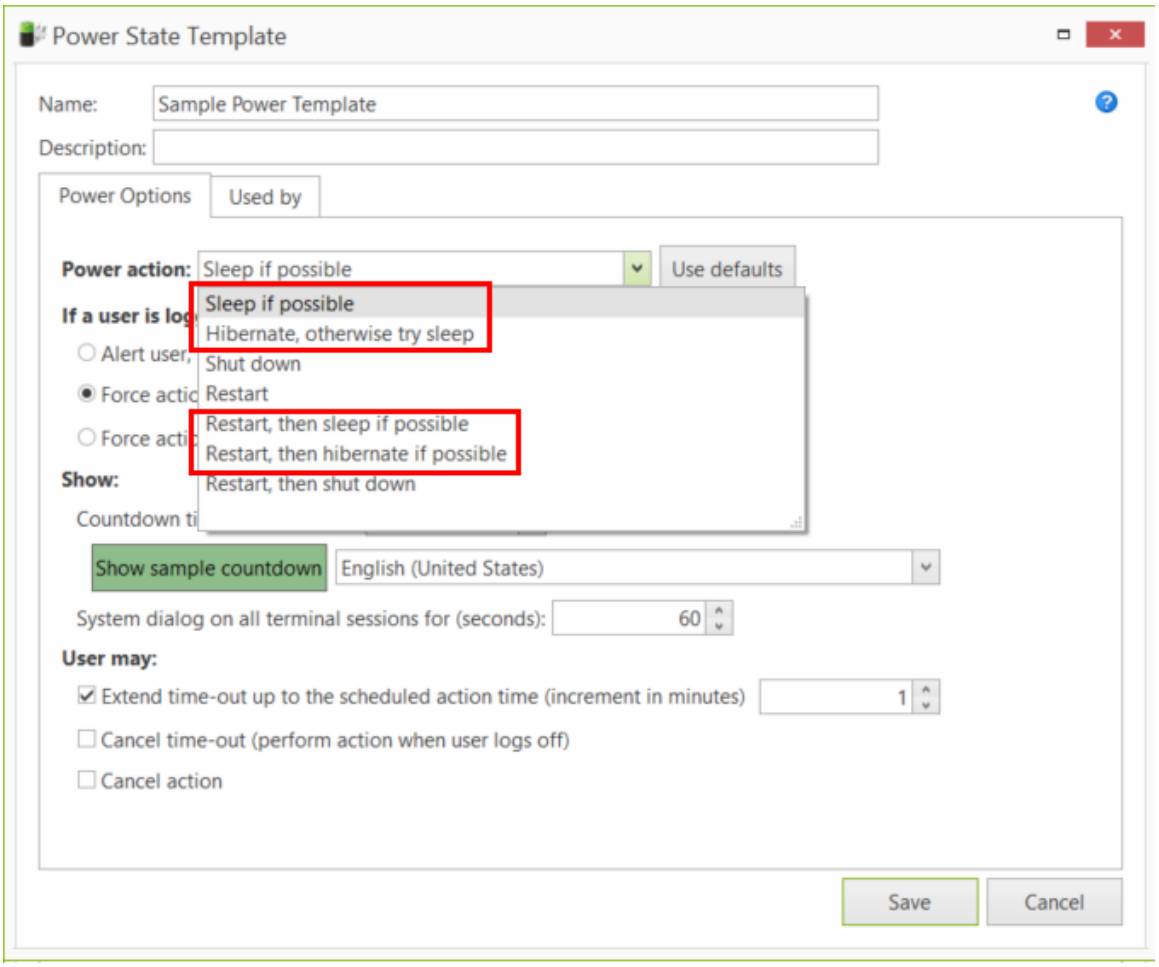
- **Scan now/Run:** The operation is initiated immediately and the **Operations Monitor** is displayed.
- **Schedule:** The operation is scheduled on the target machine.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Sleep and Hibernation Implementation Notes

You can use a power state template to put your machines into a sleep state or a hibernate state.

- **Sleep state:** This is a low power state that eliminates power to all unneeded areas of the machine.
- **Hibernate state:** This is very similar to sleep state, with the difference being that the machine's RAM is copied to a storage area (such as a hard drive) before hibernate state is initiated. This enables a user to very quickly restart the machine, restore the previous state, and resume working. If a target machine is not configured to allow hibernation, the program will instead attempt to put the machine into a sleep state. If the machine cannot be put into a sleep state no action will occur.



The machines can be put into sleep or hibernate state immediately, or they can be restarted before being left in the desired power state.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Like any other job that is scheduled from the console, the power state job will only work on those target machines that are in a fully powered on state when the job is initiated. Machines that are in a reduced power or powered off state are not affected.

The following table indicates when a sleep or hibernate command will work on a target machine:

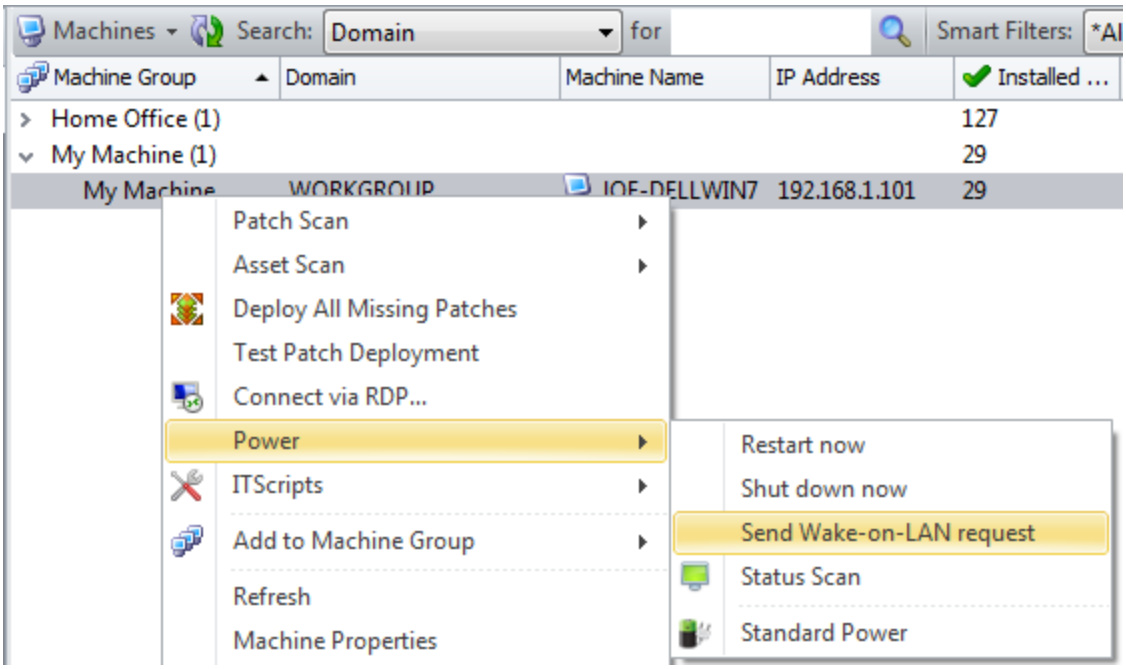
Initial Power State of Target Machine	Logged On Users?	Action Taken?
Fully powered on	Yes	Yes, unless the user cancels the action
	No	Yes
Sleep state	N/A	No action
Hibernate state	N/A	No action
Powered off	N/A	No action

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Wake-on-LAN Implementation Notes

IMPORTANT! You must perform a hardware asset scan on your target machines prior to initiating a WoL request. The scan is required in order to obtain the MAC address of each machine.

The Wake-on-LAN (WoL) feature is used to wake up machines that are powered off or in reduced power states. This is performed from Machine View or Scan View by using a right-click command.

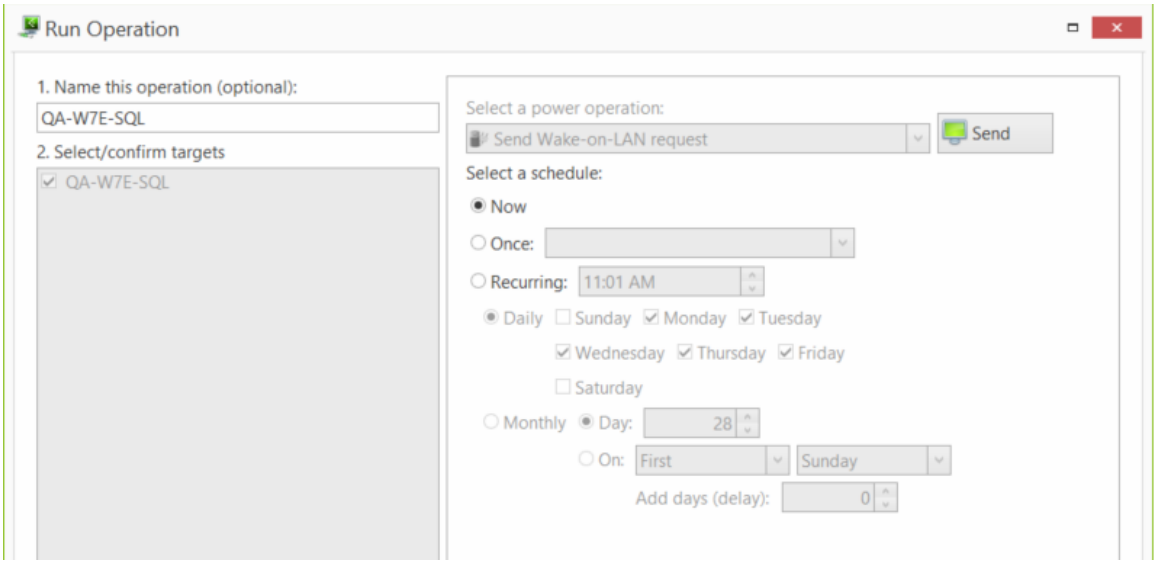


Machines that are sleeping, hibernating, or powered off cannot be restarted or awakened using a power state template, they must be awakened using the Wake-on-LAN feature.

Any connected machine that is sleeping, hibernating, or powered off (but with power available to the network card) can be awakened by a WoL request. One typical reason for using WoL is to turn on machines that have been powered off overnight or over a long holiday weekend, making the machines ready for use for the coming work day. Another reason may be to power on machines prior to performing maintenance tasks such as console-based patch or asset scans. Machines that are sleeping, hibernating, or powered off cannot be scanned, so using the WoL feature ensures that your maintenance tasks will be performed on schedule.

The Wake-on-LAN request can be issued immediately, or it can be scheduled to awaken machines at a certain time. It's like scheduling a wakeup call for each machine.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



The **Power > Send Wake-on-LAN request** command works with the following target machine states:

Initial Target Machine Power State	Target Machine Awakened?
Fully powered on	No action
Sleep state	Yes
Hibernate state	Yes
Powered off	Yes

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Shutdown Implementation Notes

There are two methods you can use to shut down the connected machines in your organization.

- You can use the right-click **Power > Shut down now** shortcut command from within Machine View or Scan View. With this method:
  - The console machine is not affected
  - The selected machines will be shut down immediately
  - No warning will be issued to active users of those machines
- You can use a power state template to schedule a shutdown. With this method:
  - The console machine is eligible to be shut down
  - You can schedule the shutdown to happen immediately or at some point in the future
  - A warning will issued to all active users of those machines

The Shutdown command works with the following target machine states:

Initial Power State of Target Machine	Target Machine Shut Down?
Fully powered on	Yes
Sleep state	No action
Hibernate state	No action
Powered off	No action

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Machine Restart Implementation Notes

There are two methods you can use to restart the connected machines in your organization and leave them in a fully powered on state.

- You can use the right-click **Power > Restart now** shortcut command from within Machine View or Scan View. With this method:
  - The console machine is not affected
  - The selected machines will be restarted immediately
  - No warning will be issued to active users of those machines
- You can use a power state template to schedule a reboot. With this method:
  - The console machine is eligible for a restart
  - You can schedule the reboot to happen immediately or at some point in the future
  - A warning will issued to all active users of those machines

The Restart command works with the following target machine states:

Initial Power State of Target Machine	Target Machine Left in Fully Powered On State?
Fully powered on	Yes
Sleep state	No action
Hibernate state	No action
Powered off	No action

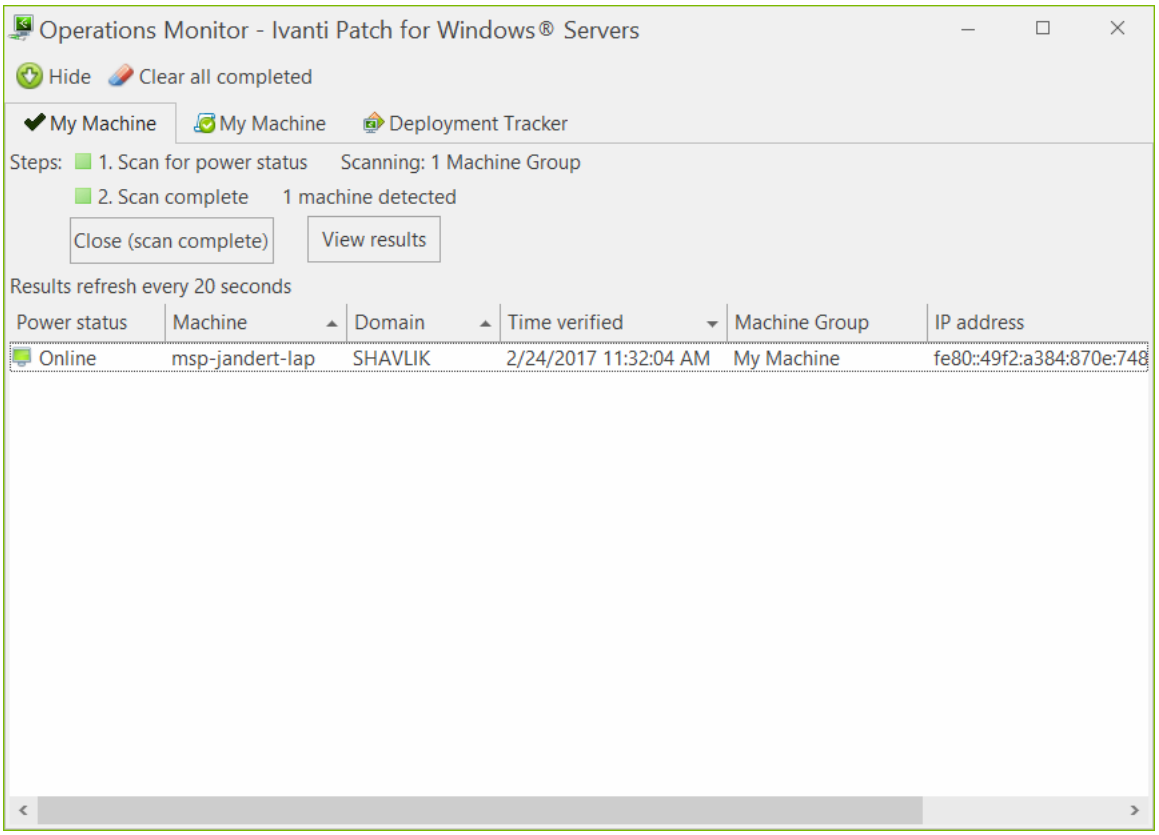
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Monitoring a Power Task

The Operations Monitor is automatically displayed whenever an agentless power management task is initiated. This includes:

- Restart now
- Shut down now
- Send Wake-on-LAN request (Run now)
- Power state template (Run now)
- Power Status scan (this is a special case, see Monitoring a Power Status Scan)

The Operations Monitor will show the requested action, the status, and any errors that occur.



The Operations Monitor will display the status of power tasks that are performed immediately. It will also show whether scheduled tasks are successfully scheduled on the target machines. See Monitoring a Scheduled Power Task for more details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Monitoring a Scheduled Power Task

When you click **Schedule** on either the home page or the **Run Operation** dialog, a scheduled task is created on the console that will launch the scan at the appointed day and time. To view the scheduled task, select **Manage > Scheduled Remote Tasks**. If the power task is scheduled to run against the console, you can view that by selecting **Manage > Scheduled Console Tasks** and then selecting the **Local Patch Deployments** tab.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Initiating and Monitoring a Power Status Scan

You can easily determine the current power state of one or more machines in your organization by performing a power status scan.

Initiating a Power Status Scan

You can initiate a power status scan a number of different ways:

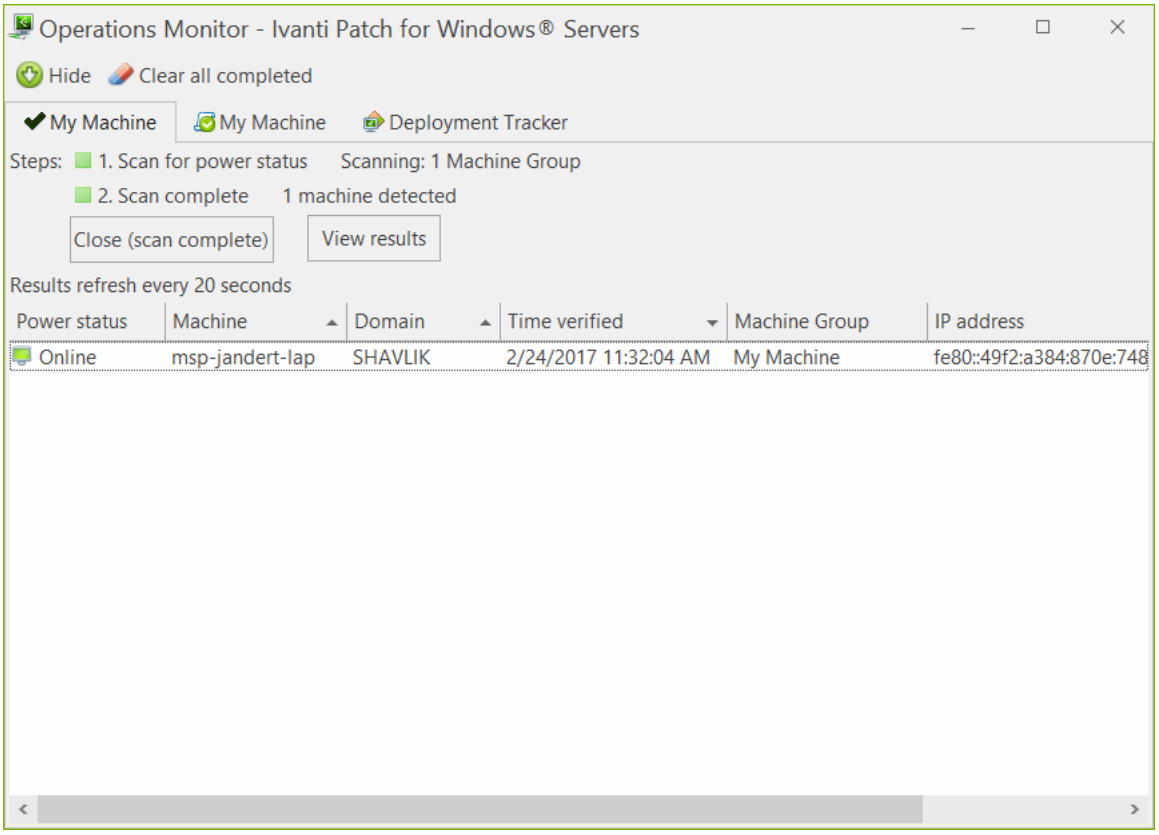
- From the home page by selecting the desired machines and then selecting **Power Status Scan**.
- From Machine View or Scan View by right-clicking the desired machines and then selecting **Power > Status Scan**.
- From a machine group by clicking Run Operation and then selecting **Power Status Scan**.

For more details see How to Initiate Power Management Tasks.

Monitoring a Power Status Scan

In all cases the Operations Monitor will be used to display the status of the power status scan.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



When the power status scan is complete you can:

- View the results by clicking **View results**. The Operations Monitor will be closed and the scan results will be displayed. See Viewing Power Status Scan Results for details.
- Remove the current tab by clicking **Close (scan complete)**. Any other tabs on the Operations Monitor will remain open.
- Minimize the Operations Monitor by clicking **Hide**. No tabs are removed from the Operations Monitor.
- Remove the current tab and all other tabs by clicking **Clear All Completed**.
- Generate a Power Status report.
- View summary information about each machine that was scanned. Right-click on a column heading and select **Column Chooser** to add or remove columns from the display.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

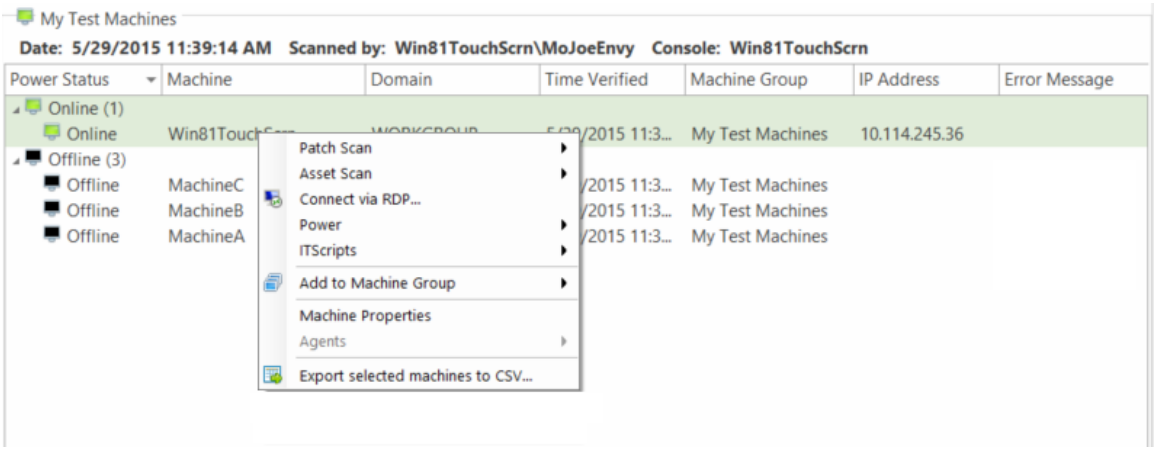
Viewing Power Status Scan Results

Power status scan results are available immediately following a successful scan by clicking the **View results** link on the **Operations Monitor** dialog (see Performing a Power Status Scan). The scan results are also available when you select a scan from the **Results** pane.

TIP: Another option for viewing results is to generate a Power Status report.

You use the **Power Status** column to determine the current power state of the scanned machines. Machines will be categorized as either offline or online. The summary table contains a number of other columns that uniquely identify each machine. You can click on a column heading to sort the table by that information. You can also specify what information is presented by right-clicking the table heading and using **Column Chooser** to add or clear items.

Finally, you can right-click one or more machines and perform the following actions:



Patch Scan	Enables you to initiate a patch scan of the selected machines using any of the available patch scan templates.
Asset Scan	Enables you to initiate an asset scan of the selected machines using any of the available asset scan templates.
Connect via RDP	Enables you to make a Remote Desktop connection to the selected machine. See How to Initiate a Remote Desktop Connection for more details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Power	Enables you to modify the power state of the selected machines. You can immediately restart, shut down, or awaken the machines, or you can use a power state template to schedule a reboot of the machines and leave them in a particular state (fully powered on, in sleep mode, in hibernate mode, or powered off). See How to Initiate Power Management Tasks for more information. You can immediately restart or shut down the machine(s).
ITScripts	Enables you to either open a Windows PowerShell™ prompt or select and execute an approved script. See How to Execute a Script for details.
Add to Machine Group	Enables you to add the selected machines to a new machine group or to an existing machine group. See Creating A New Machine Group for more information. IMPORTANT! Machines you add to the machine group are automatically assigned the associated machine credentials. (Hosted virtual machines are the exception, they are assigned the last known machine group credentials.) If no machine credentials are available, no credentials will be assigned and the default credentials will be used in any subsequent scans. If the default credentials are not valid for the machines, and if the account credentials of the person currently logged on to the program are also not valid for the machines, scans of the machines you just added to the group will fail. To prevent scanning errors, always supply credentials for machines you add to a machine group. See Supplying Credentials for more information.
Machine Properties	Enables you to view and edit machine properties. See Managing Individual Machine Properties for more information.
Agents	Enables you to: • Install an agent, assign a different policy to the agent,or uninstall an agent.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• Send a number of different commands to the selected agents. The commands apply only to machines that already have agents installed, that are online, and that are configured to be listening agents. See the Send command description for detailed information about the available commands. • **(Machine View only)** Initiate any of the tasks currently defined within the selected agents. When you select a task a confirmation dialog is displayed. If you choose to continue, the task is immediately started on the agent machines. See Creating a New Agent Policy for information on the types of tasks that may be available.
Export selected machines to CSV	Export information about the selected machines to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Using Patch Deployments to Perform Power Tasks

A power state template is not the only means for putting your machines into a sleep or hibernation state, you can also use a patch deployment template to perform these tasks. The **Post-deploy Reboot** tab can be used to configure the program to place your machines into the desired state following a patch deployment. For more details see Deployment Template: Post-deploy Reboot Tab.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About Machine View

Machine View is an extremely powerful and flexible tool. It enables you to display current information about every machine in your network that has been previously scanned and whose information resides in the database. It organizes all of the scanned machines so they are displayed in one comprehensive view, regardless of when the machines were scanned. Machine View provides an easier method to both view and manage the current security state— across both agent-based and agentless systems. Machine View differs from Scan View, which requires you to first locate the scan in which the machine was assessed before drilling down to view the machine's scan summary.

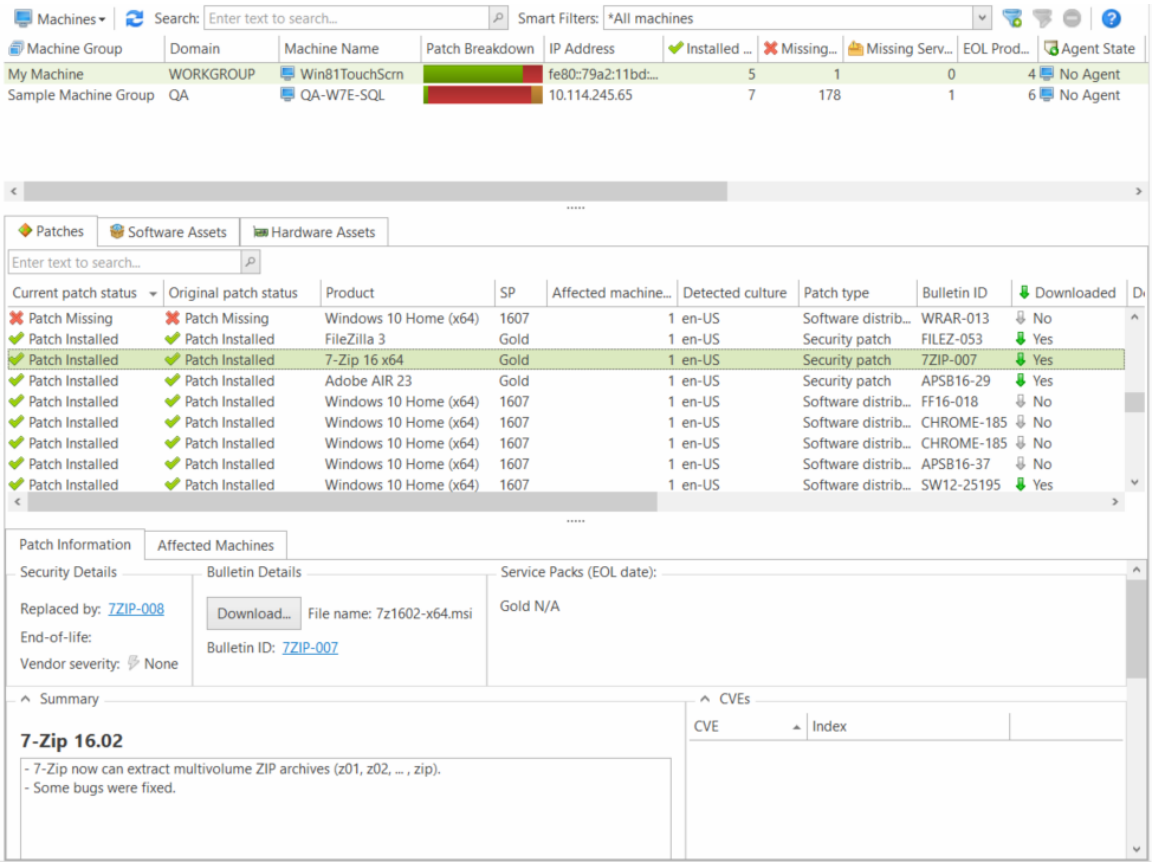
The advantages of Machine View include:

- You are not restricted to viewing just those machines involved in a particular scan. You can view all the machines that have ever been scanned.
- You can quickly assess the status of all machines in your organization.
- You can view patch and asset information at the same time. With Scan View you can only view patch information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Accessing Machine View

Machine View is accessed from the main menu by selecting **View > Machines**.



For information on using Machine View, see Navigating Machine View.

Machine View will be empty if you view it immediately after installing the program. This is because there is no machine information in the database to display.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Navigating Machine View

Machine View consists of three panes. Each pane displays unique information and provides unique functionality. The panes are interrelated -- the information presented in a lower pane is dependant on what is selected in the pane directly above it. This "top down" approach means you use the top pane to view high-level information and the two lower panes to drill down to more detailed information.

- The top pane displays all machines that have been scanned at some point and that are "known" by the program. See the following topics for information on using the top pane:
  - Searching Machine View
  - Filtering Machine View
  - Performing Actions on Machines
  - Customizing the Column Headers
- The middle pane displays patch and assetpatch information about the machine selected in the top pane. See the following topics for information on using the middle pane:
  - Viewing Patch Summaries
  - Performing Actions on Patches
  - Viewing Software Asset Summaries
  - Viewing Hardware Asset Summaries
  - Customizing the Column Headers
- The bottom pane displays detailed information about the patch selected in the middle pane. See the following topics for information on using the bottom pane:
  - Viewing Patch Details
  - Viewing Machines Missing A Selected Patch
  - Viewing Machines Containing A Selected Patch
  - Customizing the Column Headers

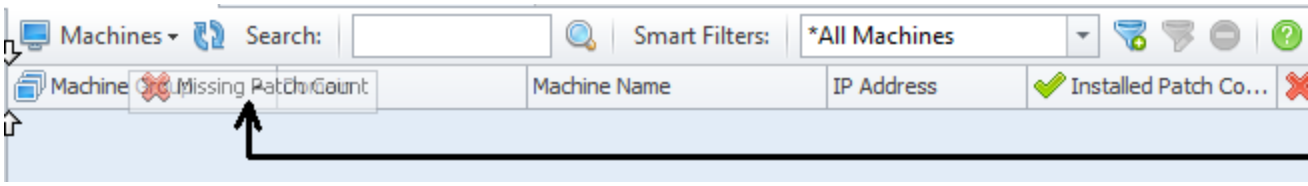
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Customizing the Column Headers

You can easily customize the way information is displayed within any of the panes in Machine View or Scan View.

- You can reorder the columns by clicking and dragging the column headers to new locations.

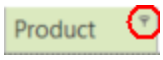
  For example, if you want missing patch information to be displayed in the first column of the top pane, simply click on the **Missing Patch Count** icon and drag it to the first column.



  TIP: When reordering columns, the column header you are moving will always be placed in front of the column you drag it to.

- You can apply filters to one or more column headers.

  Hover over a column header and then click the filter icon located in the upper-right corner. For example:

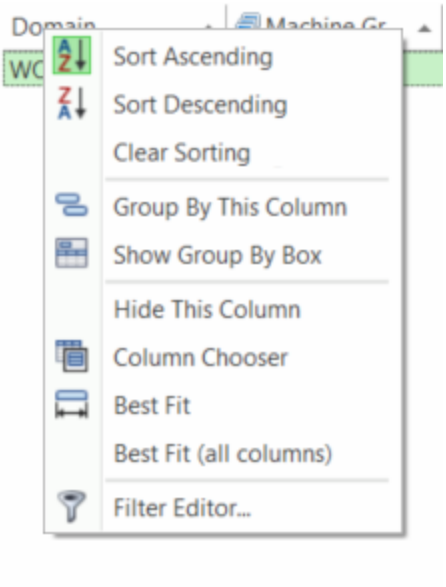


  Use the filter menu to select which of the values currently contained in the column should be displayed. When you apply a column filter, the filter definition will be displayed beneath the pane. You can use this to confirm which column filters have been applied to the current display, and you can edit the filter. For example:



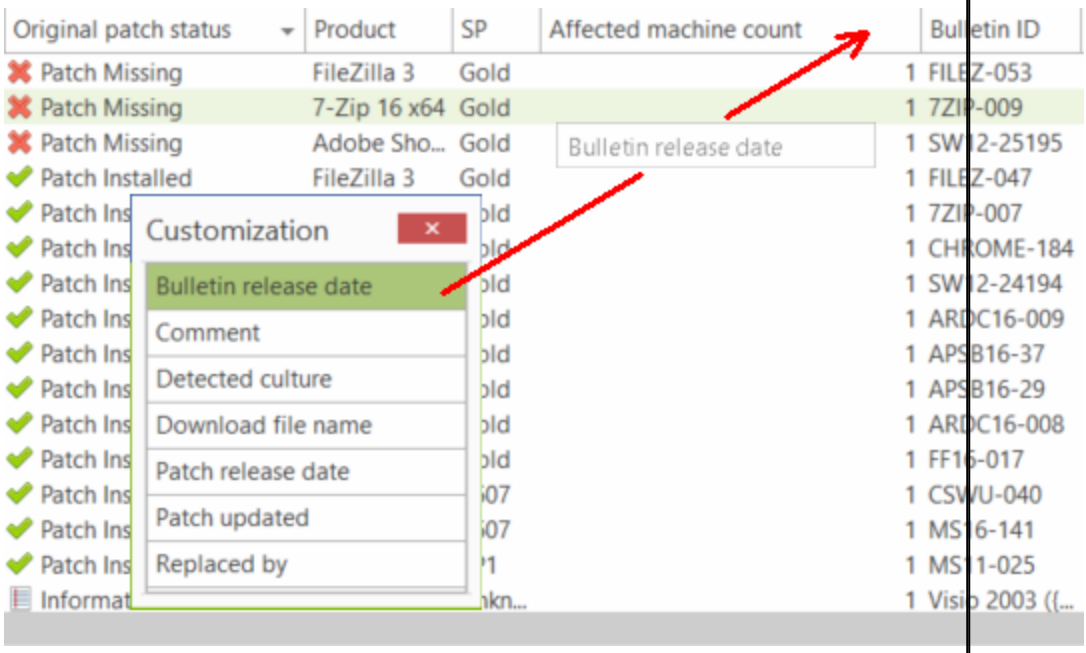
- You can right-click within a column header and perform a number of additional actions.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Sort Ascending	Sorts the selected column in ascending order.
Sort Descending	Sorts the selected column in descending order.
Clear Sorting	Clears the ascending or descending sorting criteria currently set for a column.
Clear All Sorting	Clears the sorting criteria currently set for any column in the table.
Group By This Column	Groups the table by the data in the selected column. It does this by moving the data into expandable lists that are located in the body of the grid. One expandable list will be created for each possible column value. If you perform this action on any subsequent columns, that data will be presented as nested groups at increasingly lower levels within the expandable lists. If **Show Group By Box** is enabled, this will also create a "Group By" box in the area immediately above the column headers. TIP: To turn off the **Group By This Column** feature and revert to the original view: Enable **Show Group By Box**, drag the Group By boxes back to the column header and then right-click in the column header and select **Hide Group By Box**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Show Group By Box / Hide Group By Box	Displays or hides an area immediately above the column headers that contains "Group By" boxes. One Group By box will be displayed for each column header for which **Group By This Column** is currently enabled. You can also drag column headers to and from this area. The table will be grouped according to the data in the box. If there are two or more boxes then the grouping will be nested, with the left-most box presented at the highest level, the second box presented at the second level, etc.
Hide This Column	Removes the column from the table. You can add the column back to the table using the **Column Chooser**.
Column Chooser	Enables you to add and hide information within a pane. When you select **Column Chooser** the **Customization** dialog is displayed. This dialog is used to store the columns you don't currently want displayed within the pane. Simply click and drag the desired column headers from the table to the Customization dialog. For example, if you decide you want to add the Bulletin release date column to the table, simply drag that column header from the Customization dialog to the table. For example, if you decide you don't want Language and Last Scan Template information displayed in the table, simply drag those column headers into the Customization dialog.  If you decide you want an item back in the table, simply click and drag it from the Customization dialog back to the table.
Best Fit	Resize the width of the selected column so that the header text is displayed in the optimal amount of space.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Best Fit (all columns)	Resize the width of all columns in the table so that the header text is displayed in the optimal amount of space.
Filter Editor	The **Filter Editor** dialog will show any filters that are currently active in the column headers. You can use the editor to modify the existing filter criteria and to build new criteria using the available filter conditions and logical operators.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Machine View Top Pane Summary

The top pane in Machine View displays a table containing detailed information about every machine in your network that has been scanned and whose information resides in the database. Click on a column heading to sort the table by that information. You can also specify what information is presented by right-clicking the table heading and selecting or clearing the available items. Right-click on a column heading and select **Column Chooser** to add or remove columns from the display.

, , or	Indicates whether the computer is a physical machine or an online virtual machine (), an offline virtual machine (), or a virtual machine template ().
Machine Group	The assigned machine group at the time of the scan.
Domain	The domain of the scanned machine.
Machine	The machine name.
IP Address	The IP address of the scanned machine.
Virtual Server	The name of the server that is hosting the virtual machine. This column does not apply to physical machines.
VM Name	The name of the virtual machine. This column does not apply to physical machines.
Path	The full path name of the hosted virtual machine. This column does not apply to physical machines.
Installed Patch Count	The total number of patches found on the scanned machine.
Missing Patch Count	The total number of patches missing on the scanned machine.
Missing Service Pack Count	The total number of service packs missing on the scanned machine.
Patch Breakdown	A visual representation of the percentage of installed patches (green) vs. missing patches (red) and missing service packs (yellow). If you choose to sort this column, the sort value for each machine is computed as follows: number of missing patches + (number of missing service packs * 10).
EOL Products	The number of software products on the machine that have been designated as at End-of-Life by their vendor.
Agent State	The current state of the agent installed on the machine. If an agent is not installed the **No Agent** icon is displayed.

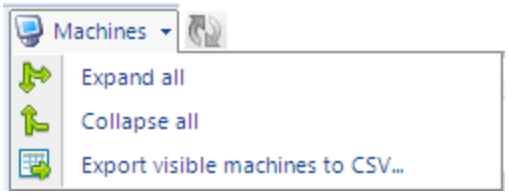
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Assigned Agent Policy	The name of the agent policy currently assigned to the scanned machine.
Last Agent Check In	Shows the last time the agent checked in with the console.
Agent Version	The version number of the agent currently installed on this machine.
Latest Patch Scan Date	Shows the last time a patch scan was performed on the scanned machine.
Operating System	The operating system being used on the scanned machine. If the operating system is shown inredit indicates that it has reached its end-of-life (EOL) phase and the vendor will limit support for the product.
Assigned Credential Name	The credentials currently assigned to this machine.
Console	The console that most recently managed this machine.
Asset Definition	The version of the Asset Definition data used in the last asset scan of this machine.
Last Asset Scan Template	The Asset Scan Template used in the latest asset scan of this machine.
Last Scan Tempate	The Patch Scan Template used in the latest patch scan of this machine.
Last Asset Scan Date	The date of the most recent asset scan of this machine.
Operating System Language	The locale of the machine operating system (e.g., en-US).
Patch Definition	The version of the Patch Definition data used in the last patch scan of this machine.
Reported Agent Policy	This applies only to agent machines. This is the agent policy last reported by the agent. It may differ from the Assigned Agent Policy if a new policy has been assigned but the agent has not checked in since the assignment was made.
Machine Criticality	The criticality assigned to this machine in the Manage Machine Properties dialog. Right-click one or more machines and select **Machine Properties** to edit this value.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Custom1 **Custom2** **Custom3**	These columns display text entered in the Custom tab of the Manage Machine Properties dialog. Right-click one or more machines and select **Machine Properties** to edit these values.

The **Machines** menu enables you to perform the following actions on the machines in the top pane.



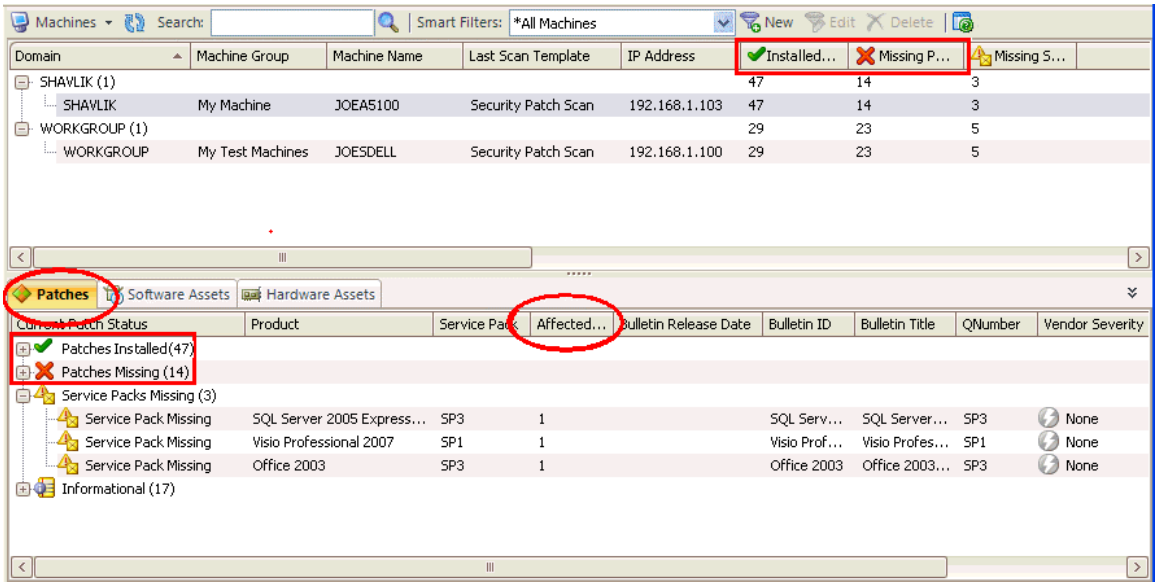
Expand all	Expands all machine trees in the top pane.
Collapse all	Collapses all machine trees in the top pane.
Export visible machines to CSV	Export information about the machines in the top pane to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program.

In addition, the refresh icon ( ) refreshes all machine information in the top pane. The latest information for all machines is retrieved, and newly scanned machines may appear.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Understanding Patch Count Data

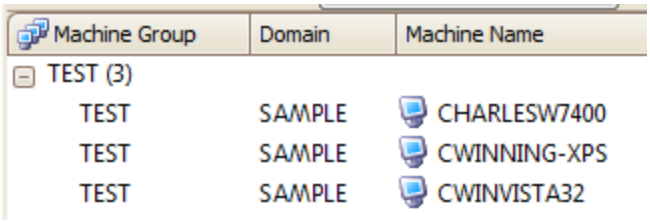
The values for the **Installed Patch Count** and **Missing Patch Count** columns in the top pane may not always match the values shown in the middle pane. This is because the top pane counts every patch on every machine, while the middle pane counts only unique patches and ignores duplicates. You can use the **Machines Missing** tab in the bottom pane to determine if a particular patch is missing on multiple machines.



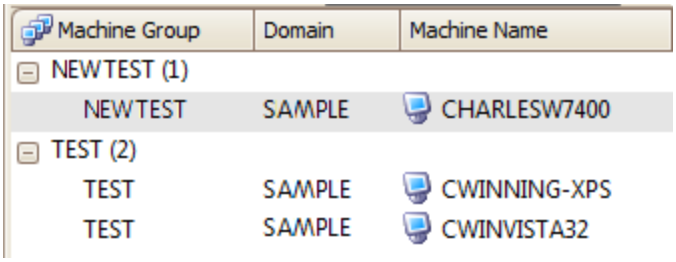
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Machine Group Information is Dynamic

The machine group information that is displayed is based on the machine group used to perform the most recent action on each machine. So it is possible for the machine group information to change. For example, if you perform a scan of a group containing three machines, the information displayed will be similar to the following:



If you then re-scan the first machine from a different machine group, the refreshed display will reflect this change:



The first machine is no longer listed with its original group because the most recent scan of the machine was initiated from a different machine group.

When agents check in with the console they will be listed with the machine group from which they were last scanned from the console.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Searching for Machines in the Top Pane

You can easily search for machines contained in the top pane. All searches are performed using the Search tool.



To initiate a search you type the machine name you want to find and then press **Enter** or click the search icon (). Only those machines matching the search criteria are displayed; all other machines are hidden.

Tips for Using the Search Tool

- The Search tool works only on the information currently visible in the top pane.
- If a Smart Filter is applied, only machines matching BOTH the search criteria and the smart filter criteria are displayed.
- All partial matches are displayed. For example, if you search for machines named *Test*, any machine with "test" in its name will be considered a match (e.g. TestMachine1, Contest, etc.).
- A semicolon (;) can be used to concatenate multiple search terms into one search string. For example, specifying "server;workstation" will return all items containing either of the two terms.
- The use of wildcards in the Search tool is not allowed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Using Smart Filter to Filter Information in the Top Pane

Information displayed in the list can be easily filtered to narrow the focus to only those machines of interest. One way to do this is by using the Smart Filter.



The Smart Filter contains several default filters. You can also define your own custom filters.

Another option is to apply filters to individual columns. For more information, see Customizing the Column Headers.

Default Filters

The default filters are identified by a leading asterisk. Default filters cannot be modified or deleted. The default filters include the following:

- ***All Machines**: All machines are displayed, including servers and workstations.
- ***Servers**: Only servers are displayed.
- ***Workstations**: Only workstations are displayed.
- ***Today**: Only those machines that have been scanned within the last 24 hours are displayed.
- ***Last 7 Days**: Only those machines that have been scanned within the last seven days are displayed.
- ***Last 14 Days**: Only those machines that have been scanned within the last 14 days are displayed.
- ***Last 30 Days**: Only those machines that have been scanned within the last 30 days are displayed.
- ***Last 60 Days**: Only those machines that have been scanned within the last 60 days are displayed.
- ***Last 90 Days**: Only those machines that have been scanned within the last 90 days are displayed.
- ***Missing at least 1 patch**: Only those machines that are missing at least one patch are displayed.
- ***Has an Agent Policy**: Only those machines that have Ivanti Patch for Windows® Servers Agent installed are displayed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- ***Does not have an Agent Policy**: Only those machines that do not have Ivanti Patch for Windows® Servers Agent installed are displayed.

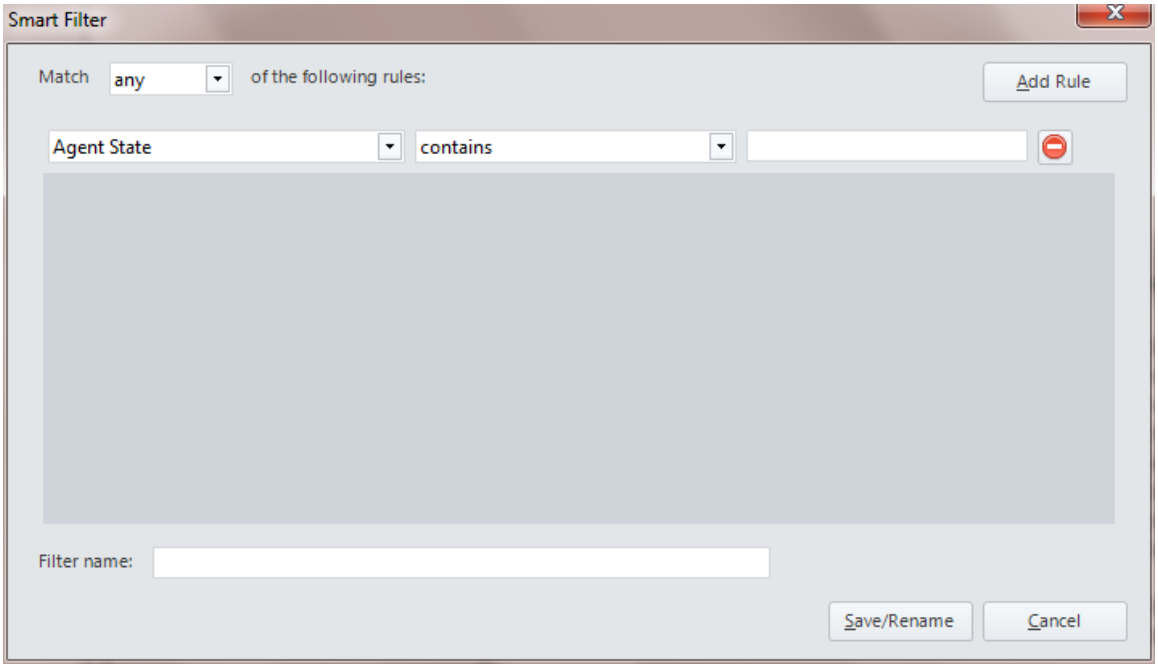
Custom Filters

You can create your own custom filters. This is a powerful tool that enables you to specify exactly which machines you want displayed in the top pane. Each custom filter is comprised of one or more rules. You can define as many rules in a filter as needed.

To create a new filter:

1. Click the Create a New Smart Filter icon ( ).

   The **Smart Filter** dialog is displayed.



2. Specify which rules in the filter must be matched.
   - **All**: Only those machines that match all the rules in the filter will be displayed.
   - **Any**: Machines that match at least one rule in the filter will be displayed.
3. Define one or more rules.

   To define a rule, select an option in each of the first two logic boxes and then type the criteria in the third box. To add another rule simply click **Add Rule**.

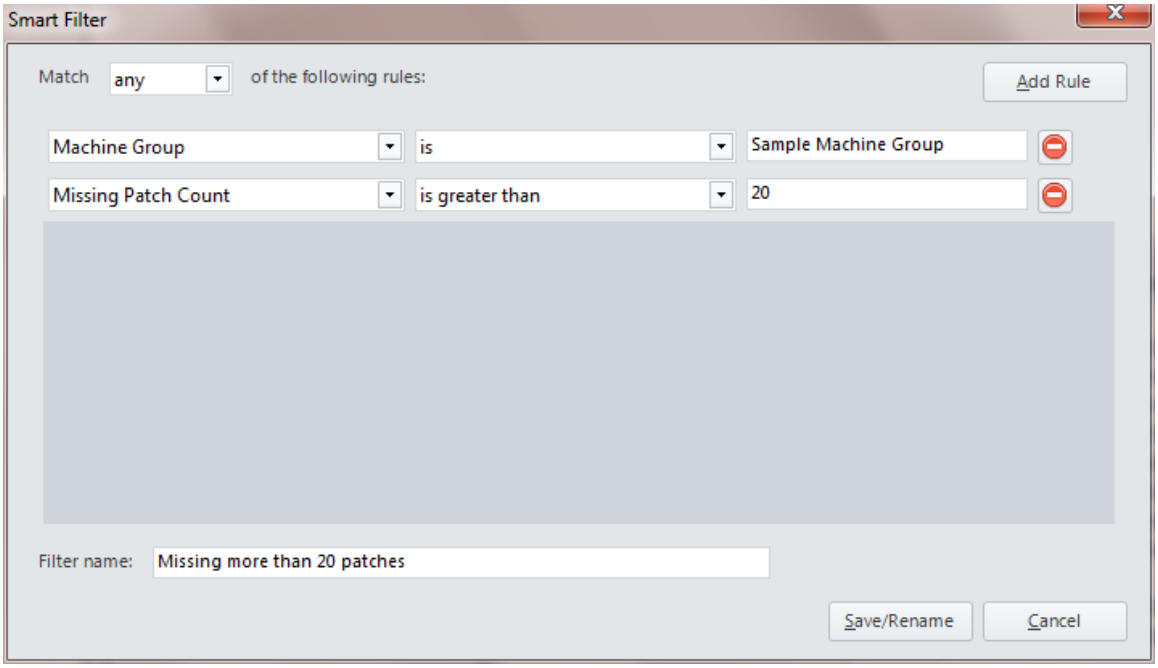
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

If you define a rule that does not make sense (for example, "Machine Name is greater than 3") the rule will simply be ignored.

4. Type a name for the filter.
5. When you are finished defining your custom filter, click **Save/Rename**.

Example

Assume you want to see which machines in a particular machine group are missing more than 20 patches. You simply create a filter similar to the following:

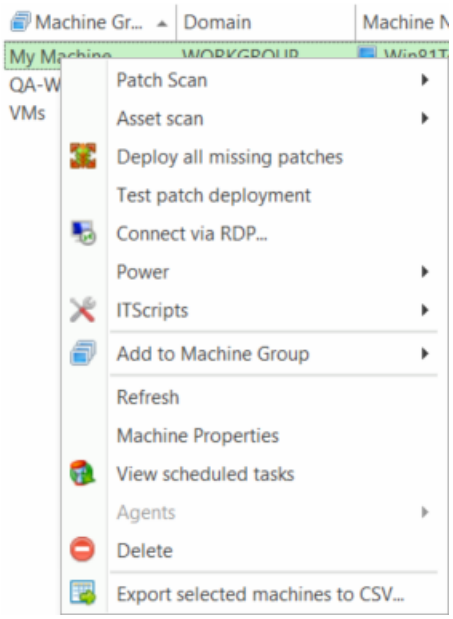


Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing Actions on Machines

Right-Click Menu

You can right-click on any machine in the top pane and perform a number of different actions.



Patch Scan	Enables you to initiate a patch scan of the selected machines using any of the available patch scan templates.
Asset Scan	Enables you to initiate an asset scan of the selected machines using any of the available asset scan templates.
Deploy All Missing Patches	Enables you to deploy (install) all patches currently missing on the selected machine. See Deploy to All Scanned Machines for more information.
Test Patch Deployment	Enables you to perform a test deployment to the selected machines. This is especially useful for patch deployments you want to schedule for a later time. Testing the deployment allows you to correct any potential problems in a deployment and make it less likely that a deployment will fail. See the Operations Monitor for more information. Test deployments will not work on **offline virtual machines** .

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Connect via RDP	Enables you to make a Remote Desktop connection to the selected machine. See How to Initiate a Remote Desktop Connection for more details.
Power	Enables you to modify the power state of the selected machines. You can immediately restart, shut down, or awaken the machines, or you can use a power state template to schedule a reboot of the machines and leave them in a particular state (fully powered on, in sleep mode, in hibernate mode, or powered off). See How to Initiate Power Management Tasks for more information. You can immediately restart or shut down the machine(s).
ITScripts	Enables you to either open a Windows PowerShell™ prompt or select and execute an approved script. See How to Execute a Script for details.
Add to Machine Group	Enables you to add the selected machines to a new machine group or to an existing machine group. See Creating A New Machine Group for more information. IMPORTANT! Machines you add to the machine group are automatically assigned the associated machine credentials. (Hosted virtual machines are the exception, they are assigned the last known machine group credentials.) If no machine credentials are available, no credentials will be assigned and the default credentials will be used in any subsequent scans. If the default credentials are not valid for the machines, and if the account credentials of the person currently logged on to the program are also not valid for the machines, scans of the machines you just added to the group will fail. To prevent scanning errors, always supply credentials for machines you add to a machine group. See Supplying Credentials for more information.
Refresh	Refreshes the information displayed in the top pane.
Machine Properties	Enables you to view and edit machine properties. See Managing Individual Machine Properties for more information.
View scheduled tasks	Enables you to view the Scheduled Remote Tasks Manager, which gives you a single location from which to monitor the power tasks and patch deployment tasks currently scheduled on this machine.
Agents	Enables you to: • Install an agent, assign a different policy to the agent, or uninstall an agent.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• Send a number of different commands to the selected agents. The commands apply only to machines that already have agents installed, that are online, and that are configured to be listening agents. See the Send command description for detailed information about the available commands. • **(Machine View only)** Initiate any of the tasks currently defined within the selected agents. When you select a task a confirmation dialog is displayed. If you choose to continue, the task is immediately started on the agent machines. See Creating a New Agent Policy for information on the types of tasks that may be available.
Delete	Deletes the selected machine from Machine View. If the machine is rescanned it will be re-added to Machine View. Deleting a machine from Machine View also affects the information displayed for that machine within Scan View (see Accessing Patch Scan Results). The machine will be moved to the **Machines Not Scanned** tab and all previous scan information for that machine will be lost.
Export selected machines to CSV	Export information about the selected machines to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program. The **Machines > Export visible machines to CSV** menu command is similar except that it exports all results in the right pane rather than just selected results.

Keyboard Shortcuts

The following keyboard shortcuts are available:

- **Ctrl+A**: Selects all machines.
- **CTRL+click**: Multiple machines can be selected by holding down the CTRL key while selecting machines.
- **SHIFT+click**: A contiguous group of machines can be selected by holding down the SHIFT key while selecting the starting and ending machines in the list.
- **SHIFT+PAGE UP**: Selects a range of machines from the one currently selected to the top of the table.
- **SHIFT+PAGE DOWN**: Selects a range of machines from the one currently selected to the bottom of the table.
- **HOME:** Moves the focus to the first cell in the table.
- **END**: Moves the focus to the last cell in the table.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

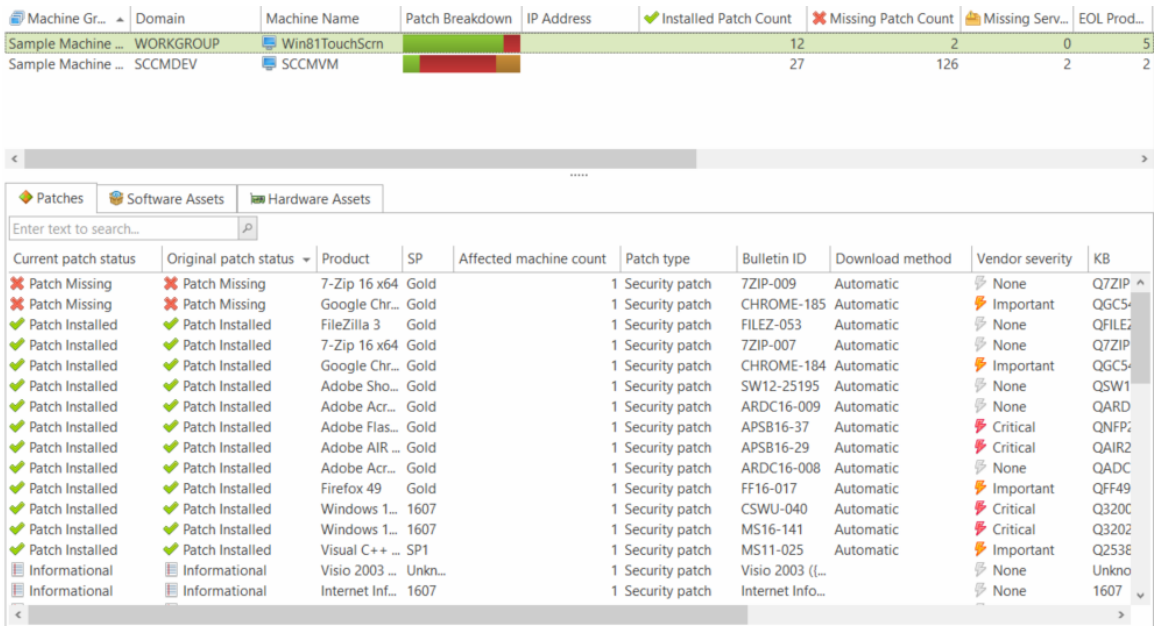
Viewing Patch Summaries in Machine View

The **Patches** tab in the middle pane displays general patch information about the machine(s) selected in the top pane. If multiple machines are selected in the top pane, this tab will display patch information for all selected machines. For example, if you select multiple domains in the top pane, summary information about all the machines in all domains will be displayed. The **Affected machine count** column indicates how many of the selected machines are affected by a specific patch or service pack.

A patch that is scheduled for deployment is considered to be still missing. This status will change after the patch is successfully installed.

The values for the **Installed Patch Count** and **Missing Patch Count** columns in the top pane may not always match the values shown in the middle pane. This is because the top pane counts every patch on every machine, while the middle pane counts only unique patches and ignores duplicates. You can use the **Affected Machines** tab in the bottom pane to determine if a particular patch is missing on multiple machines. Also, the middle pane breaks the patches into different categories and does not consider patches that are scheduled for installation or that are pending a reboot to be installed.

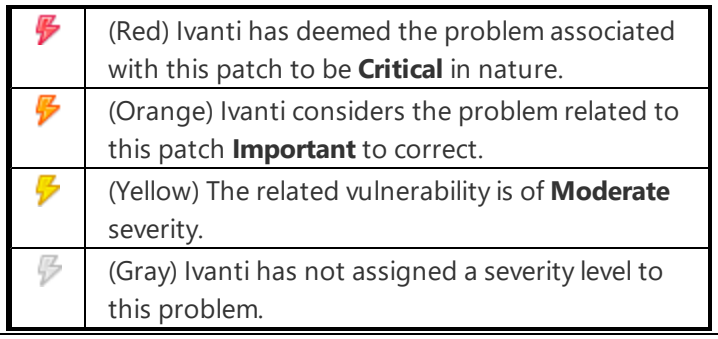
You can customize the way information is displayed within this pane. See Customizing the Column Headers for information.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Current patch status	The current status of the patch. This may be different from the status of the patch when the scan was originally performed. (For example, the patch may have been deployed since the scan was originally performed.)
Original patch status	Indicates the patch status at the time the patch scan was performed.
Product	The software product affected by this patch.
SP	The service pack level of the patch. For original patches the level will be Gold.
Affected machine count	Indicates the number of machines that are missing the patch. This number only applies to those machines that are selected in the top pane.
Patch type	Indicates the patch type. The possible types are: • **Non-security Patches:** The set of patches supported by Microsoft Software Update Services • **Security Patches:** Security bulletin-related patches • **Security Tools:** Patches for the malware tool provided by Microsoft Corporation • **Software Distribution:** Free third-party products that can be deployed by Ivanti Patch for Windows® Servers
Bulletin ID	Identifies the Microsoft Security Bulletin article that describes the threat addressed by the patch.
Bulletin Title	The descriptive title of the Microsoft Security Bulletin article that describes the threat addressed by the patch.
Download method	Indicates if the patch can be downloaded automatically by the program or if it must be downloaded manually. There may be a number of different reasons why a patch cannot be automatically downloadable. For example, you may have a patch that was created for a proprietary software program, or you may receive patches for a program that is no longer officially supported by the vendor. If the value in this column is **Automatic**, it means that Ivanti Patch for Windows® Servers can download the patch automatically. If the value is **Acquire from vendor** or some other value, it means that you must manually download the patch on your own and then move it into the patch download directory. Once the patch is there it can be deployed using the normal deployment process.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Vendor Severity	One of four severity levels assigned by Ivanti based on the perceived threat of the vulnerability related to the patch.  (Red) Ivanti has deemed the problem associated with this patch to be **Critical** in nature. (Orange) Ivanti considers the problem related to this patch **Important** to correct. (Yellow) The related vulnerability is of **Moderate** severity. (Gray) Ivanti has not assigned a severity level to this problem.
KB	The knowledge base number used to identify the Microsoft-based patch.
IAVA ID	This column is available only if you have a Government Edition of Ivanti Patch for Windows® Servers. The number used to identify patches in the Information Assurance Vulnerability Alert (IAVA) XML file compiled by the U.S. Government.
Uninstallable	Indicates if the patch can be uninstalled. Uninstalling a patch restores a machine to its original state before the patch was deployed. Patches must be uninstalled in the reverse order in which they were installed.
Downloaded	Indicates if the patch has been downloaded to the patch download directory.
EOL	The number of software products on the machine that have been designated as at End-of-Life by their vendor.
Bulletin release date	The original publication date of the security bulletin that identifies the vulnerability.
Comment	A user-supplied comment about the patch.
Detected culture	The local form of the operating system language detected on the target machine.
Download file name	The file name used by Ivanti Patch for Windows® Servers when downloading and deploying the patch. The name may include a three letter identifier that specifies the operating system language supported by the patch.
Patch release date	The date the patch was originally published.
Patch updated	The date an updated version of the patch was published.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

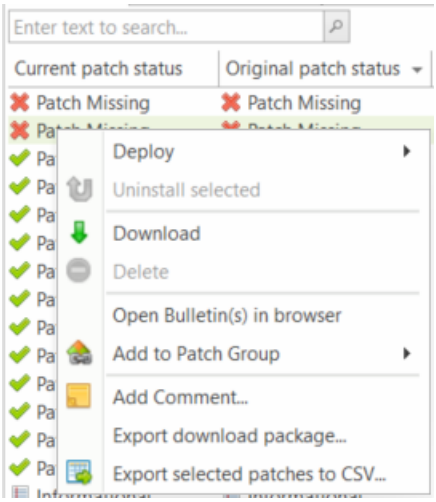
Replaced by	The bulletin ID that identifies a more recent update for the vulnerability.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing Actions on Patches

You can easily search for patches contained in the middle pane. All searches are performed using the Search tool. To initiate a search you type the alphanumeric characters that you want to find and then press **Enter** or click the search icon ( ). Only those patches matching the search criteria are displayed; all other patches are hidden. For tips on using the Search tool, see Searching for Machines.

In addition, you can right-click on any patch in the middle pane and perform a number of different actions. For example:



Deploy	Enables you to deploy (install) patches or service packs currently missing on the machine(s) selected in the top pane. See Deploying One or More Patches to a Machine for more information.
Uninstall Selected	Enables you to uninstall (rollback) the selected patch. See How to Uninstall Patches for more information.
Download	Enables you to download to the patch download directory the selected patches or service packs. See Downloading Patches for more information. The **Download** command is only available if the patch can be downloaded automatically. For more information see the description of the **Download method** column.
Delete	Enables you to delete selected patches from the patch download directory.
Open Bulletin(s) in Browser	Displays the related Microsoft security bulletin within a Web browser.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Add to Patch Group	Enables you to add the selected patch(es) to an existing patch group or to a new patch group. See Creating and Editing a Patch Group for more information.
Add Comment	Enables you to add your own specific comment about the patch.
Export download package	Export the download links for the selected patches to a Comma Separated Values (CSV) file. This is especially useful for a console that is in a disconnected environment. The CSV file can be used by a connected machine to download the patches and the patches can then be copied into the disconnected console's patch directory. A File Downloader PowerShell script is available to assist with the file download process; contact the Support group for more details.
Export selected patches to CSV	Export information about the selected patches to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program.

Keyboard Shortcuts

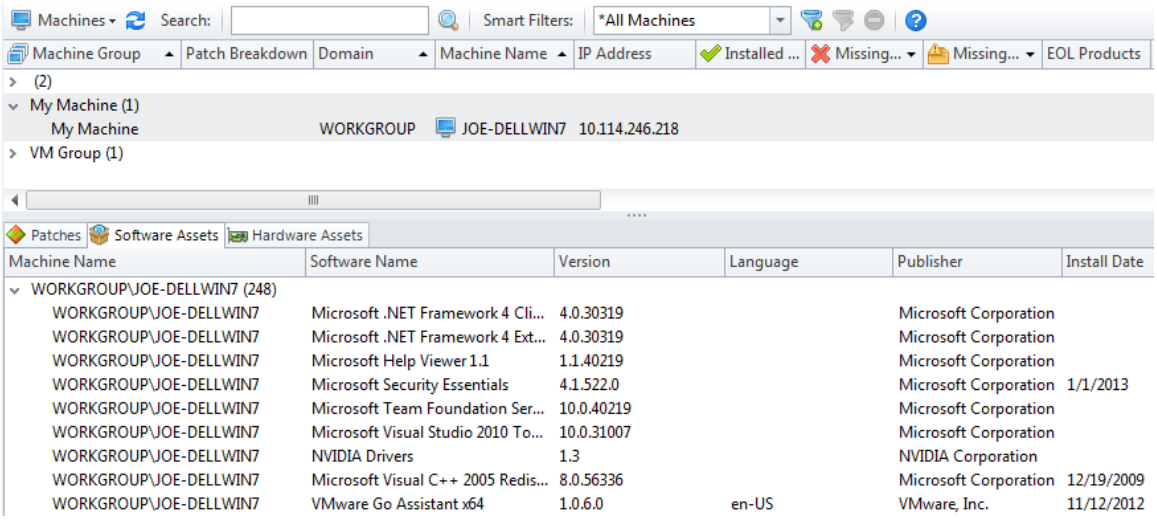
The following keyboard shortcuts are available:

- **Ctrl+A**: Selects all patches.
- **CTRL+click**: Multiple patches can be selected by holding down the CTRL key while selecting patches.
- **SHIFT+click**: A contiguous group of patches can be selected by holding down the SHIFT key while selecting the starting and ending patches in the list.
- **SHIFT+PAGE UP**: Selects a range of patches from the one currently selected to the top of the table.
- **SHIFT+PAGE DOWN**: Selects a range of patches from the one currently selected to the bottom of the table.
- **HOME:** Moves to the top of the table.
- **END**: Moves to the bottom of the table.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Software Asset Summaries

The **Software Assets** tab on the middle pane contains results from an asset scan that was performed on the machine. The tab displays information about the software contained on the machine(s) selected in the top pane. If multiple machines are selected in the top pane, this tab will display software asset information for all selected machines. For example, if you select two domains in the top pane, summary information about all the machines in both domains will be displayed.



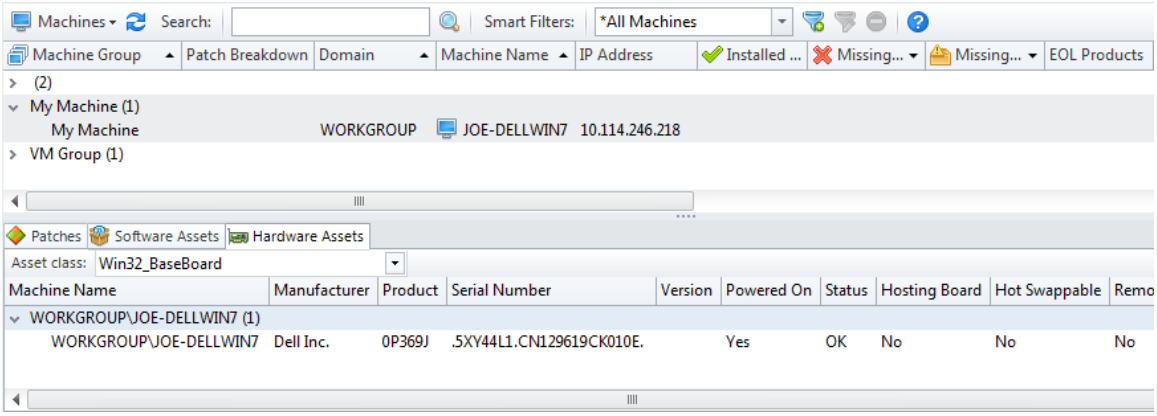
You can customize the way information is displayed within this pane. See Customizing the Column Headers for information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Hardware Asset Summaries

The **Hardware Assets** tab on the middle pane contains results from an asset scan that was performed on a physical machine or online virtual machine. The tab displays information about the hardware components contained on the machine(s) selected in the top pane. If multiple machines are selected in the top pane, this tab will display hardware asset information for all selected machines. For example, if you select two domains in the top pane, summary information about all the machines in both domains will be displayed.

Results are not available for virtual machines that were offline at the time of a scan.



The information that is displayed is dependent on the platform and on the product vendor. Not all vendors make every piece of information available so some columns may be blank. You can customize the way information is displayed within this pane. See Customizing the Column Headers for information.

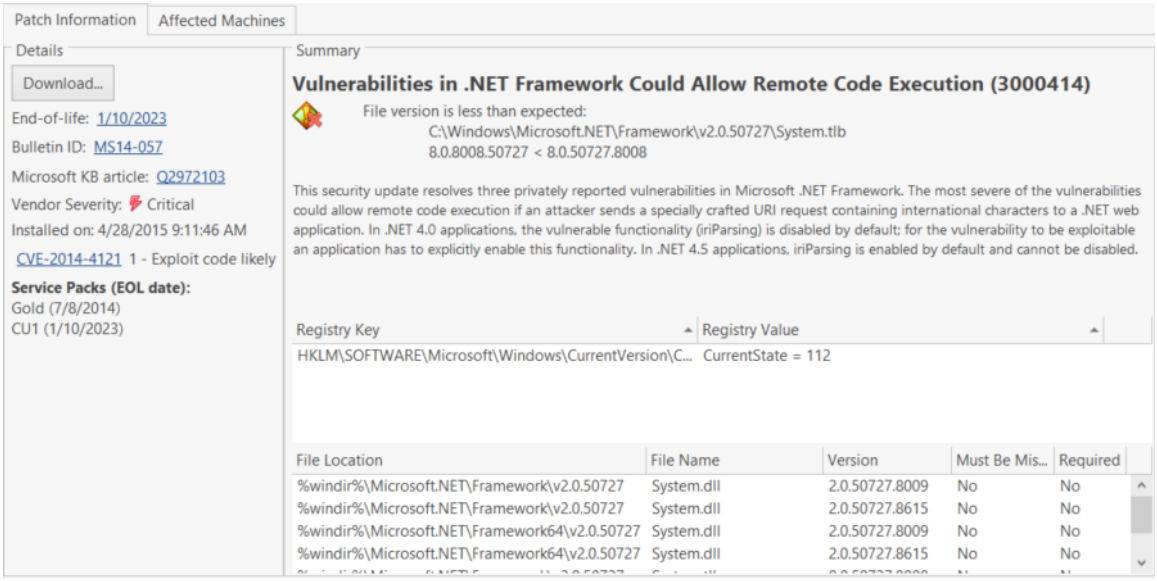
Filtering the Contents

You can use a filter to specify the type of hardware information that is displayed. The number of filters available within the **Filter by** box is dependent on the hardware components that were enabled on the asset scan template used to perform the scan.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Patch Information

The **Patch Information** tab in the bottom pane displays detailed information about the patch, service pack, or informational item selected in the middle pane. Detailed information will not be displayed if multiple patch items are selected in the middle pane.



Download	Enables you to download the patch to the patch download directory. When you click this button the **Patch Download Status** dialog is displayed. Use this dialog to select which language version of the patch you want to download. On the dialog, if the download icon is grayed out ( ) it indicates the patch has not yet been downloaded. If the icon is green ( ) it indicates the patch has already been downloaded and verified.
End-of-life	Indicates the End of Life date for the patch. You can click the link to view additional information.
Bulletin ID	Provides a link to the Microsoft Security Bulletin article that describes the threat addressed by this patch.
Replaced by	If shown, indicates that the patch is replaced by another more recent patch.
Microsoft Knowledge Base Article	Provides a link to the associated Knowledge Base article that provide more information about the flaw.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Vendor Severity	Ivanti assigns one of four severity levels based on its perceived threat of the vulnerability related to the patch.  (Red) Ivanti has deemed the problem associated with this patch to be **Critical** in nature.  (Orange) Ivanti considers the problem related to this patch **Important** to correct.  (Yellow) The related vulnerability is of **Moderate** severity.  (Brown) The related vulnerability is of **Low** severity.  (Gray) Ivanti has not assigned a severity level to this problem.
Installed on	If shown, indicates the date and time that the patch was installed on the machine.
Service Packs (EOL date)	If shown, indicates that the patch is contained in one or more service packs. Also indicates the End Of Life (EOL) date for the service pack.
Description	Identifies the product that is affected by this patch, and describes how the product is vulnerable.
Summary	Provides a concise description of the threat addressed by this patch.
Comments	If shown, provides comments from Ivanti about this patch.
Registry Key table	Identifies the registry key information used to determine whether the product in question exists on the target machines. This table can be sorted by clicking within a column header.
File Location table	Shows the file criteria used for determining whether or not a patch is installed. This table can be sorted by clicking within a column header.

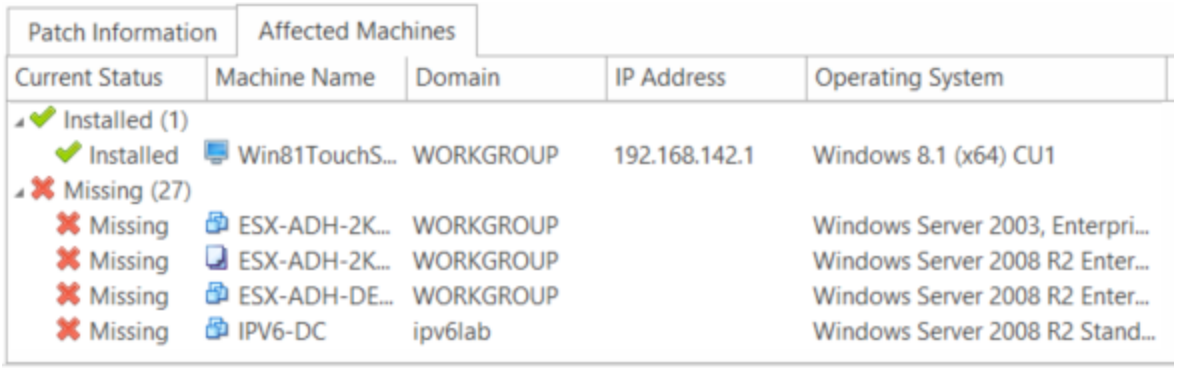
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Viewing Machines Affected by a Selected Patch

The **Affected Machines** tab in the bottom pane displays which of your selected managed machines are affected by the patch that is selected in the middle pane. The listed machines will be in one of two lists:

- **Missing:** These machines are vulnerable to the threat corrected by the patch.
- **Installed:** These machines already contain the selected patch.

Managed machines that are not listed are not affected by the selected patch.



The **Affected Machines** table can be sorted and customized. See Customizing The Patch View Column Headers for more information.

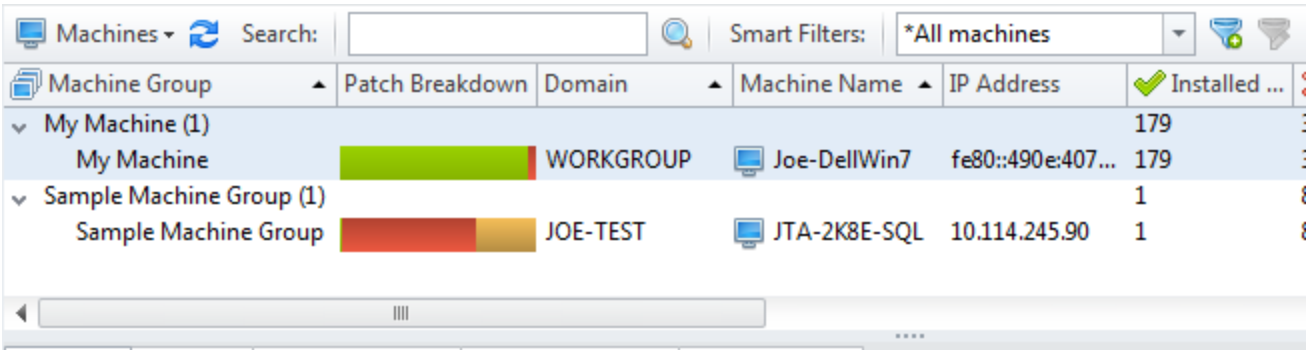
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Typical Uses of Machine View

Machine View is extremely powerful and flexible, and there are many, many uses for it. Here are just a few examples.

- "Do I have any machines that are missing a large number of patches?"

  To see if your network contains one or more machines that are "bad eggs," simply click the **Missing Patch Count** column header and sort the table in descending order. The machines that are missing the most patches are shown at the top of the table. The following figure shows a very simple example containing two scanned machines. One of the machines needs a little work (it is missing 3 patches), but the other machine needs immediate attention as it is missing 89 patches. You can immediately rectify the situation by simply right-clicking the machine and selecting **Deploy All Missing Patches**.



- "Can I compare all the machines within a machine group?"

  Yes. Simply click and drag the **Machine Group** column header to the first column. This will order the machines by machine group. Expand the machine group to view all machines within the group.

- "A recently released patch has been deemed mandatory by my organization. How do I see which machines have the patch installed and which machines are missing the patch?"

  You can do this very easily. In the top pane select the desired domain or machine group, in the middle pane select the patch, and then in the bottom pane use the **Machines Missing** and the **Machines Installed** tabs.

- "How do I know which machines have Ivanti Patch for Windows® Servers Agent installed?"

  In the heading row, click the **Agent State** column heading. This will sort the table, grouping together all machines that have Ivanti Patch for Windows® Servers Agent installed and placing that group at the top of the table. Click the icon a second time to move to the top of the table the group of machines without Ivanti Patch for Windows® Servers Agent installed. For more information, see Determining Which Machines Have Agents.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

What is Event History?

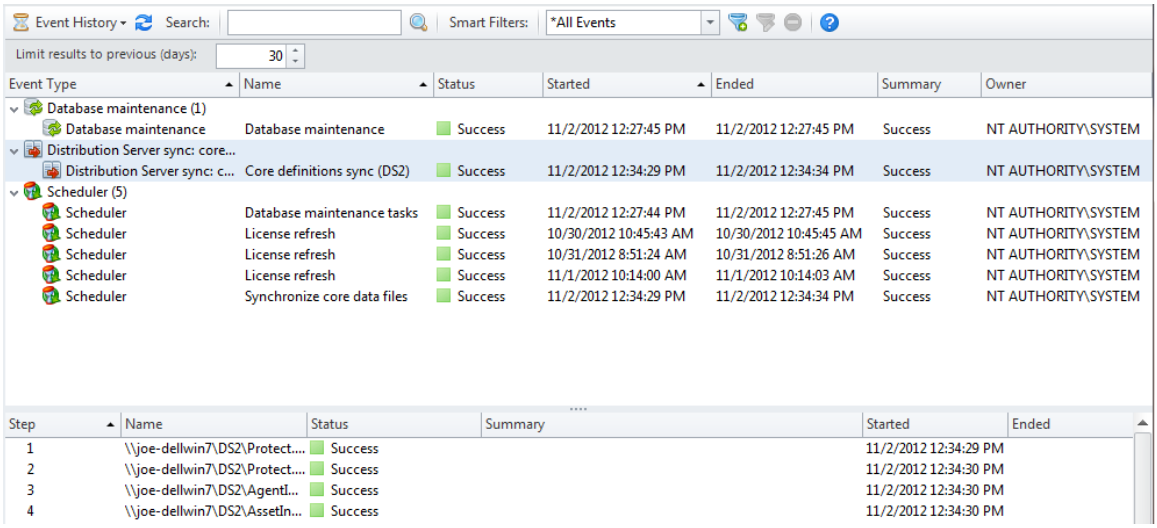
Event History is accessed from the main menu by selecting **View > Event history**. Event History provides a way to view the background operational events that occur within Ivanti Patch for Windows® Servers. Entries are generated for a large number of events, including:

- Database maintenance
- Distribution server synchronization
- Scheduler events
- Core engines/definitions downloads
- Core engines/definitions synchronization
- Predictive Patch downloads
- Operation result imports (patch scans, etc.)
- ESXi Hypervisor patch deployments
- Agent policy synchronization using Protect Cloud
- Console maintenance (a daily background task that checks the status of the certificates used by Ivanti Patch for Windows® Servers) and determines if they are nearing their expiration date

When a background event occurs, the associated log entries are automatically recorded to Event History. Events that are scheduled will not generate any log entries until after the events have been initiated or finished.

A sample Event History is shown here. You can adjust the amount of information that is displayed by using the **Limit results to previous (days)** option. By default, all background operational events that have been generated within the last 30 days will be displayed. A maximum of 10,000 events can be displayed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Event History will be empty if you view it immediately after installing the program; this is because there are no event log entries to display.

For additional information, see:

- Searching for Event Entries
- Using the Event History Smart Filter

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Searching for Event Entries

You can easily search for log entries contained in Event History. All searches are performed using the Search tool.



To initiate a search you type the term you want to find and then press **Enter** or click the search icon (). Only those event entries matching the search criteria are displayed; all other event entries are hidden.

Tips for Using the Search Tool

- The Search tool works only on the information currently visible in the pane. The **Limit results to previous (days)** option can be used to adjust the amount of information that is displayed.
- If a Smart Filter is applied, only event entries matching BOTH the search criteria and the smart filter criteria are displayed.
- All partial matches are displayed. For example, if you search for entries named *data*, any entry with "data" in its name will be considered a match (e.g. Synchronize core data files, database, etc.).
- A semicolon (;) can be used to concatenate multiple search terms into one search string. For example, specifying "maintenance;scheduler" will return all items containing either of the two terms.
- The use of wildcards in the Search tool is not allowed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Using the Event History Smart Filter

Information displayed within Event History can be easily filtered to narrow the focus to only those event entries of interest. One way to do this is by using the Smart Filter.



The Smart Filter contains several default filters. You can also define your own custom filters.

The **Limit results to previous (days) option** can be used to adjust the amount of information displayed within Event History prior to using the Smart Filter.

Default Filters

The Smart Filter contains several default filters that are identified by a leading asterisk. Default filters cannot be modified or deleted. The default filters include the following:

- ***All Operations**: All event entries are displayed.
- ***Failures:** Only those entries whose status is **Failure** are displayed.
- ***In Progress:** Only those entries whose status is **In progress** are displayed.
- ***Last 7 Days:** Only those entries that have been generated within the last 7 days are displayed.
- ***Today**: Only those entries that have been generated within the last 24 hours are displayed.

Custom Filters

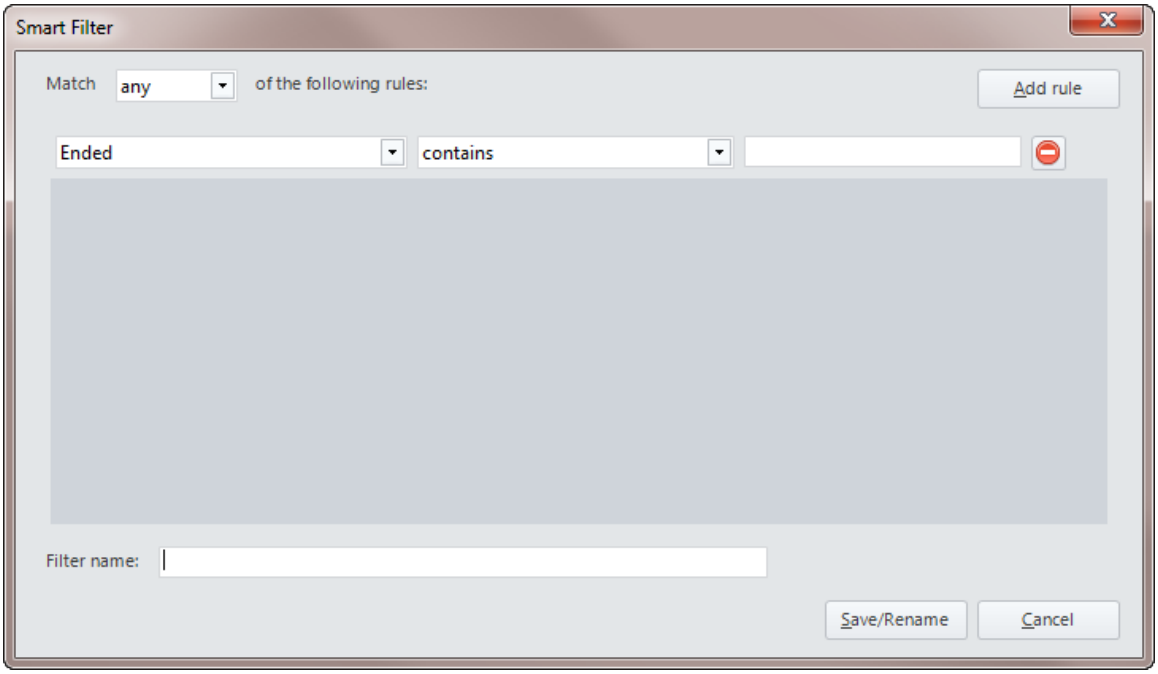
You can create your own custom filters. This is a powerful tool that enables you to specify exactly which entries you want displayed. Each custom filter is comprised of one or more rules. You can define as many rules in a filter as needed.

To create a new filter:

1. Click the New Smart Filter icon ( ).

   The **Smart Filter** dialog is displayed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



2. Specify which rules in the filter must be matched.
   - **All**: Only those entries that match all the rules in the filter will be displayed.
   - **Any**: Entries that match at least one rule in the filter will be displayed.
3. Define one or more rules.

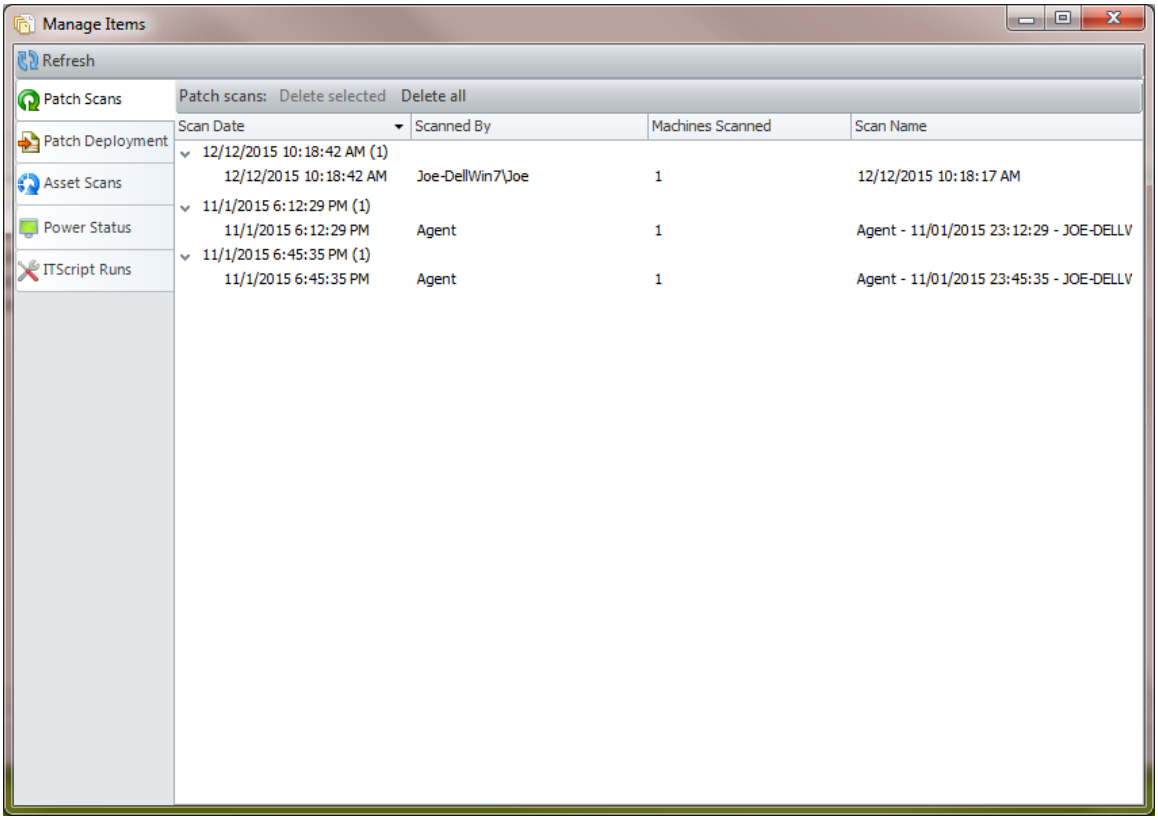
   To define a rule, select an option in each of the first two logic boxes and then type the criteria in the third box. To add another rule simply click **Add Rule**.

   If you define a rule that does not make sense (for example, "Name is greater than 3") the rule will simply be ignored.
4. Type a name for the filter.
5. When you are finished defining your custom filter, click **Save/Rename**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Manage Items

You can get a complete list of available prior scans, script executions, and patch deployments by selecting **Manage > Items**.



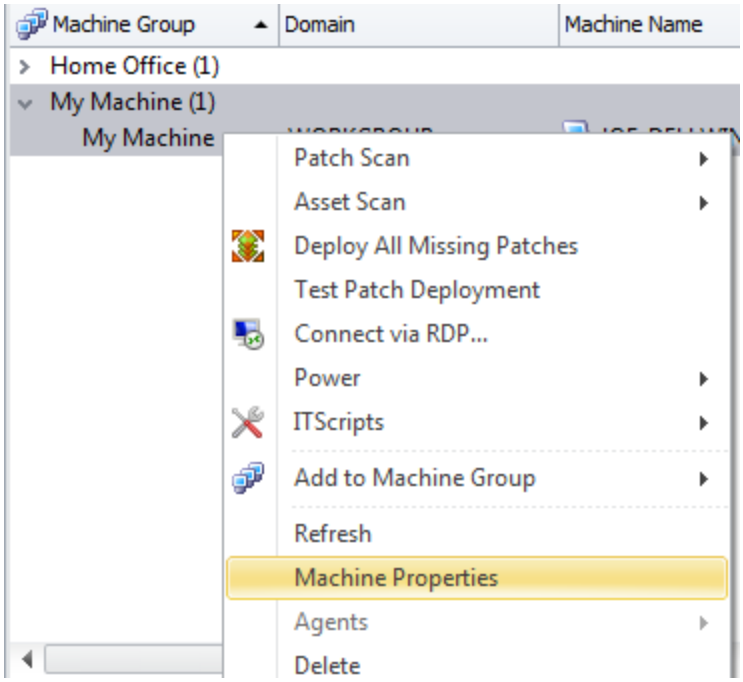
If you want to delete certain items in a list, select the desired items in the list and then click **Deleted Selected**. If you would like to remove all items in a list, click **Delete All**. Deleting an item here also deletes it from its associated list (Today's Items, Recent Items, or Archive Items) in the **Results** pane and permanently removes it from the database.

TIP: When deleting a large number of items it is smarter to use the database maintenance tool rather than **Manage Items**. The database maintenance tool will perform the task in the background and allow you to perform additional console tasks at the same time. **Manage Items** performs the task in the foreground and you must wait for the task to complete before performing additional console tasks.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Accessing Machine Properties

You can define several different properties for each machine contained in Ivanti Patch for Windows® Servers's database of managed machines. You can assign properties to individual machines or to a set of selected machines. You access the **Machine Properties** dialog from within Machine View or Scan View by right-clicking the desired machine(s) and selecting **Machine Properties**.

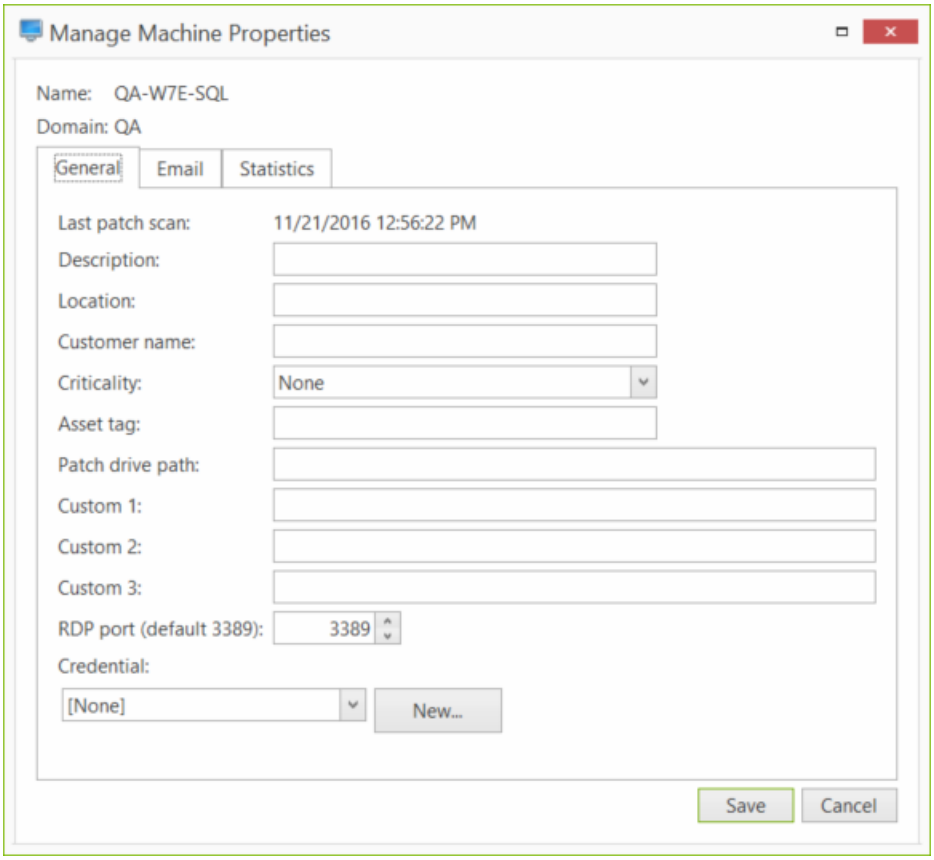


The **Machine Properties** dialog is displayed. See Managing Individual Machine Properties if you are defining properties for an individual machine or Managing Multiple Machine Properties if you are defining properties for two or more machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Managing Individual Machine Properties

The **Manage Machine Properties** dialog contains several tabs that enable you to define many different properties for an individual machine.



General tab	Enables you to define a variety of general information about the machine, including: • **Patch drive path:** Enables you to specify the drive and the path to use on the target machine when patches are downloaded during a patch deployment. Do this only if you do not want to use the default location (C:\Windows\ProPatches). For example, if the C: drive on your target machines is low on space, you might specify that the patches are instead written to the D: drive. The "ProPatches" name is automatically appended to whatever path you specify. For example, if you specify "D:\ABC," the final destination for the patches will be "D:\ABC\ProPatches."

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **Custom 1 - 3:** These three fields enable you to write custom notes about properties that are unique to this machine. For example, you might use Custom 1 to specify the machine type (laptop, desktop, server, etc.), Custom 2 to specify the machine location (St. Paul, Dallas, Seattle, etc.), and Custom 3 to specify the department that owns the machine (HR, Accounting, IT, etc.). You can use the fields to filter or sort machines within Machine View and Scan View and when scheduling reports. • **RDP port:** Defines the Remote Desktop Protocol (RDP) port to use when making a remote desktop connection with this machine. • **Credential:** Specifies the credential used when authenticating Ivanti Patch for Windows® Servers to the machine. The credential you supply here will override credentials specified in other areas of the program. If you select **None** you effectively remove the credential currently assigned to the machine. There may be several reasons for providing different credentials to a machine after a scan has been performed. If you have multiple administrators in your organization and each is responsible for a different domain, they will need to set their own credentials before performing an action. Or, your organization's policy may be to separate scan (assessment) duties from deployment duties, in which case different credentials are probably required. • **Virtual Server Credential:** Applies only to hosted virtual machines. Same as **Credential** except that you are changing the credential used to access the virtual server that is hosting the virtual machine.
Email tab	Enables you to specify which reports should be automatically sent and to whom the reports should get sent. The specified reports will be sent whenever the machine is involved in a scan or a deployment. To configure reports: 1. Select a report in the **Report** list. 2. In the **Report recipients** list, select the groups and/or individuals you want to email the report to. 3. Repeat Step 1 and Step 2 for each report you want to be automatically sent. 4. When finished, click **Save**. You can use the **Machine owner** and **Machine admin** boxes to define the owner and administrator of this machine. If you need to define a new contact or change the email address for a contact, select **Manage > Address Book**.

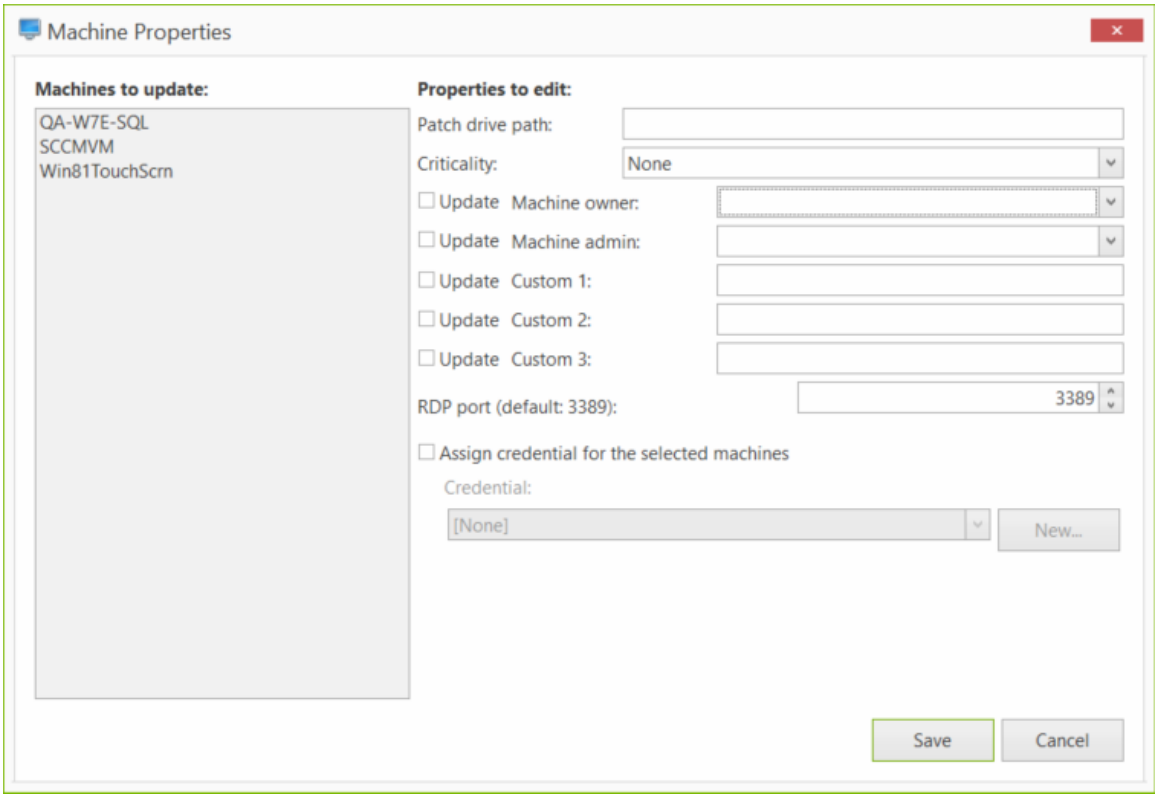
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Statistics tab	Displays a trend chart showing the number of found and missing patches detected in the last several scans. This enables you to quickly determine if the patch security state of a machine is trending up or down.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Managing Multiple Machine Properties

The **Machine Properties** dialog enables you to define several common properties for two or more machines.



Machines to update	Contains a list of the machines that will be affected by the properties you define.
Patch drive path	Enables you to specify the drive and the path to use on the target machines when patches are downloaded during a patch deployment. Do this only if you **do not** want to use the default location (C:\Windows\ProPatches). For example, if the C: drive on your target machines is low on space, you might specify that the patches are instead written to the D: drive. The "ProPatches" name is automatically appended to whatever path you specify. For example, if you specify "D:\ABC," the final destination for the patches will be "D:\ABC\ProPatches."
Criticality	Enables you to specify a custom criticality level for the listed machines. This value is something you assign and use for your own purposes. For example, if you have a set of machines that are of particular importance to your company, you can assign a criticality level to the machines and then use the filtering and sorting capabilities in Machine View to quickly locate the machines and determine their status.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	If you assign a custom criticality level, the flag displayed in the **Machine Criticality** column of Machine View will change to the appropriate color.  (Red) Critical  (Orange) High  (Yellow) Medium  (Gray) Low  (White) Ignore
Machine owner	Defines the owner of the selected machines. If you need to define a new contact or change the email address for a contact, select **Manage > Address Book**. Use the **Update** check box to specify if you want this field to be updated when you click **Save**.
Machine admin	Defines the administrator of the selected machines. If you need to define a new contact or change the email address for a contact, select **Manage > Address Book**. Use the **Update** check box to specify if you want this field to be updated when you click **Save**.
Custom 1, Custom 2 and Custom 3	**Custom 1 - 3:** These three fields enable you to write custom notes about properties that are unique to the listed machines. For example, you might use Custom 1 to specify the machine type (laptop, desktop, server, etc.), Custom 2 to specify the machine location (St. Paul, Dallas, Seattle, etc.), and Custom 3 to specify the department that owns the machine (HR, Accounting, IT, etc.). You can use the fields to filter or sort machines within Machine View and Scan View and when scheduling reports. Use the **Update** check box to specify if you want these fields to be updated when you click **Save**.
RDP Port	Defines the Remote Desktop Protocol (RDP) port to use when making a remote desktop connection with the machines.
Credential	Specifies the credential used when authenticating Ivanti Patch for Windows® Servers to the machines. The credential you supply here will override credentials specified in other areas of the program. If you select **None** you effectively remove the credential currently assigned to the machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	There may be several reasons for providing different credentials to machines after a scan has been performed. If you have multiple administrators in your organization and each is responsible for a different domain, they will need to set their own credentials before performing an action. Or, your organization's policy may be to separate scan (assessment) duties from deployment duties, in which case different credentials are probably required.
Virtual Server Credential	Applies only to hosted virtual machines. Same as **Credential** except that you are changing the credential used to access the virtual server that is hosting the virtual machine.

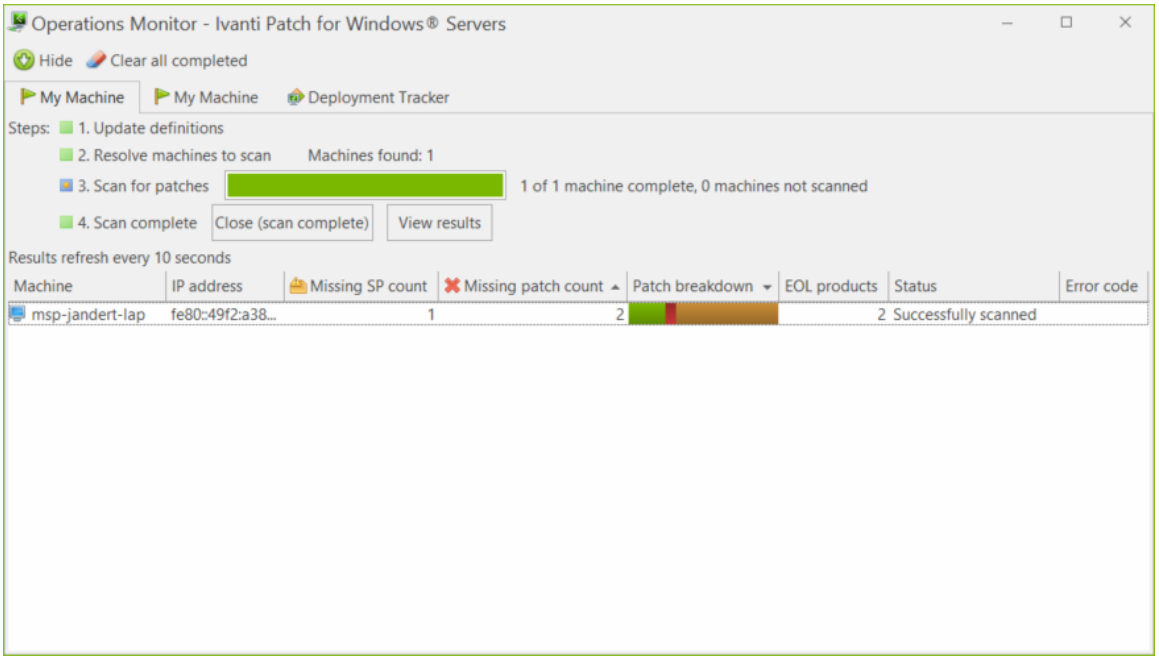
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About the Operations Monitor

The Operations Monitor is designed to give you a single console from which to monitor background tasks. The background tasks currently monitored include patch scans, patch downloads, patch deployments, ESXi Hypervisor scans and deployments, asset scans, power management tasks, agent installations and results, script executions, and test patch deployments.

The Operations Monitor is displayed automatically whenever one of these background tasks is performed. To manually access the Operations Monitor, select **View > Operations Monitor**.

You can export machine information from any of the Operations Monitor tabs by right-clicking in the machine grid and selecting **Export selected machines to CSV**. To add or remove columns in the bottom pane, right-click on a column heading and select **Column Chooser**.



Hide	Minimizes the Operations Monitor dialog.
Clear All Completed	Removes all completed tasks from all tabs.
Patch scans	Displays a unique tab for each machine group, domain, or favorite that is being scanned. The tab shows the steps involved in the patch scan and the progress of each step. See Monitoring a Patch Scan for more information.
Patch downloads tab	Displays status information about patch downloads that have been initiated from the console.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deployment Tracker tab	Monitors the status of patch deployment tasks. See About the Deployment Tracker Dialog for more information.
ESXi Hypervisor scans	Displays a unique tab for each ESXi Hypervisor scan operation. The tab shows the steps involved in the scan and the progress of each step. The results of the scan can be found on the **Bulletins** tab of your managed or unmanaged hypervisor. Remember to refresh the **Bulletins** tab to view the most current information.
ESXi Hypervisor deployments	Displays a unique tab for each ESXi Hypervisor deployment operation. The tab shows the steps involved in the deployment and the progress of each step. When the operation is complete, a summary of the deployment steps is available within the **Event History** log, which you can get to by clicking the **View deployment details** link.
Asset scans	Displays a unique tab for each machine group, domain, or favorite that is being scanned. The tab shows the steps involved in the asset scan and the progress of each step. See **Monitoring an Asset Scan** for more information.
Power Tasks	Displays status information about power management tasks that run immediately after they are initiated. For more information on power commands initiated using the Power Management function, see Monitoring a Power Task. For information about power commands initiated using the Virtual Inventory feature, see Performing Actions on Virtual Machines.
Agent Installations tab	Displays status information about agents that have been "push installed" from the console to the machines in your network.
Agent Command Results tab	Displays status information about commands that have been issued to your agents.
Script executions	Displays a unique tab for each script that is executed. The tab shows when a script is running, when it is complete, and the status of the script when it is complete (successful, error, etc.).
Test Patch Deployment tab	Ivanti Patch for Windows® Servers includes the ability to perform a test deployment for any patches that are to be deployed. This is especially useful for patch deployment that has been scheduled for a later time. Testing the deployment allows you to correct any potential problems in a deployment and make it less likely that a deployment will fail. The **Test Patch Deployment** tab displays the results of a test deployment. A test deploy returns either a pass or a fail depending on what it finds. For example, if the Workstation or Scheduling services are not started in a particular machine, Ivanti Patch for Windows® Servers cannot deploy patches to it and a test deploy will return a failing result.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About the Scheduled Console Tasks Manager

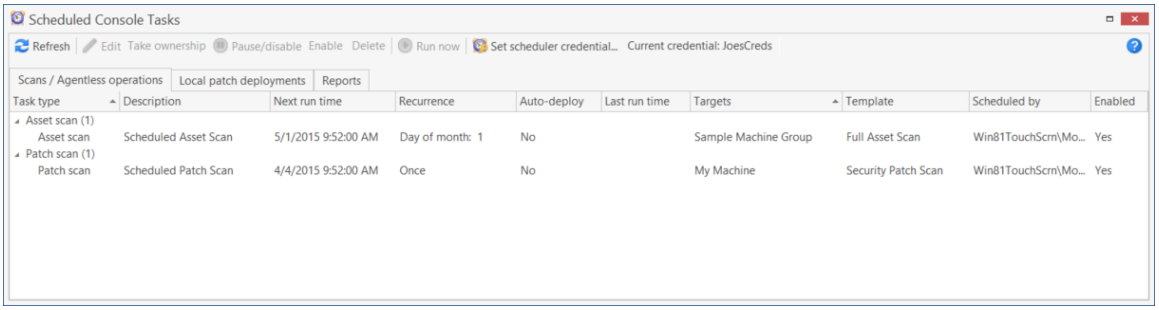
The Scheduled Console Tasks Manager is designed to give you a single location from which to monitor the tasks currently scheduled on the console. These tasks can include patch scans, asset scans, patch deployments to the console machine, patch deployments to hosted virtual machines, power tasks run against the console, script executions, and scheduled reports. The Scheduled Console Tasks Manager uses the services of the Microsoft Task Scheduler to schedule and initiate each task. If you prefer, you can view the tasks within the Microsoft Scheduler by accessing the **Task Scheduler** dialog on your Windows console machine and then expanding the **Task Schedule Library > LANDESK > Protect** tree.

To monitor scheduled tasks on your remote machines, use the Scheduled Remote Tasks Manager.

You can use the Scheduled Console Tasks Manager to modify and delete the scheduled tasks. For example, if you know a certain machine will be unavailable on a certain day you can reschedule any scans that are set to be performed on that machine.

How to Access the Scheduled Console Tasks Manager

You access the Scheduled Console Tasks Manager by selecting **Manage > Scheduled Console Tasks**.



The following commands are available using the buttons on the dialog or by right-clicking a task on any of the tabs.

Refresh	Refreshes the content in the dialog.
Edit	Edit the selected task.
Take ownership	Transfers ownership of the selected task(s) to you. For example, you may need to take ownership of one or more tasks that were originally scheduled by someone who is no longer a Ivanti Patch for Windows® Servers administrator.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	IMPORTANT! Before taking ownership, make sure you have the credentials needed to access the machines targeted by this scheduled task.
Pause/disable	Pause or temporarily disable the selected task(s). This button is only available if the selected task(s) are currently enabled.
Enable	Enable the selected task(s). This button is only available if the selected task(s) are currently disabled.
Delete	Delete the selected task(s).
Run now	Run the selected task(s) right now. The task(s) will not be deleted and will also be run at their scheduled date and time.
Set scheduler credential	Specify the credential to use for all scheduled tasks. In order to succeed the scheduler credential must match the credential of the person logged on to the console when the schedule process is initiated. If you have more than one administrator, each administrator should set their own unique scheduler credential. If you delete the credential that is designated as the scheduler credential, the next time you schedule a console task you will be prompted to assign a new scheduler credential.
Current credential	Identifies which credential is currently being used as the scheduler credential.
Scans / Agentless operations tab	Displays tasks that are scheduled on the console and performed on your target machines. This includes all scheduled patch scans, asset scans, script operations runs, Wake-on-LAN requests, patch deployments to offline hosted virtual machines and virtual machine templates, etc.
Local patch deployments tab	Displays all patches that are scheduled to be deployed to the local (console) machine. Power tasks that will run against the console will also be displayed here.
Reports tab	Displays all reports scheduled to be generated.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About the Scheduled Remote Tasks Manager

The Scheduled Remote Tasks Manager is designed to monitor the power tasks and patch deployment tasks currently scheduled on a remote target machine. You can use it to modify and delete the scheduled tasks. For example, if you know a certain machine will be unavailable on a certain day you can reschedule any tasks that are set to be performed on that machine.

The Scheduled Remote Tasks Manager uses the services of either the IvantiScriptLogic Scheduler or the Microsoft Task Scheduler 2.0 or later to display and manage the scheduled tasks on a target machine. Only those tasks performed by the IvantiScriptLogic Scheduler, however, will be recorded in the log. If the IvantiScriptLogic Scheduler is configured to be the preferred scheduler but it is not available on a target machine when the Scheduled Remote Tasks Manager is launched, you will be prompted to manually install the IvantiScriptLogic Scheduler.



The Scheduled Remote Tasks Manager is different than Deployment Tracker. The Scheduled Remote Tasks Manager enables you to monitor and modify*scheduled* power andpatch deployment tasks, while Deployment Trackeronly enables you to monitor*active*deployment tasks (and not power tasks).

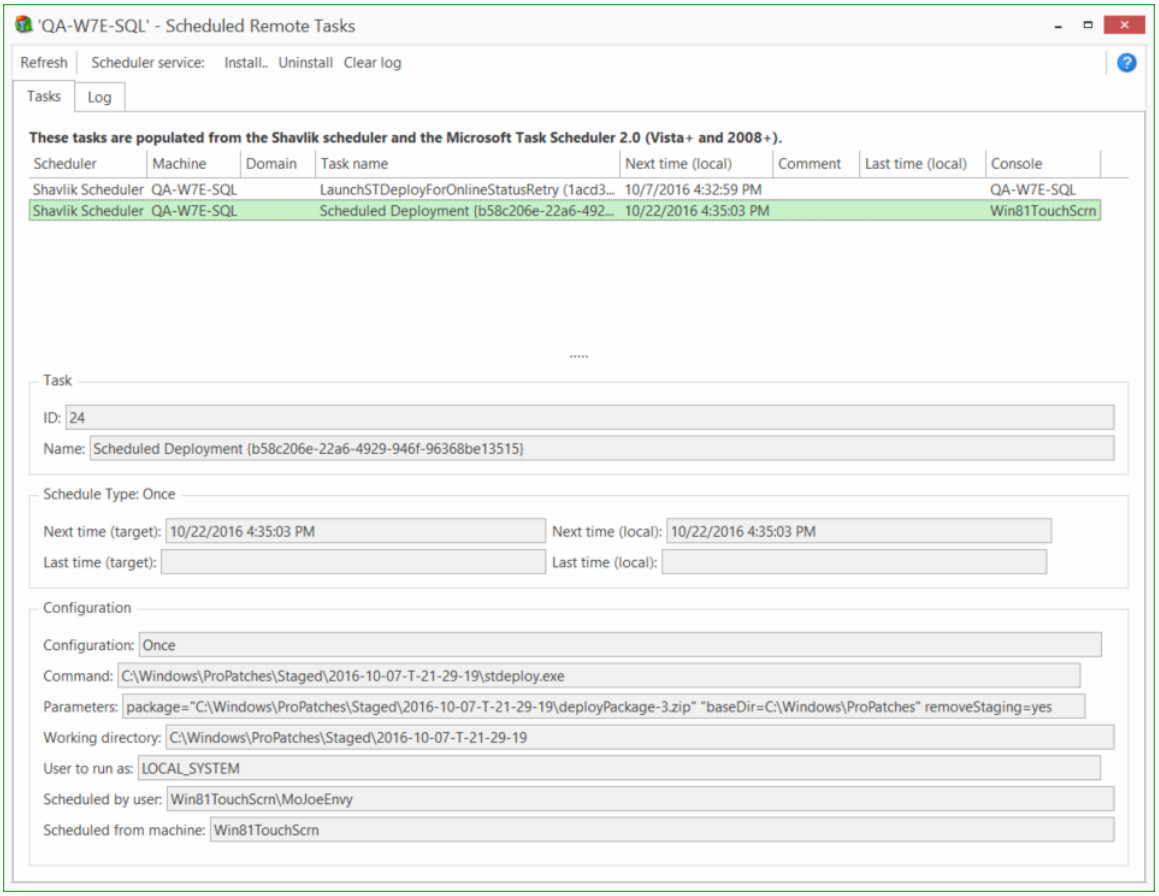
How to Access the Scheduled Remote Tasks Manager

You access the Scheduled Remote Tasks Manager from Machine View or Scan View by right-clicking on a machine and then selecting **View scheduled tasks**. Multiple instances of the Scheduled Remote Tasks Manager can be active at the same time.



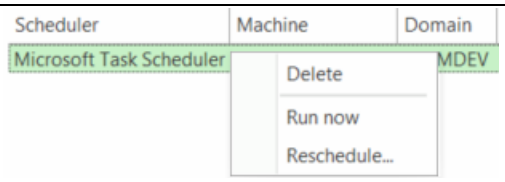
If you are experiencing problems using the Scheduled Remote Tasks Manager to communicate with a machine, it could be you need to install the latest version of the IvantiScriptLogic Scheduler on the machine.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



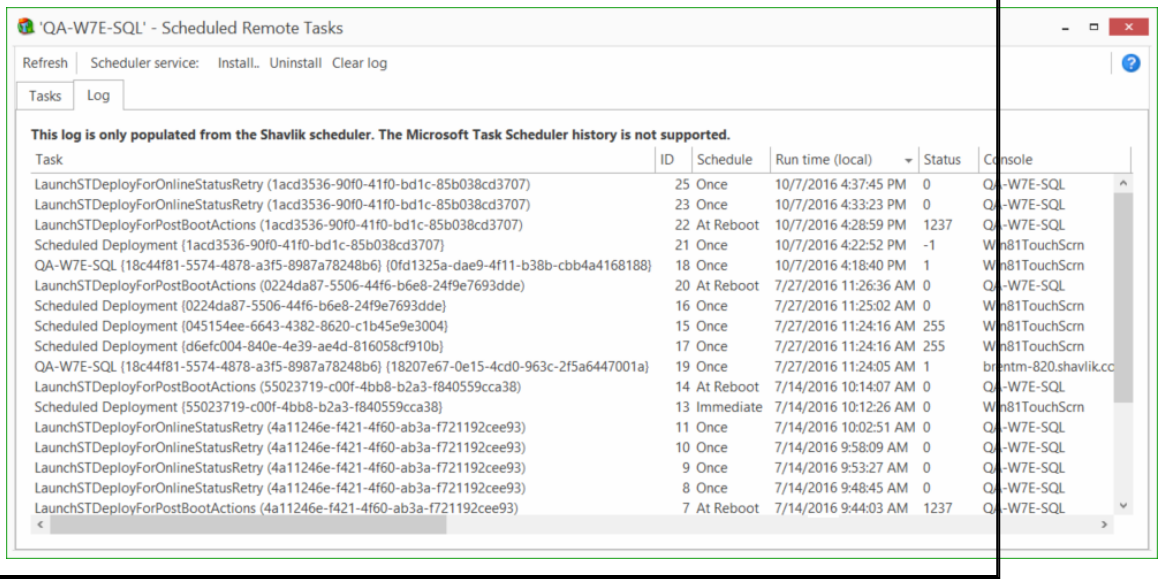
Refresh	Refreshes the information displayed in the dialog.
Install	Installs the IvantiScriptLogic Scheduler on the machine.
Uninstall	Removes the IvantiScriptLogic Scheduler from the machine.
Clear log	Clears all information contained in the log.
Tasks tab	The **Tasks** tab contains a table that displays the tasks (if any) that are currently scheduled for the selected machine. If you select a task, details about that task are displayed in the lower pane. You can sort this table a number of different ways simply by clicking the individual column headers. You can also perform a number of actions by right-clicking on a task.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Log tab

The **Log** tab contains a table that displays the available log files for the selected machine, providing a history of the jobs that have been performed on the machine. You can sort this table a number of different ways simply by clicking on an individual column header. Only tasks performed by the IvantiScriptLogic Scheduler will be recorded in the log.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

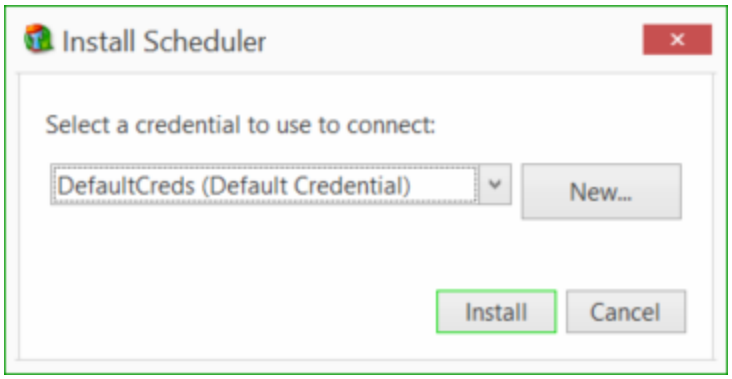
Manually Installing and Uninstalling the IvantiScriptLogic Scheduler

If the IvantiScriptLogic Scheduler is configured to be the preferred scheduler for Ivanti Patch for Windows® Servers (see Scheduling Options), it will be automatically installed on each machine during patch scans, asset scans, and patch deployments. You also have the option to manually install the IvantiScriptLogic Scheduler from within the Scheduled Remote Tasks Manager.

You can manually verify if the IvantiScriptLogic Scheduler is installed on an individual machine by selecting **Administrative Tools > Services** and looking for the **ST Remote Scheduler Service**.

1. On the **Scheduled Remote Tasks** dialog, click **Install**.

   The **Install Scheduler** dialog is displayed.



2. Select a credential that has administrative privileges on the machine.
3. Click **Install**.

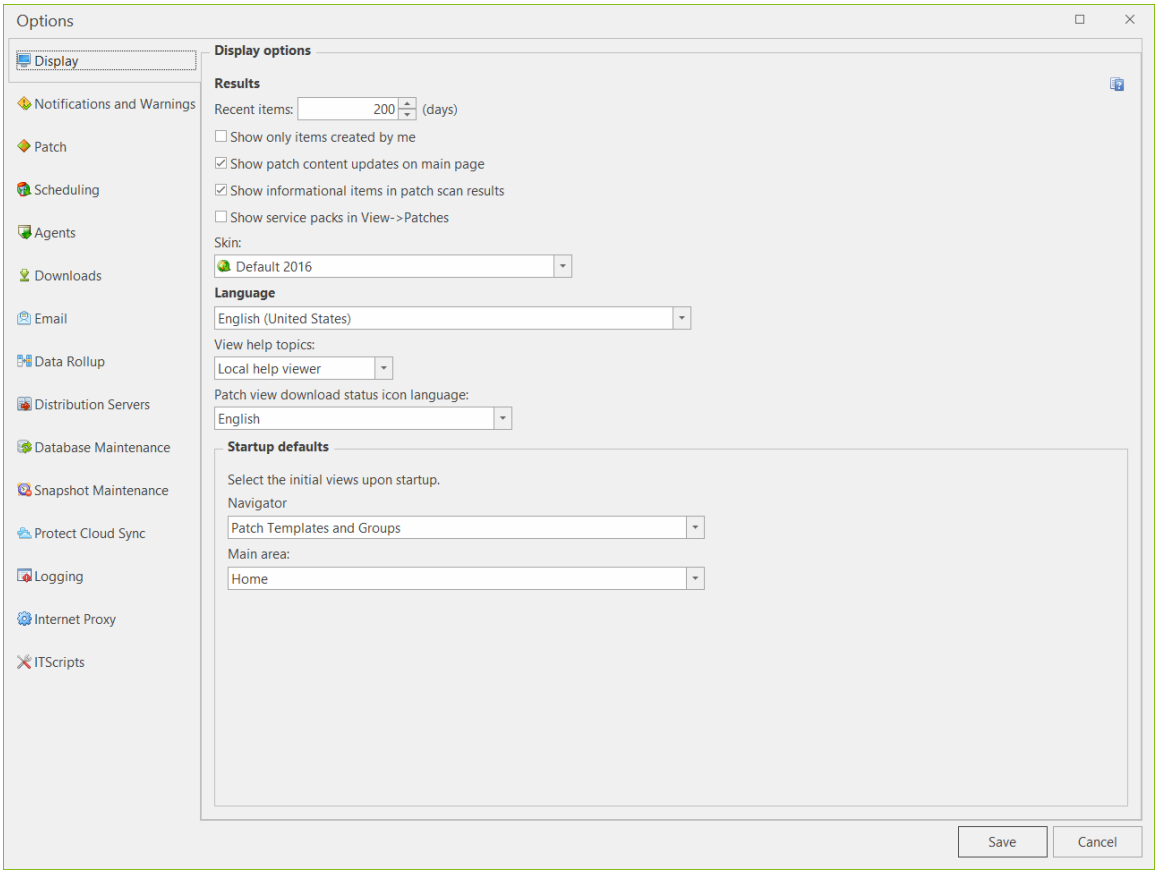
To manually uninstall the IvantiScriptLogic Scheduler from a target machine, click **Uninstall** from the **Scheduled Remote Tasks** dialog.

Configuration Options Overview

You can configure a number of different options within Ivanti Patch for Windows® Servers. For example, you can define the physical appearance of the program, you can define what notification messages you will see, etc.

The configuration options are all available from the **Tools > Options** menu, which will cause the **Options** dialog to appear.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

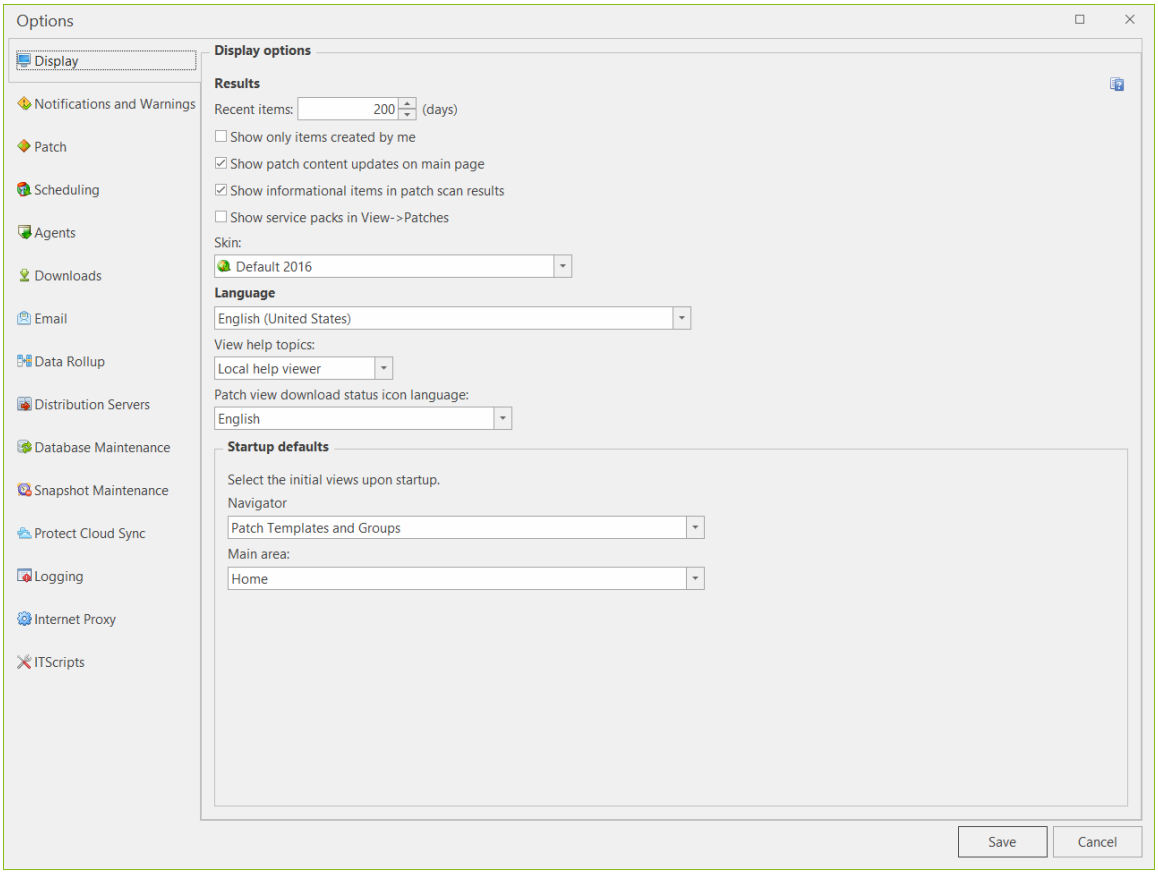


To configure an option category, simply select the appropriate tab in the left-hand pane and then configure the related options that appear in the right-hand pane. Each option category is described in detail in the remainder of this section.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Display Options

The **Display Options** dialog allows you to specify the optional items you want displayed in the program.



Recent Items	Specifies how many days' worth of scans and deployments to show in the **Results** list in the navigation pane. It also defines how many days' worth of recent patch deployments to show in Deployment Tracker. The default value is 200 days.
Show only items created by me	If enabled, shows only those scans and templates that have been created by the current user.
Show patch content updates on main page	If enabled, displays the date that the patch content was last updated. The date is displayed in the upper-right corner of the interface. If you click the date the **Patch Content Update Details** dialog is displayed. Use this dialog to view more detailed information about the current patch data and about previous patch data releases. For more information, see Navigating the Interface.

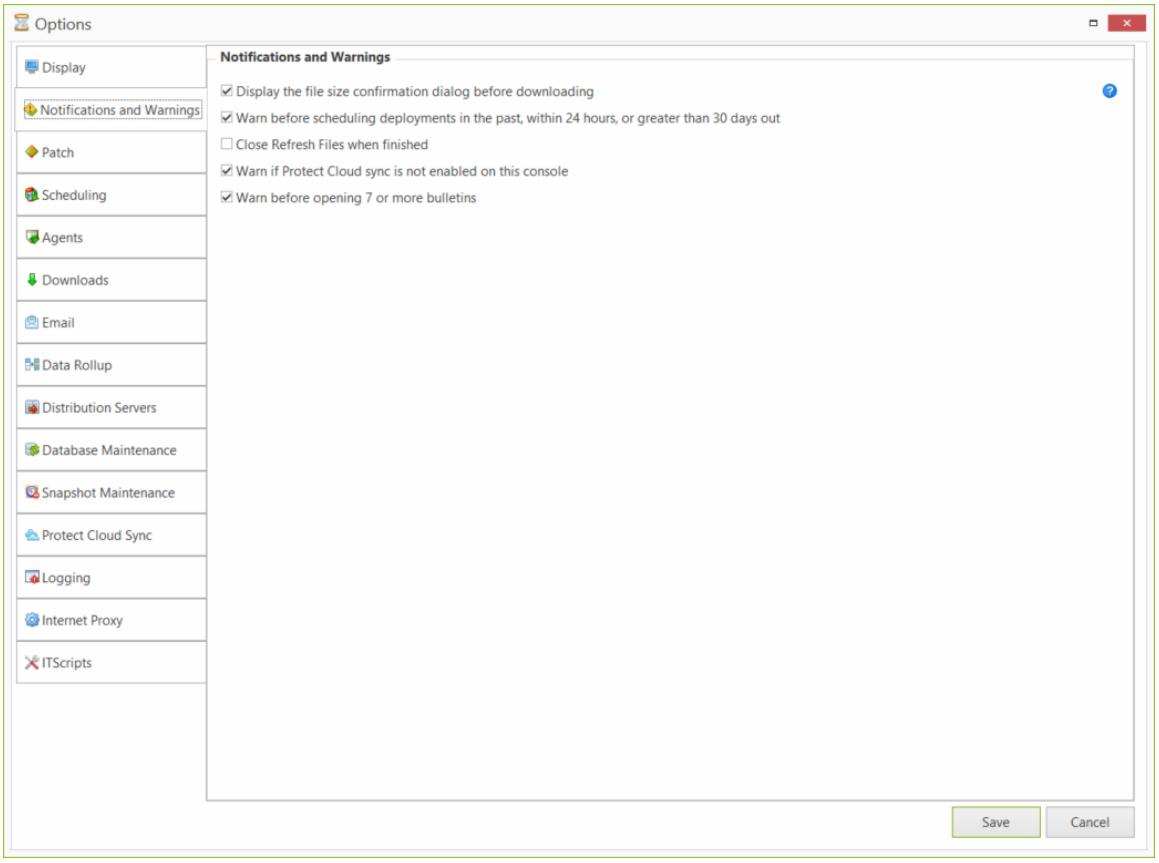
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Show informational items in patch scan results	If enabled, displays informational items on the **Patches** tab in Scan View and Machine View.
Show service packs in View > Patches	If enabled, displays service packs in Patch View. Service packs are by default filtered out from the content displayed in Patch View. This is because service packs are typically not needed in this view; they cannot be added to patch groups and you cannot view detailed information about service packs like you can for patches. The most common reason to display service packs in Patch View is so you can download them in advance of a deployment.
Skin	Specifies the color theme you want to use for the Ivanti Patch for Windows® Servers interface. If you make a change, the new skin is temporarily applied to the interface so that you can determine if you like it. To make the change permanent, click **Save**; to revert to the original selection, click **Cancel**.
Language	Specifies the language that will be used within the Ivanti Patch for Windows® Servers interface.
View help topics	Specifies how to view Ivanti Patch for Windows® Servers help topics. • **On the web:** The help topics will be displayed using a web browser. The help text will be localized according to the language specified in the **Language** box. This option requires an Internet connection to the console. • **Local help viewer:** The help topics will be displayed locally on the console using a .chm file. The help text will be in English.
Patch View download status indicator language	Click the drop-down list and select the language that will be represented by the download status indicator located in the top pane of Patch View. If you select the **Universal Installer** option, it represents the universal patch package file that can be used by all languages. For example, assume you select German in this field. If you then go to Patch View and the download status indicator for a particular patch looks like this  (colored) it means the German language version of the patch has been downloaded. If the download status indicator looks like this  (clear), however, it means the German language version of the patch has **not** been downloaded. If the universal installer icon is shown it means that only universal patches are available for the product. For more information, see How to Download Different Language Versions of a Patch.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Notifications and Warnings Options

The **Notifications and Warnings** dialog allows you to specify when you want Ivanti Patch for Windows® Servers to inform you about potential operational issues.



Display the file size confirmation dialog before downloading	Specify if you want the program to inform you of the file size of the patch before it is downloaded. You may want to enable this option if you have a low-speed Internet connection and you want the ability to cancel the download of particularly large files.
Warn before scheduling deployments in the past, within 24 hours, or greater than 30 days out	If enabled, will cause a warning dialog to be displayed anytime you attempt to schedule a patch deployment to run within in the past, within the next 24 hours, or more than 30 days out. The dialog is a reminder that the deployment may run immediately depending on the time zone of the target machine(s).

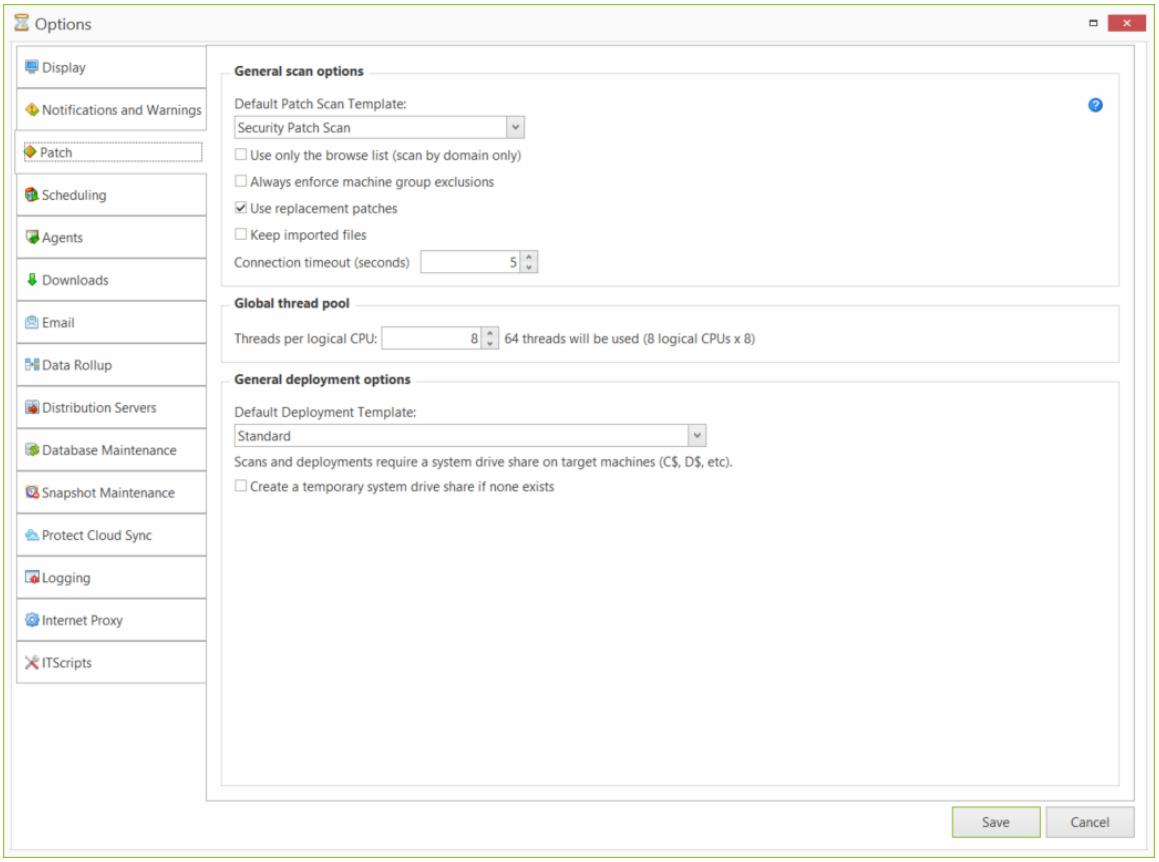
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Close Refresh Files when finished	If enabled, whenever files are automatically refreshed within the program, the refresh dialog will close automatically. This affects the **Help > Refresh files** command and the **Import ITScripts** dialog that is displayed whenever you select **Manage > ITScripts**.
Warn if Protect Cloud sync is not enabled on this console	If you are using multiple Ivanti Patch for Windows® Servers consoles, and if one of your consoles is using Protect Cloud sync and another is not, enabling this check box will notify you of this situation. This is especially important if two or more consoles are sharing the same database. Each console that uses a Protect Cloud sync-enabled policy must be registered with Protect Cloud.
Warn before opening 7 or more bulletins	If enabled, will cause a warning dialog to be displayed anytime you select seven or more patches and then use the right-click menu to **Open Bulletin(s) in Browser**. Opening many vendor bulletins at once may be a slow process and can degrade the performance of your machine.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Patch Options

The **Patch Options** dialog allows you to specify patch scanning and deployment options.



Default Patch Scan Template	The scan template you wish to set as the default when performing patch scans.
Use only the browse list (scan by domain only)	When scanning domains, the machines scanned are those contained in the "browse list" of machines in your Microsoft network rather than all the machines in the domain as specified by the domain controller. Using this option will typically reduce the number of machines that the program will attempt to connect to when performing the scan. For more information, see Enumerating Machines.
Always enforce machine group exclusions	When using multiple machine groups in a scan operation, if a machine is excluded from one machine group but is included in another, the machine will be excluded from the operation. If the **Always enforce machine group exclusions** check box is not enabled, for this same situation the machine will be included in the operation. **Examples:**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• On the home page you select two machine groups that you want to scan. MachineA is excluded from one group but is included in the other group. If the **Always enforce machine group exclusions** check box is enabled, MachineA will not be included in the scan. If the **Always enforce machine group exclusions** check box is not enabled, MachineA will be included in the scan. • You scan a nested group that consists of two groups. In one of the groups the domain ABC.com is excluded, while the other group contains three machines from the ABC.com domain. If the **Always enforce machine group exclusions** check box is enabled, the three machines will not be included in the scan. If the **Always enforce machine group exclusions** check box is not enabled, the three machines will be included in the scan.
Use replacement patches	Instructs Ivanti Patch for Windows® Servers to only scan for patches that are not replaced, ignoring patches that have been replaced by other patches. For example, instead of reporting on all missing Internet Explorer patches, only the latest and most current IE patches will be reported.
Keep imported files	The results files used by a scan operation are stored on disk indefinitely rather than being deleted after the results are imported into the program.
Connection timeout (seconds)	The maximum amount of time to wait for a target machine to respond to the console during a scan. If the console cannot make a connection to the target machine in the specified number of seconds the machine is skipped. A connection attempt may timeout earlier than the specified value, this simply puts a maximum value on the wait time.
Global thread pool	Specifies the total number of threads that can be used during a patch scan or deployment, an asset scan or a power status scan. The value you specify will be multiplied by the number of logical CPUs on the console machine to determine the maximum number of threads that may be used during a scan instance. One thread will be used to scan one machine, so if you specify a maximum of 64 threads it means that 64 machines can be simultaneously scanned during one scan. Allowing many machines to be scanned at the same time requires more network resources. Reduce this number if you are scanning over a slow link.
Default Deployment Template	Specifies the deployment template to use as the default. Any new deployment templates you previously defined will be included in the drop-down list. For more information see About Deployment Templates.

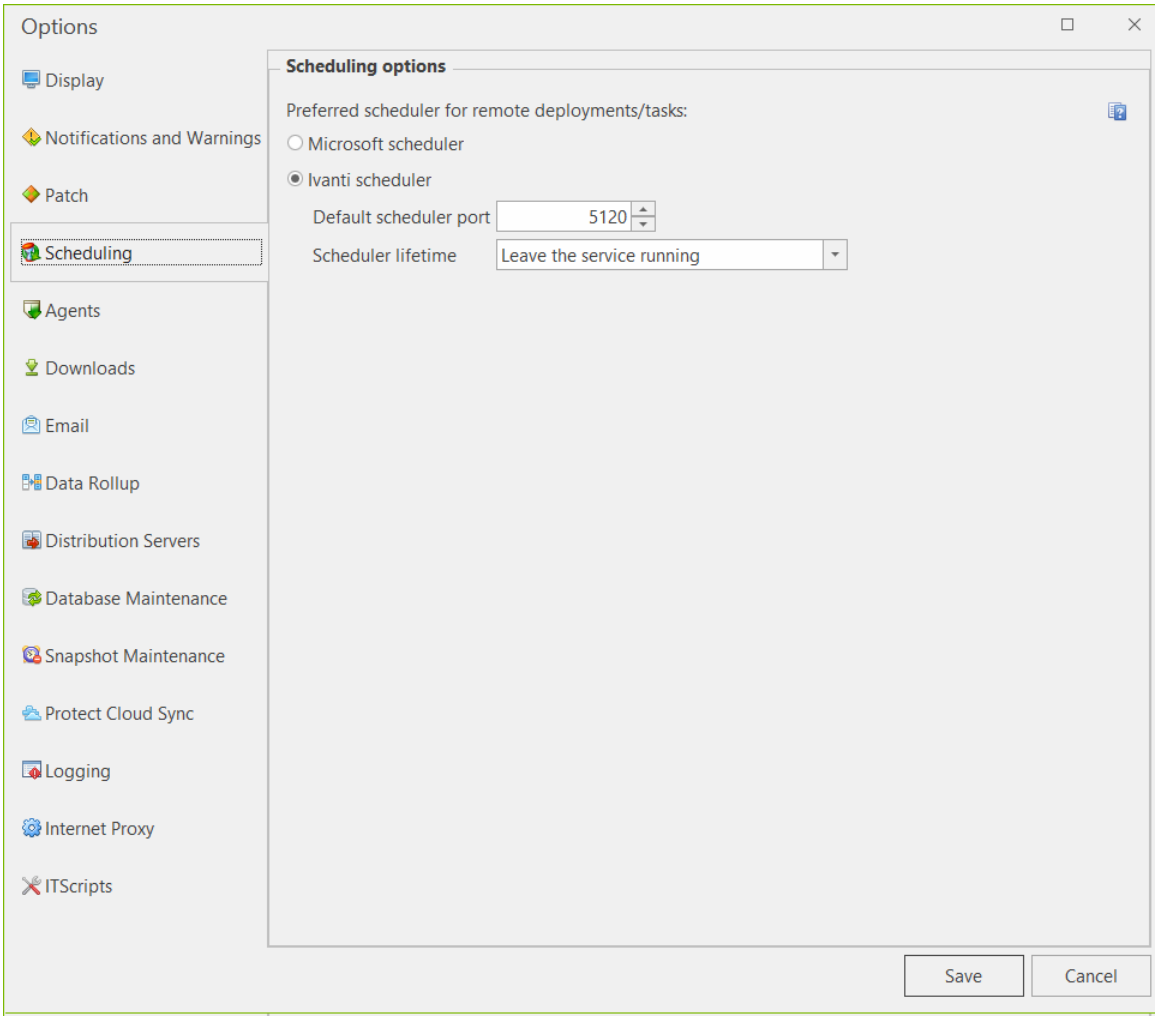
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Create a temporary system drive share if none exists	Enables Ivanti Patch for Windows® Servers to create and use a temporary administrator share name on a target machine during the authentication process. The share name will be removed from the target machine when the scan or deployment is complete. While this option does not apply to most organizations, if you are an organization that for whatever reason has disabled or renamed the administrator share names (C$, D$, etc.) on your target machines, then you must enable this check box in order for Ivanti Patch for Windows® Servers to access those machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Scheduling Options

The **Scheduling Options** dialog enables you to specify which scheduler service you prefer to use on each remote machine when performing power state and patch deployment tasks. The scheduler is used to initiate the tasks at the specified time, whether immediately or at some specified time.



Microsoft Scheduler	Use the Microsoft Scheduler service in those circumstances where it provides the needed functionality.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

IvantiScriptLogic Scheduler	The IvantiScriptLogic Scheduler service is faster and more secure than the Microsoft Scheduler service. A copy of the IvantiScriptLogic Scheduler service is pushed to each target machine where it is used to initiate the tasks. With the IvantiScriptLogic Scheduler service you can specify what should happen to the service after it is finished performing its tasks. You can install the IvantiScriptLogic Scheduler to individual machines using the Scheduled Remote Tasks Manager. The IvantiScriptLogic Scheduler is the default scheduler service. If the IvantiScriptLogic Scheduler should for some reason fail or be unavailable, the Microsoft Scheduler will be automatically invoked.
Default Scheduler Port	Specifies the port used by IvantiScriptLogic Scheduler service. By default the IvantiScriptLogic Scheduler service listens on TCP port 5120. If desired, you can override this global default on a machine-by-machine basis (see Managing Individual Machine Properties).
Scheduler Lifetime	This specifies what to do with the IvantiScriptLogic Scheduler service after it completes its tasks on the target machine. • **Leave the service running**: Leaves the service running so it is instantly available for future scans or deployments. • **Stop the service and leave it installed in service control manager**: Stops the service and leaves it installed in service control manager. This doesn't use CPU time on the target machine but it keeps the service available for future use. • **Stop the service and remove it from service control manager:** Stops the service and removes it from service control manager. Certain files are left on the system for easy reuse.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Agents Options

The **Agents Options** dialog allows you to specify how agents that are manually installed will authenticate themselves to the console during the registration process. The options are:

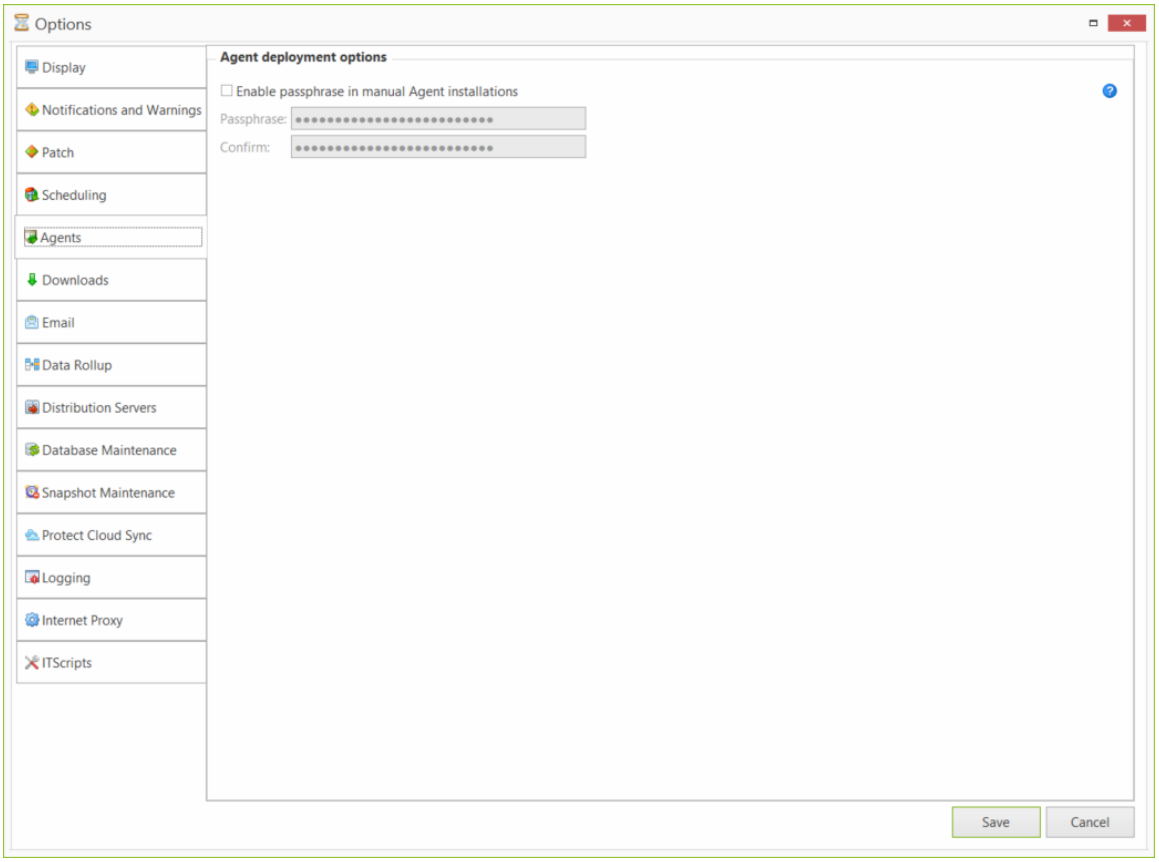
- **Passphrase authentication**: If the **Enable passphrase in manual Agent installations** check box is enabled, users will be required to specify a matching passphrase during the manual agent installation process. Passphrase authentication is best used when individuals without administrative credentials will be manually installing agents. For example, in large organizations it may not be feasible for one administrator to manually install agents on hundreds of different machines. Specifying a passphrase allows individuals to install agents on their own machines without the need for console credentials.
- **Windows authentication**: This will be used if the **Enable passphrase in manual Agent installations** check box is **not** enabled. Credentials with administrator rights on the Ivanti Patch for Windows® Servers console will be required when manually installing an agent on a machine.



CAUTION! Be careful when using Windows authentication. If the machine on which you are installing the agent is already infected with malware that is capable of capturing passwords, your credentials could be compromised. For this reason, passphrase authentication is the recommended option.

In some cases it may make sense to use a combination of methods. You might use passphrase authentication to initially install the bulk of your agents and then switch to Windows authentication for all future manual installations.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

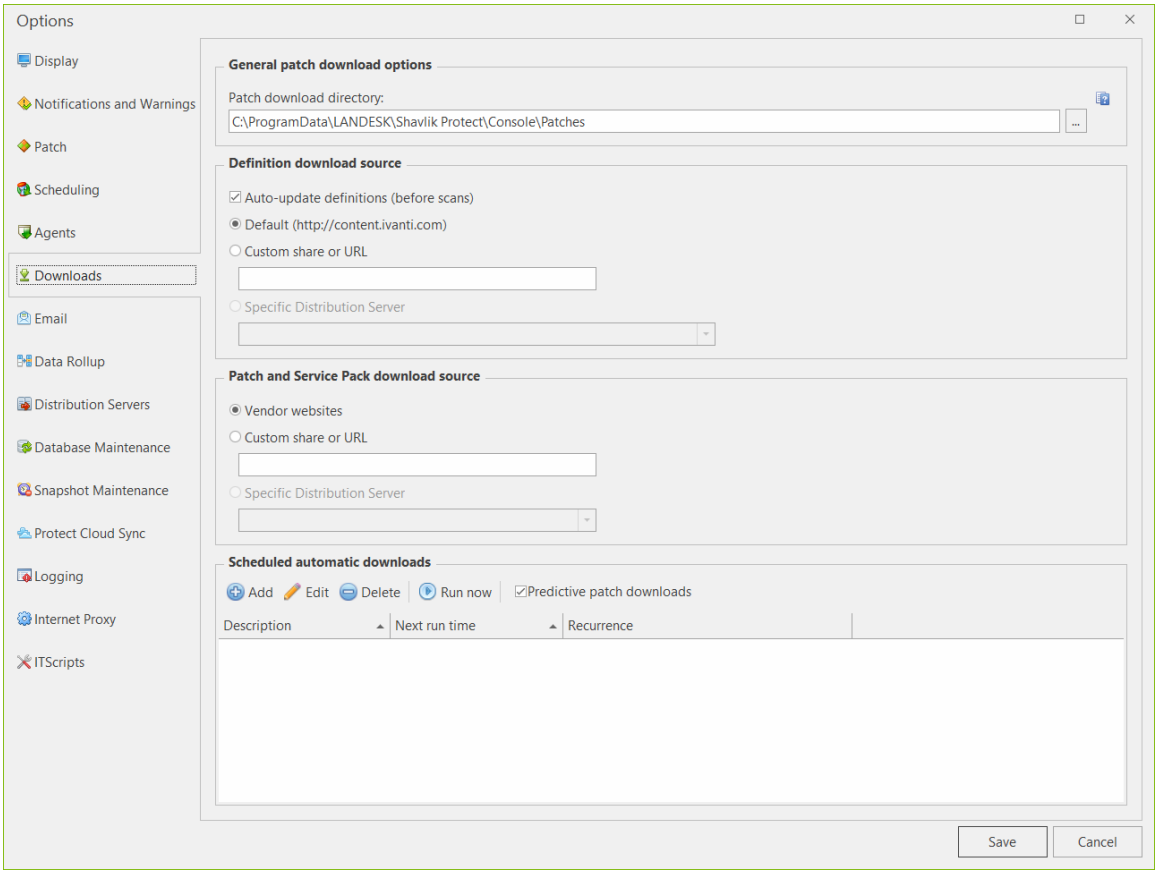


Enable passphrase in manual Agent installations	• If enabled, indicates that a passphrase will be used to authenticate to the console when manually installing an agent. • If not enabled, indicates that Windows authentication will be used when manually installing an agent.
Passphrase	If the **Enable passphrase in manual Agent installations** check box is enabled, type the passphrase you want users to use during the manual agent installation process. The passphrase can be any number of words or characters and is case-sensitive.
Confirm	Retype the same passphrase in this box to confirm the passphrase.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Download Options

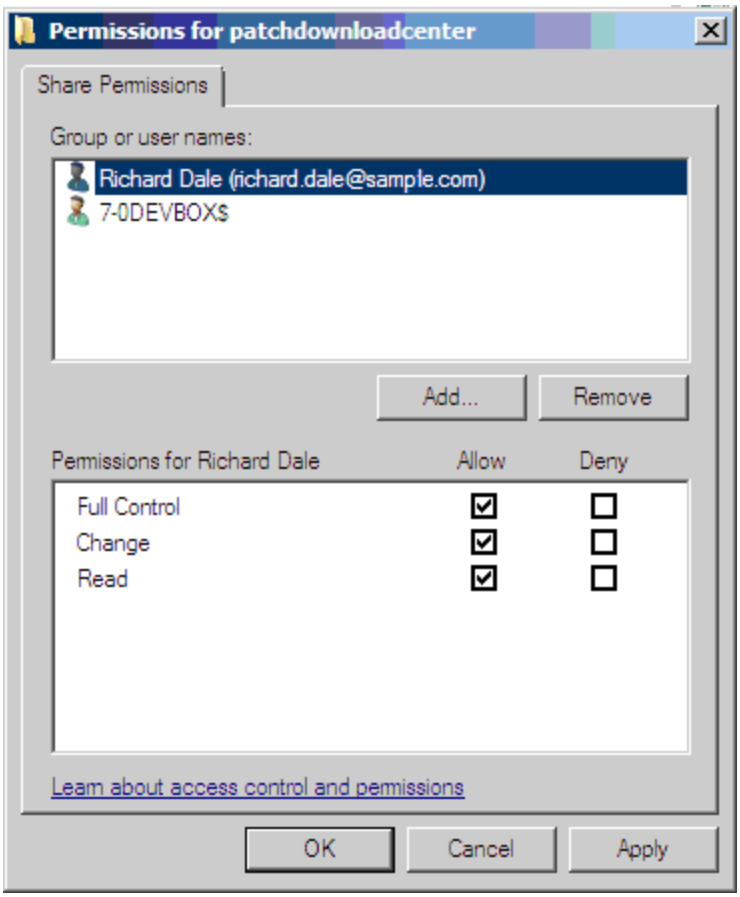
The **Downloads** tab allows you to specify the location from which the files used by the program will be downloaded and refreshed. The files include the scan engines, the news file displayed on the home page, and the deployment information file, as well as download source for the patch and service pack files. The program will check an Internet location or the specified distribution server to determine if newer versions of the files are available.



Patch download directory	Displays the location of the patch download directory. This directory is used to store all patches that are downloaded in advance of a patch deployment. To change the location, click the browse button. IMPORTANT! If the directory resides on a network drive be sure to use the UNC naming convention; DO NOT SPECIFY A MAPPED DRIVE. **Using a Remote UNC Share Directory**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

If desired, you can specify a remote share directory for the patch download directory. In order for this to work, appropriate permissions need to be set on the remote directory. Both the Ivanti Patch for Windows® Servers console user and the console machine need to be granted access to the download directory. The console user should have read/write permission to the share and the console machine needs read access. When specifying share permissions for a machine, you must append a "$" to the end of the machine name.



In some configurations additional users may need to be granted access to the download directory. If you specify machine or machine group credentials for machines that download patches from a distribution server, the specified user accounts will require read access to the download directory share.

Making the download directory share readable by everyone may or may not be an effective strategy. It depends on:

- Whether the credential users and the download directory host belong to the same (or trusted) domain(s)
- The specifics of the local security policy

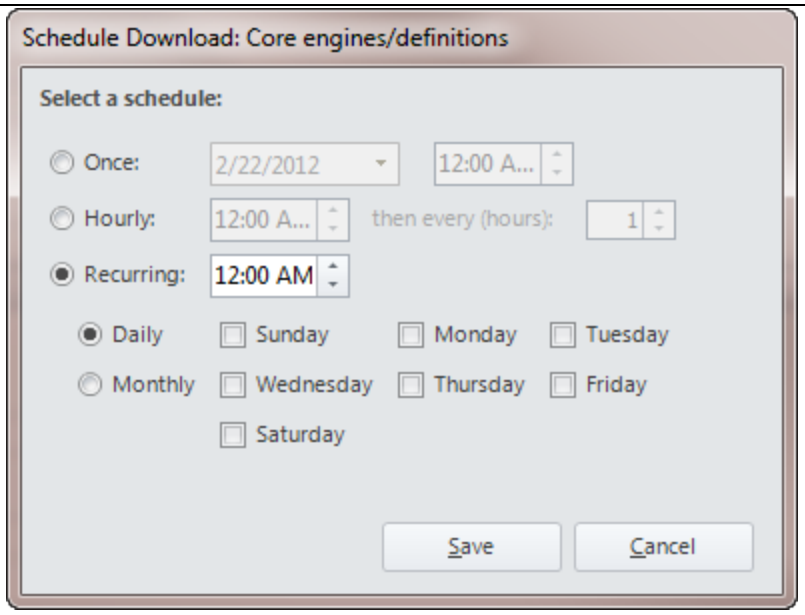
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Definition download source	You can specify where the latest scan engines and data files downloaded by this console are located. The available options are: • **Auto-update definitions (before scans)**: If enabled, will cause the program to automatically check for and download updated data definition files whenever a new scan is performed. Enabling this check box will also enable the **Tools > Auto-update definitions** menu command. • **Default (http://content.ivanti.com)**: Indicates you want to use the default location when downloading the files. The files are located at http://content.ivanti.com. • **Custom share or URL**: You must specify the path name of the share or the URL of the website that will be used when downloading files. It is the administrator's responsibility to make the files available at this location. • **Specific Distribution Server**: You must select the name of the distribution server that will be used when downloading files. You must have previously configured one or more distribution servers in order for the names to be pre-populated in this box. The newest versions of engines and data files can be periodically downloaded and copied to the distribution servers using the server synchronization feature. There are unique credential requirements when using a distribution server as the download source. For more information see Configuring Distribution Servers.
Patch and Service Pack download source	You can specify where the latest patch and service pack files downloaded by this console are located. The available options are: • **Vendor websites:** Patches deployed from the console are downloaded directly from the websites of the companies that author the patches. This is the default. The location of the websites are stored in the patch information file. The other two download options are used if this console does not have an Internet connection or when the patches and service packs are being pre-downloaded to some central location. • **Custom share or URL**: If enabled, you must specify the path name of the share or the URL of the website that will be used when downloading files. It is the administrator's responsibility to make the files available at this location.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **Specific Distribution Server**: If enabled, you must select the distribution server that will be used when downloading patch files. You must have previously configured one or more distribution servers in order for the names to be pre-populated in this box. For more information see Configuring Distribution Servers. This option is typically used by unattended console or disconnected console configurations. The patches and service packs are downloaded by a central console, which then pushes the files to the distribution server. One interesting but necessary side effect of enabling this option is that you will not be able to schedule an automatic synchronization for the distribution server you specify here. Why? Because in this particular case you do not want the console to synchronize with the distribution server. Doing so would cause the contents of the distribution server (the patches and service packs) to be overwritten by the contents of the console (which may not contain anything at all).
Scheduled automatic downloads	You can configure the program to automatically download the latest versions of the patch scan engine, the asset scan engine, and all XML data files on a regular basis. This can speed your scan processes by making the necessary files available in advance of a scan. You can also choose to automatically download patches and service packs that are likely to be used in future patch deployments. 1. Click **Add**. The **Schedule Download** dialog appears.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



2. Specify when you want the download to occur.

   The **Add delay (days)** box (available if you download on a monthly basis) allows you to delay the download by up to 20 days. For example, you might use this to schedule a monthly download that is always performed four days after Patch Tuesday. You do this by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by four days.

3. Click **Save**.

   The new scheduled download entry appears. At the scheduled time, the appropriate engines and definition files will be downloaded to the console.

4. If you want to use the Predictive Patch feature, enable the **Predictive patch downloads** check box.

   If enabled, patches that are likely to be deployed in the near future are automatically downloaded to the patch download directory. The patches will be downloaded immediately following the scheduled download of the core engines and definitions. Downloading patches in advance of their anticipated deployment will help speed the deployment process. This feature is beneficial for agentless deployments and for agents that deploy patches using the services of a distribution server.

   Here are some additional details about Predictive Patch:

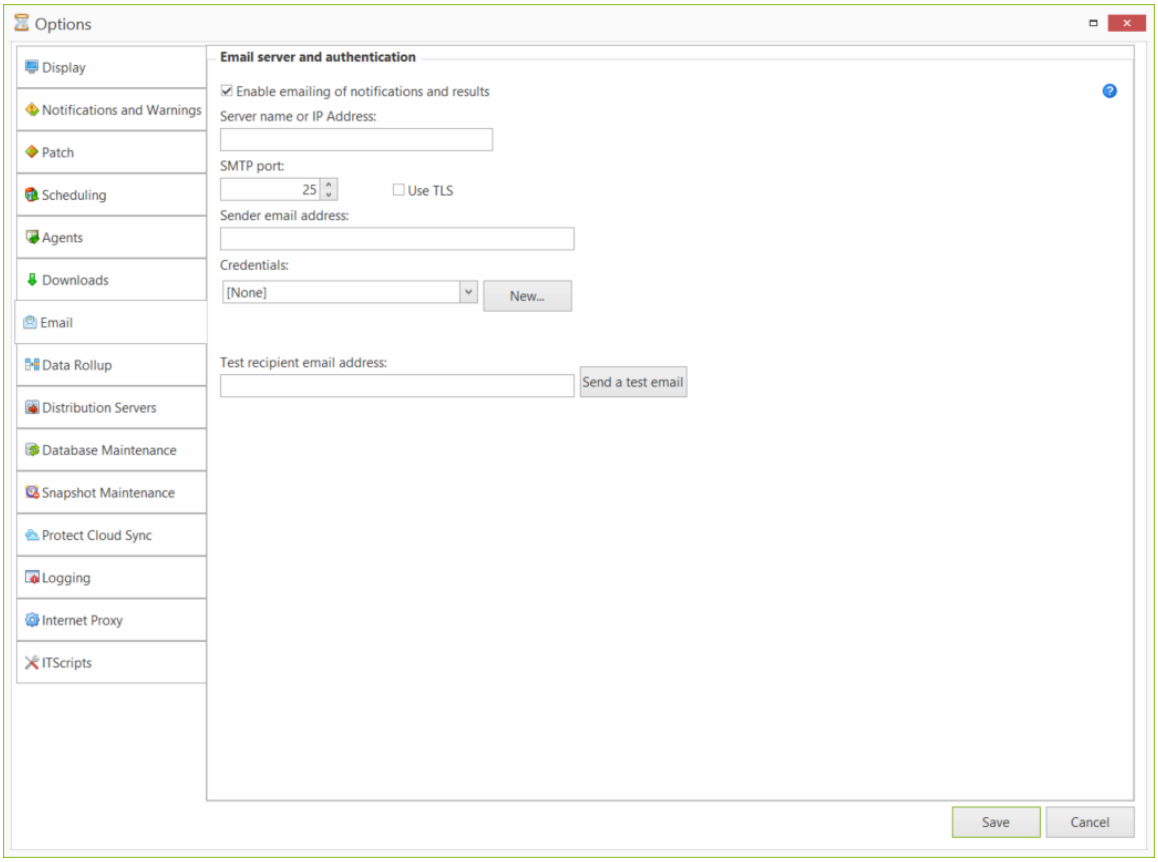
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• The following patches will be downloaded to the console's download directory:
	  • Missing patches that were detected by recent scans but that have not yet been downloaded. A recent scan is defined as a patch scan that was performed within the last 45 days.
	  • Missing patches for products that Ivanti Patch for Windows® Servers can deduce are on your target machines
	  • New patches that were recently added to the XML patch data file and that apply to products on your target machines.
	• New or missing service packs will be downloaded
	• The patches and service packs will be downloaded according to age (the most recent will be downloaded first)
	• The process will download up to 5GBs of patches and service packs during a scheduled download session
	• Patches that already exist in the download directory will not be downloaded.
	• You can synchronize Predictive Patch with your distribution servers so that they receive copies of the downloaded patches
	• An entry is recorded in Event History every time patches are downloaded to the console by Predictive Patch
	• The patch download is triggered by either a scheduled download of the core engines and definitions or by clicking **Run now** when **Core engines/definitions** is selected
	• If a patch contains different packages for different languages, only those languages supported by your products are downloaded
	• Predictive Patch will not download software distribution patches (patches that are actually installation packages for free third-party applications)

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Email Options

The **Email** tab enables you to specify if you want to use the email feature, and it lets you define the properties of the SMTP server used for sending the email messages and alerts. (See Email Overview for more details). To use this feature, enable the **Enable emailing of notifications and results** check box and then specify the name or IP address of the SMTP server you use.



Enable emailing of notifications and results	If you want to use the email feature, enable this check box. Enabling this check box enables the related options on this dialog.
Server name or IP Address	Specify the name or IP address of your local SMTP server. For example: Exchange2.YourCompany.com
SMTP Port	Specify the port used by the SMTP server. The default value is 25.
Use TLS	If you want the target machines to contact the SMTP server using a Transport Layer Security (TLS) connection, enable this check box.

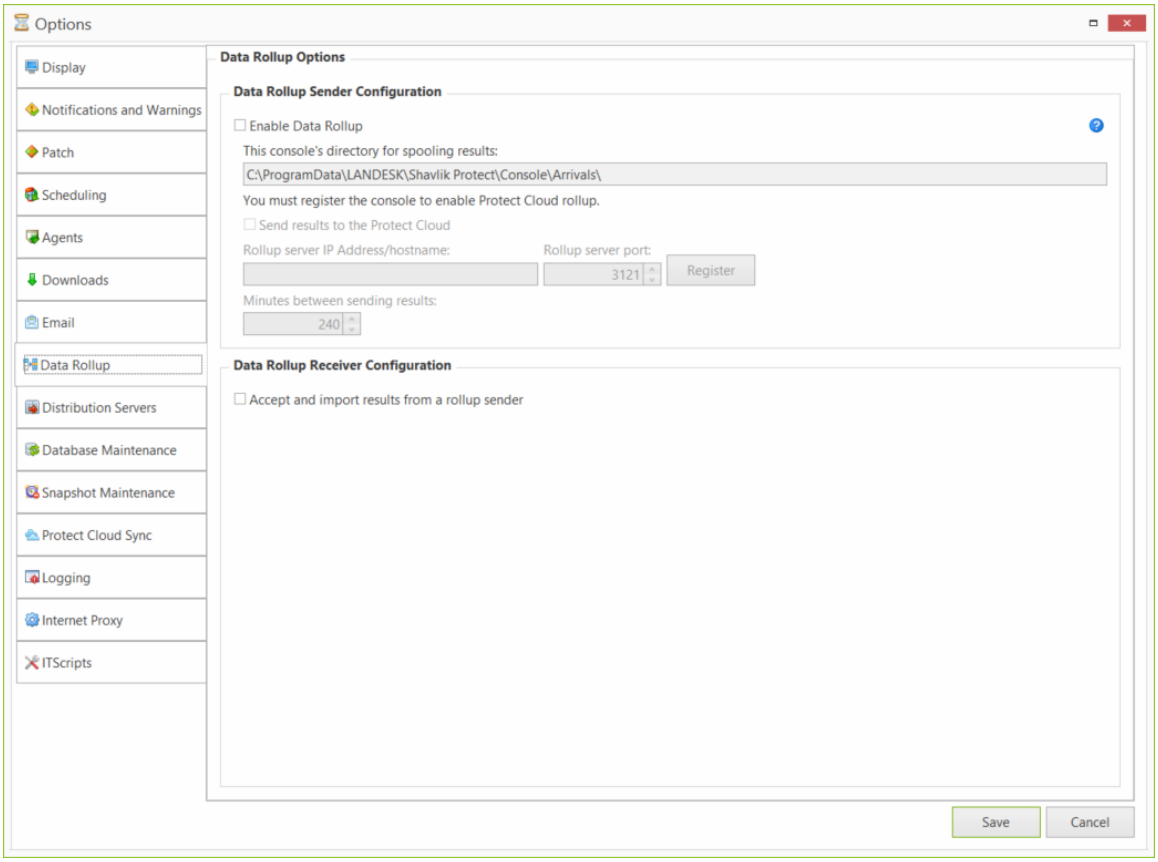
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Sender email address	Specify the email address that will be inserted into the **From:** address field of messages that are sent to users. If the default address causes problems for your SMTP server, change the address to an email address accepted by your SMTP server. (Some SMTP servers only accept mail from particular addresses or domains.)
Credentials	Select the credential (the user name and password pair) used to authenticate to the SMTP server. Only shared credentials are contained in this list. If the credential you are looking for is not listed it probably means it is not defined as a shared credential. See Defining Credentials for information on how to share a credential.
Test recipient email address	Specify a known email address you want to use when testing the email process.
Send a test email	To verify the program can use the specified credentials to contact the SMTP server, click this button.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Data Rollup Options

The **Data Rollup** tab enables you to specify how this console will interact with agents and with other consoles.



Enable Data Rollup	If you want this console to roll up and send its scanning and deployment data to a central console, enable this check box. The other options in this area are not available unless this check box is enabled.
This console's directory for spooling results	Specifies the directory that will be used to store results sent to this console by Ivanti Patch for Windows® Servers Agent and/or by other consoles. The directory path cannot be changed. The directory will be: **C:\ProgramData\LANDESK\Shavlik Protect\Console\Arrivals** **C:\ProgramData\ScriptLogic Corporation\Patch Authority Ultimate\Console\Arrivals**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Send results to the Protect Cloud	If enabled, patch scan and deployment results will be periodically sent to Protect Cloud. If you are an Ivanti Empower user, the patch data will be periodically retrieved from Protect Cloud by Empower and the data can then be viewed within Ivanti Empower. You cannot send results to both Protect Cloud and to a rollup console; the options are mutually exclusive. This option is only available if you have registered the console with Protect Cloud.
Rollup server IP Address/hostname	Specify the IP address or hostname of your Ivanti Patch for Windows® Servers rollup console. The rollup console will receive scanning and deployment data that is rolled up to it from this console.
Rollup server port	Specify the port used by the rollup console to listen for incoming data from agents and other consoles. The default value is 3121.
Register	To enable this console to send results to the rollup console, click **Register**. This will establish a secure binding between this console and the rollup console. TIP: The registration process will also automatically generate an entry in the **Edit Database Description** dialog on the central console. You can use this dialog to track how many remote consoles are configured to roll up their results to the central console. See Editing the Database Description for more details.
Minutes between sending results	Specify how often you want data from this console to be sent to the rollup console. Valid values are from 10 - 10080 (10 minutes - one week). The default value is every 240 minutes (four hours). Although you can roll up data as often as once every 10 minutes, this is typically impractical. How often you choose to roll up data will depend on a number of things, including how often the console is performing scans and deployments, and how often you want that information reflected in the aggregate database on the rollup console.
Accept and import results from a rollup sender	If enabled, this console will act as a rollup console and will accept scan and deployment data that is sent to it from other consoles. In addition, the sending console(s) must register with this console in order to complete the data rollup configuration.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

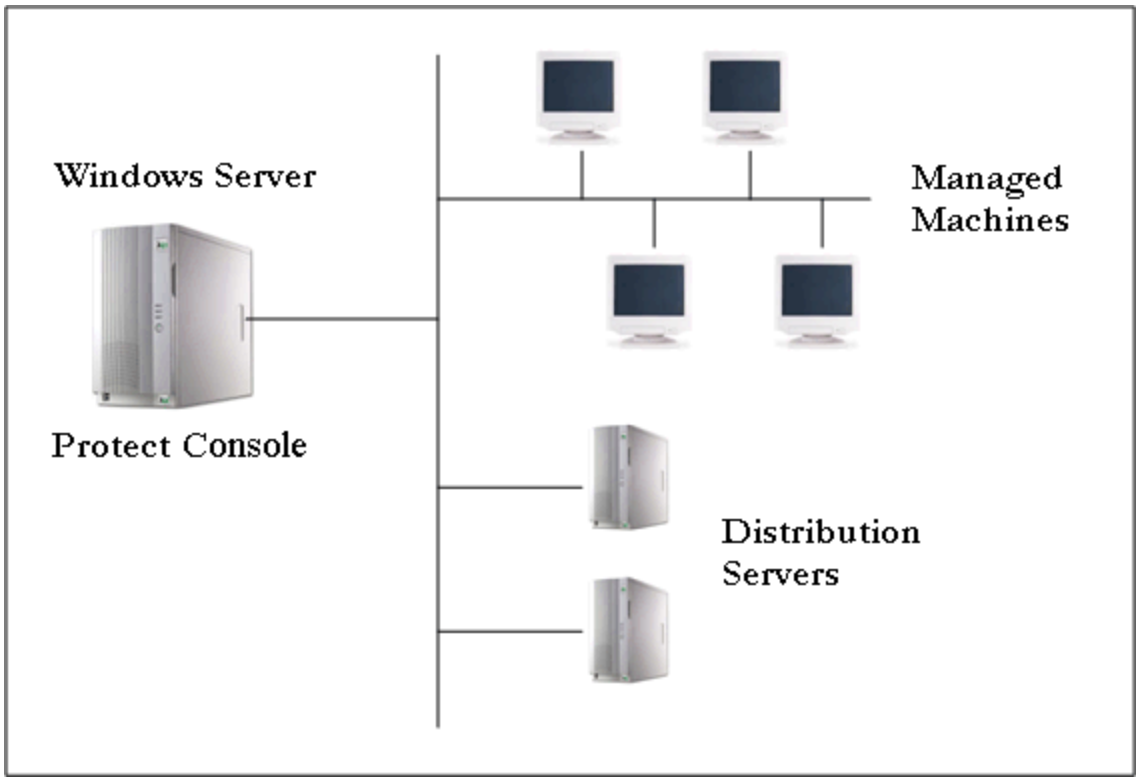
Why Use a Distribution Server?

Distribution servers can be used in a number of different scenarios:

- Distribution servers can be used to store patches that you wish to deploy. Distribution servers can be physically located near each group of machines you are managing. The console can copy patches to the distribution servers only, rather than to each individual machine. Each machine can then download the patches it needs from the nearest distribution server. This can greatly reduce network traffic in a distributed environment and be of huge benefit in wide-area networks. This is true in both agentless environments and agent-based environments. In agentless environments, using distribution servers means the console does not need to push patches to individual machines and individual machines do not need to download patches from patch vendor. In an agent-based environment, it can keep each machine from downloading the patches it needs from the patch vendor over the Internet.
- Distribution servers can be used to store the most up-to-date engines and XML files that are available. In a multi-console or agent-based environment, this can reduce the number of machines that need to download updated files over the Internet.
- Distribution servers allow consoles and agents to operate in environments where they do not have Internet access but still need access to the most up-to-date engines and XML files. See What is a Disconnected Console Configuration for more information.
- Distribution Servers can be used to store any custom patches you may have defined. This is particularly important for agent-based environments. See Preparing to Use Agents for more information.

The following figure illustrates the use of distribution servers in a network.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Determining How Many Distribution Servers to Use

Do You Need a Distribution Server?

To determine if you should use one or more distribution servers with Ivanti Patch for Windows® Servers, apply the following formula:

- If **# of machines * 10Kb > available bandwidth**, then you need at least one distribution server.

Examples

Assume available bandwidth = 500 Kb:

- 100 machines: 100 machines * 10Kb = 1000Kb > 500Kb (need distribution server)
- 20 machines: 20 machines * 10Kb = 200Kb < 500Kb (do not need distribution server)

If You Need Distribution Servers, How Many?

If (using the formula above) you determine you need one or more distribution servers, you still need to determine exactly how many distribution servers are needed. Determining the number of distribution servers that are needed is very simple. The general rule is:

- Use one distribution server for every 2500 machines

For example, if you have 7500 machines you should plan on using three distribution servers.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

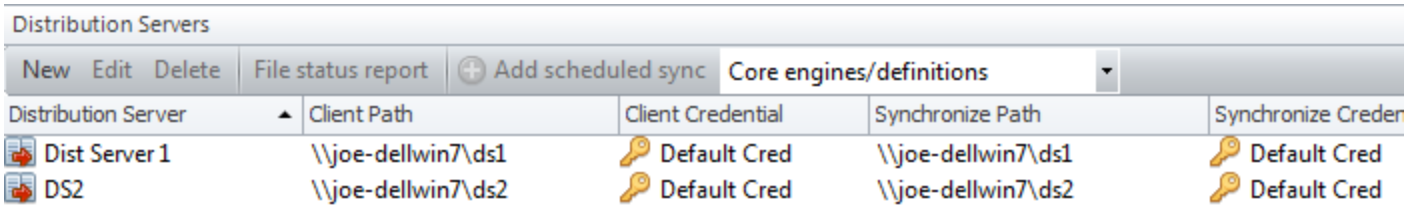
Configuring a New or Existing Distribution Server

IMPORTANT! In addition to using the **Distribution Servers** dialog to configure the distribution server within Ivanti Patch for Windows® Servers, under certain conditions you will need to provide the LOCAL SYSTEM machine account with the proper sharing and security permissions. See Configuring System Account Permissions for details.

There are a number of reasons why you may choose to use a distribution server. For details, see Why Use a Distribution Server?.

How to Access Your Distribution Servers

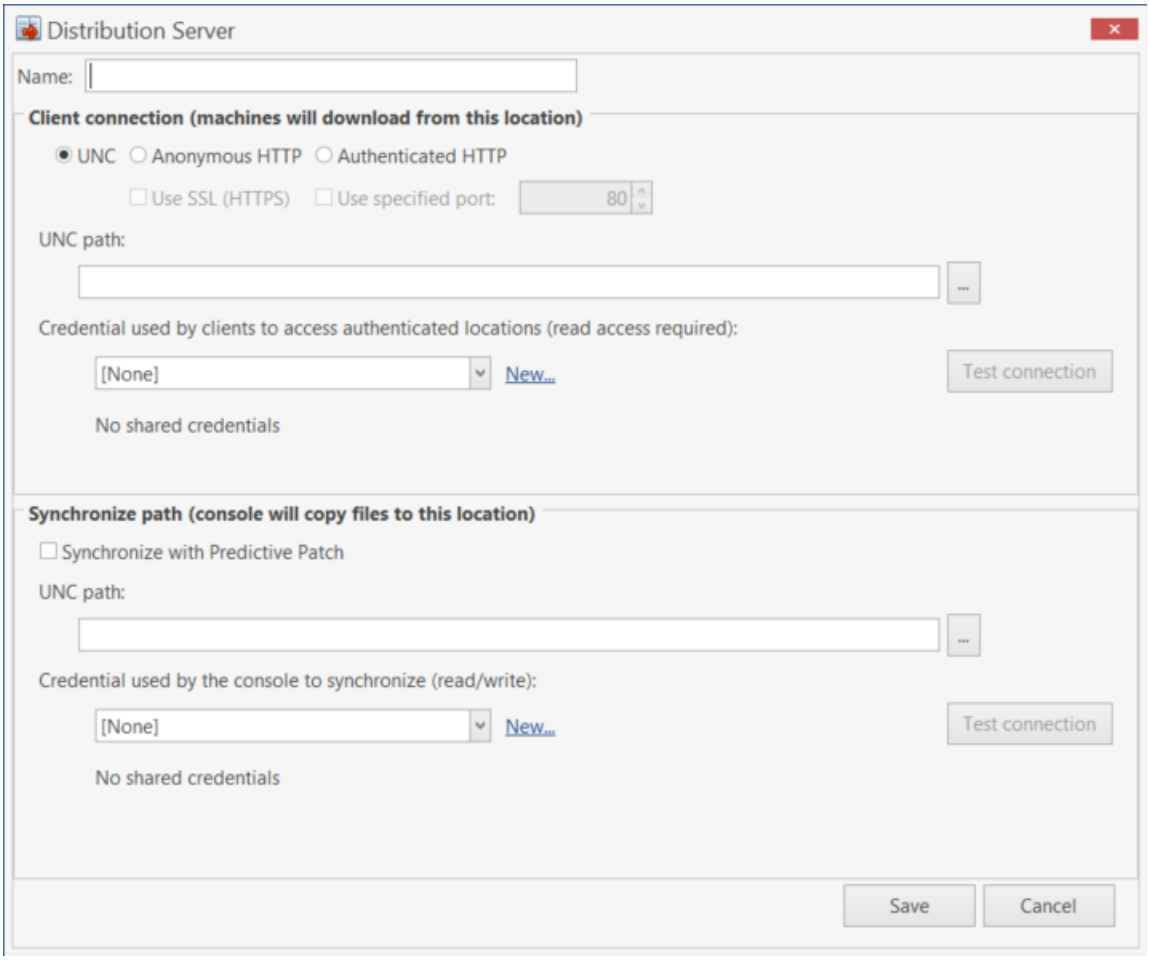
To configure a distribution server, select **Tools > Options** and then select the **Distribution Servers** tab. Any currently defined distribution servers are displayed in the top pane.



You cannot delete a distribution server that is currently being used by an agent policy. Also, if you edit and save a distribution server that is being used by an agent policy, the agents using that policy will be updated the next time they check in with the console.

To configure an existing distribution server, select the distribution server and then click **Edit**. To configure a new distribution server, click **New**. The **Distribution Server** dialog is displayed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



In the top half of the dialog, be sure to specify a location and authentication method that all the target machines can use when accessing the server. The lower half of the dialog is used to specify how the console will connect to this same location on the distribution server. Although the physical location you specify must be the same in both halves of the dialog, in the top half you can specify the *method* used by the target machines when accessing the data (**UNC** vs. **Anonymous HTTP** vs. **Authenticated HTTP**).

Name	The name you want to give to the distribution server you are configuring. The name can contain letters, numbers, and special characters.
Connection method	Specify how the target machines will access the file repository on the distribution server.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **UNC**: If you want to specify both the path name of the repository on the distribution server and the logon credentials used by the target machines when logging on to the distribution server, enable this option. You must also define the **UNC Path** and the **Assign credentials** options. • **Anonymous HTTP**: If you want the target machines to access the repository via the Internet using an anonymous (unauthenticated) Web connection, enable this option. You must also define the **URL** option. • **Authenticated HTTP**: If you want the target machines to access the repository via a Web browser using a secure Web connection, enable this option. You must also define the **Port**, **URL**, and **Assign credentials** options.
Use SSL (HTTPS)	If you want the target machines to contact the distribution server using an SSL connection, enable this check box. This check box is not available if UNC is selected as a client connection.
Use specified port	Specifies the port used by the target machines when contacting the distribution server via the Web. The default value is 80, or 443 if SSL is selected.
UNC path / URL	The name of this field changes depending on whether UNC or HTTP is selected as the connection method. Specify the UNC path name or the URL path to the repository on this distribution server. The physical location you specify here for the target machines to use should be the same as the location you specify for the console to use (on the **UNC path** option). The *method* (UNC, Anonymous HTTP, Authenticated HTTP) the target machines use when connecting to the distribution server may be different, but the physical location should be the same.
Credential used by clients to access authenticated locations	This box applies only if **UNC** or **Authenticated HTTP** is specified. Select the credential (the user name and password pair) used by the target machines to access the distribution server. To define a new credential click **New**. Only shared credentials are contained in this list. If the credential you are looking for is not listed it probably means it is not defined as a shared credential. See Defining Credentials for information on how to share a credential.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Test Connection	If you want to test the authentication credentials used to access the distribution server, click **Test Connection**. For HTTP[S] distribution servers, a default content page (default.htm) is needed in the distribution server directory in order for the test to work.

The lower half of the dialog is used to specify how the console will connect to and synchronize with the distribution server.

Synchronize with Predictive Patch	This is different than the automatic synchronization feature, which enables you to synchronize all engines, definitions, and patches contained on the console. If enabled, those patches that have been downloaded to the console by the Predictive Patch feature will be synchronized with (copied to) this distribution server. Service packs are not included in this synchronization. The **Patch Sync** column in the top pane of the **Distribution Servers** tab will indicate if Predictive Patch is enabled for a distribution server. A background task will be created when the synchronization is performed. You can track the progress of the synchronization task using Event History.
UNC Path	The Universal Naming Convention (UNC) path name of the repository share on the distribution server. This share must be accessible by the console and is used when synchronizing the contents of the distribution server with the patches and/or scan engines and XML definition files contained on the console. If you don't remember the exact path you want to specify in the **UNC Path** box, or if you need to create a new folder, click ... to search for or create the path name.
Credential used by the console to synchronize	Access to a distribution server requires authentication. Select the credential (the domain\user name and password pair) used by the console to authenticate to the distribution server. To define a new credential click **New**. Only shared credentials are contained in this list. If the credential you are looking for is not listed it probably means it is not defined as a shared credential. See Defining Credentials for information on how to share a credential. Please note the following:

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• If the distribution server is being used as the download source for the definition files, the credentials of the user currently logged on to the console will be used to connect to the server rather than the credentials you supply here. This means the distribution server UNC path must be accessible by all Ivanti Patch for Windows® Servers administrator accounts. This also means the server must reside in either the same domain as the console or in a trusted domain that will recognize the integrated credentials. • If you do not specify a credential then by default integrated Windows authentication will be used (the authentication credentials of the person currently logged on to the console machine). • If automatic synchronization is being used and there are multiple administrators in your organization using Ivanti Patch for Windows® Servers, at least one of the administrators must specify their credentials here. If you do not specify a credential AND you are using the automatic synchronization feature, you must provide the console machine's LOCAL SYSTEM account with read and write access to the distribution server folder. See Configuring System Account Permissions for details.
Test Connection	If you want to test the authentication credentials used to access the distribution server, click **Test Connection**. The credentials cannot be verified if the current session is already connected to the share.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Configuring System Account Permissions

In addition to using the **Distribution Servers** dialog to configure the distribution server within Ivanti Patch for Windows® Servers, if the following conditions apply you will need to provide the SYSTEM machine account with the proper sharing and security permissions:

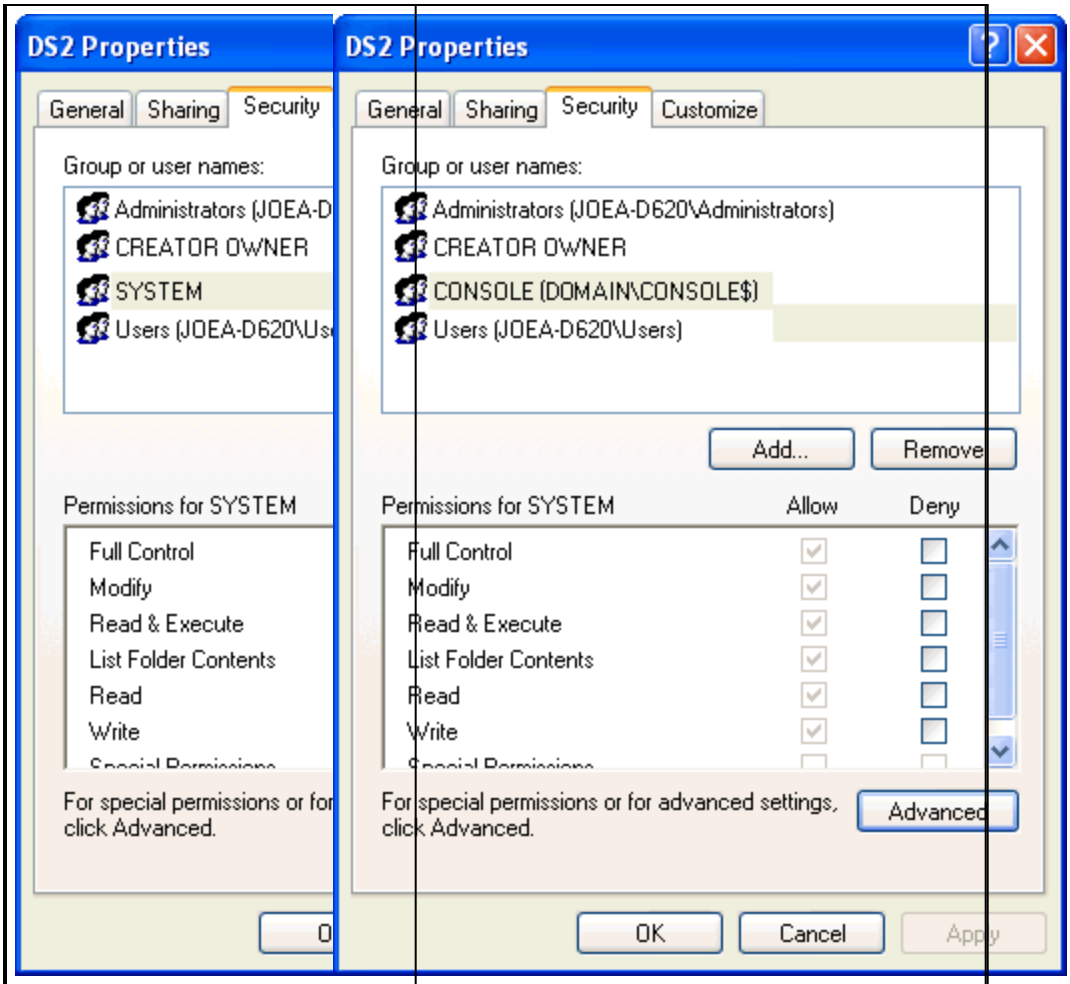
- If the distribution server resides on the same machine as the console, the local machine's SYSTEM account must have read and write access to the distribution server folder.
- If an agent will be installed on the distribution server machine, the machine's SYSTEM account must have read access to the distribution server folder.
- If you did not specify credentials for the console to use when authenticating to the distribution server AND you are using automatic synchronization, the Ivanti Patch for Windows® Servers console machine's SYSTEM account must have read and write access to the distribution server folder.

In these three special cases it is the SYSTEM account that is used to access the distribution server and not the credentials supplied on the **Distribution Servers** dialog. If sharing and security permissions are not set, distribution server synchronization errors may occur and/or the local agent may fail to update.

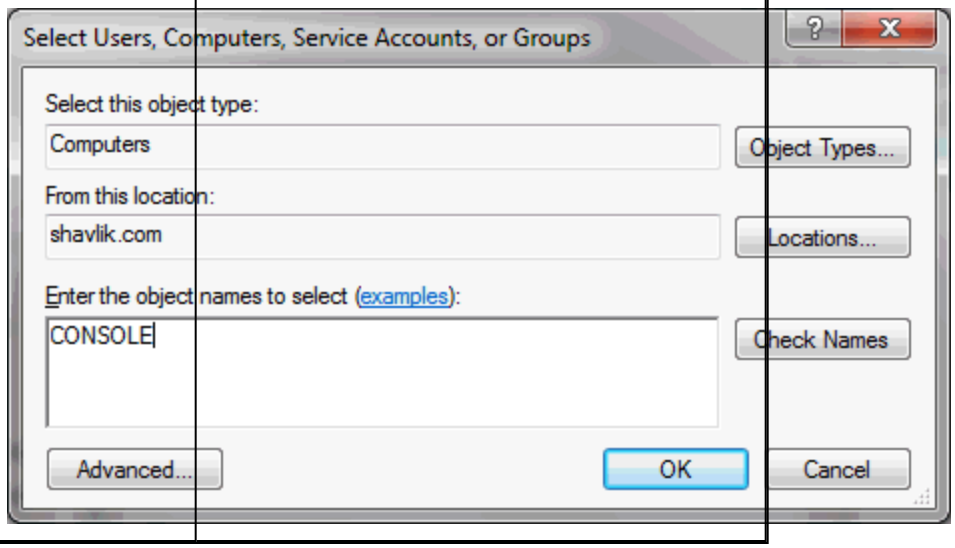
Use Windows Explorer to set the account permissions by right-clicking the distribution server folder, selecting **Properties**, and the clicking the **Sharing** and the **Security** tabs. When setting permissions for the console machine's SYSTEM account (per bullet item #3), you will need to add the console machine's SYSTEM account name to the **Group or user names** list before you can set its permissions. Be sure you specify **Computers** as an object type when adding the name (see Example 2).

Example 1: Local SYSTEM Account	Example 2: Console Machine SYSTEM Account

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

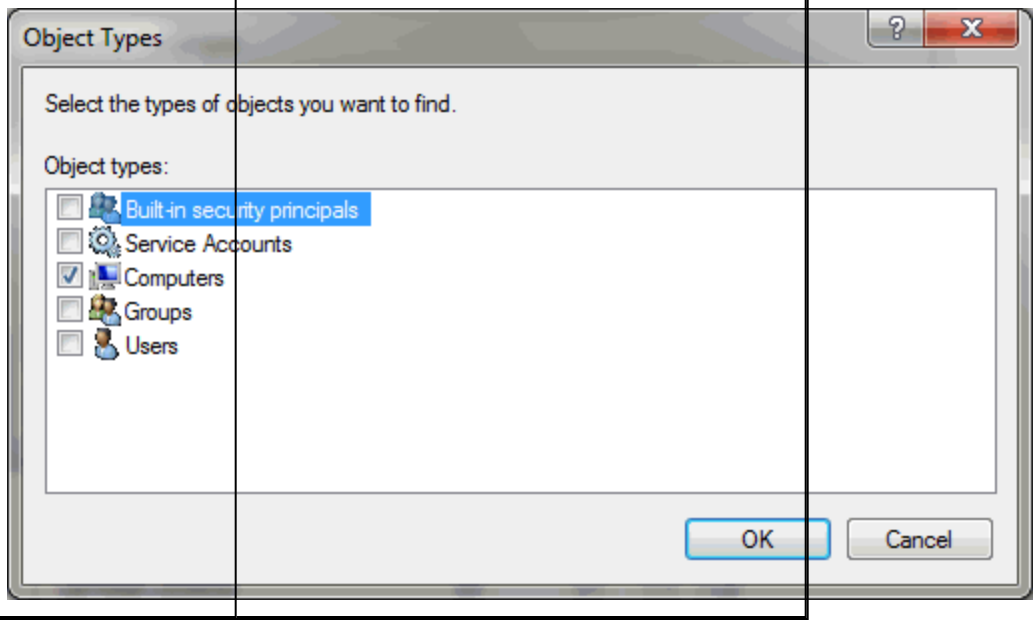


When adding the console SYSTEM account name...



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	... verify that *Computers* is enabled on the *Object Types* dialog.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

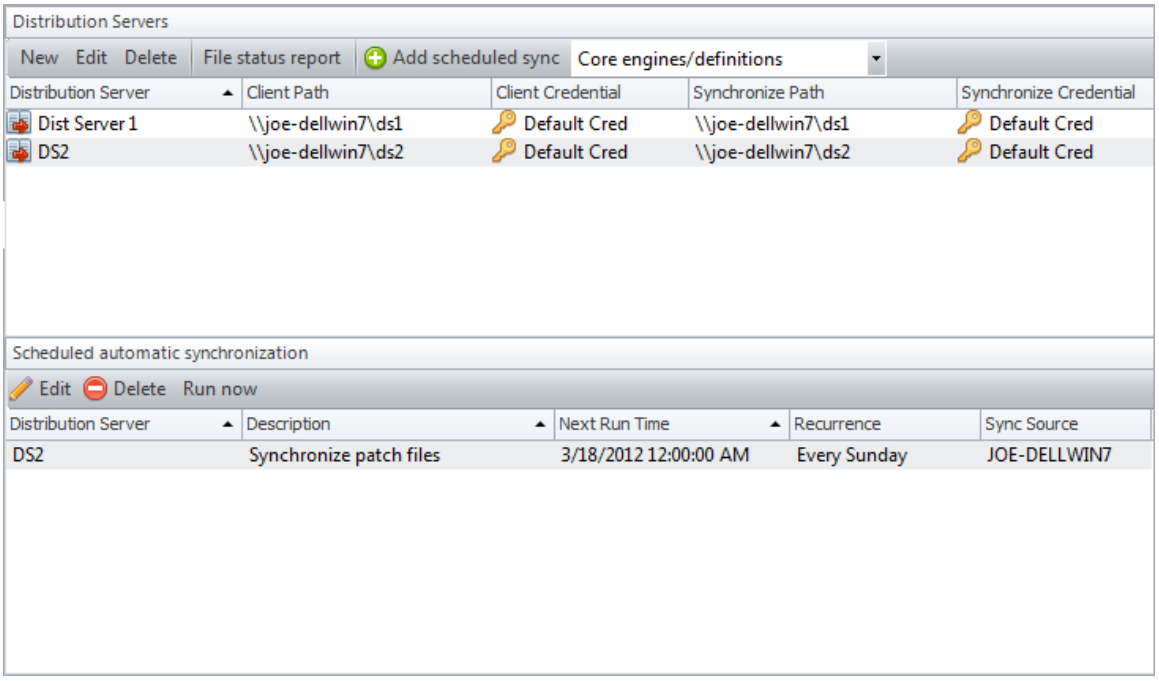
Synchronizing Distribution Servers

When you synchronize a distribution server it means you are updating the server with the latest patches and/or scan engines and XML definition files contained on the console. To synchronize your distribution servers, select**Tools > Options**and then click the**Distribution Servers**tab.

You can automatically synchronize distribution servers on a periodic basis. You can also manually synchronize the distribution servers directly. This section will cover both options.

Make sure the console contains the necessary files before attempting to synchronize all your distribution servers. For information on downloading patches to the patch download directory, see Downloading Patches. To download the latest engines to the console, select **Help > Refresh files**.

Another option for automatically synchronizing your distribution servers is to use Distributed File System (DFS) Replication. DFS Replication is available beginning with Windows Server 2003 R2 and requires the use of Active Directory.



Creating a Status Report

If you want to create a report that shows which of the patches contained in the download directory are missing or are out-of-date on the distribution servers, select the desired distribution server(s) and then click **File Status Report**. The report will list which downloaded patches are not contained on the selected distribution servers or are out of date. The report does not report if engines and data files are missing or out of date.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Automatically Synchronizing Distribution Servers

To configure the program to automatically synchronize engines, definitions, and/or patches with a distribution server:

1. In the **Add scheduled sync** box in the top pane, select the component you want to synchronize.

   The components that you can choose to synchronize are:

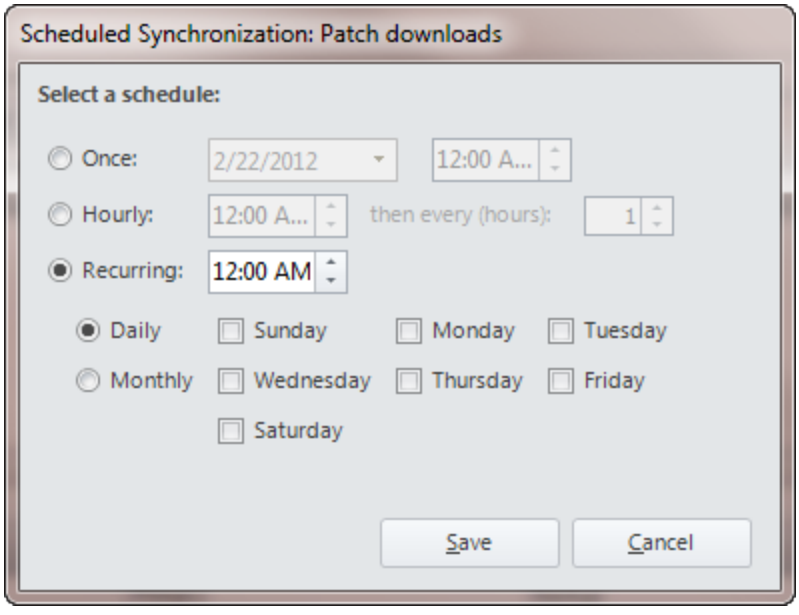
   - **Core engines/definitions:** The latest versions of the patch scan engine, the asset scan engine, and all XML data files will be copied to the distribution server. If you have more than one console sharing a database, only one console can synchronize core engines/definitions to a given distribution server.
   - **Patch downloads:** All patches contained in the console's patch download directory will be copied to the distribution server.
   - **All engines, definitions, and patch downloads**: All relevant components are synchronized.

2. In the top pane, select which distribution server you want to synchronize with the console.

   If the **Add scheduled sync** button becomes unavailable after you select a specific distribution server, it probably means the server is being used as the download source for patches and service packs.

3. Click **Add scheduled sync**.

   The **Scheduled Synchronization** dialog appears.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

4. Specify when you want the synchronization to occur.

   The **Add delay (days)** box (available if you synchronize on a monthly basis) allows you to delay the synchronization by up to 20 days. For example, you might use this to schedule a monthly synchronization that is always performed four days after Patch Tuesday. You do this by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by four days.

5. Click **Save**.

The new scheduled synchronization entry appears in the **Scheduled automatic synchronization** pane. At the scheduled time, the appropriate files will be copied to your distribution server. If the synchronization time happens to coincide with a download of new files to the console, the synchronization process is queued and is performed when the download is complete.

The **Scheduled automatic synchronization** pane will show scheduled synchronizations for all consoles that share the database. If you select a schedule created by a different console, you can delete the schedule but you cannot edit it or run it immediately. This allows you to move the synchronization process to the current console by deleting the remote schedule and then creating a new local schedule. It also allows you to delete schedules for consoles that no longer exist.



If you did not specify credentials for the console to use when authenticating to the distribution server, in order for automatic synchronization to work the console machine's SYSTEM account must have read and write access to the distribution server folder. See Configuring System Account Permissions for details.

Manually Synchronizing Selected Distribution Servers

You have the option to manually synchronize a distribution server with the console. This initiates a synchronization right now so you don't have to wait for the next scheduled interval. A background task will be created to perform the synchronization. You can continue using the rest of the program while the synchronization process is performed.

To perform a manual synchronization:

1 If you are manually synchronizing the scan engines and XML data files, make sure you have the latest files on the console by selecting **Help > Refresh files**.

   This will download the latest files from the location specified on the **Tools > Options > Downloads** page and store them in the console's default data directory:

   C:\ProgramData\LANDESK\Shavlik Protect\Console\DataFilesC:\ProgramData\ScriptLogic\Patch Authority\Console\DataFiles

2. If you are manually synchronizing patches, make sure the console's patch download directory contains all the patches you want on your distribution server(s). See Downloading Patches for details.

   The patches are contained in the default patches directory:

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

C:\ProgramData\LANDESK\Shavlik Protect\Console\Patches\ScriptLogic\Patch Authority\Console\Patches

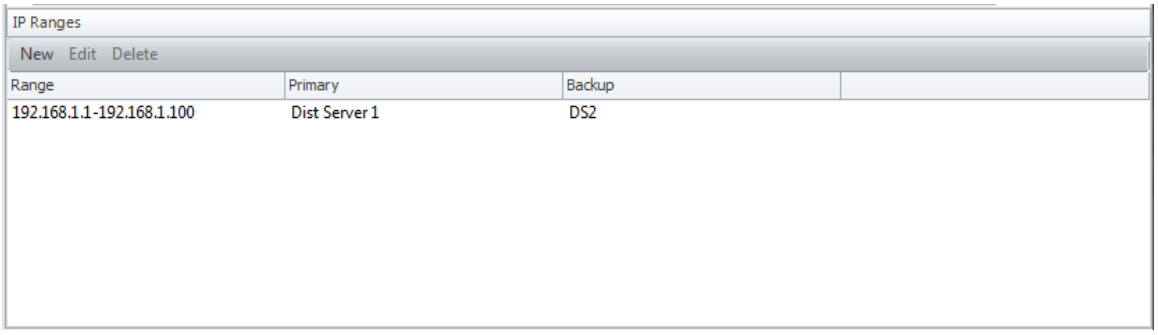
3. In the **Schedule automatic synchronization** pane, select one or more scheduled synchronization entries.
4. Click **Run now**.

This will immediately copy all appropriate files from the console to the specified distribution server(s). You can use Event History to track the progress of the synchronization task.

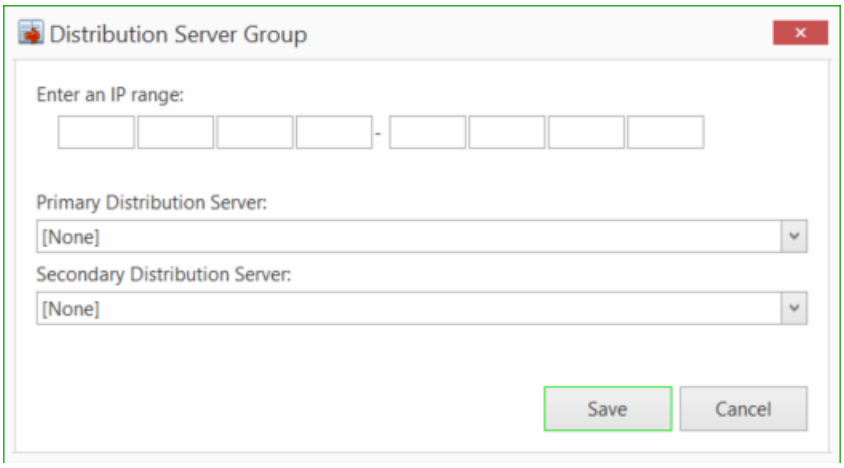
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Assigning IP Addresses to Distribution Servers

You define which target machines will use a particular distribution server by assigning the IP addresses of the target machines to the distribution server. To assign one or more IP address ranges to a distribution server, select **Tools > Options** and then select the **Distribution Servers** tab. Any currently defined IP address ranges are shown in the **IP Ranges** pane.



To modify an existing entry, select the entry and then click **Edit**. To define a new range of IP addresses, click **New**. The **Distribution Server Group** dialog is displayed.



Enter IP range	Use the available fields to define the new IP address range.
Primary Distribution Server	Select the distribution server you want to use as the primary distribution server for this collection of target machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Backup Distribution Server	(Optional) Select the distribution server you want to use as the secondary distribution server for this collection of target machines. The secondary distribution server is only used if the primary distribution server is unavailable.
Save	To accept the current settings, click **Save**.
Cancel	To cancel without saving your changes, click **Cancel**.

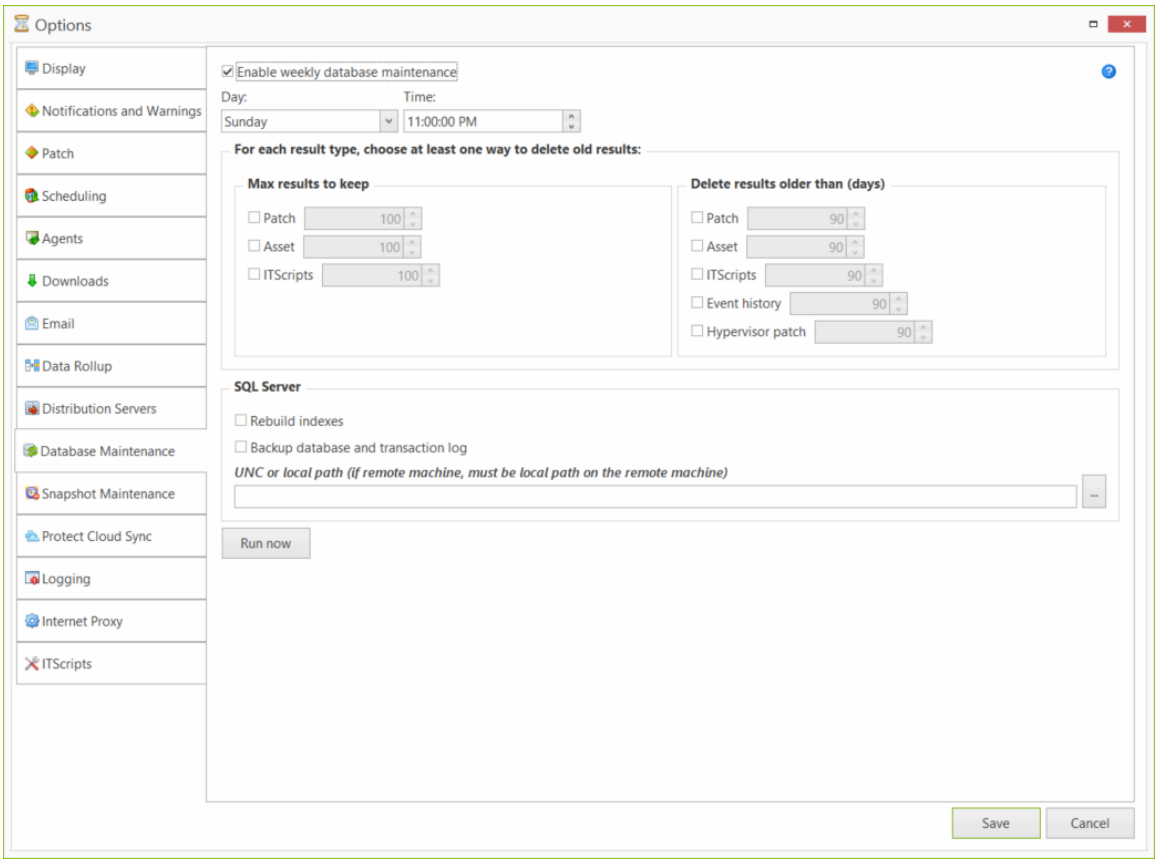
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Database Maintenance

In order to keep Ivanti Patch for Windows® Servers operating at peak efficiency, it is important to perform periodic maintenance on your database. Ivanti Patch for Windows® Servers's database maintenance tool enables you to:

- Delete old results
- Rebuild your SQL Server indexes
- Create backups of your database

You do this by selecting **Tools > Options > Database Maintenance** and then specifying exactly when and how your database maintenance tasks should be performed.



If the options on this dialog are unavailable it probably means that another administrator currently has control over the database maintenance operations. See the **Take ownership** option (below) for more details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Enable weekly database maintenance	If enabled, will perform database maintenance tasks on the specified day and time. The scheduled job is managed by the Ivanti Patch for Windows® Servers console service; the job cannot be tracked using the Scheduled Task Manager. Maintenance tasks should be performed after hours or on a weekend when database use is at a minimum. If this check box is not enabled you can still configure the remaining database maintenance options on this dialog, but in order to run the maintenance task you must initiate it using the **Run now** button. The database maintenance tasks will not be performed on a regularly scheduled basis.
For each result type, choose at least one way to delete old results	There are two ways to delete old results: • **Max results to keep:** Enables you to specify the maximum number of patch scans, asset scans and script run records you want to store in the database. If the specified number is exceeded, scans will be deleted based on their age (the oldest scans are deleted first). Any patch deployments that are associated with the scans are also deleted. Valid values are 10 - 10,000 for each scan type. Be careful if you are using Ivanti Patch for Windows® Servers Agent on your machines. Agents report their results to the console and each result constitutes a scan. If you have many agents there is a chance of exceeding the threshold rather quickly. In this scenario you should consider using the **Delete results older than (days)** option. • **Delete results older than (days):** Enables you to specify the maximum number of days that patch results, asset results, event logs, and script run records are allowed to be stored in the database before being deleted. Any patch deployments that are associated with the scans are also deleted. Valid values are 1 - 10,000 days. As a general rule, results that are over 90 days old should be considered too old to accurately depict the current state of your organization. If you choose to implement both methods for a result type, the method that deletes the least number of results is the one that will be used.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	Example: Assume that for patch results you specify **Max results to keep** = 100 and **Delete results older than (days)** = 90. Also assume that there are 150 patch results currently stored in the database but only 10 of them have been there for more than 90 days. When the database maintenance task is run the oldest 10 results will be deleted; the 140 results that are less than 90 days old will be left alone. **About the Different Result Types** Each result type consists of the following: • **Patch:** Patch scans and any associated patch deployments • **Asset:** Asset scans • **ITScripts:** Script run records • Event history: Log entries for operational events such as database maintenance and synchronization activities • **Hypervisor patch:** ESXi hypervisor scans and bulletin deployments
Rebuild indexes	If enabled, each time the database maintenance task is performed it will instruct SQL Server to rebuild the database indexes after the old result data are removed. Doing so will improve the performance of your database. This is particularly valuable when deleting large amounts of data. This option will work on any of the supported editions of SQL Server but it is best suited for use with SQL Server Express editions. If you are using a full edition of SQL Server you might consider using the SQL Server Maintenance Wizard because it provides more control and functionality.
Backup database and transaction log	If enabled, each time the database maintenance task is performed it will instruct SQL Server to create backup copies of the database and the transaction log before removing any data. You must specify where the backup files will be written. You can use either a UNC path (for example: \\server\backup) or a local path (for example: c:\backup) to specify the backup location. The recommendation is to use a UNC path format that specifies a location on a different machine than the one currently running SQL Server. The path name you specify here is simply passed along for use during the backup. No validation is performed on the name. **Notes:** • If you are using a remote SQL Server and you specify a local path, the path you are specifying is located on the remote SQL Server and NOT on the console machine.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• If you specify a UNC path to a location on SQL Server, your SQL Server account must have access to the path. If a built-in account is being used (such as Local System or Network Service) then the machine account needs access to the path.
Take ownership	This button is only displayed if you have two or more consoles that share one database. If your organization uses multiple Ivanti Patch for Windows® Servers consoles that share the same database, only one console will be authorized to use the Database Maintenance tool. If an administrator at another console wants to perform maintenance on the database, that administrator must take ownership of the task before the program will allow the administrator to continue. Any existing maintenance tasks will be allowed to complete before ownership is transferred to another administrator.
Run now	Immediately initiates the database maintenance task. The task is run in the background and requires no user intervention. The task is performed using the current configuration. The current configuration is saved for future use, and if the **Enable weekly database maintenance** check box is enabled this will also schedule the database maintenance task. You can use the Event History log to track the progress of the maintenance task. In addition, after the task completes there should be fewer items in the **Results** list and in the Manage Items list. If you have access to SQL Server Management Studio you can also use its Database Properties feature to track the progress of the task.
Save	Saves the current database maintenance configuration. If the **Enable weekly database maintenance** check box is enabled this will also schedule the database maintenance task.
Cancel	Exits the **Database Maintenance** dialog without saving your most recent changes.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

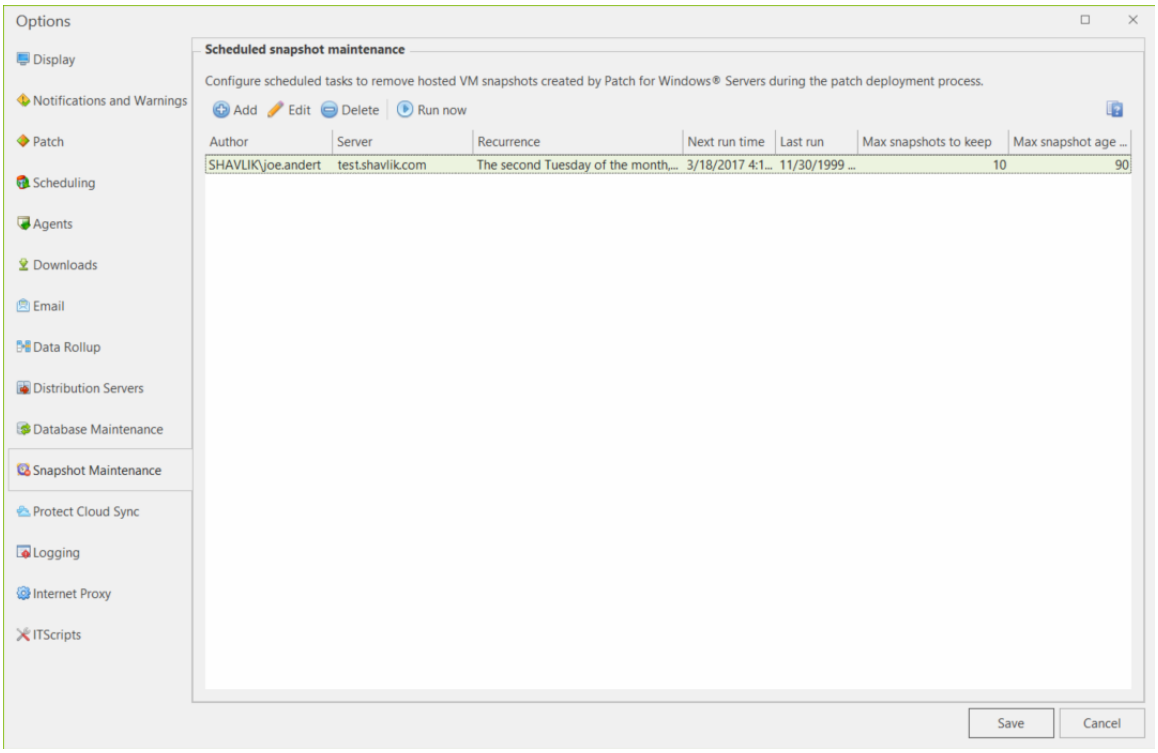
Scheduled Snapshot Maintenance

This option allows you to schedule the removal of old virtual machine snapshots. If you want to remove old snapshots in real-time (as new snapshots are created during the patch deployment process), see Deployment Template: Hosted VMs/Templates Tab.

The **Snapshot Maintenance** dialog applies only if you have virtual machines in your network that are hosted on one or more VMware servers. It allows you to configure a one-time or recurring task that will remove old virtual machine snapshots from the server. The snapshots that exist were created on the server during patch deployments to the server's hosted virtual machines.

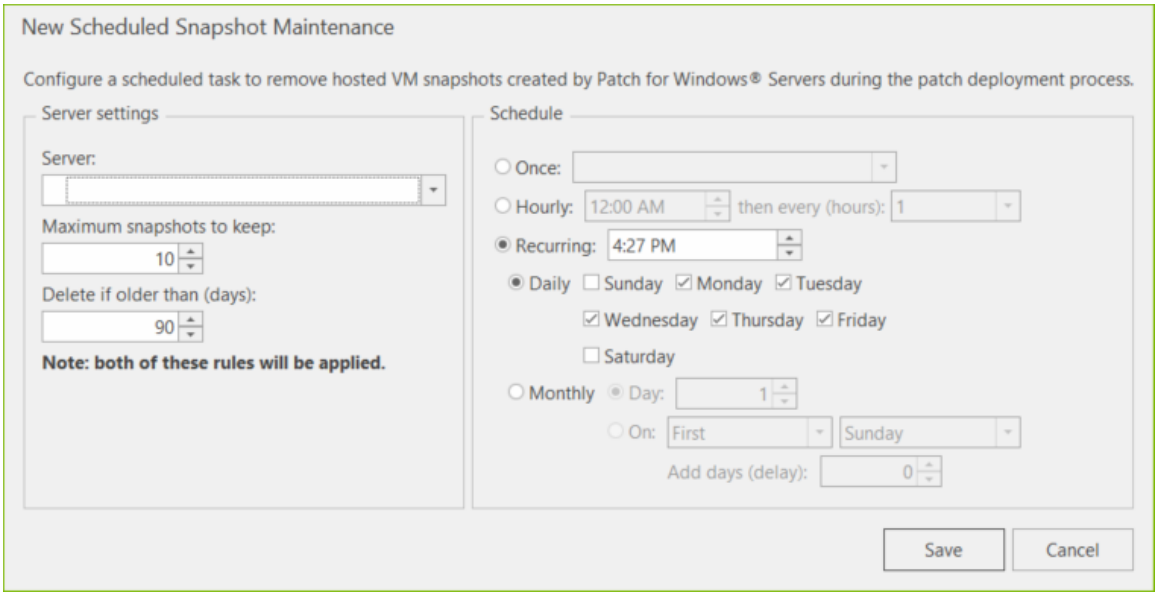
Any currently defined snapshot maintenance tasks are displayed in a list on the dialog. You can perform the following actions:

- **Add:** Adds a new snapshot maintenance task
- **Edit:** Edits the selected snapshot maintenance task
- **Delete:** Deletes the selected maintenance task
- **Run now:** Causes the selected maintenance task to be run right now



When you click **Add** or **Edit**, the **Scheduled Snapshot Maintenance** dialog is displayed. This dialog is used to configure the snapshot maintenance task.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Server	Choose the VMware server from which you want to remove virtual machine snapshots.
Maximum snapshots to keep	Indicates the maximum number of snapshots created by Ivanti Patch for Windows® Servers that will be allowed to remain on the server. If the threshold is exceeded, the oldest snapshots are deleted until the number of snapshots no longer exceeds the limit.
Delete if older than (days)	Indicates the number of days a snapshot created by Ivanti Patch for Windows® Servers will be allowed to exist. Snapshots older than the specified number of days are automatically deleted. The threshold is checked each time this maintenance task is run.
Schedule	There are three scheduling options: • **Once** indicates that the operation will be run once at the specified day and time. • **Hourly** indicates that the operation will be run multiple times a day. The operation will be run at the start time and then again every X hours. • **Recurring** allows an administrator to regularly schedule operations at a specific time and using a specified recurrence pattern. For example, using this option, an operation could be run every night at midnight, or every Saturday at 9 PM, every weekday at 11 PM, or at any other user selected time and interval.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	You can also use the **Recurring** option to schedule an operation in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly snapshot maintenance task to occur four days after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add days (delay)** option to delay the operation by four days.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Protect Cloud Synchronization Overview



Show Me!

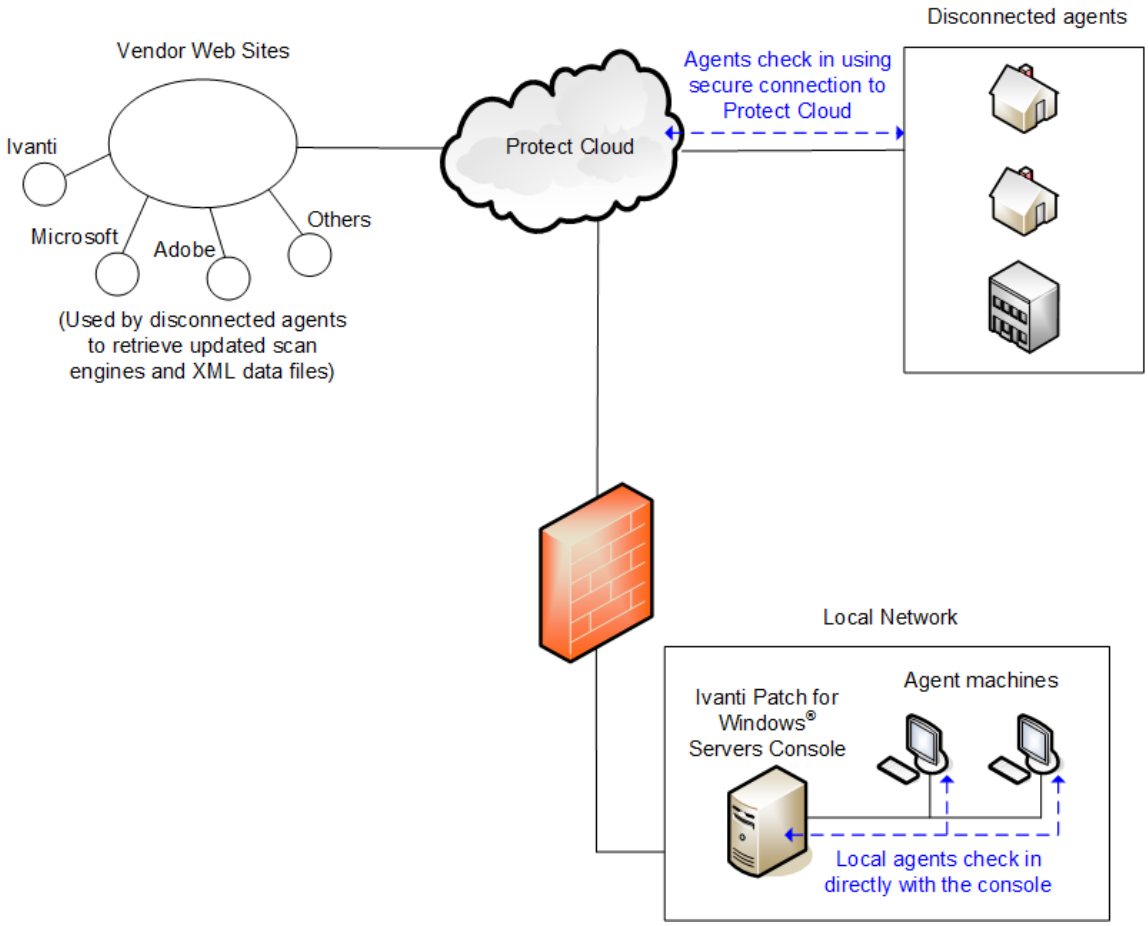
To view a video tutorial on this topic, click the video icon on the left.

The Protect Cloud synchronization feature enables your agents to check in and receive policy updates from the cloud. This allows you to manage agents on machines that are not able to communicate directly with the console. This feature also provides you with the ability to install a Ivanti Patch for Windows® Servers Agent using the cloud.

Agents that are configured to use Protect Cloud will have two check-in options: they can continue to check in with the Ivanti Patch for Windows® Servers console, but they will also be capable of checking in and receiving policy updates via the cloud. This is particularly useful for disconnected agent machines that are away from the corporate network and unable to contact the console for updates. As long as an agent machine has Internet access, it will be able to send results and get updates using the cloud.

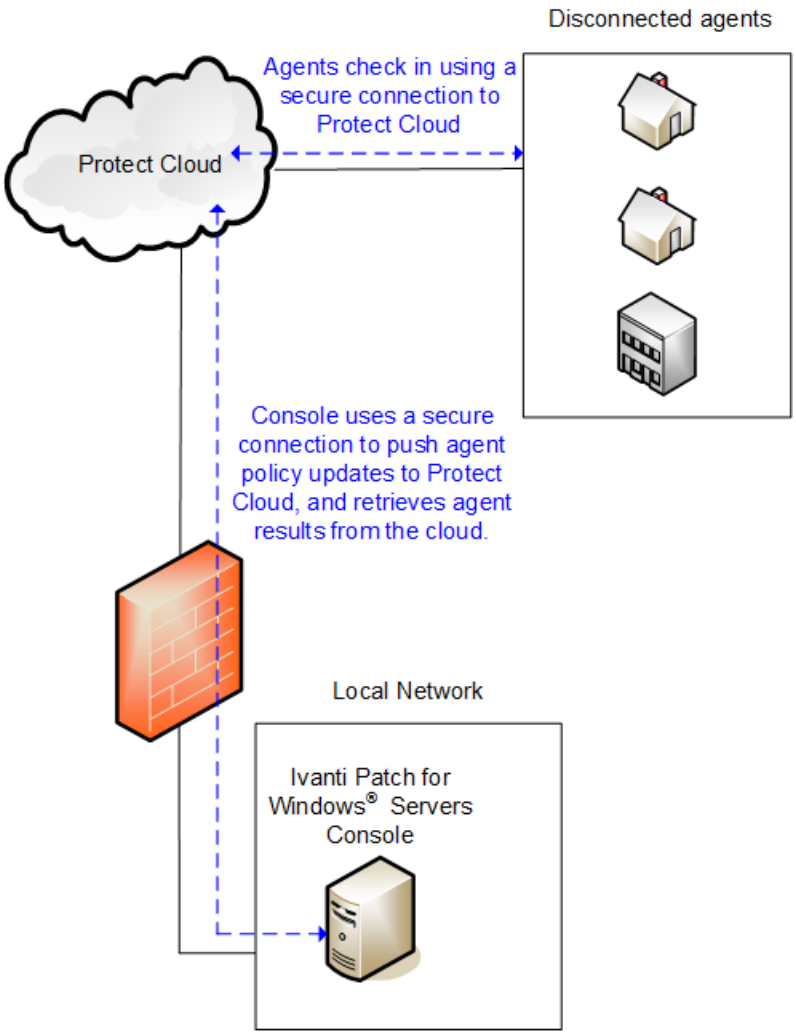
The following diagram illustrates the two agent check-in options:

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Protect Cloud Synchronization Requirements and Usage Notes



Requirements

- Must be running Ivanti Patch for Windows® Servers Standard orIvanti Patch for Windows® Servers Advanced
- Must have a Protect Cloud account
- Applies only to agents that are configured to use Protect Cloud synchronization
- The console must have a reliable Internet connection

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- Outgoing TCP ports 80 (http) and 443 (https) must be available when communicating with Protect Cloud
- The URL *protectservices.shavlik.com* must be accessible when communicating with Protect Cloud

Usage Notes

- When using Protect Cloud synchronization, the agent check-in process is as follows: At the scheduled check-in time, the agent will attempt to check in with the console. If the agent can access the console it will check in directly with the console. If the agent does not have access to the console but it does have Internet access, it will perform the check-in using the cloud.
- When a disconnected agent checks in with the cloud it reports the same information (scan results, etc.) that it would to the Ivanti Patch for Windows® Servers console. Protect Cloud provides a generous amount of storage to cache results until the consoles retrieves the data. The console will automatically retrieve data from the cloud several times every hour.
- Scan engines and XML data are not a part of the Protect Cloud synchronization process. Agents will continue to receive updated engines and XML data from either the console or the vendor websites. If an agent is using a policy that specifies the use of a distribution server, it is strongly recommended that you enable the **Use vendor as backup source** check box.
- A listening agent is treated no differently than any other agent. If a listening agent is on the local network and receives notice from the console that there is a policy change, it will receive the updated policy from the console. If a listening agent is away from the local network and unable to communicate with the console, it will perform its check-in using the cloud.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How to Enable Protect Cloud Synchronization

1. (Recommended) Select **Tools > Edit database description** and make sure that the name the program uses when referring to the console database is a friendly name that has some meaning or significance to other users.

   This is the name that will be displayed within Protect Cloud after you register the Ivanti Patch for Windows® Servers console. For more information on changing the name, see **Editing the Database Description**.

2. Select **Tools > Options > Protect Cloud Sync** and register the Ivanti Patch for Windows® Servers console with the cloud service.

   The registration process establishes a secure communication channel between the console and the specified Protect Cloud account. For details on the console registration process, see Protect Cloud Sync Operations.

3. In a new or existing agent policy, enable the **Sync with Protect Cloud** check box.

4. In the agent policy click **Save and update Agents**.

   A copy of the agent policy and all necessary components is written to the associated Protect Cloud account. You can view the steps in the policy synchronization process by viewing the Event History log.

   The next time your agents check in with the console they will receive an updated policy that allows them to use the cloud as a backup source for reporting information and receiving policy updates. This provides a layer of redundancy and is the primary benefit of using Protect Cloud synchronization.

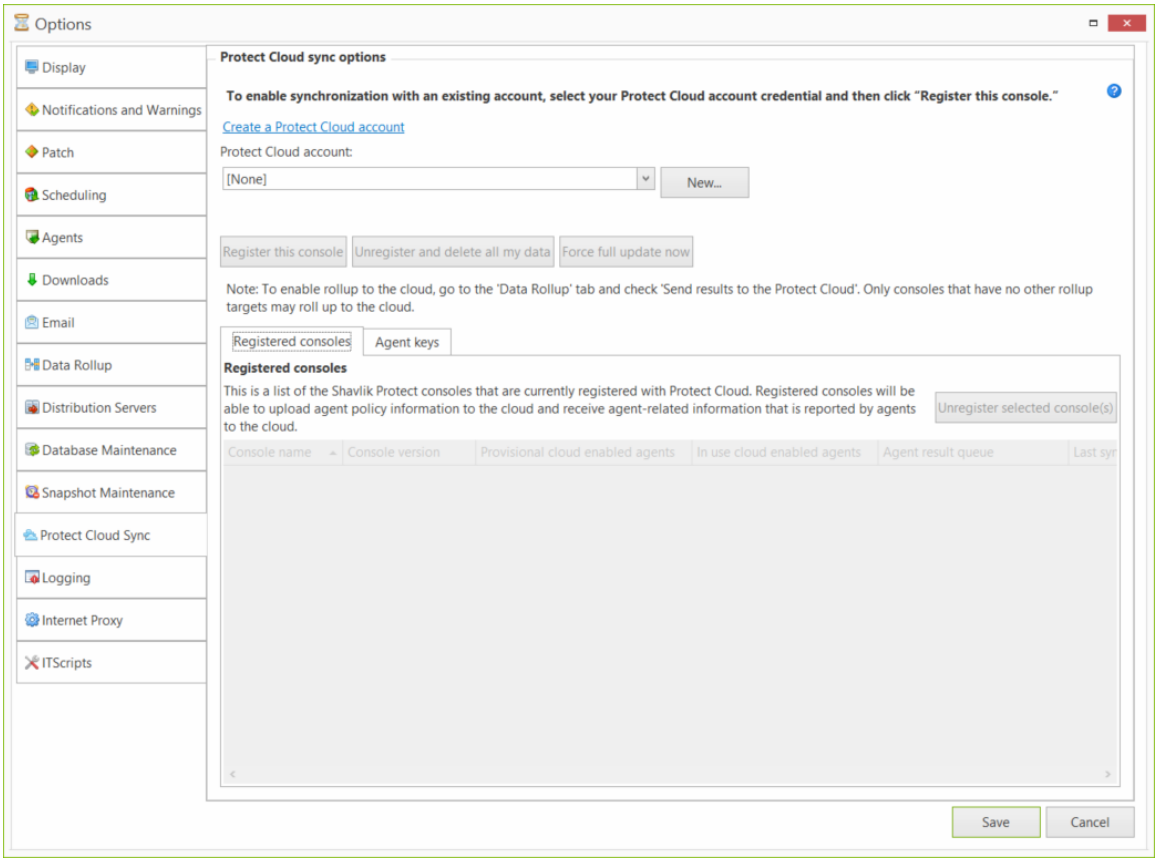
5. (Optional) If you are using multiple Ivanti Patch for Windows® Servers consoles, and if one of your consoles is using Protect Cloud synchronization and another is not, you can be notified of this situation by selecting **Tools > Options > Notifications & Warnings** and enabling the **Warn if Protect Cloud sync is not enabled on this console** check box.

   This is especially important if two or more consoles are sharing the same database. Each console that uses a Protect Cloud sync-enabled policy must be registered with Protect Cloud.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Protect Cloud Sync Options

The **Tools > Options >Protect Cloud Sync** tab is used to register your Ivanti Patch for Windows® Servers console with the Protect Cloud service. Registering the console is the first step you must perform when configuring and using the Protect Cloud synchronization feature. After the registration process is complete, the console will be able to upload agent policy information to the cloud service and it will be able to receive agent-related information that is reported to the cloud service by agents.



Create a Protect Cloud account	If you do not have a Protect Cloud account, you can create an account by clicking this link. You can configure your Ivanti Patch for Windows® Servers agents to use Protect Cloud as a cloud-based source for checking in and receiving policy updates.
Protect Cloud account	Select the credential (the user name and password pair) that you use to authenticate to your Protect Cloud account. If you have not defined your Protect Cloud credentials within Ivanti Patch for Windows® Servers, you can do so by clicking **New**. For more information, see Defining Credentials.

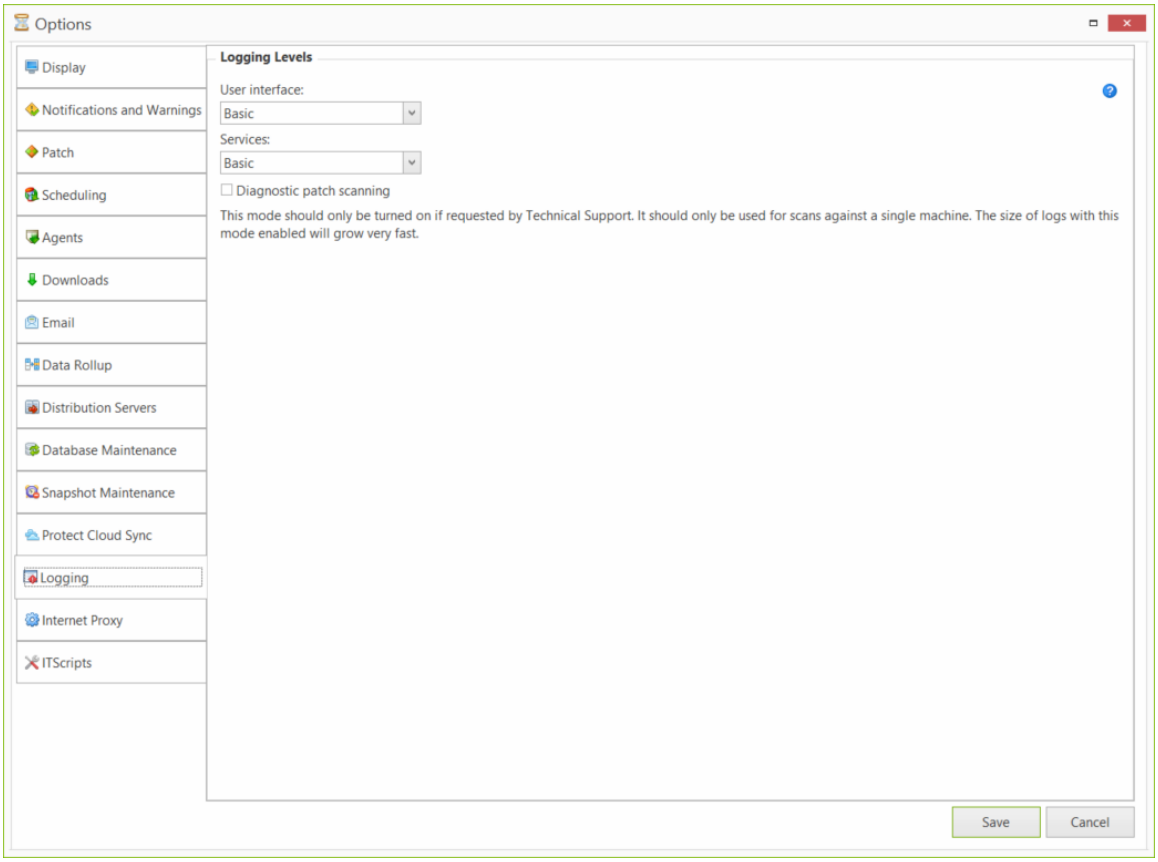
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Register this console	Uses the specified credentials to contact your Protect Cloud account and register the Ivanti Patch for Windows® Servers console. When the process is complete the message **This console is registered** is displayed. You can also find a record of the registration within Event History.
Unregister and delete all my data	Unregisters the console and deletes all policy and agent data that resides on Protect Cloud. IMPORTANT! Any agent that communicates with the console solely via Protect Cloud will be effectively orphaned and will eventually uninstall itself.
Force full update now	Initiates an immediate update of your Protect Cloud account. Current copies of all agent policies that are configured to use Protect Cloud are synchronized with Protect Cloud. You should perform this action only if you have a concern that the agent policy data contained on the cloud service is not up to date. Outbound port 443 must be available to complete this action.
Registered consoles / Agent keys	These two tabs show the console machines and agent keys that are being managed by Protect Cloud. For more information, see Installing Agents from the Cloud.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Logging Options

The **Logging Options** dialog allows you to specify how much data you want the program to record in the program logs.



Logging levels	Specify how much data you want the program to record in the program logs. You can specify different recording levels for user interface activity and for background services activity. For each category the options are: • **All:** Records all events in the log, including *Start*, *Stop*, *Suspend*, *Transfer*, and *Resume* events. • **Basic:** Records *Critical*, *Error*, *Warning*, and *Information* events in the log. This is the default value.
Diagnostic patch scanning	If enabled, captures a large amount of diagnostic data in order to troubleshoot patch scanning issues. IMPORTANT! Do not enable this check box unless directed by Technical Support.

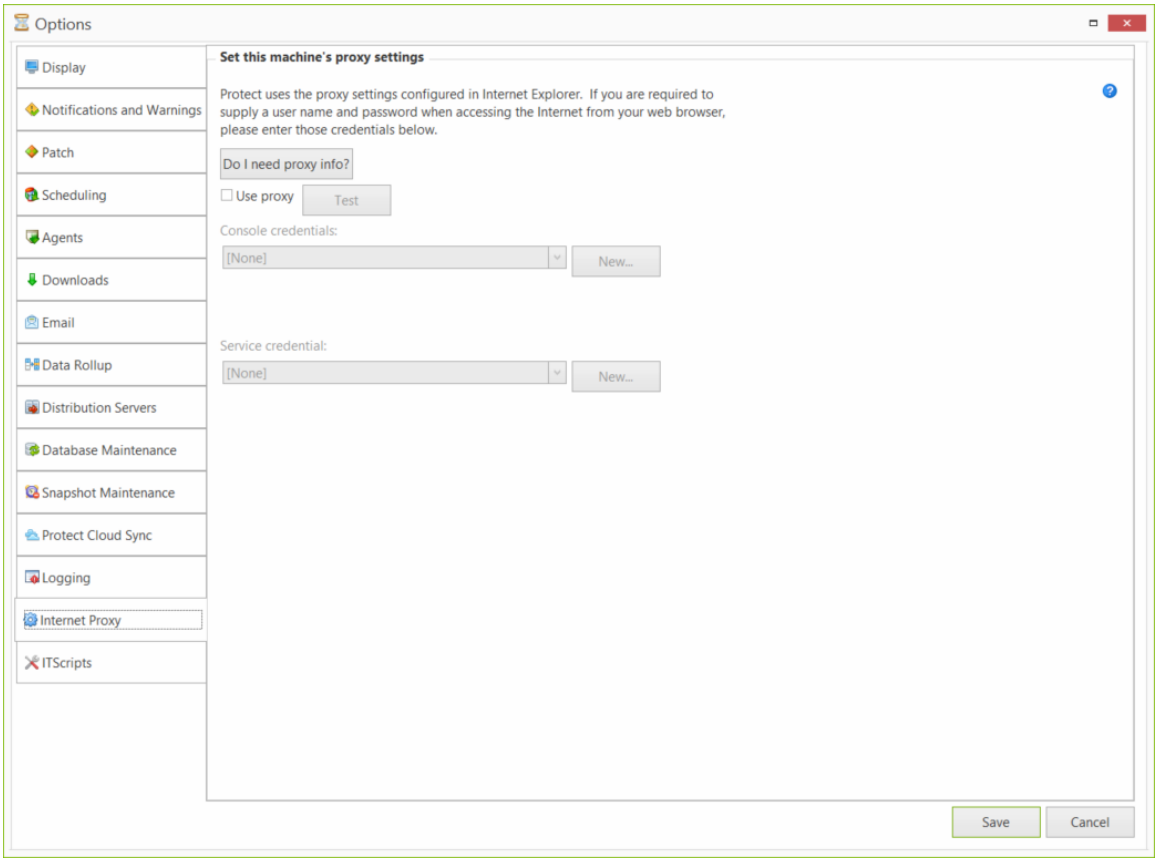
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Log file locations	The logs are located in the following directory on the console: **C:\ProgramData\LANDESK\Shavlik Protect\LogsC:\ProgramData\ScriptLogic Corporation\Patch Authority Ultimate\Logs** Several of the log files will include the administrator's name as part of the file name. This is especially useful when two or more administrators have access to the program.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Internet Proxy Options

The **Internet Proxy Options** dialog allows you to modify the proxy settings used by Ivanti Patch for Windows® Servers when accessing the Internet using your Web browser. In general, Ivanti Patch for Windows® Servers checks the proxy settings in Internet Explorer and conducts an Internet connectivity test to determine whether or not proxy server settings are necessary. If Ivanti Patch for Windows® Servers is unable to access the Internet using these settings, or if you are required to enter a user name and password each time you launch your browser and browse the Internet, you will need to configure the proxy options.



Do I need Proxy Info?	To see if Ivanti Patch for Windows® Servers can use your current Internet Explorer proxy settings to access the Internet and perform other operations, click this button. If the test is successful then nothing further is required. If the test fails it typically means you utilize authorization and you need to modify your proxy settings by specifying console and service credentials.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

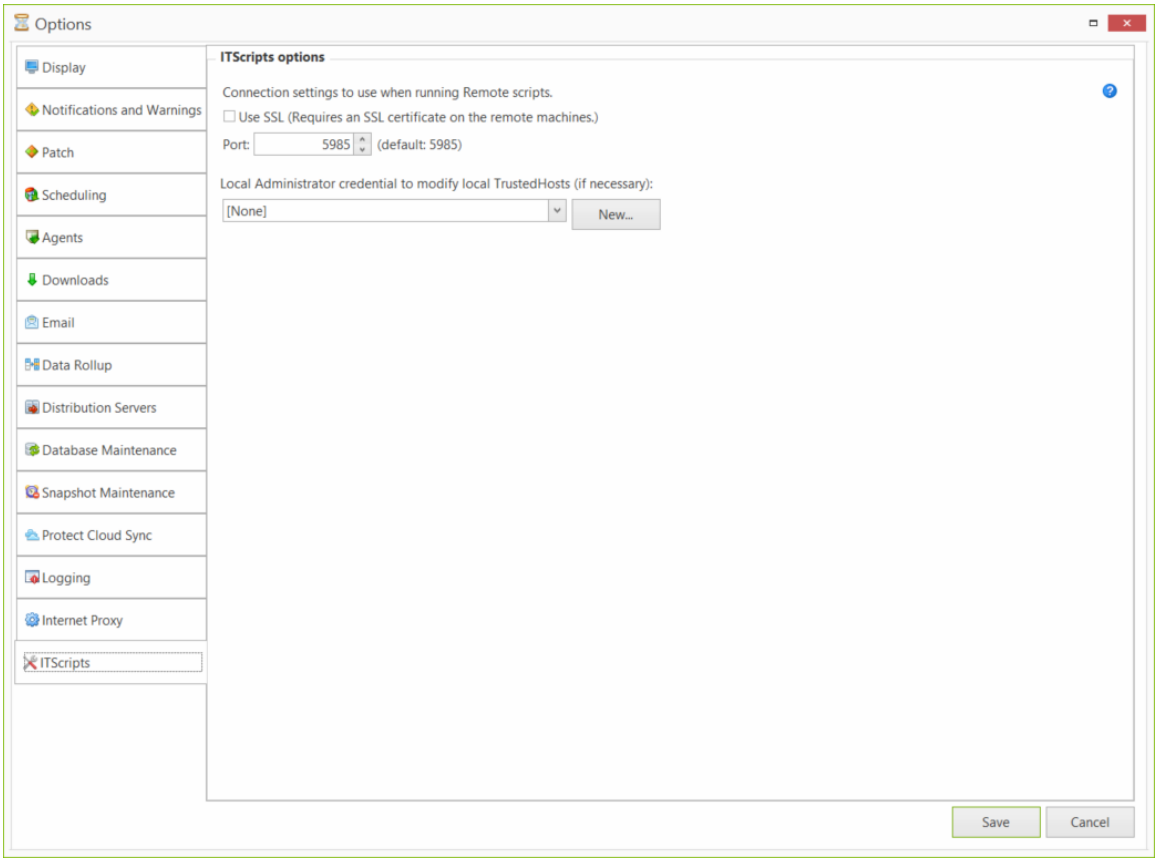
Use proxy	If enabled, indicates that you will supply proxy credentials and allows you to specify user name and password information. If you clear the check box after specifying credentials, the credentials will be saved but not used.
Console credentials	Select the credential (the user name and password pair) you use when accessing the Internet with your Web browser. It may be necessary to specify a domain as part of your user name (for example: mydomain\my.name). There may be multiple credentials available here for selection, one for each of your Ivanti Patch for Windows® Servers administrators.
Service credentials	Select the credential (the user name and password pair) used by the program service when accessing the Internet. The same service credential can be used by different administrators. Only shared credentials are contained in this list. If the credential you are looking for is not listed it probably means it is not defined as a shared credential. See Defining Credentials for information on how to share a credential.
Test	To test the credentials, click this button.

IMPORTANT! See HTTP Proxy Post Installation Notes for additional details about using an HTTP proxy.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

ITScripts Options

The **ITScripts Options** dialog enables you to specify how the console will connect with target machines when running scripts using WinRM (PowerShell remoting).



Use SSL	If you want the console to contact the target machines using an SSL connection, enable this check box. In addition, each target machine must contain a signed certificate and a WinRM HTTPS Listener. For more details see ITScripts Requirements.
Port	Specifies the port used by the console when contacting the target machines. The default value is as follows: • If you are NOT using SSL the default value is 5985 • If you ARE using SSL the default value is 5986

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Local Administrator credential to modify local TrustedHosts	Only shared credentials are contained in this list. If the credential you are looking for is not listed it probably means it is not defined as a shared credential. See Defining Credentials for information on how to share a credential.
	
	Select the credential (the user name and password pair) to use if it is necessary for Ivanti Patch for Windows® Servers to temporarily add a target machine to the console's TrustedHosts list when executing a WinRM script.
	
	Here's why this might be needed. The WinRM services establish trust with one another in one of three ways: (1) Kerberos (on domains), (2) trusted certificates (SSL / HTTPS transport), or (3) the target machine appears in the console's TrustedHosts list. If you are not using Kerberos or HTTPS and want to execute scripts that require remoting, you must supply a credential with administrative privilege in order for Ivanti Patch for Windows® Servers to be able to temporarily access and modify the console's TrustedHosts list.
	
	This is generally necessary only if the console is part of a workgroup rather than a domain. In this case, it is also necessary that the TrustedHosts list on the console contains the name of the computer that the console is running on. You can make this one-time change by entering the following command at a PowerShell prompt when logged in as an administrator:
	
	`Set-Item WSMan:\localhost\client\TrustedHosts <console_name>`
	
	You can verify the value of TrustedHosts by entering the following command:
	
	`Get-Item WSMan:\localhost\client\TrustedHosts`

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Email Overview

The email feature enables you to send email alerts and messages to specified users. This feature has a wide range of applications. You can send scan results and scan reports and you can notify users of pending actions such as patch deployments and reboots.

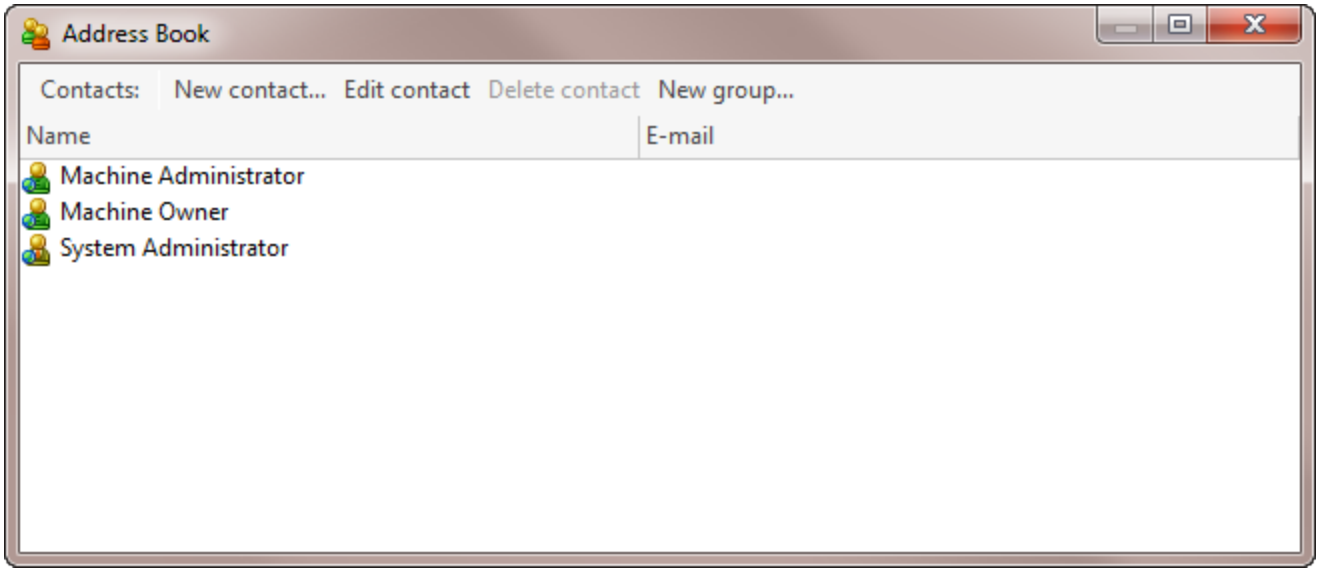
The email capability is very easy to use. You simply:

- Define your email contacts in the local Address Book
- Define the SMTP server used for email
- If necessary, specify the credentials required to send email messages
- Use the icons in the program interface to send messages to specified recipients as needed

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Populating the Address Book

The address book is used to store the email addresses of those users you want to send messages or alerts. You can also define one or more email groups. To add, delete, or modify the contents of the address book, select **Manage > Address Book**. The **Address Book** dialog is displayed.



The address book initially contains default entries for the machine administrator, the machine owner, and the system administrator. More than one contact can be defined as a system administrator.

Defining a New Contact

1. Click **New Contact**.
2. Type the name of the contact as you want it to appear in the address book.
3. Type the email address of the contact.
4. If you want the contact to receive messages that are automatically sent to all system administrators, enable the **System Administrator** check box.

Defining a New Email Group

1 Click **New Group**.

2. Type the name of the group you want to create.
3. To populate the group, enable the desired check boxes in the list of available contacts and then click **Save**.
   - If you want to add every contact in the list to the group, click **Check All**.
   - If you want to define a new contact, click **New Contact**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Deleting an Existing Contact or Group

1 Select the contact or group you want to delete.

You can select multiple entries at one time by pressing and holding the **Ctrl** key while you select each entry.

2. Click **Delete**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Automatically Sending Email Reports and Notifications

This feature applies only to agentless scans and deployments initiated from the console; it does not apply to agents that may also be using this template.

Messages containing scan reports or deployment reports can be automatically emailed by Ivanti Patch for Windows® Servers. You simply configure the scan template, the deployment template, the machine group, or the machine of your choosing so that reports are automatically sent each time the template or group is used. You can designate which reports should be sent and to whom the reports should be sent.

In order to use this feature you must enable email operations.

Templates

You can configure scan templates to automatically:

- Send PDF versions of reports upon completion of a scan

You can configure deployment templates to automatically:

- Notify users of pending patch deployments
- Send a report upon completion of a deployment

For information on configuring templates to automatically send email reports:

- **Scan templates**: Please see Creating a New Scan Template and Creating a New Asset Scan Template.
- **Deployment templates**: Please see Creating a Deployment Template.

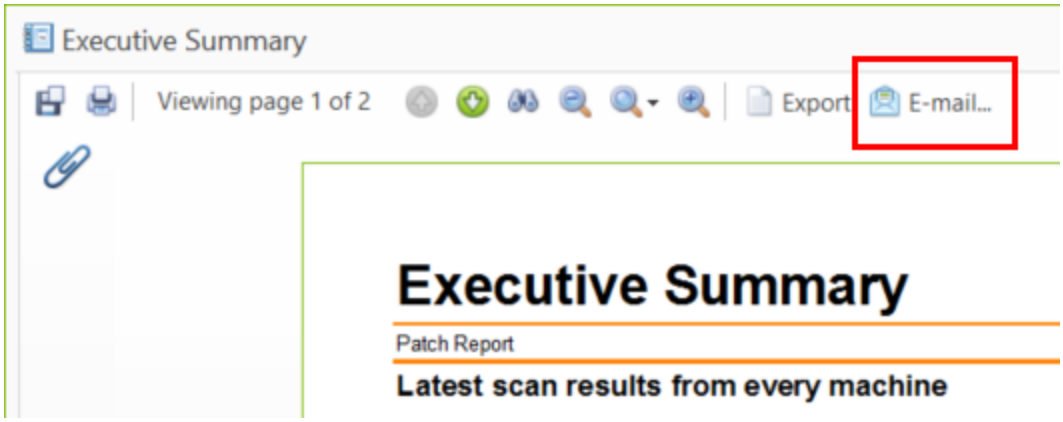
Machines and Machine Groups

For information on configuring the program to automatically send email reports when individual machines are scanned, see Managing Individual Machine Properties. For information on configuring a group of machines to automatically send email reports when the machine group is scanned, see Working With A Machine Group.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Manually Sending Email Reports and Notifications

While viewing a report you generated, you can email the report by clicking the **E-mail** button. This button is only available if you have enabled email operations.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Using Disconnected Mode

If a Ivanti Patch for Windows® Servers console is in disconnected mode it means it will not attempt to download newer definition files (scan engines and XML data files). Disconnected mode is typically used by sites that require the use of fixed versions of data that have been approved for use. Disconnected mode is also useful if your security policy requires you to perform scans and deployments without downloading data files from the Web.

There are two ways to put the console into disconnected mode:

- Select **Tools > Auto-update definitions** and make sure the command is not enabled
- Select **Tools > Options > Downloads** and then clear the **Auto-update definitions (before scans)** check box

When the console is in disconnected mode the data files already resident on your local machine will be used during all scans and deployments. See Managing Data Files for more information.



Putting a console into disconnected mode does not necessarily mean that the console is disconnected from the Internet. That is a different scenario and is described in What is a Disconnected Console Configuration?. Also, disconnected mode has nothing to do with patches. If you are connected to the Internet or a designated distribution server, the console will download required patches even if **Auto-update definitions** is disabled.

Be Careful if Your Site Uses Agents

If you use agents you must be careful when putting your console into disconnected mode. If an agent contains newer definition files than the console, and that agent tries to report new results to the console database, the console will reject the updates. If this happens you will need to manually download new definition files and copy the files to the console's *\DataFiles* directory. If you are using a distribution server you must then manually synchronize the console with the distribution server.

To prevent this issue from happening in the first place, make sure your agents get their definition files from a distribution server and that the files on the distribution server exactly match the files being used by the console.

Possible Issue with .NET Framework Prerequisite

When you run in disconnected mode the console may not detect that the full version of .NET Framework is available. See Installing the Prerequisites for a link to use to download the full version of .NET Framework.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Managing Data Files and Missing Patches in Disconnected Mode

When running in disconnected mode it is necessary to manually manage your data definition files. You can do this two different ways:

- **If your console has an Internet connection:** Select **Help > Refresh files**. This will download the most current versions of the XML files and the command files used by the program.
- **If your console does not have an Internet connection:** You must use a machine with Internet access to download the data files and then transfer the files to the Ivanti Patch for Windows® Servers console. To determine the locations currently being used as the source for the scan engines and data definition files, select **Tools > Options > Downloads**.

Data File Locations

The data files need to be located in the following directory on the Ivanti Patch for Windows® Servers console: **C:\ProgramData\LANDESK\Shavlik Protect\Console\DataFilesC:\ProgramData\ScriptLogic Corporation\Patch Authority Ultimate\Console\DataFiles**

Downloading Missing Patches

Before you can deploy missing patches you must locate and transfer the missing patches to the disconnected console.

1. Use Machine View to view the list of missing patches.
2. Export the list of missing patches to a .csv file by right-clicking **Patch Missing** and selecting **Export selected patches to CSV**.

   You can use the .csv file as a reference when downloading the patches from an Internet-facing console. Another option is to generate a report that lists the missing patches.
3. On an Internet-facing console, use the Patch View smart filters to locate the patches that are missing on the disconnected console.
4. Right-click the patches and download them to the Internet-facing console.

   The downloaded patches are stored in the following directory: **C:\ProgramData\LANDESK\Shavlik Protect\Console\PatchesC:\ProgramData\ScriptLogic\Patch Authority\Patches**
5. Copy all the files in this folder to a media that can be transported to the disconnected console.
6. Copy all the files to the same folder on the disconnected console.

The disconnected console can now deploy patches to the inside machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Available Reports

The following reports are available in Ivanti Patch for Windows® Servers. The reports you have access to is dependent upon your current license level.

For information on using Ivanti Patch for Windows® Servers database views to generate your own custom reports, please see the *Ivanti Patch for Windows® Servers* Report Views Guide at www.ivanti.com/en-US/support/product-documentation*Ivanti Patch for Windows® Servers*Report Views Guide at http://www.landesk.com/support/documentation/.

To choose a report, select **Tools > Create report** from the main menu and then select a report from the drop-down list at the top of the Report Gallery dialog. The list is divided by the different types of security programs available within Ivanti Patch for Windows® Servers.

Security Program	Report	Description
Patch Reports		
	Seat License Status	This report provides information about the number of license seats available and the number of seats used. There is no filtering capability for this option.
	Machine/OS Listing	This report lists the operating systems for each machine scanned.
	Condensed Patch Listing	A concise, six-column report displaying the machine name and patch status for each scanned host. Patch items are displayed as bulletin numbers (MS00-000).
	Deployment Detail	This report provides detailed information about a particular patch deployment.
	Deployment Percentage by Patch	This report displays the percentage of machines that have each patch installed. The percentage is based on the number of machines that require the patch.
	Deployment Status by Deployment	This report provides information about the success or failure of one or more specified patch deployments.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	Deployment Status by Machine	This report provides information about patch deployments made to one or more specified machines.
	Detailed Summary	This report shows a summary of the scan, plus it provides a list that shows each machine that was scanned and detailed information about each machine.
	End-of-Life by Product	This report shows all detected end-of-life products and the machines that have them installed.
	Executive Summary	This report provides a high-level summary about the patches and the machines discovered by the scan.
	Machine Inventory	This report provides a complete list of all software products installed on each machine discovered by the scan.
	Machine Status by Patch Count	This report displays the number of machines in groups based on the number of missing patches.
	Machine Status Summary	This report provides the patch status of each machine discovered by the scan.
	Machines by Patch	Displays patch status for each machine sorted by Bulletin ID and QNumber.
	Machines Not Scanned	This report lists all machines not scanned and the reason they were not scanned.
	Missing SP	This report is a quick overview of all machines that are missing service packs for supported products. This report skips the simple criteria filter and displays the advanced criteria filter immediately.
	Patch Annotation Information	This report lists all patch annotations.
	Patch Listing	A concise listing (one line per patch processed) of all patches for all scanned machines sorted by 'Missing', 'Found', 'Informational' and 'Warning', then sorted by user preference.
	Patch Status Detail	This report provides detailed information about each patch discovered by the scan.
	Patch Status Summary	This report provides a descriptive summary about each patch discovered by the selected scan(s). The report includes both found and missing patches. Use the Next Page and Previous Page icons to navigate through the report.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	Patches by Machine	Displays patch status for each machine sorted by machine name.
	Patches by Machine Detail	A detailed listing of every patch found sorted by machine name. For each patch, the entire summary and reason is listed in the report. Note that this report can take very long if executed against thousands of computers.
	Top Ten Missing Patches	This report lists the ten patches that are missing the most often.
	Top Ten Vulnerable Machines	This report lists the ten most vulnerable machines discovered by the program during the selected scan(s). The machines with the most missing patches and service packs are judged to be the most vulnerable.
	Machine Compliance (IAVA)	(Available only if you have a Government Edition of Ivanti Patch for Windows® Servers.) This report gives IAVA machine compliance information.
	Machine Non-Compliance (IAVA)	(Available only if you have a Government Edition of Ivanti Patch for Windows® Servers.) This report gives IAVA machine non-compliance information.
	Deployment Percentage by Patch (IAVA)	(Available only if you have a Government Edition of Ivanti Patch for Windows® Servers.) This report displays the percentage of machines that have each patch installed. The percentage is based on the number of machines that require the patch.
	Detailed Summary (IAVA)	(Available only if you have a Government Edition of Ivanti Patch for Windows® Servers.) This report gives a detailed scan summary.
	Machine Status by Patch Count (IAVA)	(Available only if you have a Government Edition of Ivanti Patch for Windows® Servers.) This report displays the number of machines in groups based on the number of missing patches.
	Patch Status Detail (IAVA)	(Available only if you have a Government Edition of Ivanti Patch for Windows® Servers.) This report gives detailed patch status information.

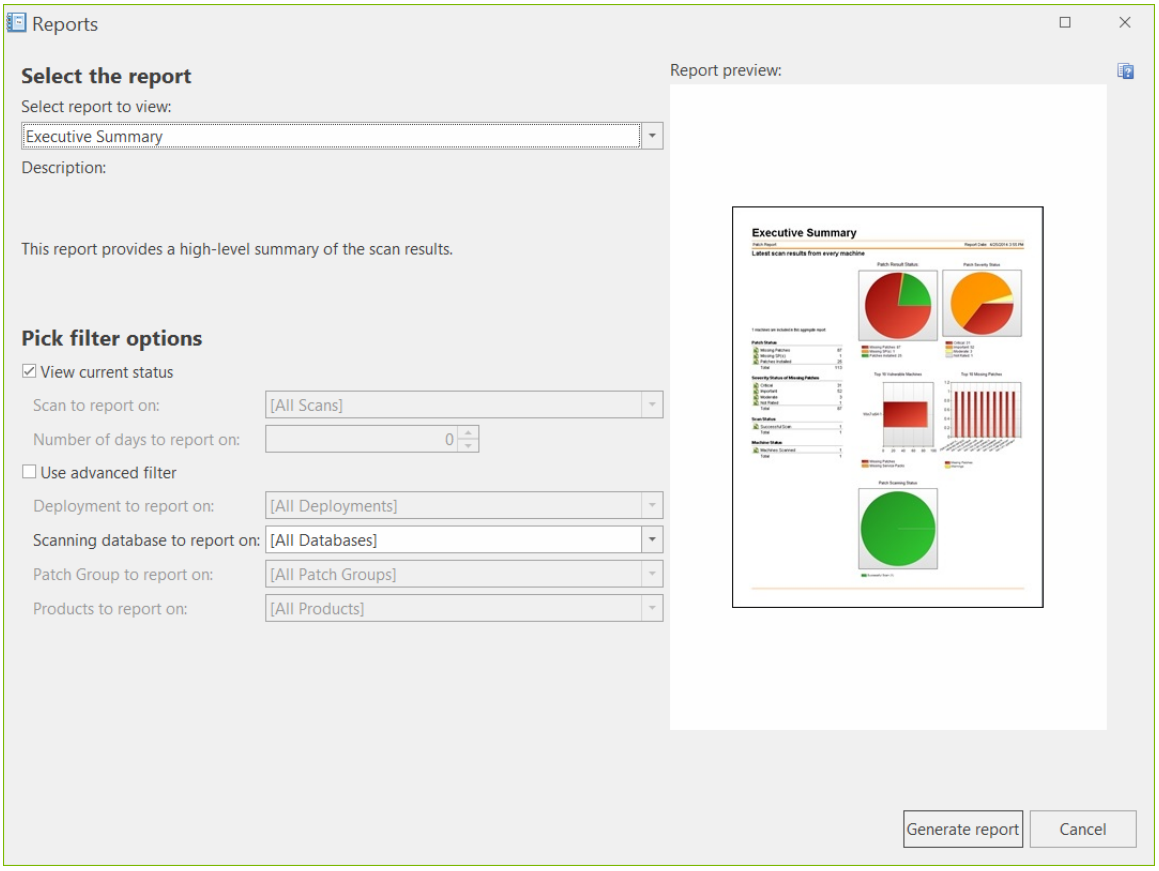
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Asset Reports		
	Software Catalog Report	This report provides a list of all software installed on the scanned machines. The version number and install count information is displayed for each software product that is detected. If multiple versions of a product are detected, the machines using a particular version are listed in multiple columns.
	Machine Hardware Detail Report	This report provides a detailed list of hardware assets on each machine.
	Machine Software Detail Report	This report provides a detailed listing of software installed on each machine.
Power Status Reports		
	Power Status Report	This report provides a list of machines and their power state at a specific time. The report is organized by machine group.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Reports Dialog

The **Reports** dialog is designed to provide you with an assortment of different report filtering options. You can open the **Reports** dialog using the **Tools > Create report** menu. The **Reports** dialog consists of a single dialog in which you make all of your selections.



Pick a Report

Use the **Select report to view** box to select which report you want to generate. When you select a report from the list, the description of that report is displayed and a sample of the report is displayed on the right side of the dialog.

Pick Filtering Options

Ivanti Patch for Windows® Servers's reporting utility includes powerful filtering options. Depending on the report you choose, you have choices between basic and/or advanced filtering options.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- If you want the report to contain information from the most recent scan of each machine managed by the console (and of each machine managed by the associated remote consoles, if this is a data rollup console), enable the **View current status** check box. Not all reports allow the use of this check box. Enabling this check box will make the **Scan to report on** option unavailable.
- The basic filtering options allow you to choose which deployments, which scanning databases, which patch groups, and what products would you like to report on.
- If you need even more granularity or different sorting options, enable the **Use advanced filter** check box. The advanced filter options are presented in a separate dialog when you click **Generate Report**.

View the Report

Once you have made your selections, click **Generate Report** to see the results. If the **Use advanced filter** check box is enabled this will cause the **Advanced Report Settings** dialog to appear; the report will be generated after you specify your advanced filtering options.

Scheduling a Report

If you want to schedule a report to run at some time in the future, select **Tools > Schedule report**. A scheduled report can be generated once or on a recurring basis. See How to Schedule a Report for more information.

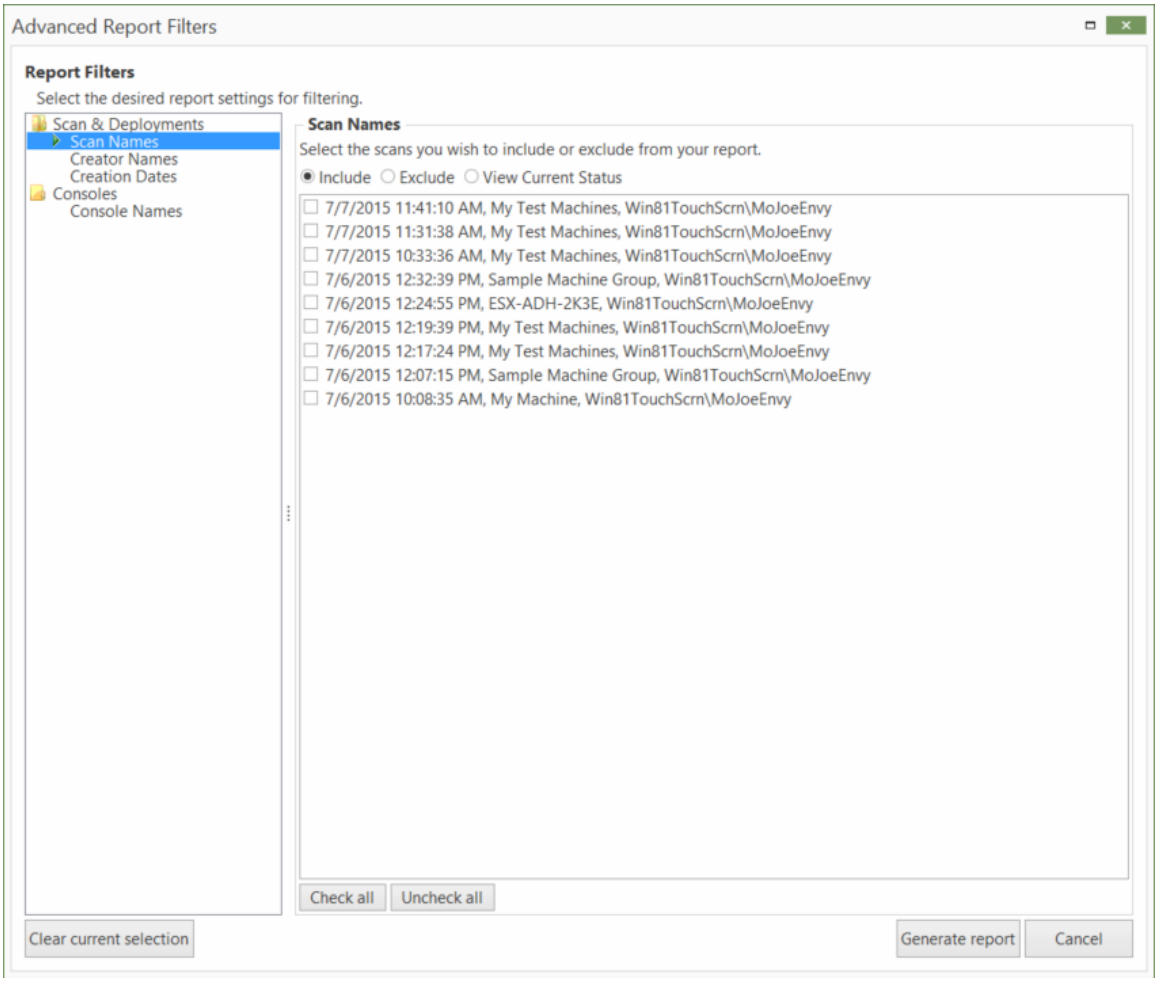
Generating a Report from a Data Rollup Console

If a console is a data rollup console, in addition to containing information about each machine it manages, it will also contain information about all the machines managed by the associated remote consoles. The information sent by the remote consoles and collected by the data rollup console is stored in an *aggregate database*. When you generate reports from the rollup console you automatically have access to all the information contained in the aggregate database.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Advanced Filtering

The **Advanced Report Settings** dialog enables you to effectively drill deeper into your scan and deployment results and extract more meaningful information. It does so by enabling you to select exactly which information you want to include in the report.



To use the **Advanced Report Settings** dialog:

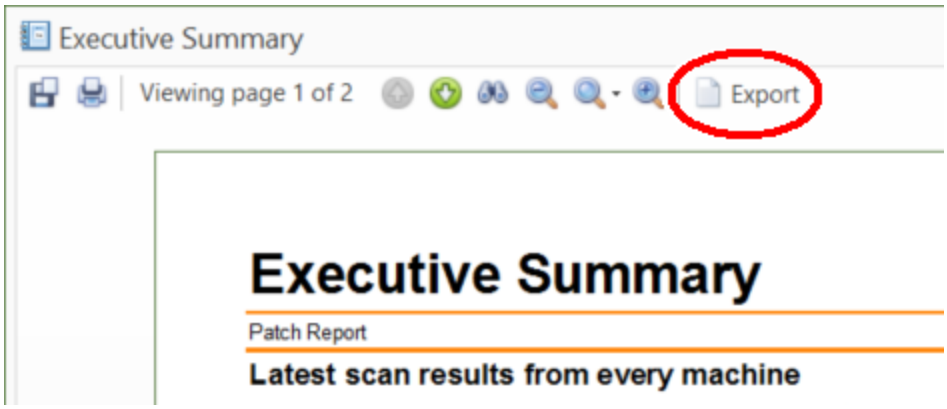
1. Select each of the available options one at a time from the list on the left and on the right-hand side specify the items you want to include or exclude.
2. When you are ready to generate the report, click **Generate report**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Exporting Reports

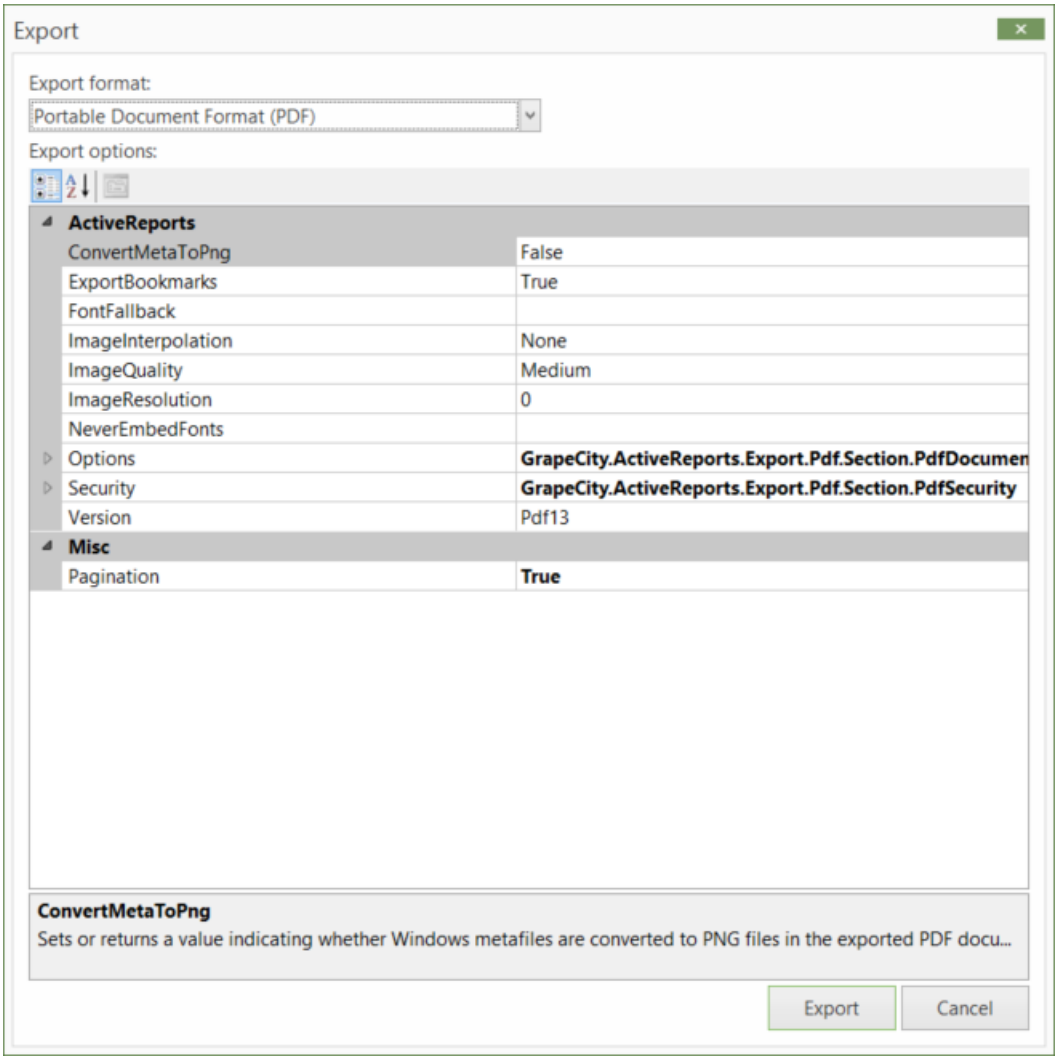
After a report is generated, it can be exported to a different format from the report viewer.

1. Click **Export** on the toolbar.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

The **Export**dialog is displayed.



2. Select the export format and any available options and then click **Export**.

   The **Save As** dialog appears.

3. Specify the name and location of the report file and then click **Save**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

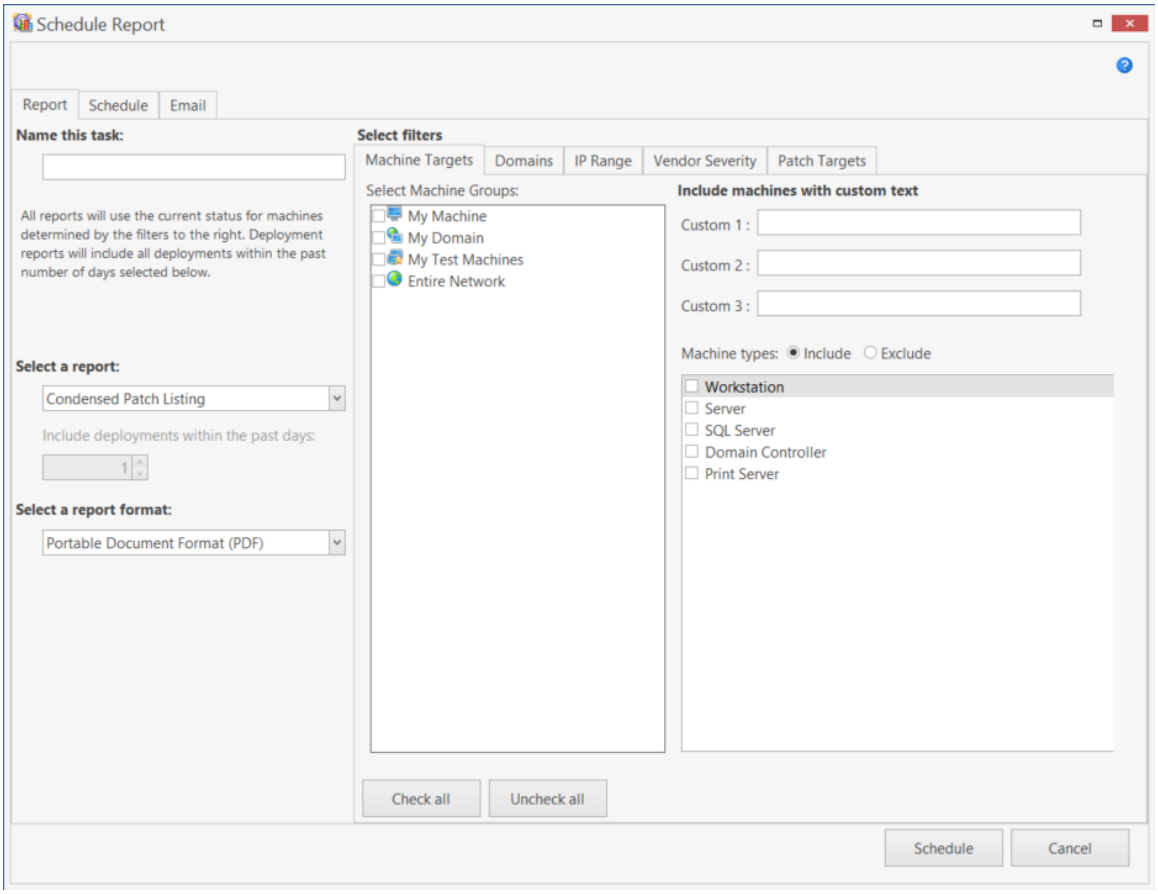
How to Schedule a Report

The **Schedule Report** dialog enables you to automatically generate a report at some time in the future. The report can be automatically generated once or on a recurring basis. The report content will be based on the last known status of the machines (as determined by the latest scan).

The generated reports can be found here: **C:\ProgramData\LANDESK\Shavlik Protect\Console\TempReports**. In addition, the reports can also be sent as an email attachment to one or more recipients.

How to Access the Scheduling Dialog

To schedule a report select **Tools > Schedule report**. The **Schedule Report** dialog is displayed.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Report Tab

This tab enables you to specify which report you want to generate and what file format to use when saving the report. This tab also provides several powerful filtering options that enable you to specify the exact information you want to include in the report. The filtering options that are available will vary depending on the report you choose. If you do not specify any filtering options, the report will contain information on all of the machines detected in the latest scan.

Name this task	The name that you wish to assign to the task that will generate the scheduled report.
Select a report	Select the report that you want to generate. The filters that are available in the right pane will change depending on which report you select.
Select a report format	The report will be generated in the format you choose.
Machine Targets tab	Use this tab to specify which machines you want to include in the report. You can specify filtering criteria in any or all of the available areas. • **Select Machine Groups:** You can select one or more existing machine groups. • **Include machines with custom text:** If you have provided custom notes about the properties of your machines, use this filter to specify which of those machines are included in the report. All machines not containing the specified custom text will be excluded from the report. • **Machine types:** You can include or exclude specific machine types. **Example:** If you select **Entire Network** in the **Select Machine Groups** area and **Server** in the **Machine types area**, only the server machines in your network will be included in the report. **Example:** If you select **Entire Network**, specify **St. Paul** in the **Custom 2** box, and **Server** in the **Machine types** area, only the server machines located in the city of St. Paul will be included in the report.
Domains tab	Select the domains that you want to include or exclude from the report. Only those domains that have been detected by previous scans are available for selection.
IP Range tab	Specify the starting and ending IP addresses of the target machines you want to include or exclude from the report.
Vendor Severity tab	Specify the vendor severity level(s) of the patches that you want to include or exclude from the report. The vendor severity is assigned to each patch by Ivanti based on the perceived threat of the vulnerability related to the patch.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Patch Targets tab	Select the patch groups that you want to include or exclude. Only those patch groups that you have previously defined are available for selection. In addition, you can specify the patch status(es) that you want to include or exclude. The patch status is the current status of a patch on a target machine. You can specify a patch status without specifying a patch group (and vice versa).

Schedule Tab

Use this tab to specify when you want the report to be generated. The report must be scheduled at least five minutes in the future.

Once	If you only want to generate the report once at some date and time in the future, choose this option. Click in the box to select the date that you want to generate the report. The time will automatically default to the current time. Click in the box to manually change the time to the desired value.
Recurring	If you want to generate the report on a recurring basis, choose this option. Use the day and time boxes to specify when the report should be generated. The **Add delay (days)** box (available if you generate a report on a monthly basis) allows you to delay the generation of the report by up to 20 days. For example, you might use this to schedule a monthly report that is always generated four days after Patch Tuesday. You do this by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by four days.

Email Tab

Use this tab to specify who will receive the report as an attachment in an email message.



You must configure the SMTP server in order to send an email message. See Email Operations for details on configuring the server.

Email subject	Specify what should appear in the subject line of the email message.
Select recipients	Select the groups and/or individuals you want to receive the report. You can define new groups or contacts if needed.

Scheduling the Report

Once you have made your selections, click **Schedule** to schedule the report. You can view the scheduled report task by selecting **Manage > Scheduled Console Tasks** and then selecting the **Reports** tab.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

If scheduled credentials are not currently assigned the **Scheduled Console Scans/Operations Credential** dialog is displayed. You must assign a shared credential to perform a schedule action. You can use the **Set scheduler credential** button on the **Scheduled Console Tasks** dialog to view and modify which credential is being used as the scheduler credential.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Why Use Multiple Consoles?

Organizations with many office sites located across the country may choose to maintain multiple Ivanti Patch for Windows® Servers consoles. One console is typically deemed the *central* console. The central console will typically reside at a central site, such as your company headquarters. Each remote office site will contain a *remote* console. Each remote console is responsible for performing scans and patch deployments on the machines in their local network and for rolling up the results of these actions to the central console.

The central console can be thought of as a *Central Policy Manager*. It is the console capable of tracking the results of actions performed on all the other consoles. Likewise, a remote console can be thought of as a *Distributed Policy Manager*. It is responsible for enforcing your organization's patch policies at remote locations. By adding a distribution server into the mix you can implement a *Distributed Policy Service*. The distribution server can be used to store the XML data files that effectively represent your organization's policy. The files are downloaded and used by the remote consoles, thus implementing your policy.

There are several additional advantages to maintaining multiple consoles:

- The consoles can reside at physically distinct locations and be close to the machines they are managing
- You can distribute the workload across multiple consoles
- The scans and deployments are performed much quicker
- You won't tie up your network trying to scan hundreds of geographically distinct machines from one location
- It cuts down on a lot of network traffic, especially over WANs (which can be expensive)
- The results from each console can be rolled up to and viewed from one central location

There are many possible multiple console configurations, from a basic data rollup configuration to an advanced configuration that combines multiple consoles with Ivanti Patch for Windows® Servers Agent. Each of these multiple console configurations is described in detail in the following sections:

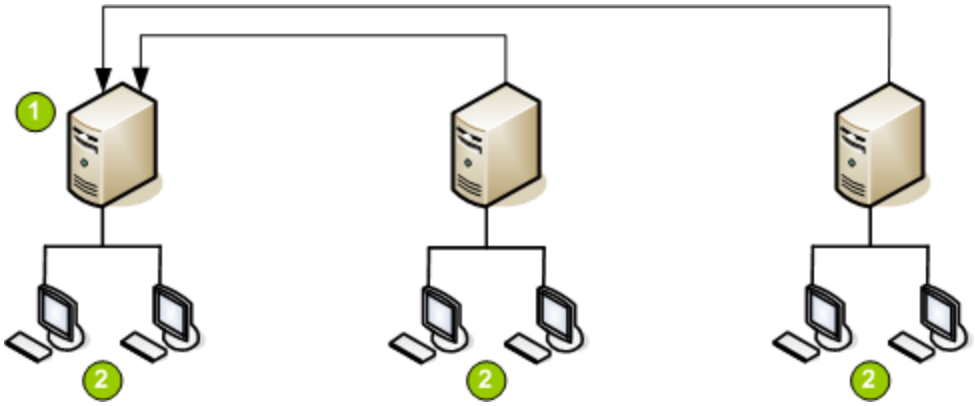
- What is a Data Rollup Configuration?
- What is an Unattended Console Configuration?
- What is a Disconnected Console Configuration?

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

What is a Data Rollup Console Configuration?

In a data rollup console configuration, one console acts as the central console. In addition to receiving scan and deployment data from the machines it manages, the central console also receives data about machines managed by other consoles. The central console is therefore also known as the *rollup console* because the data from all the other consoles is rolled up to it. This enables you to track what is happening throughout your organization from one central site.

The following figure illustrates a data rollup console configuration.



1	Rollup console
2	Managed machines

For more information, see Implementing a Data Rollup Configuration.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Implementing a Data Rollup Configuration

Implementing a data rollup console configuration is very easy. You simply perform a few configuration steps on the central console and on each remote console.

If your SQL Server does not run on the same machine as the Ivanti Patch for Windows® Servers console, you will need to run Ivanti Patch for Windows® Servers with user credentials that have access to SQL Server. For more detailed information see SQL Server Notes.

On the Central Console

1. Select **Tools > Options > Data Rollup**.
2. In the **Data Rollup Receiver Configuration** area, enable the **Accept and import results from a rollup sender** check box.

On Each Remote Console

You must configure each remote console to roll up its results to the central console.

1 Select **Tools > Options > Data Rollup**.

2. In the **Data Rollup Sender Configuration** area, enable the **Enable Data Rollup** check box.
3. Specify the IP address/hostname of the central (rollup) console and the port used by the rollup console to listen for incoming data.
4. In the **Minutes between sending results** box specify how often the data will be rolled up from the remote console to the central console.
5. Click **Register**.

TIP: The registration process will also automatically generate an entry in the **Edit Database Description** dialog on the central console. You can use this dialog to track how many remote consoles are configured to roll up their results to the central console. See Editing the Database Description for more details.

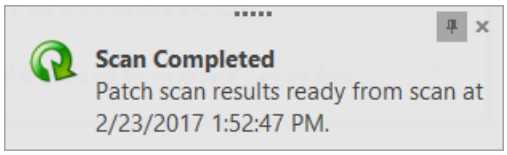
See Data Rollup Operations for more detailed configuration information.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Watching For Data Rollup Activity

A notification dialog box is displayed in the lower-right corner whenever a remote console rolls data up to the central console. The dialog box will be displayed for several seconds before slowly fading away. You can pin the dialog box in place by clicking the pin icon. If you are viewing results, the display will not be automatically updated when new results arrive. In order to see the new information related to the data rollup, you can click the notification dialog box or you can select **View > Refresh** from the main menu.

Notification dialogs are not displayed if Ivanti Patch for Windows® Servers is not running on the console machine.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

What is an Unattended Console Configuration?

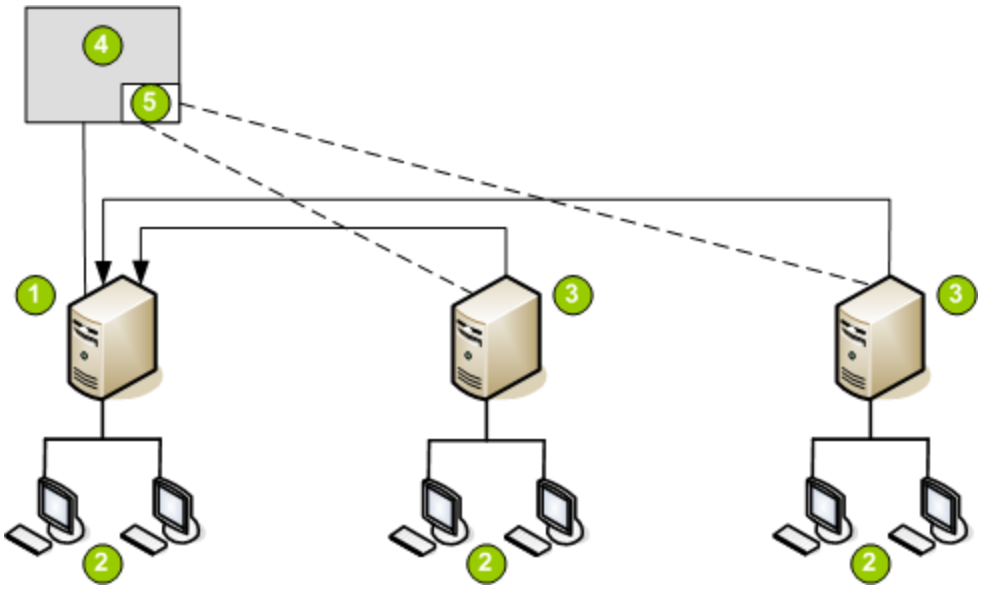
An unattended console is a console you set up once. After that the console automatically updates its own files and manages its machines without human assistance.

Here's how it works: The unattended console is configured to automatically perform periodic scans and to automatically deploy any patches it detects as missing on its target machines. The console will contain a patch scan template that is defined to look for a particular set of patches. The set of patches is contained in a patch list that resides on a distribution server.

Now, when new patches are released by a vendor (for example, the monthly patches released by Microsoft Corporation), an administrator simply updates the patch list on the distribution server. When the unattended console performs its next scheduled scan it will automatically reference the updated list and will patch its target machines, all without human intervention.

Of course, the unattended consoles can also be configured to use the data rollup feature so that you can track what is happening on each of your unattended consoles from one central site.

The following figure illustrates an unattended console configuration.



1	Rollup console
2	Managed machines

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

3	Unattended console
4	Distribution server
5	Patch list

For more information, see Implementing an Unattended Console Configuration.

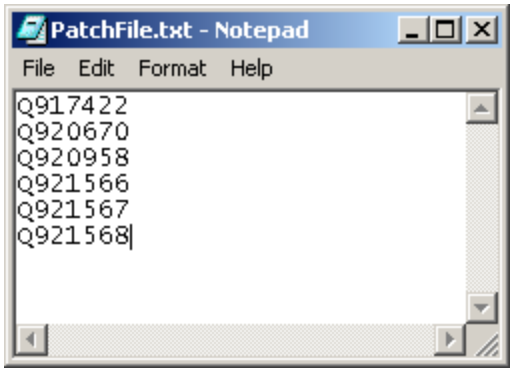
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Implementing an Unattended Console Configuration

This scenario assumes all the consoles have Internet access.

On the Distribution Server

Create a text file that contains the list of patches you want each unattended console to scan for and deploy. You manually create the text file and save it on the distribution server. The text file must contain just the QNumbers associated with each patch, one entry per line.



The QNumber is the unique identifier for the patch.

TIP: You can use Patch View to determine the QNumber associated with each patch.

On Each Unattended Console

1. Create a patch scan template that scans for just the patches specified in the custom patch file.

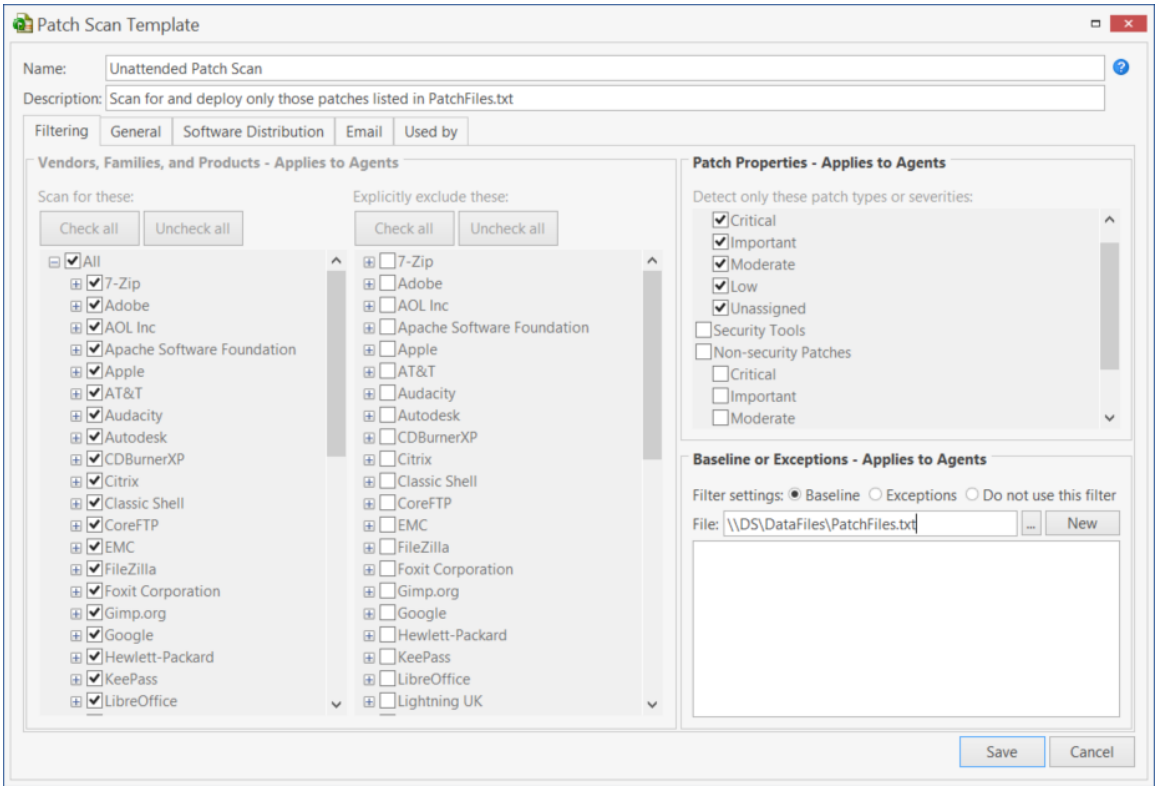
   a.) From the main menu select **New > Patch Scan Template**.

   b.) Type a name and a description.

   c.) On the **Filtering** tab, enable the **Baseline** filter.

   d.) In the **File** box, specify the UNC path to the patch text file that is located on your distribution server.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



For more detailed information about creating patch scan templates, see Creating a New Patch Scan Template.

2. When you schedule the periodic patch scans, make sure you:
   - Select the patch scan template you created in Step 1
   - Enable the **Auto-deploy patches after scan** check box
   - Specify what deployment template to use and when the deployment should occur

Ongoing Maintenance

You simply update the patch list on the distribution server as needed. The unattended console will automatically reference the updated list the next time it performs a scan and will deploy the missing patches to each of its managed machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

What is a Disconnected Console Configuration?

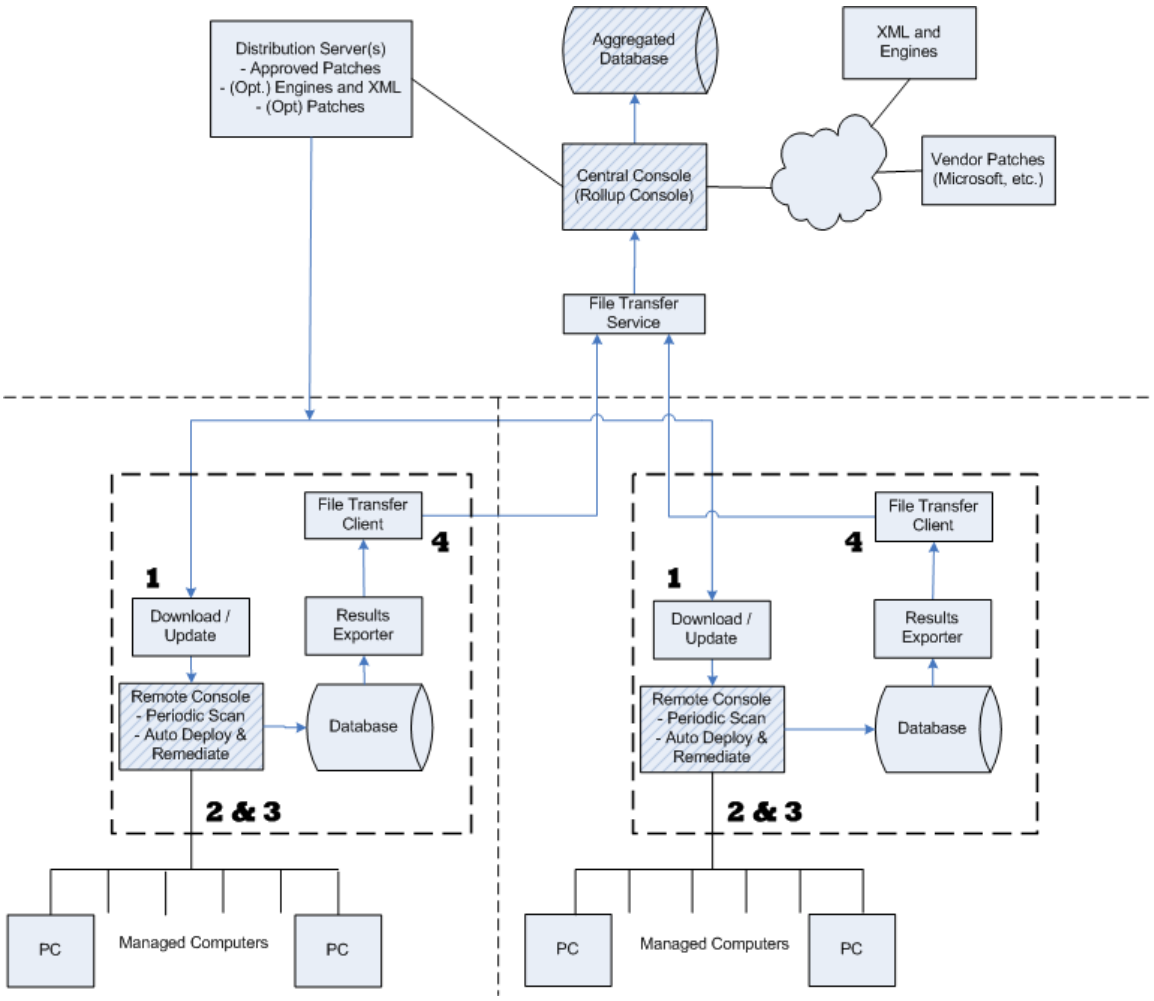
A disconnected console is a remote console that does not have Internet access. The remote console does, however, have access to a local WAN. In this scenario the remote consoles must retrieve patch, scan engine, and XML data files from a networked distribution server rather than from the Web. The central console (which does have Internet access) is responsible for downloading the latest scan engines, XML data files, and patches from the Web and for placing these files on one or more distribution servers. The remote consoles can then use the distribution servers to download the required information before performing their scans.

Once the central console has copied the necessary files to the distribution servers, the basic process is as follows:

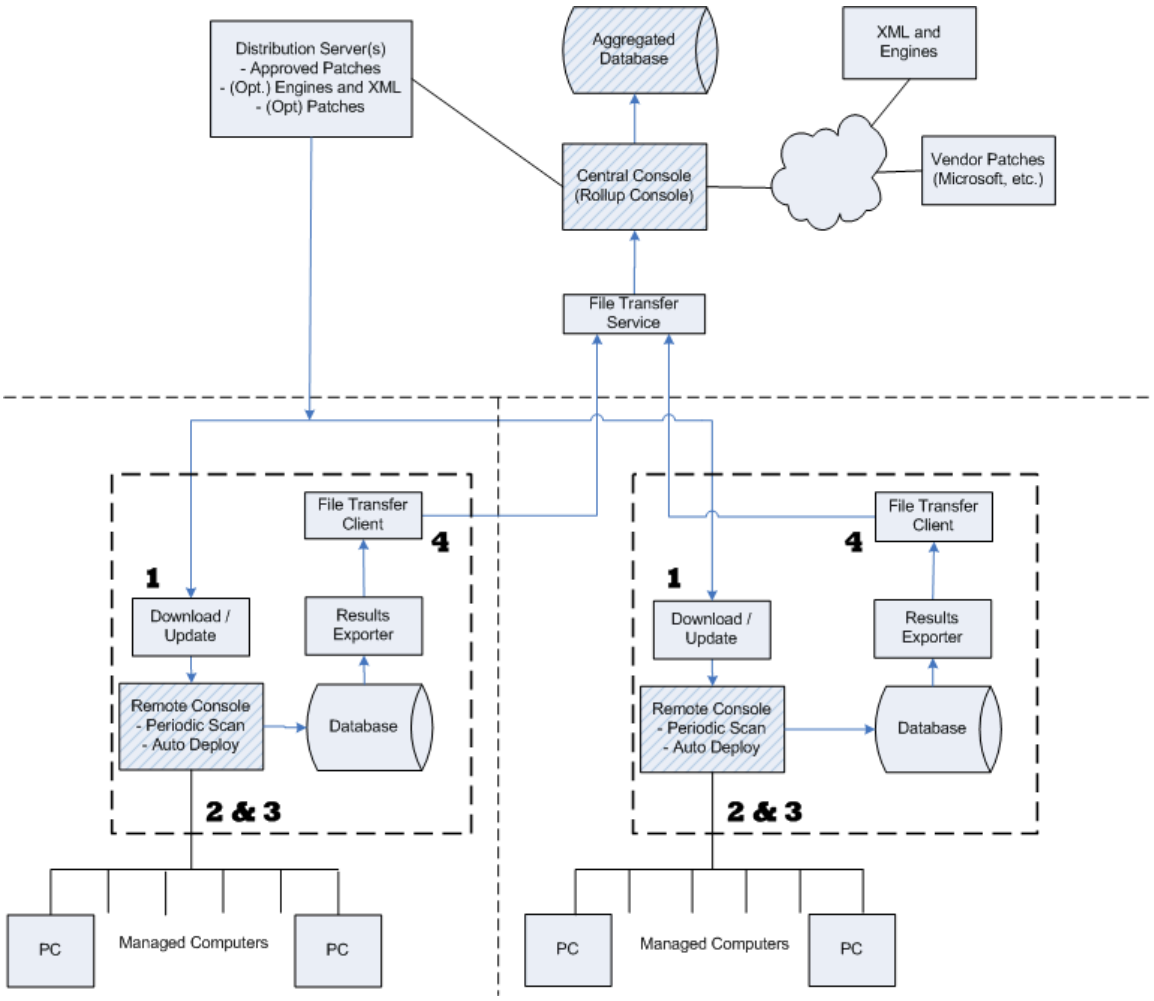
1. The remote console downloads the latest files from a distribution server.
2. The remote console performs a scan.
3. Based on the scan the remote console performs the necessary patch deployments.
4. The remote console then rolls up the results to the central console, which contains an aggregate database of all scan and patch deployment activity in the network.

The following figure illustrates this process.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Tasks Performed by the Central Console

In this scenario, the main functions of the central console are to:

- Download the latest patches, scan engines, and XML data files from the Web
- Copy the scan engines, XML data files, and patches to one or more distribution servers
- Act as the data rollup console by collecting the results of the scans and deployments performed by the remote consoles

For more information, see Configuring the Central Console in a Disconnected Configuration.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Tasks Performed by the Remote Consoles

Each remote console is responsible for patching itself and any managed machines that are located at the same site. There may or may not be an administrator at the remote site and the remote sites may or may not have Internet access. The main functions of each remote console in this scenario are to:

- Get the latest scan engines and XML data files over the WAN from a distribution server
- Scan all the machines at their site
- Download the missing patches from a distribution server
- Deploy all approved patches that are missing
- Roll up the results of the scans and deployments to the central console

For more information, see Configuring the Remote Consoles in a Disconnected Configuration.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Configuring the Central Console in a Disconnected Configuration

I. (Optional) Configure the Data Rollup Service

While this is optional, the recommendation is to use the data rollup feature so that you can track what is happening on each of your remote consoles from one central site.

1. Select **Tools > Options > Data Rollup**.
2. Enable the **Accept and import results from a rollup sender** check box.

II. Set Up a Distribution Server

You must set up a distribution server that the remote consoles can access. The central console will download required files to the distribution server and the remote consoles will download these same files from the distribution server.

See Configuring Distribution Servers for detailed information on configuring a distribution server.

III. Update the Distribution Server with the Latest Files

You must first download the latest scan engines, XML data files, and patches from the Web to the central console's patch download directory.

1 Download the patches that have been approved by your organization.

   See Downloading Patches for detailed information on downloading patches.

2. Download the latest scan engines and XML data files by selecting **Help > Refresh Files.**

Copy the scan engines, XML data files, and patches from the central console to the distribution server by synchronizing the central console with the distribution server. For information on this, see Synchronizing Servers.

You can also configure Ivanti Patch for Windows® Servers to automatically download the latest engines and XML data files and synchronize all your distribution servers. See Synchronizing Servers for details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Configuring the Remote Consoles in a Disconnected Configuration

Here are the major steps you must perform when configuring each remote console in a disconnected console configuration.

I. (Optional) Configure the Data Rollup Service

While this is optional, the recommendation is to use the data rollup feature so that you can track what is happening on each of your remote consoles from one central site. To implement data rollup, you must configure each remote console so that it rolls up its results to the central console.

1. Select **Tools > Options > Data Rollup**.
2. Enable the **Enable Data Rollup** check box.
3. Specify the IP address/hostname and port number used by the rollup console.
4. In the **Minutes between sending console's results** box, specify how often the data will be rolled up from the remote console to the central console.

   The default value is every 240 minutes (four hours).
5. Click **Register**.

II. Set Up a Distribution Server

You must set up a distribution server that each remote console can access. The remote consoles will download all necessary files (such as patch files, scan engines, and XML data files) from the distribution server. The distribution server should be the same distribution server you set up on the central console.

See Configuring Distribution Servers for detailed information.

III. Create a Machine Group of the Machines at This Site

1 From the main menu select **New > Machine Group** and name the group **All Machines** (or something similar).
2. Add all the machines that are managed by the remote console.

IV. Specify Where to Download Files

Configure the remote console so that prior to a scan it will automatically download the latest files from the distribution server.

1 Select **Tools > Options > Downloads**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

2. In the **Definition download source** area, specify the appropriate distribution server to use when downloading the latest scan engines and XML data files.
3. In the **Patch and Service Pack download source** area, specify the appropriate distribution server to use when downloading the patches and service packs.

V. Create a Patch Scan Template

1 From the main menu select **New > Patch Scan Template**.

2. Configure the patch scan template as desired.

See Creating a New Patch Scan Template for details.



If you want to scan for a particular set of patches in an unattended console configuration, see Implementing an Unattended Console Configuration for more information.

VI. Create a New Favorite and Schedule a Periodic Scan

Create a favorite containing the machine group and the scan template you created earlier and then use the favorite to schedule a scan.

1 From the main menu select **New > Favorite**.

2. In the **Select at least 1 group** list, select the new machine group you created earlier.
3. In the **Template** box, select the patch scan template you created earlier.
4. Click **Run operation**.
5. On the **Run Operation** dialog, schedule the recurring patch scan.

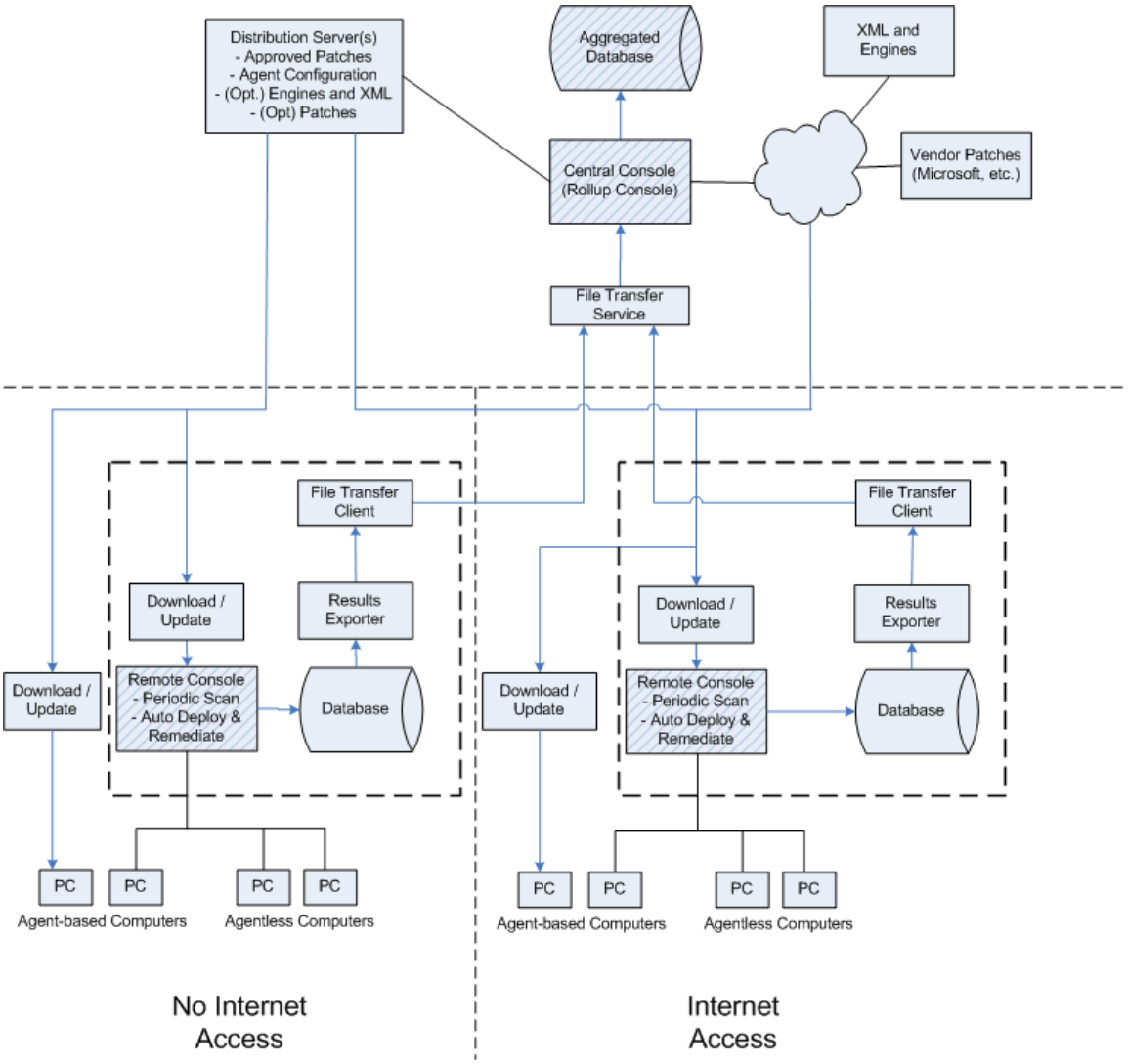
When you schedule the patch scan make sure you:

- Select the patch scan template you created in Step V
- Enable the**Auto-deploy patches after scan**check box
- Specify what deployment template to use and when the deployment should occur

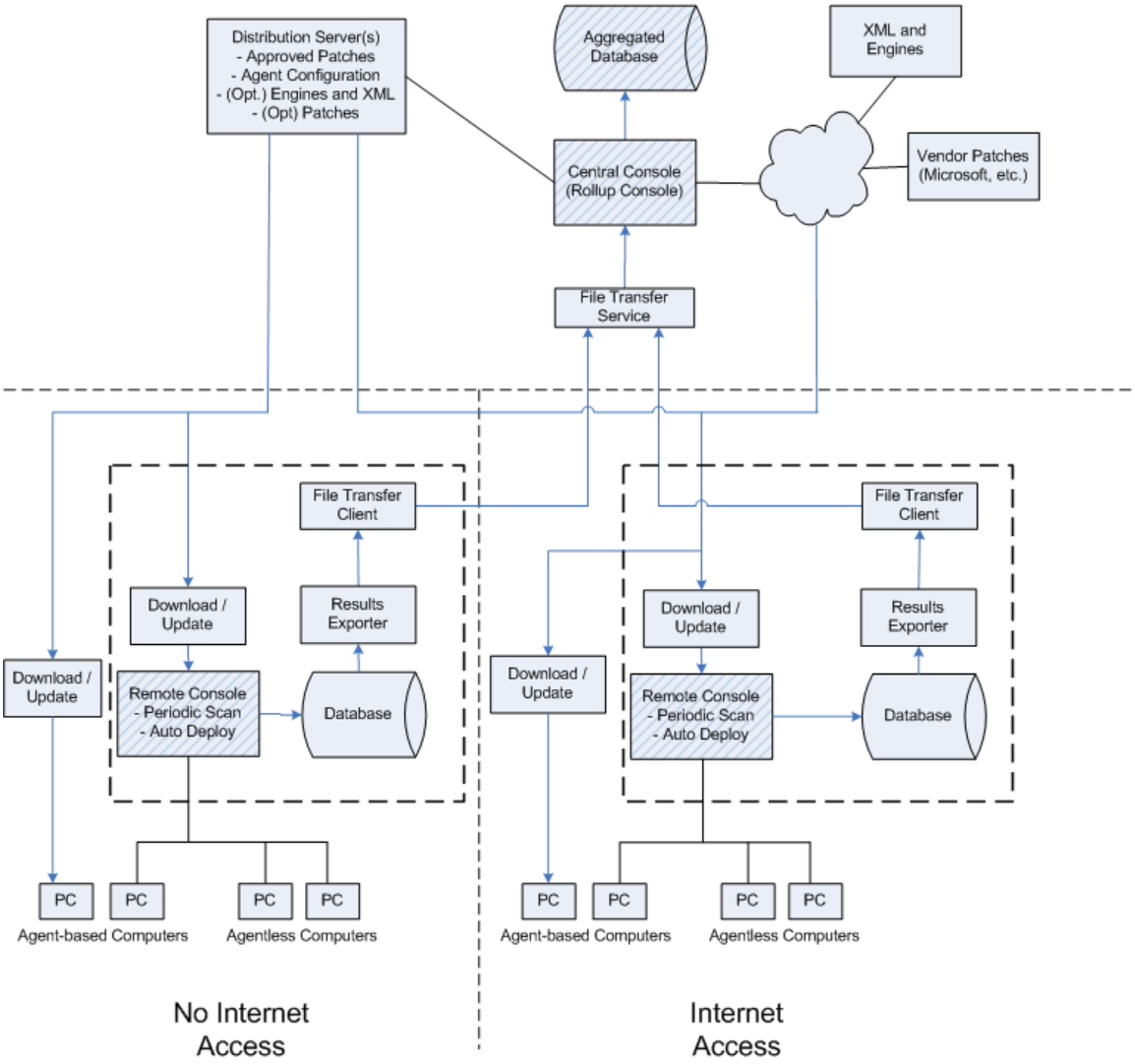
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Multiple Console Configuration with Agents

It is possible to combine the use of agentless and agent-based machines with multiple consoles. Agent-based machines are implemented using Ivanti Patch for Windows® Servers Agent. Detailed information about using Ivanti Patch for Windows® Servers Agent is provided in the following section.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Agentless vs. Agent-based Solutions

Ivanti Patch for Windows® Servers provides both agentless and agent-based solutions. This section describes, in general terms, the benefits of each solution. The sections that follow explain in more detail how to use an agent.

Agentless Solution

Agentless systems are based on push technology and on a centralized design. A central authority is responsible for scanning the machines in the enterprise and for initiating all actions on those machines. Agentless systems have a number of advantages over agent-based systems. Strict agent-based systems can only report on machines that have the agent actively running. If the agent has been disabled the machine will appear to not exist. In addition, new machines can be introduced to a network and these rogue machines will not only be agentless, they may well be invisible. Agentless systems, on the other hand, can scan ranges of IP addresses and report on machines it finds. Even if it cannot access the system, the agentless scanner will at least report that a new IP address is present on the network. In many cases agentless systems lower the cost of ownership, reduce management overhead, and provide for quick and easy deployment. This is especially true in large enterprises managing 10,000 or more machines. An administrator can be scanning and fixing their network within minutes using an agentless system.

In Ivanti Patch for Windows® Servers, all patch, asset, and power management tasks can be performed without agents.

Agent-based Solution

Patch management and asset management

Certain types of users or systems can pose problems for agentless solutions. Machines that must reside in a "de-militarized zone" (DMZ), roaming users, and disconnected or inactive machines can all prove problematic. In these cases an agent-based solution is often the best answer. Agent-based solutions consist of proprietary client-side communications software that resides on a computer and facilitates communications with server-based administrative software. The agent scans the client machine for information and then provides the information directly to the server console.

An agent-based solution is a useful complement to an agentless patch management and/or asset management solution. Outfitting your troublesome systems with agents provides the best of both worlds--agentless solutions to protect machines permanently or newly introduced to the network, and agent-based solutions for the hard-to-reach machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Power management

Power management (including Wake-on-LAN) requires either a Ivanti Patch for Windows® Servers Advance license or a separate add-on license for Ivanti Patch for Windows® Servers Standard.

An agent-based solution is also well suited for performing power management tasks. For example, if you want to be sure your portable machines are not left powered on late at night or over the weekend, an agent can be used to automatically shut down those machines. In addition to saving power and avoiding unnecessary wear, shutting down your disconnected machines during those times they are likely to be left unattended is also a smart security precaution.

Summary

Agentless

- Designed for centralized environments
- Based on push technology
- Ideal for networks with large amounts of bandwidth
- Dependent on network connectivity
- A central authority does all the scanning and deploying
- Best for performing patch management and asset management tasks on networked machines

Agent-based

- Best for frequently disconnected machines or machines in the DMZ
- Based on pull technology
- Ideal for distributed networks with remote locations that have limited bandwidth
- Less dependent on network connectivity; ideal for mobile computers that are not always connected to the network
- Each agent does its own scanning and deploying based on policies defined on the central console
- Best for performing patch management and asset management tasks on disconnected machines

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

When Should I Use Agentless and Agent-based Solutions?

Ivanti Patch for Windows® Servers is, at its roots, an agentless solution. With a few simple configuration steps, however, Ivanti Patch for Windows® Servers can also provide agent-based services. This section explains when to implement each solution.

For Patch Management and Asset Management Tasks

Start with the Agentless Features of Ivanti Patch for Windows® Servers

For large enterprises containing thousands of machines, the ease of use provided by the agentless technology of Ivanti Patch for Windows® Servers can be used to address the patch management and asset management needs of the vast majority of the machines in your enterprise. Ivanti Patch for Windows® Servers can be used to discover which target machines are missing patches and automatically deploy the missing patches. It can also scan your target machines and report on the software, hardware, and virtual assets contained on the machines. Using Ivanti Patch for Windows® Servers you can scan and fix, from one central location, the vast majority of the machines in your network within minutes.

Polish Things Off with the Agent-based Features of Ivanti Patch for Windows® Servers

Most large enterprises have machines in hard-to-reach places: machines in remote locations, laptops that roam to different locations or that park and dock outside the office, machines in protected zones (DMZs), etc. For these devices you can use the agent-based features provided by Ivanti Patch for Windows® Servers, which are implemented using Ivanti Patch for Windows® Servers Agent. With Ivanti Patch for Windows® Servers Agent you can be sure that these machines are scanned regularly, even if they are disconnected from your enterprise network.



There is one exception; agents can be used to perform software asset scans and hardware asset scans, but they cannot perform virtual asset scans.

For Power Management Tasks

A number of the power management tasks apply only to agentless situations. This includes the Shutdown now, Restart now, and Wake-On-LAN tasks that are initiated from Machne View or Scan View. These tasks require the target machines to be accessible from the console and are therefore not implemented within an agent policy.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Power management tasks that use a power state template, however, can be implemented in either an agentless or agent-based manner. You may consider using an agent-based power state task under the following conditions:

- If you want to apply your power management policy consistently across all machines within your organization (connected and disconnected).
- If you have machines that may not always be reachable from the console (for example, machines in a DMZ).
- If you are concerned with network bandwidth issues.

  An agentless power state task will push a small number of files from the console to each target machine -- if a large number of machines are involved it may affect the performance of your network.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

What Exactly is Ivanti Patch for Windows® Servers Agent?

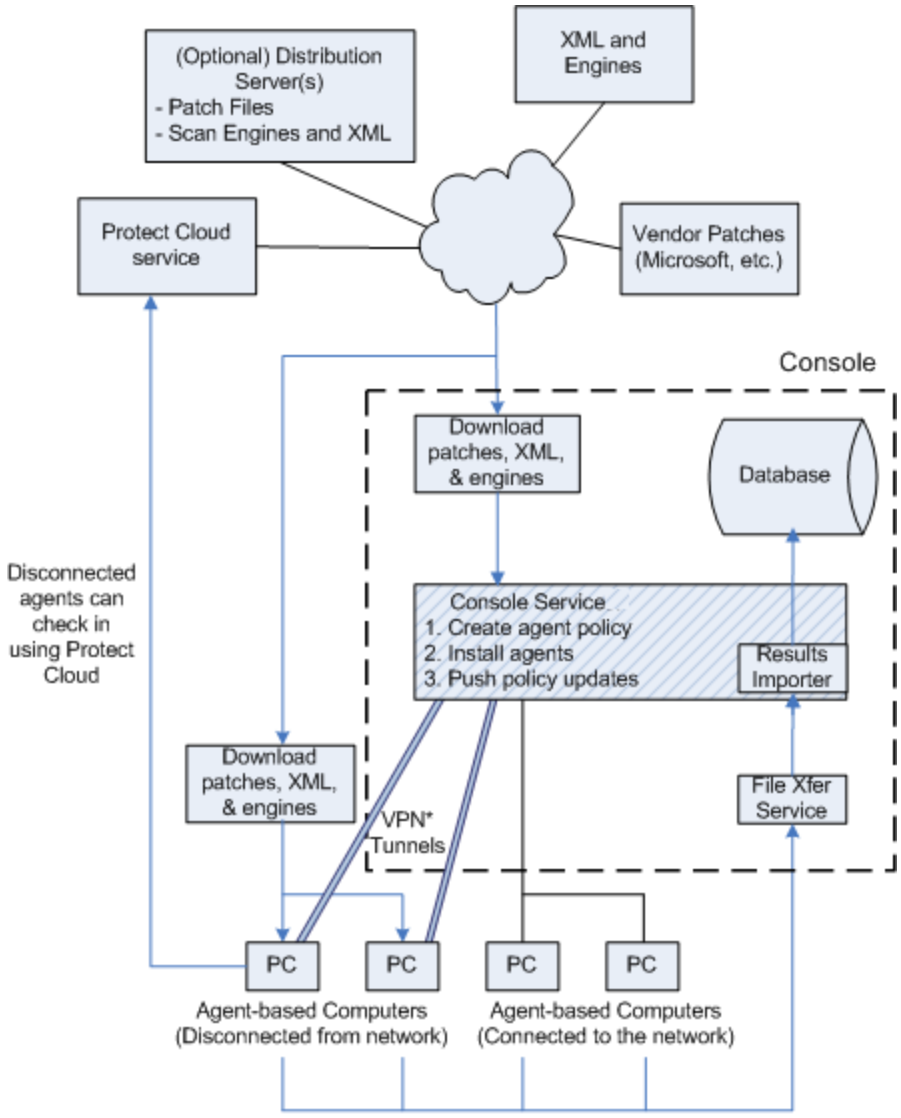
Ivanti Patch for Windows® Servers Agent is an agent service. The agents configured by Ivanti Patch for Windows® Servers Agent are distributed agents, meaning they are installed on distinct physical and online virtual machines and have the ability to independently initiate specific actions. They are configured via the Ivanti Patch for Windows® Servers interface and then installed on the desired machines either by pushing them from the Ivanti Patch for Windows® Servers console or by manually installing them on individual machines.

Depending on how they are configured, when installed on a machine a Ivanti Patch for Windows® Servers Agent can:

- Scan for and deploy missing patches
- Scan for asset information
- Shut down or restart the agent machine on specific days and times
- Listen to the console or the cloud for policy updates and download the new policy immediately
- Report the results to the local console

The following figure illustrates how Ivanti Patch for Windows® Servers Agent works in your environment.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How the Agent Process Works

Agents are configured via the Ivanti Patch for Windows® Servers interface and then installed on the desired machines. Once installed, each agent will periodically check in with the console, or if it is a disconnected agent it may check in with the Protect Cloud service. How often an agent checks in is a configurable item, but the check-ins typically occur at least once a day. An agent can also be configured to listen to the console for policy updates and download the new policy immediately.

During each check-in the agent checks with the console and does the following:



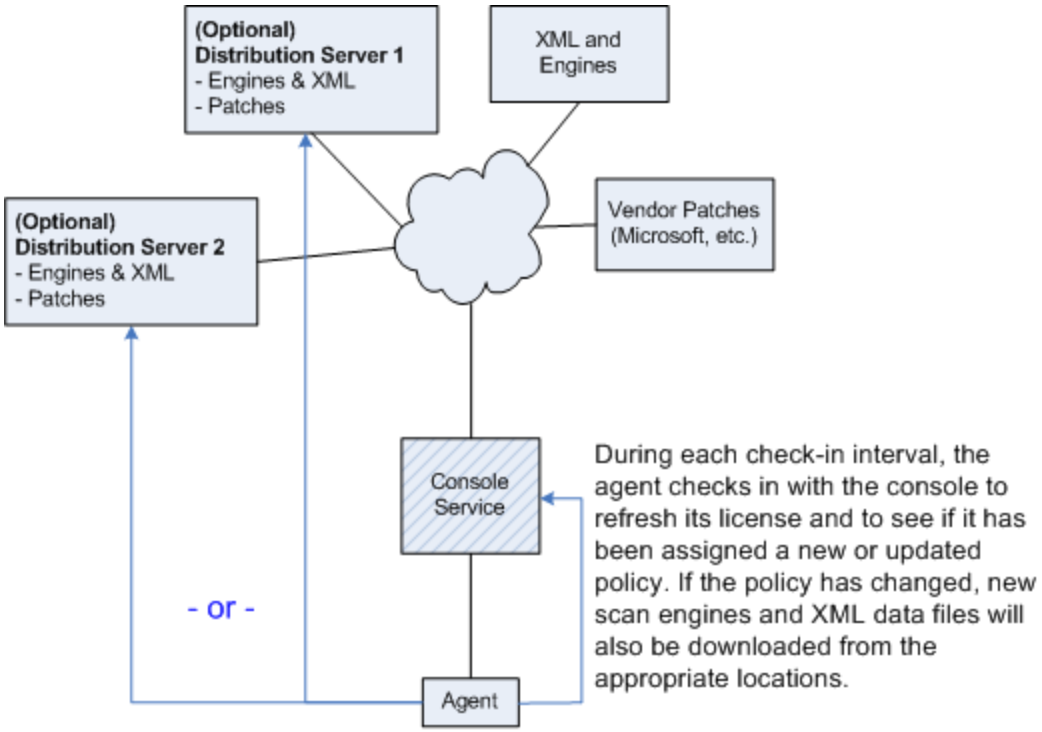
The process is a bit different if you are using Protect Cloud synchronization; see Protect Cloud Synchronization Overview for details.

- It refreshes its license. An agent license is valid for 45 days from the most recent check-in.
- It checks if it is assigned a distribution server, and if so, which one.
- It checks for any policy configuration changes. If the policy has been changed, the new policy will be pushed from the console to the agent. In addition, the agent will receive new scan engines and XML data from either the default websites or from its assigned distribution server.
- It receives any credential information it needs in order to authenticate itself to any distribution servers or proxy servers.

An agent will also download new scan engines and new XML data files from the default website or from its assigned distribution server whenever a scheduled scan is performed.

The following figure illustrates the agent process.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Preparing to Use Ivanti Patch for Windows® Servers Agent

All agents are configured on the Ivanti Patch for Windows® Servers console and then either push installed from the console to the desired target machines or manually installed by an administrator. The agents can be configured with any combination of patch management capabilities, asset management capabilities, and/or power management capabilities. This section provides a roadmap of tasks you must perform when preparing to use Ivanti Patch for Windows® Servers Agent.



The agent machine hardware and software requirements are found in the System Requirements topic.

I. (Optional) Set Up and Synchronize a Distribution Server

Setting Up a Distribution Server

You have the option of setting up a distribution server that the agents can periodically access to download various files. There are a couple of reasons for using a distribution server, including:

- If some of your agents do not have Internet access and therefore won't be able to download the latest scan engines, XML data files, and patch files from the default websites. In this case you will need to store these files on a distribution server that the agents can access.
- If you have defined custom patches that are not available from the default websites. You must make the custom patches available by manually copying the patches to one or more distribution servers.

See Configuring Distribution Servers for detailed information on configuring a distribution server. In addition, when you configure your agent policy you should specify which distribution server your agents should use; see Configuring General Settings for details.

Synchronizing the Distribution Server

To update a distribution server with the latest patches, scan engines, and XML data files you *synchronize* the server with the files contained on the console. See Synchronizing Servers for detailed information. Custom patches must be manually copied to the distribution server.

II. Create and Configure a Ivanti Patch for Windows® Servers Agent Policy

1. From the main menu select **New >Agent Policy**.
2. Type a unique name for the policy.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

There are many features you can configure within an agent policy. See Creating A New Agent Policy for complete details.

III. Install the Agent on the Desired Machines

There are a couple of ways you can push install an agent on one or more machines.

- For machines that have been scanned at least once and are contained in the program database, you can use the Machine View right-click menu (**Agents > Install/Reinstall with Policy**).
- For machines that have not been scanned and are not contained in the database, you can create a machine group containing all the machines that will run a particular agent policy and then use the **Install Agent** button to install an agent on those machines that are online.

See Installing Agents from the Console for detailed information on installing agents on target machines.



When performing a push install of an agent, each target machine must have a network connection to the console during the installation. This connection is required in order to exchange security information that will be used to establish an encrypted link for all future communication between the console and its agents. The agent machines must also be able to perform name resolution in order to locate the console machine.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How to Install Ivanti Patch for Windows® Servers Agent from the Console



Show Me!

To view a video tutorial on this topic, click the video icon on the left.

You can use the console to "push install" the Ivanti Patch for Windows® Servers Agent to connected target machines. In order to perform the push install, each target machine must be online and have an active network connection to the console during the Ivanti Patch for Windows® Servers Agent installation. This connection is required in order to exchange security information that will be used to establish an encrypted link for all future communication between the console and its agents. The agent machines must also be able to perform name resolution in order to locate the console machine.

You must have the proper credentials in order to authenticate to each of the target machines. See Credential Precedence for details.

Some target machines may have a firewall enabled that blocks the incoming ports required to install Ivanti Patch for Windows® Servers Agent. On these machines you must manually install Ivanti Patch for Windows® Servers Agent. See Manually Installing Agents for details.

Installing an agent on a distribution server is a special case that requires the server machine's SYSTEM account to have read access to the distribution server folder. See Configuring System Account Permissions for details.

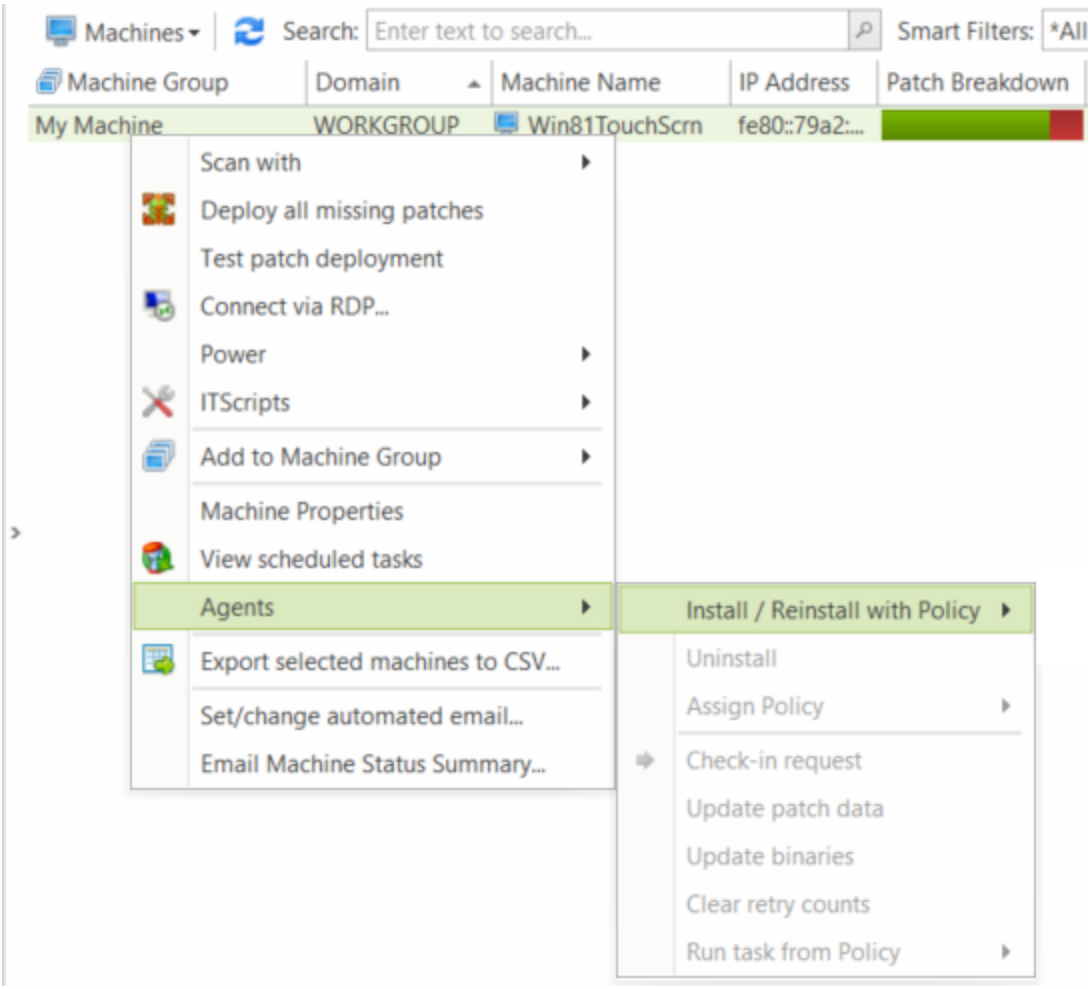
You can perform a push install of the Ivanti Patch for Windows® Servers Agent service two different ways from the console.

For Machines That Have Been Previously Scanned

You can install agents onto machines that have been previously scanned and that are contained in the program database.

1. Go to either Machine View or Scan View.
2. Right-click the desired machines, select **Agents > Install/Reinstall with Policy** and then select the desired agent policy.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

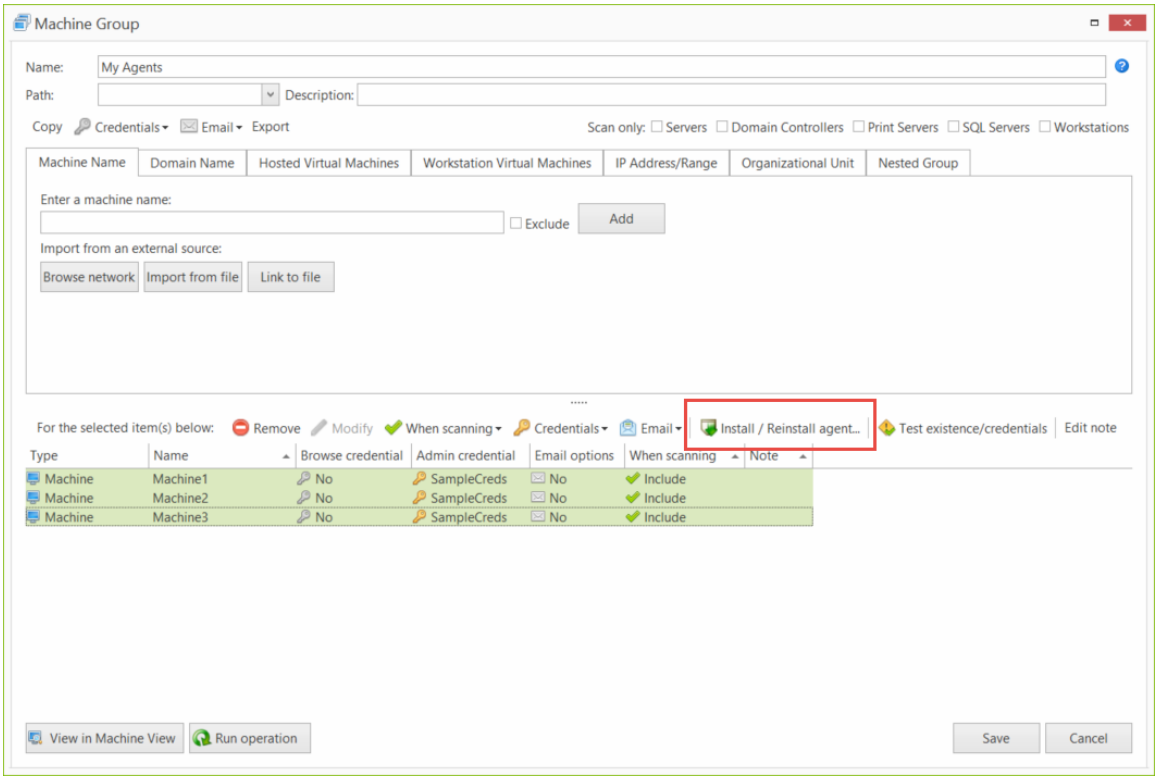


For Machines That Have Not Been Previously Scanned

You can install agents on machines that have not been previously scanned and are therefore not contained in the machine database. You simply create a machine group that contains all the machines that will run a particular agent policy and then use the **Install / Reinstall Agent** button to install an agent policy on those machines.

There are a couple of caveats:
- The machines must be added to the machine group using a machine name, domain name, or IP address. You cannot use the **Install / Reinstall Agent** button to install agents on machines that were added as organizational units, nested groups, or IP address ranges.
- The machines must be online and connected to the network. If the console cannot make a connection to a machine the install will fail for that machine.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



You will be prompted to select the policy you want installed. See Creating A New Agent Policy for information on configuring policies.

The following occurs when you push install the Ivanti Patch for Windows® Servers Agent service to a machine:

- The **Operations Monitor** is displayed and shows the status of the installation request.
- You can verify the installation was successful by doing the following:
  - By using Machine View to check the status of the machine. You'll have to wait until the next time the agent machine checks in with the console, but once that occurs, the Agent State column should indicate that the machine contains an agent.
  - By using the Service Control Manager on the agent machine to verify that the agent services are running (stDispatch, stAgent).
- Once the Ivanti Patch for Windows® Servers Agent configuration is successfully installed on a target machine, the agent is automatically started on the machine. See Using Agents on a Target Machine for information on using the agent.
- After an agent is installed on a machine, that machine becomes a managed machine and can be viewed using Machine View.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Manually Installing Ivanti Patch for Windows® Servers Agent

You must manually install Ivanti Patch for Windows® Servers Agent on machines that are guarded by a firewall. You do this by copying the agent installation files to the desired target machines and then running the Ivanti Patch for Windows® Servers Agent installation wizard on each machine.

Requirements

- The target machines must be able to communicate with the console.
- You must configure at least one Ivanti Patch for Windows® Servers Agent policy before manually installing an agent. See Preparing to Use Agents for details.
- You must specify how the agent will authenticate itself to the console during the registration process. See Agent Options for details.
- Installing an agent on a distribution server is a special case that requires the server machine's SYSTEM account to have read access to the distribution server folder. See Configuring System Account Permissions for details.

Installation Procedure

1. On the Ivanti Patch for Windows® Servers console, locate the **STPlatformUpdater.exe** file.

   The file is located in the **C:\ProgramData\LANDESK\Shavlik Protect\Console\DataFiles C:\ProgramData\ScriptLogic\Patch Authority\Console\DataFiles** directory.

2. Copy the .exe file to the desired target machines.

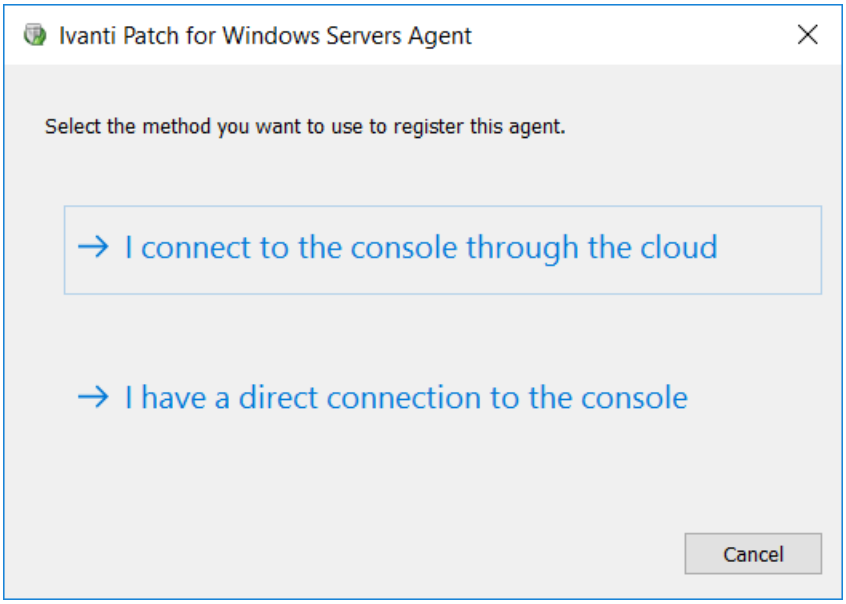
   You can distribute this file using Active Directory, or you can simply copy it to a physical media such as a CD or flash drive and manually distribute it to the desired machines.

   > When distributing this file you may choose to create an installation script that automatically passes all necessary information to the installation wizard.

3. Log on to the target machine using an administrator account.
4. Double-click the file named **STPlatformUpdater.exe**.

   The agent is installed. When the installation is complete the **Agent Registration** dialog is displayed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

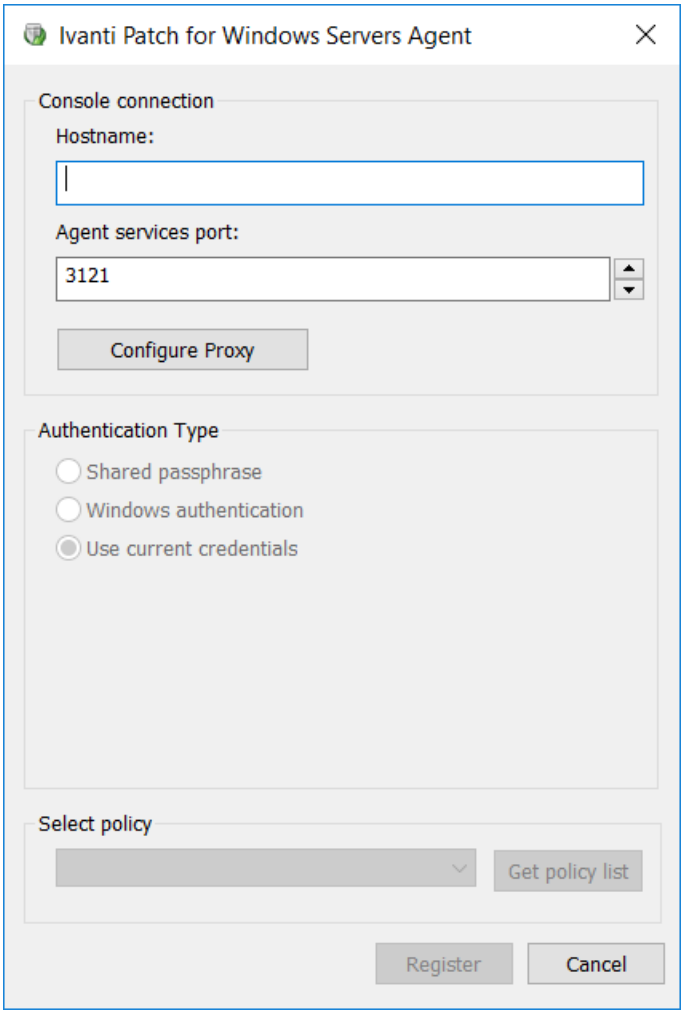


5. Click **I have a direct connection to the console**.

> The **I connect to the console through the cloud** button is used if you are installing the agent via the cloud.

The following dialog is displayed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



6. Provide the required information.

- **Hostname**: Type either the hostname or the IP address of the Ivanti Patch for Windows® Servers console. Examples: Myconsole or 192.168.1.100.

If an IP address is used, the IP address must be added to the Console Alias list.

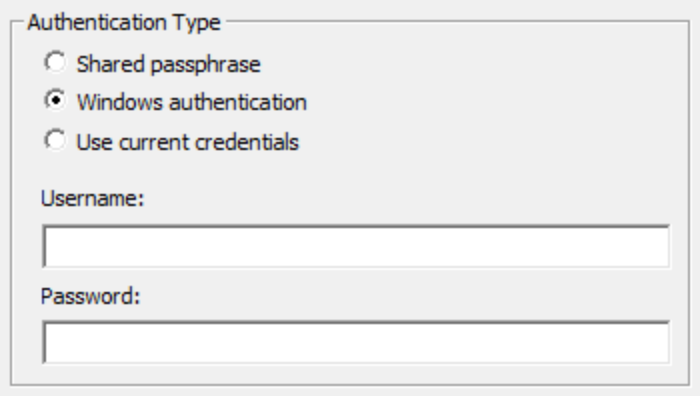
- **Agent services port**: Specify the port number used for forwarding information to the console. 3121 is the default port number.
- **Configure Proxy**: Click this button to specify the proxy settings the agent will use during the registration process. See **Configuring Proxy Server Settings** for details.
- **Authentication Type**: You must choose the authentication method dictated by the **Tools > Options >Agents** dialog.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- If the **Enable passphrase in manual Agent installations** check box is enabled on that dialog, then choose **Shared Passphrase** and type the matching passphrase.
- Otherwise, choose either **Windows Authentication** or **Use current credentials**.

- If the credentials you used to log on to the target machine can also be used to log on to the Ivanti Patch for Windows® Servers console, then choose **Use Current Credentials**. The credentials must be for a user in the Administrators group on the console.

- Otherwise, choose **Windows Authentication** and provide the necessary administrator credentials for the Ivanti Patch for Windows® Servers console. The credentials must be in domain\user.name format and they must have administrator rights on the Ivanti Patch for Windows® Servers console.



- **Select policy**: Click **Get policy list** to connect to the console and populate the **Select policy** box with the list of all available agent policies. Select the policy you want assigned to this agent.

7. On the **Agent Registration** dialog click **Register**.
8. On the **Agent Setup Wizard** dialog, click **Finish**.

5 Provide the required information.

- **Hostname**: Type either the hostname or the IP address of the Ivanti Patch for Windows® Servers console. Examples: Myconsole or 192.168.1.100.

If an IP address is used, the IP address must be added to the Console Alias list.

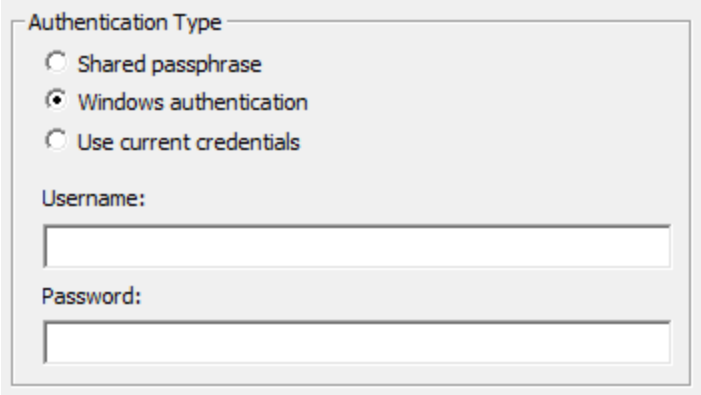
- **Agent services port**: Specify the port number used for forwarding information to the console. 3121 is the default port number.
- **Configure Proxy**: Click this button to specify the proxy settings the agent will use during the registration process. See **Configuring Proxy Server Settings** for details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **Authentication Type**: You must choose the authentication method dictated by the **Tools > Options >Agents** dialog.
  - If the **Enable passphrase in manual Agent installations** check box is enabled on that dialog, then choose **Shared Passphrase** and type the matching passphrase.
  - Otherwise, choose either **Windows Authentication** or **Use current credentials**.

  - If the credentials you used to log on to the target machine can also be used to log on to the Ivanti Patch for Windows® Servers console, then choose **Use Current Credentials**. The credentials must be for a user in the Administrators group on the console.

  - Otherwise, choose **Windows Authentication** and provide the necessary administrator credentials for the Ivanti Patch for Windows® Servers console. The credentials must be in domain\user.name format and they must have administrator rights on the Ivanti Patch for Windows® Servers console.



- **Select policy**: Click **Get policy list** to connect to the console and populate the **Select policy** box with the list of all available agent policies. Select the policy you want assigned to this agent.

6. On the **Agent Registration** dialog click **Register**.
7. On the **Agent Setup Wizard** dialog, click **Finish**.

The agent installation routine will:

- Install the necessary .exe and other supporting files in the **C:\Program Files\LANDESK\Shavlik Protect AgentC:\Program Files\ScriptLogic Corporation\Patch Authority Ultimate Agent** directory
- Install the certificates needed to communicate securely with the console
- Acquire an agent license
- Retrieve the assigned policy, the scan engines, and the XML data files and store them.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

The files are stored in the **C:\ProgramData\LANDESK\Shavlik Protect\AgentC:\ProgramData\ScriptLogic\Patch Authority\Agent** directory.

When the download is complete the agent will be started automatically. You can check the status of the agent using the Ivanti Patch for Windows® Servers Agent client program, available by selecting **Start > All Programs > Ivanti Patch for Windows® Servers > Ivanti Patch for Windows® Servers AgentStart > All Programs > ScriptLogic > ScriptLogic Agent**. You can use this program to configure any settings that were marked as user-configurable.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Installing Agents from the Cloud

If you are using Protect Cloud synchronization, you have the ability to install a Ivanti Patch for Windows® Servers Agent from the cloud. This is particularly helpful if you have target machines that are away from the corporate network and unable to contact the console.

Requirements

- The target machine must have Internet access
- The Ivanti Patch for Windows® Servers console must be registered with Protect Cloud
- Outgoing TCP ports 80 (http) and 443 (https) must be available when communicating with Protect Cloud
- The URL *protectservices.shavlik.com* must be accessible when communicating with Protect Cloud
- There must be at least one agent policy that is configured to allow synchronization with Protect Cloud
- You cannot install a cloud-based agent on a Ivanti Patch for Windows® Servers console machine
- Each user that installs an agent must have administrator access on their target machine

Installation Instructions

From Your Web Browser

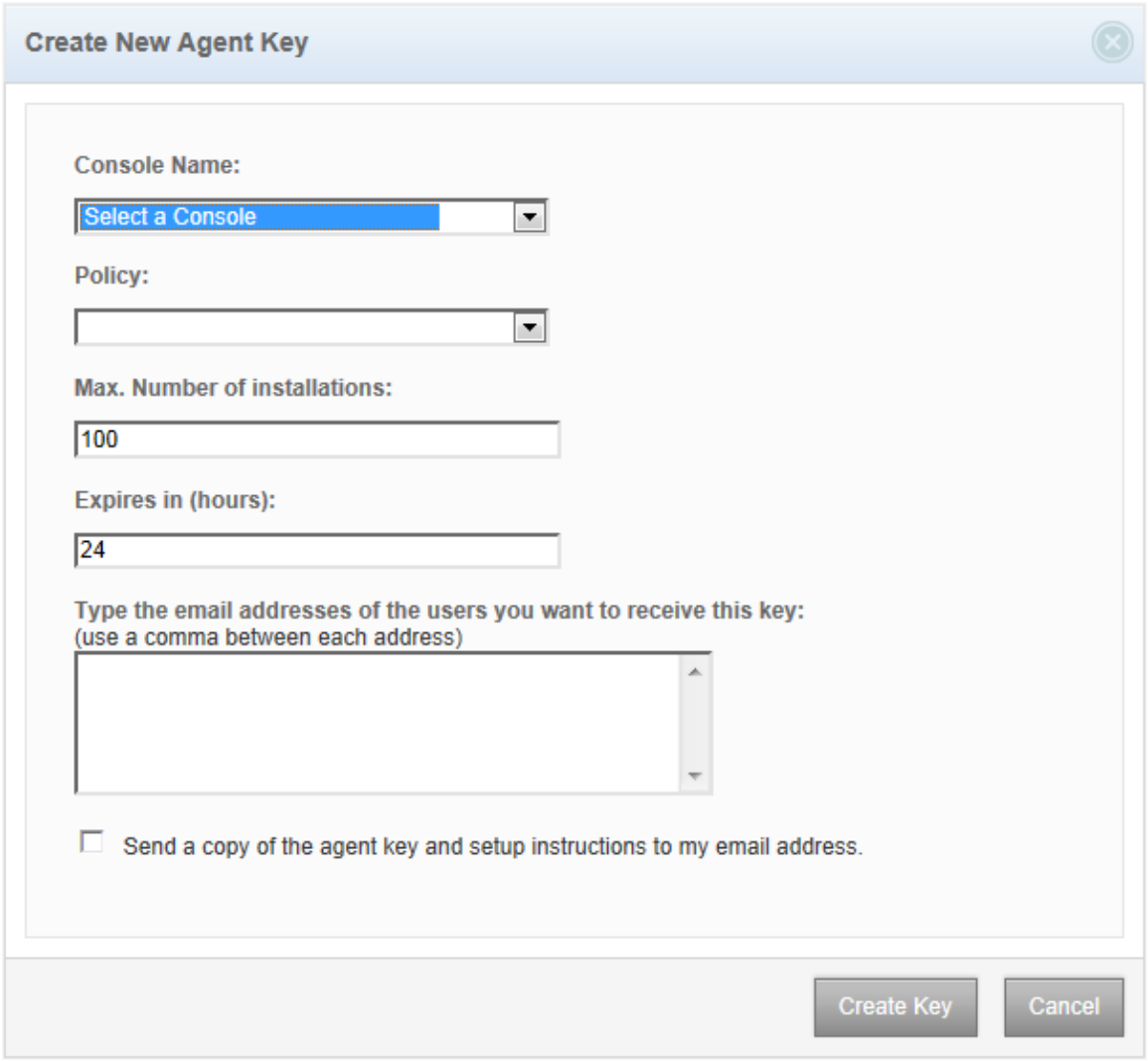
1. Go to http://protectcloud.shavlik.com and log on to your account.

   If you don't already have an account, click **Register** to quickly setup an account.

2. On the **Registered Consoles** tab, verify that your Ivanti Patch for Windows® Servers console is registered with Protect Cloud.
3. Select the **Agent Keys** tab.
4. Click **New**.

   The **Create New Agent Key** dialog is displayed. Use this dialog to create an activation key that can be used to install one or more agents. You also use this dialog to specify the email addresses of the users you want to receive this key.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Console Name	Select the Ivanti Patch for Windows® Servers console that will be used to manage the agent. TIP: If the console does not contain a user-friendly name that has some significance to other users, before proceeding you might consider changing the name within Ivanti Patch for Windows® Servers and then re-registering the console with Protect Cloud.
Policy	Select the agent policy that you want to assign to the agent. Only those policies that are configured for synchronization with Protect Cloud will be available for selection.
Max. Number of installations	Specify the maximum number of agent installations you will allow to be performed using this agent key.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	Example: Assume you want to install agents on all of the machines at a remote site. You are not certain how many machines are at the site but you are confident that there are fewer than 10 machines. By specifying a maximum of 10 installations for this key, you are enabling all the machines at the remote site to install agents and yet limiting the number of license seats that can be consumed using this key. You cannot install an unlimited number of agents because the Ivanti Patch for Windows® Servers console will not allow you to exceed your license count.
Expires in (hours)	Specify how long the key can be used to install new agents. For example, if you know that an administrator will be at a remote site for two days to help with the agent installations, you can specify that the key is only valid for 48 hours. This allows you to control your exposure to other people consuming license seats from the console.
Type the email addresses of the users you want to receive this key	An email message containing the agent key will be sent to each address. Use a comma to separate each address.
Send a copy of the agent key and setup instructions to my email address	If you want to receive a copy of the email message that will be sent to the specified recipients, enable this check box.

5. Provide all necessary information and then click **Create Key**.

   The agent key is created and then emailed to the specified recipients. The email message also contains a web link for downloading the agent installation program and detailed instructions on how to install the agent.

On the Target Machine

1 Log on to the target machine using an administrator account.

2. Open the Protect Cloud Sync email message that contains the agent key and the installation instructions.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

If you do not have access to the Protect Cloud Sync email message but you have a Protect Cloud account, you can create your own agent key by opening a web browser on the target machine and then following the instructions shown above in the **From your web browser** section. After the key is created and while you are still logged in to Protect Cloud, click the **Download Agent** link that is located to the right of the new key; this enables you to download the agent installation program to the target machine.

3. Use the instructions to install and register the agent.

   You will install the agent, specify that you are connecting to the console through the cloud, paste the activation key, and then click **Register**.

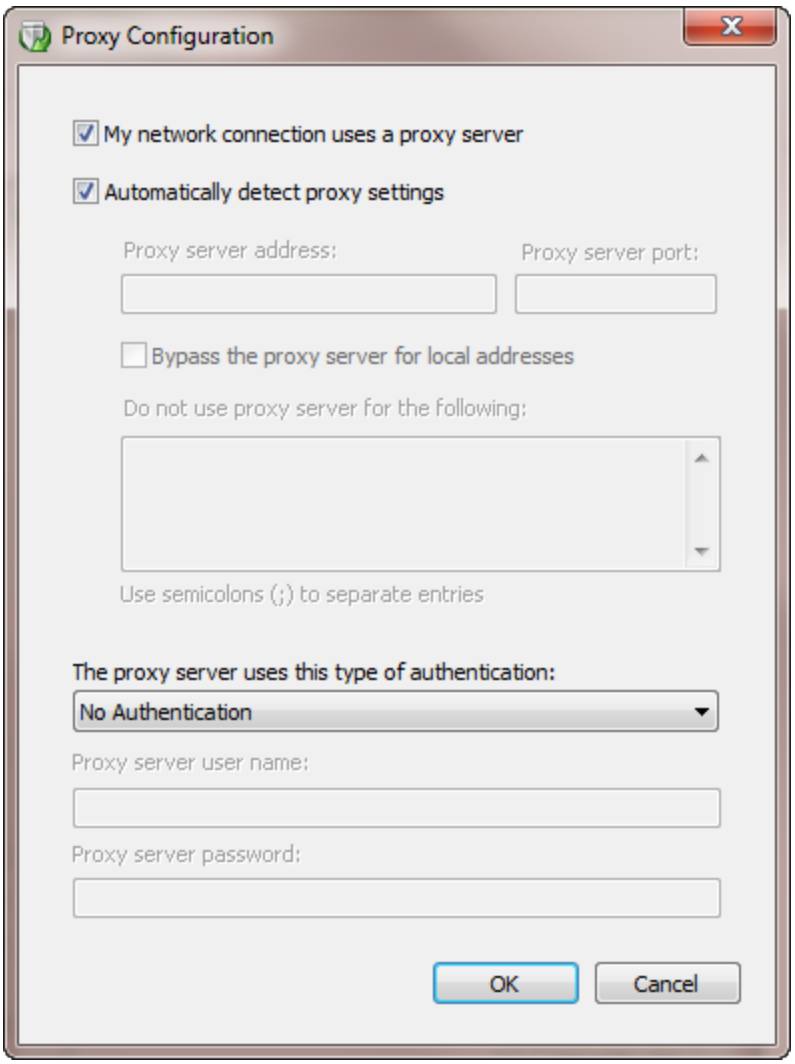
4. Wait for the agent registration process to complete; this may take up to 20 minutes or more to complete.

   The agent will be initially placed into a temporary provisional state while the registration is processed. During this time the Ivanti Patch for Windows® Servers console will learn about the registration request, verify that enough license seats are available, and provide the Protect Cloud service with the necessary files. After the registration process is complete, at the next check-in time the agent will retrieve its assigned agent policy from the cloud and will become a fully-functional agent.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Configuring Proxy Server Settings for Ivanti Patch for Windows® Servers Agent

When you click the **Configure Proxy** button on either the direct connection or cloud-based **Ivanti Patch for Windows® Servers Agent Registration** dialog, the **Proxy Configuration** dialog is displayed. This dialog enables you to specify the proxy settings the agent will use during the registration process.



My network connection uses a proxy server	If you are required to enter a user name and password each time you launch your browser and access the Internet, it typically means you are using a proxy server and you should enable this check box. If you do not use a proxy server, clear this check box and then click OK (you can ignore the rest of this dialog).

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Automatically detect proxy settings	If you want the program to automatically determine the proxy settings by using the Web Proxy Auto Discovery protocol, enable this check box. In this case you can skip the **Proxy server address** and the **Proxy server port** options.
Proxy server address	Type the IP address of your proxy server.
Proxy server port	Type the port number used when accessing your proxy server.
Bypass the proxy server for local addresses	If enabled, this specifies that the proxy server should not be used when the agent connects to a device on the local network.
Do not use proxy server for the following	You can specify one or more IP addresses that do not use the proxy server. If you specify multiple exception entries they must be separated by semicolons.
The proxy server uses this type of authentication	The options are: • **Basic Authentication:** The credentials are sent across the network to the proxy server in plaintext. • **Digest Authentication:** The credentials are encrypted using a hash function before they are sent across the network to the proxy server. • **NTLM Authentication:** Windows NT LAN Manager (NTLM) authentication is used when sending credentials to the proxy server. • **Negotiate Authentication:** The agent and the proxy server will negotiate to determine which authentication method to use.
Proxy server user name	Type the user name to use when authenticating to the proxy server. After the registration process is complete and the agent has a policy, the agent will use the proxy credentials specified in the agent policy rather than the user name and password you specify here.
Proxy server password	Type the password to use when authenticating to the proxy server.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating and Using a Manual Installation Script

When manually installing Ivanti Patch for Windows® Servers Agent on machines, one option is to create a script that will automatically pass all necessary agent information to the installation wizard. You can copy the script to a key fob or a USB flash drive and then easily move from machine to machine installing the agent.

The following scripts are provided only as examples. Do not attempt to use these scripts in your organization without modifying the input values and performing adequate testing.

Example script for passphrase authentication

STPlatformUpdater.exe /wi:"/qn /l*v install.log SERVERURI=*https://consolename:3121* POLICY=*policyname* AUTHENTICATIONTYPE=PASSPHRASE PASSPHRASE=*secret*"

Example script for Windows authentication

STPlatformUpdater.exe /wi:"/qn /l*v install.log SERVERURI=*https://consolename:3121* POLICY=*policyname* AUTHENTICATIONTYPE=WINDOWS SERVERUSERNAME=*domainname\Your.Name* PASSWORD=*secret*"

Example script for cloud-based agent installation

STPlatformUpdater.exe /wi:"/qn /l*v install.log ACTIVATIONKEY=*12345abc-2abc-3abc-4abc-123456789abc*"

Where:

- **STPlatformUpdater** is a bootstrap installer for the agent platform installation
- **/wi** means pass this to Windows Installer.
- **/qn** means no user interface activity from the installer.
- **/l*v** means write a log for the installation attempt. It has one parameter that specifies the log file name.
- **SERVERURI** is the address, port, and scheme (e.g. https://) used to connect to the console for registration and check-in.
- **POLICY** is the name of the agent policy that will be assigned to the agent.
- **AUTHENTICATIONTYPE** is either PASSPHRASE or WINDOWS (this is dictated by the **Tools > Options >Agents** dialog).
- **PASSPHRASE** is the passphrase used to authenticate the agent to the console (used only if AUTHENTICATIONTYPE=*PASSPHRASE*).

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **SERVERUSERNAME** is the name of a user who has rights to install an agent (used only if AUTHENTICATIONTYPE=*WINDOWS*).
- **PASSWORD** is the password used to authenticate the user to the console (used only if AUTHENTICATIONTYPE=*WINDOWS*).
- **USECURRENTCREDENTIALS=1** can be used in place of SERVERUSERNAME and PASSWORD if you want to authenticate using the credentials of the person who logged on to run the script.
- **ACTIVATIONKEY** is the activation key that was created using the Protect Cloud service.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Troubleshooting Agent Installation Errors

If an error occurs during an agent installation, the error messages displayed in the Operations Monitor are the best place to begin the troubleshooting process.

- **Failure copying files:** This normally indicates a problem with the credentials being used to connect to the agent machine. The default credentials or "last used" credentials may not be the correct credentials to use for a particular machine.
- **Registration failure:** This normally indicates that the agent cannot establish a connection with the console. There may be a firewall issue, there may be ports that are unopened, there may be a DNS issue, or the agent service may not be active on the agent machine.
- **Check-in failure:** This normally indicates a timeout or network issue, and the agent will fail to download all necessary files.

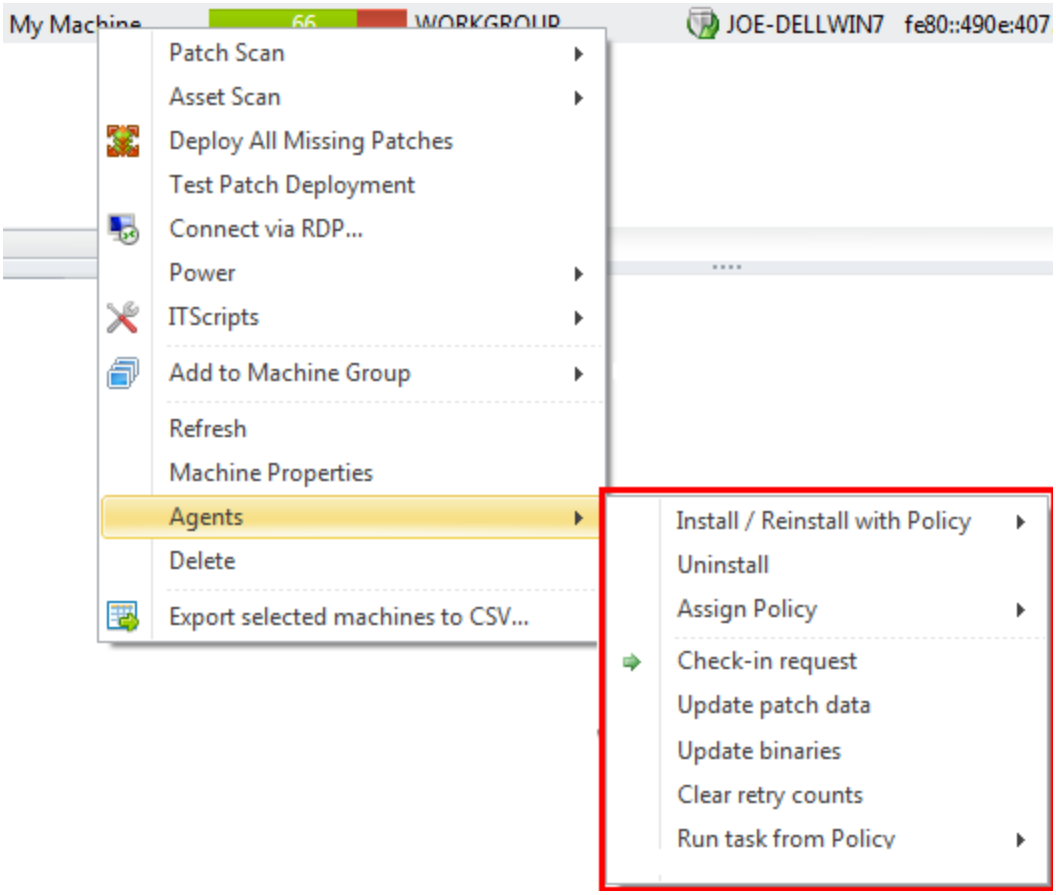
You can also view the Ivanti Patch for Windows® Servers Agent installation log on the agent machine. The log file is located in the **C:\WINDOWS\Temp\<GUID>** directory. The installation log will show any error messages that were generated during the agent installation process.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Managing Your Agents

You can use Machine View or Scan View to manage the machines that are running an agent policy. You can install an agent onto machines, you can assign a different policy to machines that already contain an agent, you can uninstall agents from machines, and you can issue a number of commands. You can also use the **Agent State** column in Machine View to determine which machines have Ivanti Patch for Windows® Servers Agent installed.

All actions are performed by right-clicking the desired machines and then selecting the **Agents** menu.



Install / Reinstall with Policy	Installs an agent on the selected machine(s). If an agent already exists on a machine, it will reinstall the agent with the selected policy. The installation process will begin immediately. The target machine(s) must be online and able to communicate with the console. If a machine is not online the installation will fail.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	TIP: If you have target machines that are away from the corporate network and unable to contact the console, consider installing agents from the cloud.
Uninstall	Will remove the agent from the selected machine(s). • If an agent machine is online and configured to listen for policy updates, the agent will be uninstalled immediately. • If an agent machine is online but is not configured to listen for policy updates, the agent will be uninstalled the next time the agent checks in with the console. • If an agent machine is not currently online, the uninstall will be performed the next time the agent is online and checks in with the console or the cloud.
Assign Policy	Applies only to machines that already have agents installed. It will assign a different policy to the selected agent machines. • If an agent machine is online and configured to listen for policy updates, the new policy will be assigned immediately. • If an agent machine is online but is not configured to listen for policy updates, the new policy will be assigned the next time the agent checks in with the console. • If an agent machine is not currently online, the new policy will be assigned the next time the agent is online and checks in with the console or the cloud. The advantage of **Assign Policy** over **Install / Reinstall with Policy** is that it is quicker. This is because it is only updating policy files and not installing an entire agent.
	The following commands apply only to machines that already have agents installed, that are online, and that are configured to be listening agents.
Check-in request	Forces the selected agent machines to immediately check-in with the console and download the latest policy.
Update patch data	Directs the agents to download the latest patch data.
Update binaries	Directs the agents to download the latest scan engines and data files.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Clear retry counts	Clears all patch counters on the agents. A unique patch counter exists for every patch an agent tries to download and for every patch an agent tries to install. A patch counter will increment whenever a patch download or a patch installation fails. Failed download and installation attempts will be recorded in the patch log. If a patch fails to download after 11 attempts or fails to install after 3 attempts the agent will stop trying to deploy that particular patch. The only way to resume the deployment of that patch is to clear the counter.
Run task from policy	Enables you to initiate any of the tasks currently defined within the selected agents. When you select a task name a confirmation dialog is displayed. If you choose to continue, the task is immediately started on the agent machines. See Creating a New Agent Policy for information on the types of tasks that may be available.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Monitoring Ivanti Patch for Windows® Servers Agent Actions

You cannot use the console to watch the actual scans, patch deployments, etc. as they are performed by agents on each target machine. For that you must use the agent client program. You can, however, view the most recent results of agent scans and deployments using Machine View. The results are reported to the console and displayed on the appropriate tabs in the middle pane. The top pane can be used to determine which machines have successfully installed Ivanti Patch for Windows® Servers Agent; it does this by displaying the **Active** icon in the **Agent State** column. The top pane of Machine View will also display the **Assigned Agent Policy**, the **Reported Agent Policy**, the **Last Agent Check-In**, and the time of the last scans. See Determining Which Machines Have Agents for more information.

When agents check in with the console they will be listed in the machine group from which they were last scanned from the console. See Machine Group Information is Dynamic for more information.

If you wish to produce one or more reports that show the agent activity that has been reported to the console you can do so using the Report Gallery.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Determining Which Machines Have Ivanti Patch for Windows® Servers Agent

You can use Machine View to easily determine which machines in your network have Ivanti Patch for Windows® Servers Agent installed.

1. Select **View > Machines** to view a list of all machines that have been scanned at least once by the program.

   If you want to make sure you get a list of all machines in your network, perform a scan of all machines in your network before going to Machine View.

2. In the heading row, click the **Agent State** column heading.

   This will sort the table, grouping together all machines that have Ivanti Patch for Windows® Servers Agent installed and placing that group at the top of the table. Click the icon a second time to move to the top of the table the group of machines without Ivanti Patch for Windows® Servers Agent installed.

   There are four possible states:

   -  = Ivanti Patch for Windows® Servers Agent is active on the machine
   -  = Ivanti Patch for Windows® Servers Agent is not active on the machine (meaning the service is either stopped or not installed on the machine)
   -  = an agent error has occurred
   -  = the agent has been removed

3. To sort the list by policy name, click the **Assigned Agent Policy** column heading.

TIP: Another option in Machine View is to select **Has an Agent Policy** in the **Smart Filters** box. Only machines with Ivanti Patch for Windows® Servers Agent installed will be displayed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Ongoing Maintenance Tasks

If the agents do not have Internet access, in most cases this means they will be downloading the latest scan engines, XML data files, and patch files from one or more distribution servers rather than from the default websites. In this case you will need to make sure the files on the distribution server(s) are updated on a regular basis. This can be done either automatically or manually. See Synchronizing Servers for complete details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

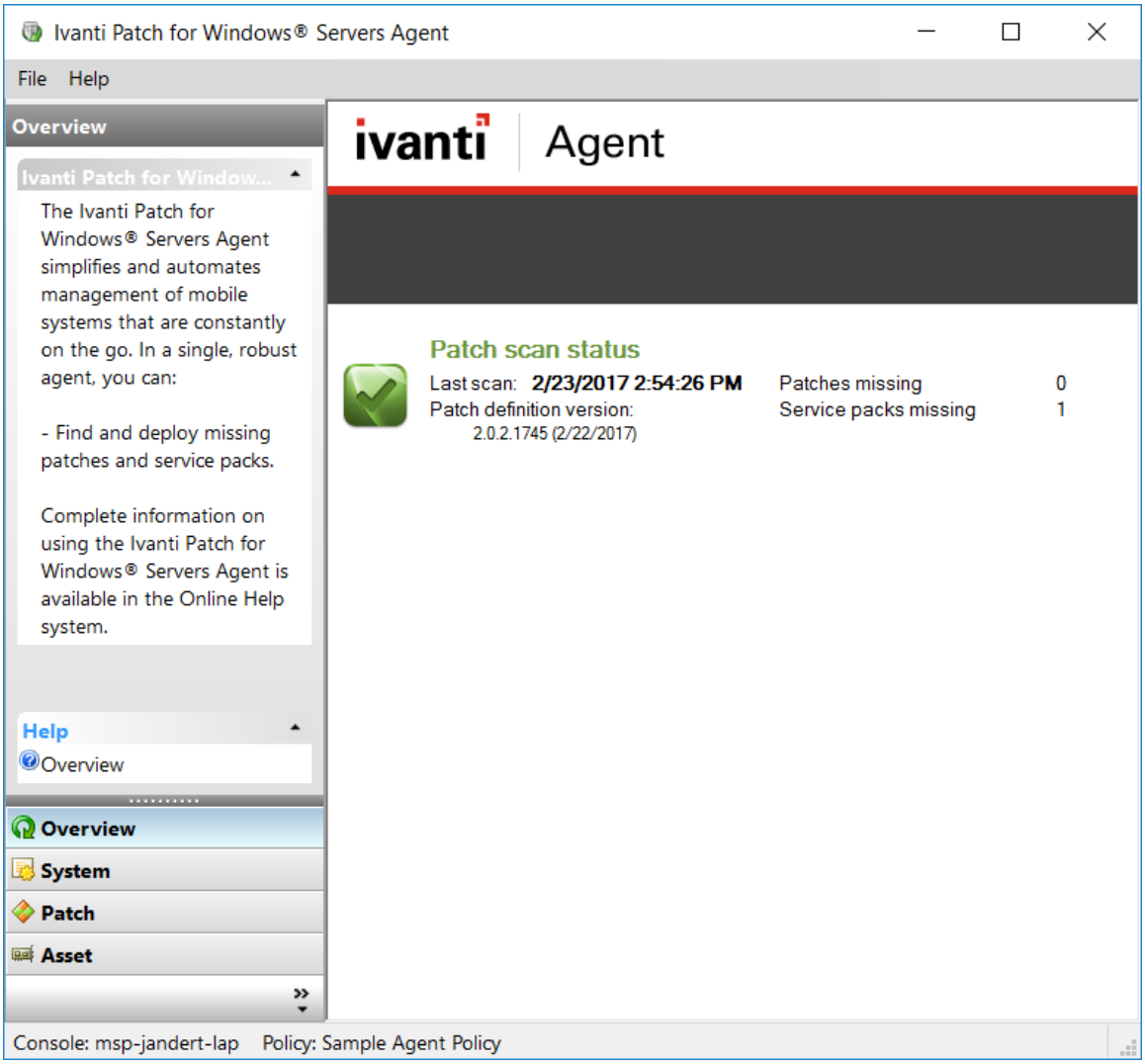
Using an Agent on a Machine

The users of each agent machine can, if you permit, control many of the Ivanti Patch for Windows® Servers Agent features on their machine. They do this using the Ivanti Patch for Windows® Servers Agent client program. To access this program they either:

- Select **Start > Ivanti Patch for Windows® Servers > Ivanti Patch for Windows® Servers AgentStart > All Programs > ScriptLogic Corporation > Patch Authority Ultimate Agent**
- Double-click the Ivanti Patch for Windows® Servers Agent service icon that may reside in their machine's system tray



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



If users want information on how to use the client program they can simply click **Help > Contents** from the main menu.

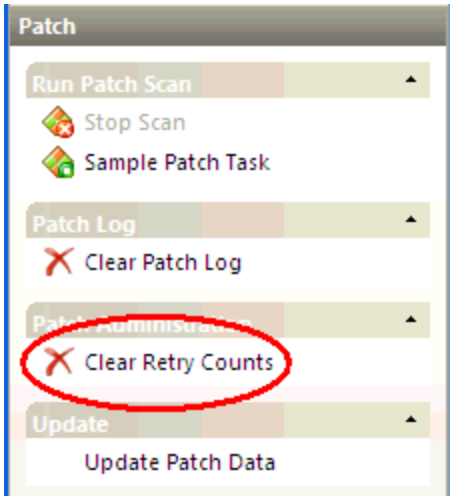
If multiple users are logged on to a machine, only one of the users will have access to the client program. The first user to launch the program will succeed, for all other users the program will fail.

Administrator Tools within the Client Program

The Ivanti Patch for Windows® Servers Agent client program contains a few tools that are intended for use by you, the system administrator.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- The lower left corner of the status bar displays the name of the console that configured the agent. It also displays the name of the agent policy that is being used. This can be extremely useful, especially if you maintain multiple consoles and/or multiple agent policies.
- The client program Patch function contains a **Clear Retry Counts** button within the Patch Administration list. This button clears all patch counters. A unique patch counter exists for every patch the program tries to download and for every patch the program tries to install. A patch counter is incremented whenever a patch download or a patch installation fails. If a patch fails to download after 11 attempts or fails to install after 3 attempts the client program will stop trying to deploy that particular patch. The only way to resume deployment attempts for that patch is to click **Clear Retry Counts**. Users may notice the deployment error messages in the Patch Log but they are unlikely to know to click this button unless directed to do so by an administrator.



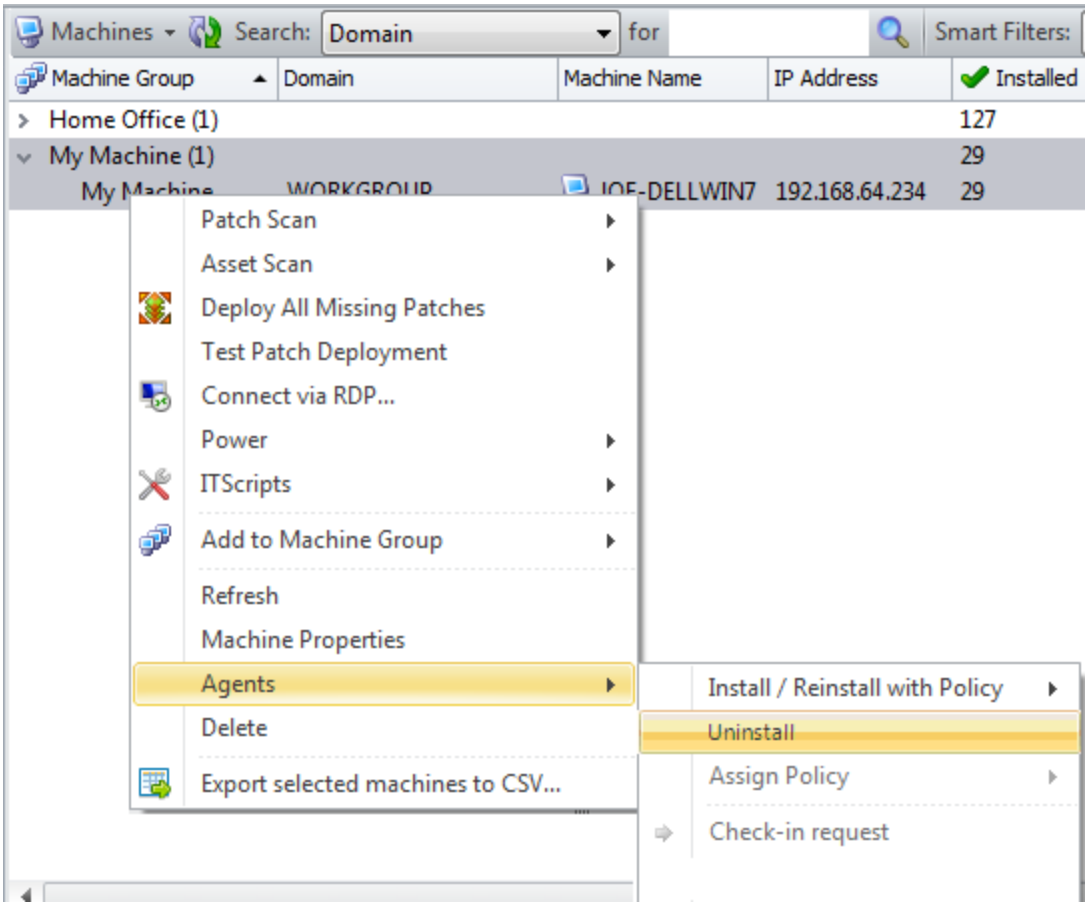
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Uninstalling Ivanti Patch for Windows® Servers Agent

Using Machine View to Uninstall Agents

You can use the console to uninstall agents from both connected and disconnected machines. The uninstall will occur immediately for agent machines that are online and able to communicate with the console. For disconnected machines, the uninstall will occur the next time the agent checks in with the console or the cloud and sees it is no longer assigned to a policy.

To initiate the uninstall, from within Machine View, right-click the selected machines and select **Agents > Uninstall**.



Manually Uninstalling Ivanti Patch for Windows® Servers Agent

To manually uninstall Ivanti Patch for Windows® Servers Agent from a target machine:

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

1. Select **Start > Settings > Control Panel > Add or Remove Programs**.

   On Windows Vista and other newer operating systems this is **Start > Settings > Control Panel > Programs and Features**.

2. If the agent policy contains a patch task, locate the program named **Ivanti Patch for Windows® Servers Patch Engine**, select it, and then click **Remove**.
3. If the agent policy contains an asset task, locate the program named **Ivanti Patch for Windows® Servers Asset Engine**, select it, and then click **Remove**.
4. Locate the program named **Ivanti Patch for Windows® Servers Agent**, select it, and then click **Remove**.

The disadvantage of using this method is that the uninstall will not be reported back to the console.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating a New Ivanti Patch for Windows® Servers Agent Policy



Show Me!

To view a video tutorial on this topic, click the video icon on the left.

An agent policy defines exactly what an agent can or cannot do. With Ivanti Patch for Windows® Servers Agent you can create as many different agent policies as is needed. This provides a great deal of flexibility, enabling you to assign different agent policies to different machines in your organization.

All agent policies are configured on the Ivanti Patch for Windows® Servers console and then either "push installed" to the desired target machines or installed manually. An agent policy can be configured with any combination of patch, asset, and/or power management capabilities.

To create a new Ivanti Patch for Windows® Servers Agent policy:

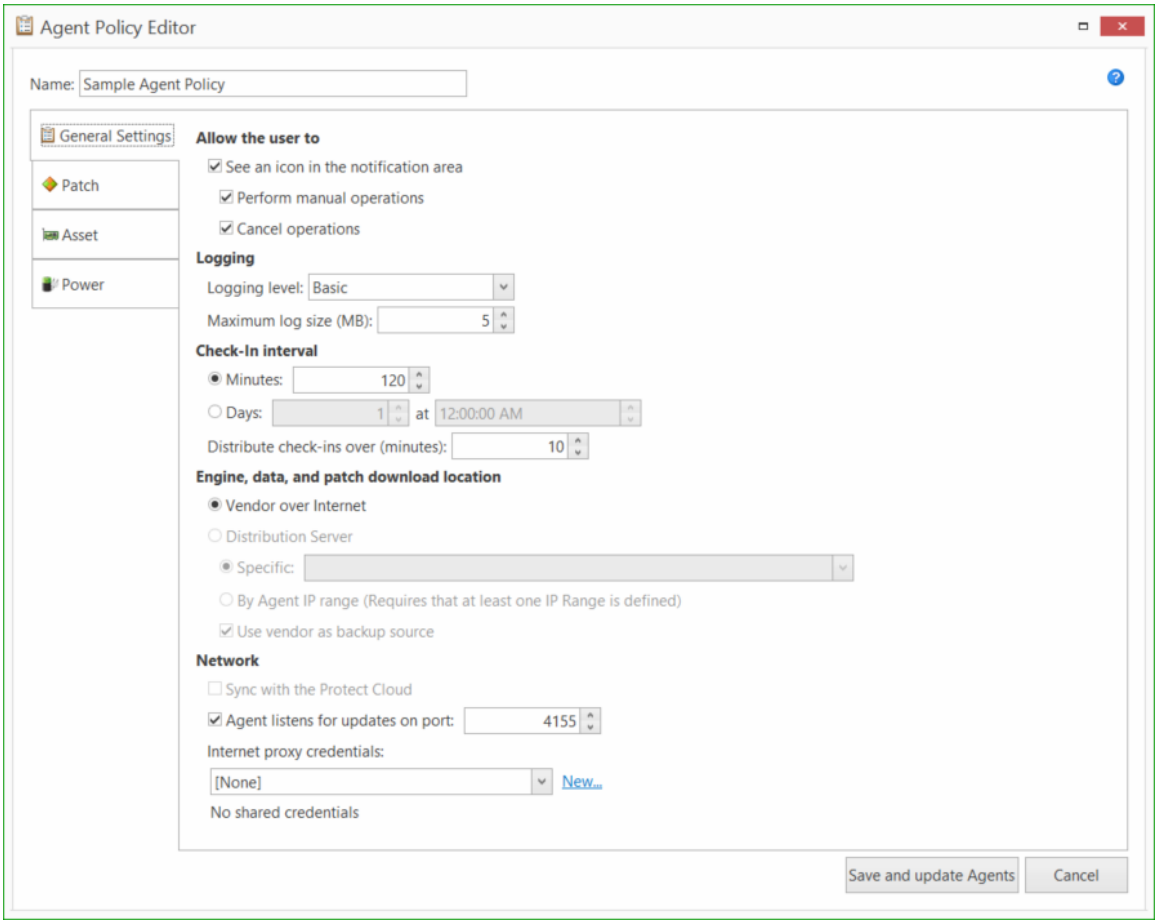
1. From the main menu select **New >Agent Policy**.
2. Type a name for the new agent policy and then click **OK**.

   The **Agent Policy Editor** window is displayed.
3. See the following topics for information on configuring the agent policy:
   - Configuring General Settings
   - Configuring Patch Tasks
   - Configuring Asset Tasks
   - Configuring Power Tasks

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Configuring General Settings for a Ivanti Patch for Windows® Servers Agent Policy

There are a number of general settings to configure for a Ivanti Patch for Windows® Servers Agent policy. You must configure these settings before installing the agents on the desired target machines.



See an icon in the notification area	The agents can be configured to run invisibly on each target machine, or you can elect to install an icon in the notification area of each machine that provides the users of the machines a certain amount of control over the service. • If you want to allow users to control certain aspects of the Ivanti Patch for Windows® Servers Agent service, enable this option. Users will be able to launch the client-based program by double-clicking the icon.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• If you do not enable this option, the icon will not appear in the notification area and the agent interface will not run unless it is launched by the user. When the agent interface is run the user will have no control other than to watch what is happening. The notification area icon will not be visible on the target machine for any currently logged on user until the next time the user logs on, or if the user starts the Ivanti Patch for Windows® Servers Agent program using the Windows Start menu.
Perform manual operations	Enables a user on a target machine to manually initiate an operation such as a patch scan.
Cancel operations	Enables a user on a target machine to stop an operation that is in progress.
Logging level	Specify the amount of logging you want the agent to perform. The options are: • **Basic**: Records *Error*, *Informational*, and *Warning* message types in the log. This is the default value. • **All**: Records *Error*, *Informational*, *Warning*, and *Verbose* message types in the log. Logging all message types is typically only necessary when performing troubleshooting tasks. The log files will reside on each agent machine in the following location: **C:\ProgramData\LANDESK\Shavlik Protect\Logs C:\ProgramData\ScriptLogic Corporation\Patch Authority Ultimate\Logs.**
Maximum log size	Specify the maximum log size. Specifying a very large log size will enable you to record a longer log history but it will of course require more system resources. The default value is 5 MB. If the log file becomes full a new log file is opened and logging will continue. If the second log file becomes full, the first log file is deleted and a new log file will be created. This means there will always be a maximum of two log files on the console.
Check-In interval	Specifies how often the agents will check in (synchronize) with the console. At each check-in the agent refreshes its license and looks for any policy changes. It also checks if it is assigned a distribution server. If it is assigned a distribution server it will use it to download the latest scan engines and XML data files. If it is not assigned to a distribution server then the agent downloads the engines and data files from the Web. If an agent machine is offline when the next check-in interval occurs, the agent will immediately check in when network connectivity is restored.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	Agent licenses must be refreshed at least once every 45 days or they will expire. • **Minutes:** Use this option if you want the agents to check in more than once a day, or if you don't care what time of day the agents will check in with the console and with the distribution server. Valid values are from 1 - 600 minutes. • **Days**: Use this option to specify the number of days between check-ins. You can also use this option to specify a specific time of day for the check-in (for example, late at night when there is more network bandwidth available). • **Distribute check-ins over (minutes)**: Staggers the exact time the agents will check-in so as not to overtax the console (and the default website or the optional distribution server) with simultaneous requests.
Engine, data, and patch download location	Specifies if a distribution server will be used by the agents when downloading the latest scan engines, XML data files, and patches. The agents will look for updated files every time they perform a scan. The available options are: • **Vendor over Internet:** Specifies that the agents will download the files from the default websites. A distribution server will not be used. • **Distribution Server:** Specifies that a distribution server will be used. You must specify which server(s) to use. If the agents are being used to deploy custom patches then you must specify the use of a distribution server. This is because there is no download URL for custom patches, meaning the agents cannot pull the custom patches from a vendor and must therefore be able to pull them from one or more distribution servers. • **Specific**: You can select the name of an existing distribution server. You must have previously configured one or more distribution servers in order for the names to be pre-populated in this box. For more information see Configuring Distribution Servers. • **By Agent IP range**: If you have multiple distribution servers defined for your network, each distribution server is typically assigned to service a particular IP address range. The distribution server used when downloading files to a target machine will be determined by the target machine's IP address. See Assigning IP Addresses to Servers for more details.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **Use vendor as backup source**: If the designated distribution server is not available, the agent will download the latest scan engines and XML data files from the default websites.
Network	• **Sync with the Protect Cloud:** Specifies that the agent will have the option to use Protect Cloud to retrieve the latest agent policy information, enabling it to perform synchronization via the cloud. This check box is only available if your console is registered with Protect Cloud. When you click Save and update Agents, a copy of the agent policy and all necessary components will be written to the Protect Cloud service. • **Agent listens for updates on port:** Specifies that the agent will listen to the console for policy updates. If an agent's policy is updated, or if it is assigned a different policy, the console will issue a "check in now" command to the agent. The agent will immediately download the new or updated policy from the console. Only agent machines that are online and able to communicate with the console will be able to receive the command. • **Port**: Specifies the port used by the agent on the target machine when communicating with the Ivanti Patch for Windows® Servers console. The default value is 4155. • **Internet proxy credentials**: If the agent machines must authenticate themselves to a proxy server when accessing the Internet, you must provide the proper credentials to the agents. Select the credential (the domain\username and password pair) used to authenticate the agent to the proxy server. To define a new credential click **New**. Only shared credentials are contained in this list. If the credential you are looking for is not listed it probably means it is not defined as a shared credential. See Defining Credentials for information on how to share a credential.
Save and update Agents	Saves all changes to the policy file and stores it on the console. Also updates any agent machines that are currently assigned this policy as follows: • If an agent machine is online and configured to listen for policy updates, the updated policy will be pushed out to that machine immediately. • If an agent machine is online but is not configured to listen for policy updates, the updated policy will be pushed out the next time the agent checks in with the console. • If an agent machine is not currently online, the updated policy will be pushed out the next time the agent checks in with the console.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	The Agent Policy Editor will be closed.
Cancel	Indicates you want to exit the Agent Policy Editor without saving your most recent changes. A "*Do you want to save your changes?*" prompt will appear that gives you a second chance to save your changes. If you click **Yes** the policy will be saved and the associated agents updated (the same as **Save and Update Agents**). If you click **No** the Agent Policy Editor will be closed without saving your changes.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating a New Patch Task

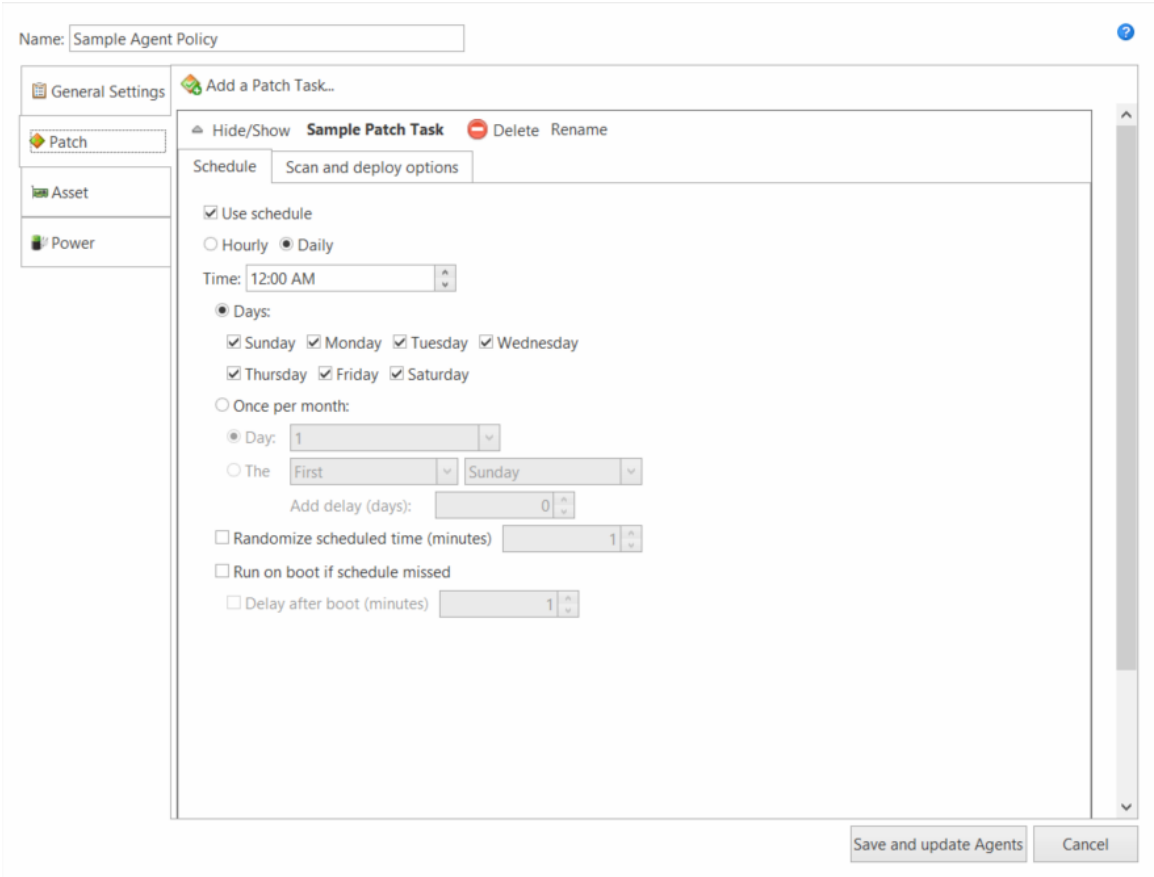
A patch task is used to define how and when the target machines will be scanned for missing patches. It can also be used to optionally deploy any patches identified as missing. If you do not create a patch task, then no patch scanning or patch deployment will be performed by agents that are assigned this policy.

You can create multiple patch tasks for one agent policy. Each task can be expanded and collapsed using the Hide/Show triangle () that resides on the task title bar. This enables you to view just the task you are working on at any one time.

While there is no theoretical limit to the number of patch tasks you can create for an agent policy, there is a practical limit. For example, it may become difficult to track and manage a policy if it contains too many patch tasks. Also, it may be problematic if you enable patch deployment on several different patch tasks. This is because that while scanning is relatively transparent to the user, deploying patches is not, as it often involves a reboot of the user's machine. In addition, you run the risk of multiple deployments occurring on one machine at the same time.

You configure agent patch tasks on the **Patch** tab. You can edit an existing patch task, or you can create a new task by clicking **Add a Patch Task**. Be sure to give the task a descriptive name because this is the name the users will see from within the client program.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



SCHEDULE TAB

The patch schedule specifies how often the task will run on a target machine. It allows you to regularly run the task at a specific time or using a specified recurrence pattern. A built-in scheduler will be provided for each agent. The scheduler will check for new patch data immediately before starting a scheduled patch task.

The agent scheduler will serialize executions of the same agent engine. For example, if you define a policy with two patch tasks that both start at 1:00 AM, they will not both start at 1:00; rather, they will be serialized (run back-to-back).

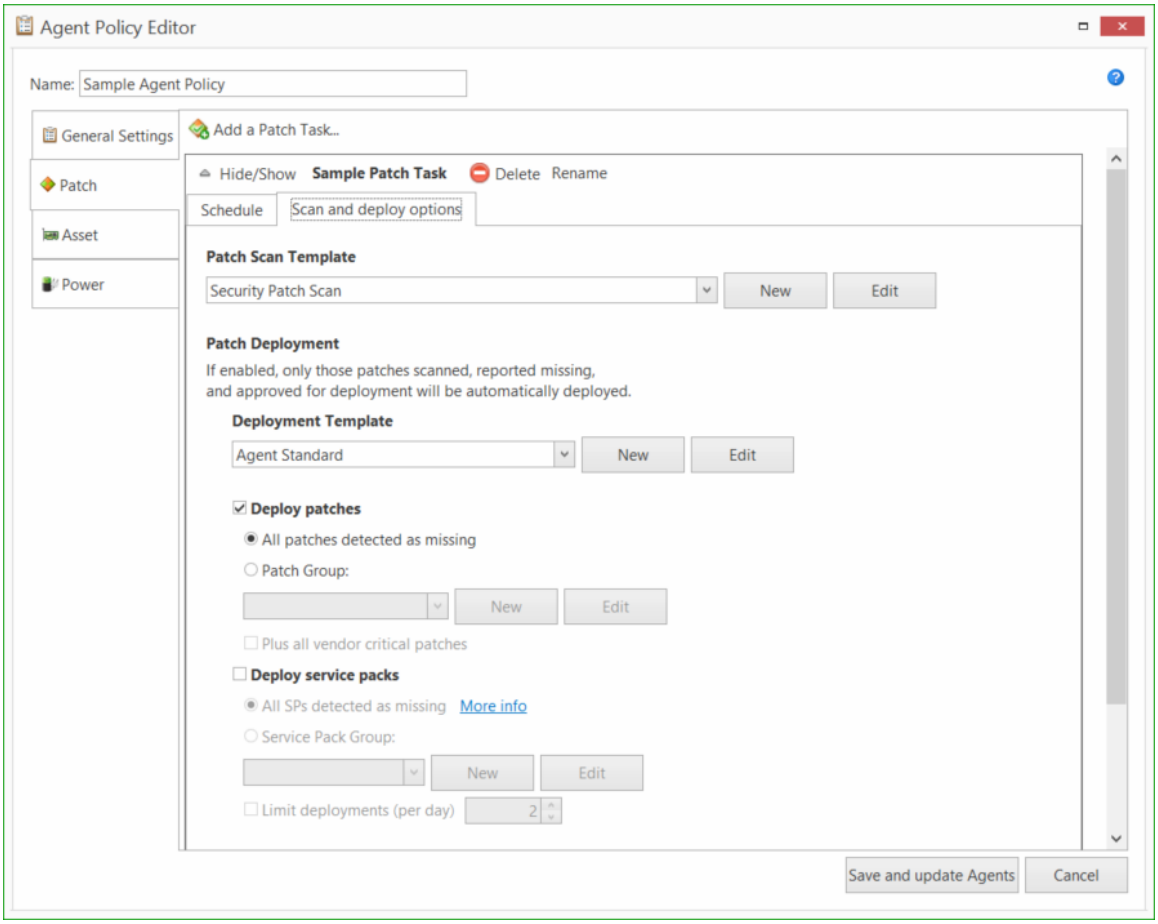
Use schedule	If enabled, the task will run on agent machines on a recurring basis according to the schedule settings. If not enabled, the schedule settings are ignored and the task must be started manually either from the console or on the agent machine.
Hourly	Allows you to schedule the task to be run on an hourly basis. • **Run every hh hours:** You can specify exactly how many hours there should be between scans. Valid values are from 1 - 100 hours.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **Starting at this time**: The first scan will begin at the specified time. Subsequent scans will be performed at the interval specified on **Run every hh hours.**
Daily	Indicates that the task will be run on the specified days, at the time of your choosing. For example, using this option a scan could be run every night at midnight, or every Saturday at 9:00 pm, or at 1:00 am the first Sunday of every month, etc. You can also use the **Daily** option to schedule a task in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly patch scan to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the task by one day.
Randomize scheduled time (minutes)	Staggers the exact time the task will be performed so as not to overtax the console or designated distribution server with simultaneous requests to download patch files, scan engines, etc.
Run on boot if schedule missed	If a scheduled task is missed while a target machine is powered off, this option enables you to force the task to automatically run whenever the machine is restarted. The task will run immediately unless you enable the **Delay after boot (minutes)** check box, in which case the execution will be delayed by the specified number of minutes.

SCAN AND DEPLOY OPTIONS TAB

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Patch Scan Template	You must specify the template to use when an agent performs a patch scan. The patch scan template dictates exactly what will be scanned for and what will be ignored during a scan. The list of templates available for selection will include the two predefined templates (Security Patch Scan and WUScan) plus any custom templates you've already defined. You can also do the following: • **New**: Enables you to create a new patch scan template from scratch. • **Edit**: Enables you to edit an existing, custom patch scan template. The predefined templates cannot be edited. If you edit and save a template that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console. If you click **New** or **Edit**, the **Patch Scan Template** dialog is displayed. See Creating a New Patch Scan Template for details on configuring the template.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	The automatic deployment function and the automatic email function on the patch scan template is not supported by Ivanti Patch for Windows® Servers Agent. If these functions are enabled they will be ignored.
Deployment Template	You must specify the template to use when an agent performs a patch deployment. The list of templates available for selection will include the predefined deployment templates (Agent Standard, Standard, and Virtual Machine Standard) plus any custom templates you've already defined. You can also do the following: • **New**: Enables you to create a new deployment template from scratch. • **Edit**: Enables you to edit an existing, custom deployment template. The predefined deployment template cannot be edited. If you edit and save a template that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console. If you click **New** or **Edit**, the **Deployment Template** dialog is displayed. See Creating a Deployment Template for details on configuring the template. Automatic email notifications, custom actions, and distribution server options that may be specified in the deployment template do not apply to a Ivanti Patch for Windows® Servers Agent.
Deploy patches	If you want the agent to be able to automatically deploy patches that are identified as missing by the patch scan, enable this check box. When the agents perform a patch deployment they will deploy only those patches that are: • Scanned for by the patch scan template, and • Reported as missing, and • Defined as *approved patches*. The approved patches can be either all patches detected as missing by a scan, or they can be limited to those patches you define in a patch group and/or to those patches deemed critical by the patch vendor. The list of approved patches defined here is bound to this particular patch task. The list will not be used by other patch tasks within the agent policy. • **All patches detected as missing:** Specifies that any patch identified as missing will be eligible for deployment.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **Patch Group:** Only those patches contained in the specified patch group will be deployed by the agent. If a scan detects missing patches not included in this group, those patches will not be deployed.

  Plus all vendor critical patches: Specifies that in addition to the patches defined in the patch group, the list of patches approved for deployment should also include any patches identified as critical by the patch vendor. This gives you the security of knowing that if your patch group is out of date you will still always be able to deploy any new critical patches.

  To deploy only vendor critical patches, enable this check box and then specify an empty patch group in the **Patch Group** box.

- **New:** Enables you to make a new patch group. For more information see Creating and Editing a Patch Group.

- **Edit:** Enables you to make modifications to the selected patch group. Be careful here, because any modifications you make will affect any other scan templates that are using the patch group. If you edit and save a patch group that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console.

If you also choose to enable the deployment of service packs (see the **Deploy Service Packs** option), on an agent machine that is missing both service packs and patches, service packs are deployed first.

Patch Deployment Process

Once the list of approved patches is determined, the patches are downloaded and installed according to their priority. Security patches are downloaded first, followed by all other patch types. The downloads occur in the background using idle bandwidth not being used by other applications. Foreground tasks such as Web browsing are not affected by the patch download process.

Each patch task is allotted a 60 minute window to download the missing patches. (This is part of a two hour total maintenance window that is allocated for downloading missing service packs and patches.) Only those patches that are successfully downloaded during this 60 minute window will be installed by the active patch task. If the patch task cannot finish downloading all missing patches during the 60 minute window, the remaining patches will be identified, downloaded, and installed the next time the patch task is run.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	If an agent machine becomes disconnected from the network during a file download, the process will be suspended and will automatically resume where it left off when the network is available again. This technique is called checkpoint/restart and is extremely useful for machines that are frequently disconnected.
Deploy service packs	If you want the agent to be able to automatically deploy service packs that are identified as missing by the patch scan, enable this check box. When the agents perform a service pack deployment they will deploy only those service packs that are: 1. Scanned for by the patch scan template, and 2. Reported as missing, and 3. Approved for deployment. The approved service packs can be either all service packs detected as missing by a scan, or they can be limited to those service packs you define in a service pack group. The list of approved service packs defined here is bound to this particular patch task. The list will not be used by other patch tasks within the agent policy. • **More info:** A link to the About Service Pack Groups Help topic that explains how service pack groups are used by the program. • **All SPs detected as missing:** Specifies that any service pack identified as missing will be eligible for deployment. • **Service Pack Group:** Only those service packs contained in the specified service pack group will be deployed by the agent. If a scan detects missing service packs not included in this group, those service packs will not be deployed. • **Limit deployments (per day):** Specifies the maximum number of service packs that can be deployed to a machine in one day. Service packs can take a long time to deploy and almost always require a reboot of the machine, so you typically want to keep this number rather small. If you do not limit the number of service pack deployments in a day you run the risk of overwhelming a machine if it is missing a large number of service packs. If a machine is missing more service packs than the specified limit, the additional service packs will be deployed the next time the patch task is run.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

TIP: Note that a "day" in this case is considered to be a calendar date and not a 24 hour period. This means the day is reset at midnight. If you were to schedule the patch task to run on an hourly basis (not recommended), it would allow you to maximize an overnight maintenance window by deploying the maximum number of service packs before midnight and then again immediately after midnight.

- **New:** Enables you to make a new service pack group. For more information see Creating and Editing a Service Pack Group.
- **Edit:** Enables you to make modifications to the selected service pack group. Be careful here, because any modifications you make will affect any patch task that references the service pack group. Also, if you edit and save a service pack group that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console.

Service Pack Deployment Process

If an agent machine is missing multiple service packs, only one service pack will be installed at a time. The patch task will begin by initiating the download of all missing service packs. Operating system service packs are downloaded at a higher priority, but whichever service pack gets downloaded first is the one that is first installed. After the service pack is successfully installed, the machine is restarted, rescanned, and the process is repeated until all service packs are deployed or until the daily limit is reached [see the **Limit deployments (per day)** option].

In addition, each patch task is allotted a 60 minute window to complete the *download* > *install* > *restart* > *rescan* process. (This is part of a two hour total maintenance window that is allocated for downloading missing service packs and patches.) Only those service packs that are successfully downloaded during this 60 minute window will be installed by the active patch task. If the patch task cannot finish downloading all missing service packs during the 60 minute window, the remaining service packs will be identified, downloaded, and installed the next time the patch task is run.

The downloads occur in the background using idle bandwidth not being used by other applications. Foreground tasks such as Web browsing are not affected by the service pack download process.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	If an agent machine becomes disconnected from the network during a file download, the process will be suspended and will automatically resume where it left off when the network is available again. This technique is called checkpoint/restart and is extremely useful for machines that are frequently disconnected.

SAVING AN AGENT

Save and update Agents	Saves all changes to the policy file and stores it on the console. Also updates any agent machines that are currently assigned this policy as follows: • If an agent machine is online and configured to listen for policy updates, the updated policy will be pushed out to that machine immediately. • If an agent machine is online but is not configured to listen for policy updates, the updated policy will be pushed out the next time the agent checks in with the console. • If an agent machine is not currently online, the updated policy will be pushed out the next time the agent checks in with the console. The Agent Policy Editor will be closed.
Cancel	Indicates you want to exit the Agent Policy Editor without saving your most recent changes. A "*Do you want to save your changes?*" prompt will appear that gives you a second chance to save your changes. If you click **Yes** the policy will be saved and the associated agents updated (the same as **Save and Update Agents**). If you click **No** the Agent Policy Editor will be closed without saving your changes.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

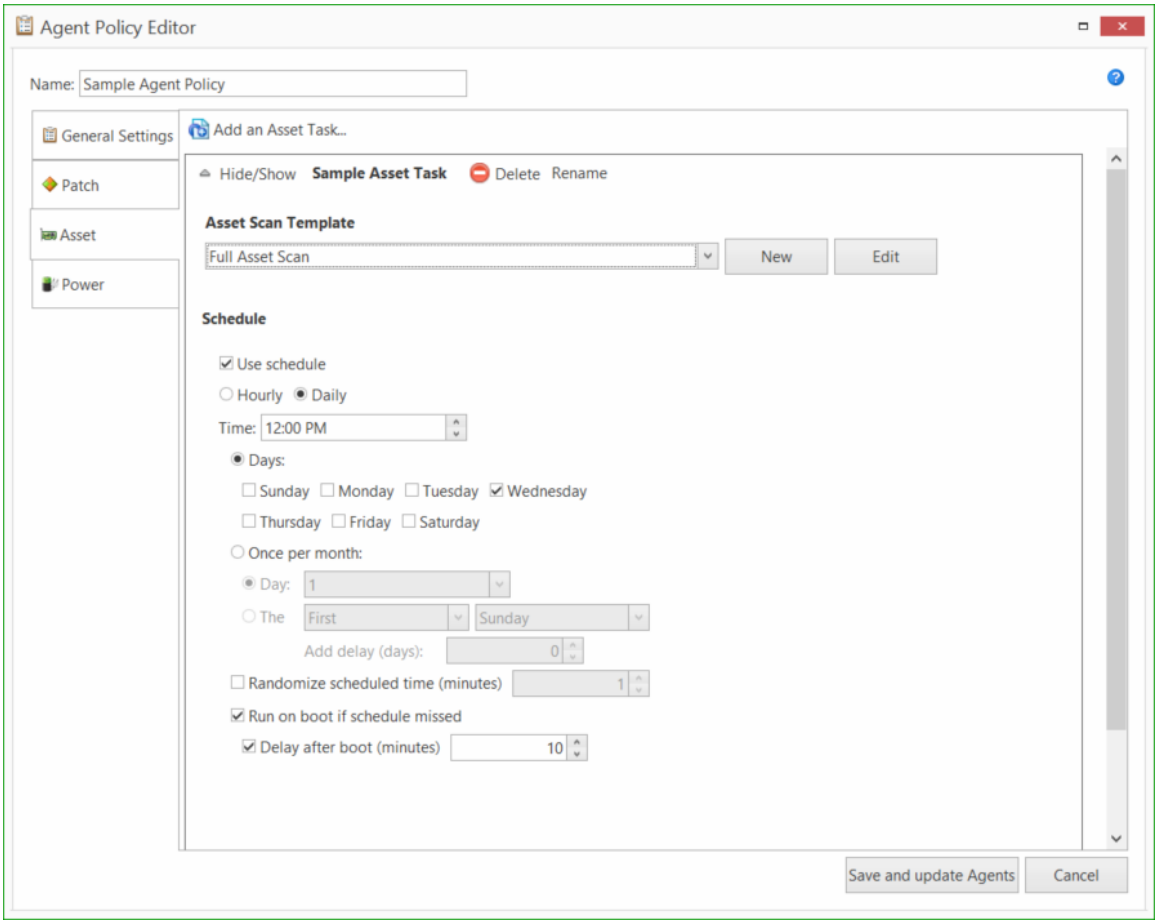
Creating a New Asset Task

An asset task is used to define how and when the target machines will be scanned to determine their software and hardware assets. If you do not create an asset task, then no asset scanning will be performed by agents that are assigned this policy. For background information about the asset management feature, see Asset Management Overview.

You can create multiple asset tasks for one agent policy. Each task can be expanded and collapsed using the Hide/Show triangle ( ) that resides on the task title bar. This enables you to view just the task you are working on at any one time.

While there is no theoretical limit to the number of asset tasks you can create for an agent policy, there is a practical limit. For example, it may become difficult to track and manage a policy if it contains too many asset tasks.

You configure agent asset tasks on the **Asset** tab. You can edit an existing asset task, or you can create a new task by clicking **Add an Asset Task**. Be sure to give the task a descriptive name because this is the name the users will see from within the client program. The results of an agent-based asset scan are reported to the console and viewable using Machine View.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Asset Scan Template	You must specify the template to use when an agent performs an asset scan. The asset scan template dictates exactly what will be scanned for and what will be ignored during a scan. The list of templates available for selection will include the predefined template (Full Asset Scan) plus any custom templates you've already defined. You can also do the following: • **New**: Enables you to create a new asset scan template from scratch. • **Edit**: Enables you to edit an existing, custom asset scan template. The predefined template cannot be edited. If you edit and save a template that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console. If you click **New** or **Edit**, the **Asset Scan Template** dialog is displayed. See Creating a New Asset Scan Template for details on configuring the template.
Schedule Area	The asset schedule specifies how often the task will run on a target machine. It allows you to regularly run the task at a specific time or using a specified recurrence pattern. A built-in scheduler will be provided for each agent. The scheduler will check for new asset data immediately before starting a scheduled asset task. The agent scheduler will serialize executions of the same agent engine. For example, if you define a policy with two asset tasks that both start at 1:00 AM, they will not both start at 1:00; rather, they will be serialized (run back-to-back). If you have an asset task and a patch task both scheduled for 1:00 AM, however, they will both be started at 1:00 AM as they use different agent engines.
Use schedule	If enabled, the task will run on agent machines on a recurring basis according to the schedule settings. If not enabled, the schedule settings are ignored and the task must be started manually either from the console or on the agent machine.
Hourly	Allows you to schedule the task to be run on an hourly basis. • **Run every hh hours:** You can specify exactly how many hours there should be between scans. Valid values are from 1 - 100 hours. • **Starting at this time**: The first scan will begin at the specified time. Subsequent scans will be performed at the interval specified on **Run every hh hours.**
Daily	Indicates that the task will be run on the specified days, at the time of your choosing. For example, using this option a scan could be run every night at midnight, or every Saturday at 9:00 pm, or at 1:00 am the first Sunday of every month, etc.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	You can also use the **Daily** option to schedule a task in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly asset scan to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the task by one day.
Randomize scheduled time (minutes)	Staggers the exact time the task will be performed so as not to overtax the console or designated distribution server with simultaneous requests to download XML files, scan engines, etc.
Run on boot if schedule missed	If a scheduled task is missed while a target machine is powered off, this option enables you to force the task to automatically run whenever the machine is restarted. The task will run immediately unless you enable the **Delay after boot (minutes)** check box, in which case the execution will be delayed by the specified number of minutes.
Save and update Agents	Saves all changes to the policy file and stores it on the console. Also updates any agent machines that are currently assigned this policy as follows: • If an agent machine is online and configured to listen for policy updates, the updated policy will be pushed out to that machine immediately. • If an agent machine is online but is not configured to listen for policy updates, the updated policy will be pushed out the next time the agent checks in with the console. • If an agent machine is not currently online, the updated policy will be pushed out the next time the agent checks in with the console. The Agent Policy Editor will be closed.
Cancel	Indicates you want to exit the Agent Policy Editor without saving your most recent changes. A "*Do you want to save your changes?*" prompt will appear that gives you a second chance to save your changes. If you click **Yes** the policy will be saved and the associated agents updated (the same as **Save and Update Agents**). If you click **No** the Agent Policy Editor will be closed without saving your changes.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

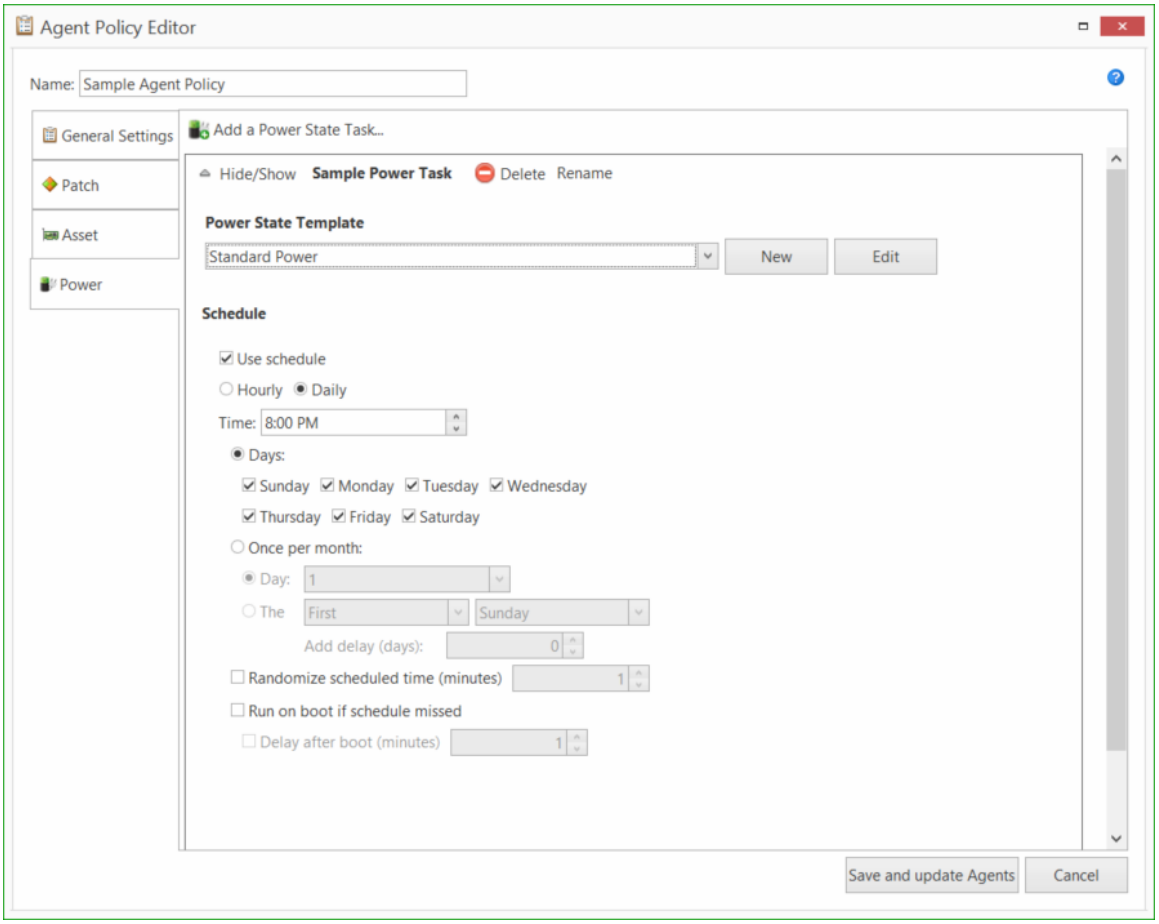
Creating a New Power Task

A power state task is used to shut down or restart the target machines and to specify what power state to leave the machines (fully powered on, sleep state, hibernate state, or powered off). If you do not create a power task, then no power state tasks will be performed by agents that are assigned this policy. For information as to why you might want to use an agent-based power state task, see When should I use each solution?. For background information about the power management feature, see Power Management Overview.

You can create multiple power tasks for one agent policy. Each task can be expanded and collapsed using the triangle ( ) that resides on the task title bar. This enables you to view just the task you are working on at any one time.

While there is no theoretical limit to the number of power tasks you can create for an agent policy, there is a practical limit. For example, it may become difficult to track and manage a policy if it contains too many power tasks.

You configure agent asset tasks on the **Power** tab. You can edit an existing power task, or you can create a new task by clicking **Add a Power State Task**.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Power State Template	You must specify the template to use when an agent performs a power task. The power state template dictates if and when the agent machines will be shut down or restarted, what control a logged on user will have over the reboot process, and what power state the machine will be left in. The list of templates available for selection will include the predefined template (Standard Power) plus any custom templates you've already defined. You can also do the following: • **New**: Enables you to create a new power state template from scratch. • **Edit**: Enables you to edit an existing, custom power state template. The predefined template cannot be edited. If you edit and save a template that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console. If you click **New** or **Edit**, the **Power State Template** dialog is displayed. See Creating and Editing a Power State Template for details on configuring the template.
Schedule Area	The power task schedule specifies how often the task will run on a target machine. It allows you to regularly run the task at a specific time or using a specified recurrence pattern. A built-in scheduler will be provided for each agent. The agent scheduler will serialize executions of the same agent engine. For example, if you define a policy with two power state tasks that both start at 1:00 AM, they will not both start at 1:00; rather, they will be serialized (run back-to-back). If you have a power state task and a patch task both scheduled for 1:00 AM, however, they will both be started at 1:00 AM as they use different agent engines.
Use schedule	If enabled, the task will run on agent machines on a recurring basis according to the schedule settings. If not enabled, the schedule settings are ignored and the task must be started manually from the console.
Hourly	Allows you to schedule the task to be run on an hourly basis. • **Run every hh hours:** You can specify exactly how many hours there should be between tasks. Valid values are from 1 - 100 hours. • **Starting at this time**: The first task will begin at the specified time. Subsequent tasks will be performed at the interval specified on **Run every hh hours.**
Daily	Indicates that the task will be run on the specified days, at the time of your choosing. For example, using this option a task could be run every night at midnight, or every Saturday at 9:00 pm, or at 1:00 am the first Sunday of every month, etc.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	You can also use the **Daily** option to schedule a task in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly power task to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the task by one day.
Randomize scheduled time (minutes)	Staggers the exact time the task will be performed. This is probably most useful if a large number of agents will be performing this power task and you don't want all your machines shutting down or restarting simultaneously.
Run on boot if schedule missed	If a scheduled task is missed while a target machine is powered off, this option enables you to force the task to automatically run whenever the machine is restarted. The task will run immediately unless you enable the **Delay after boot (minutes)** check box, in which case the execution will be delayed by the specified number of minutes.
Save and update Agents	Saves all changes to the policy file and stores it on the console. Also updates any agent machines that are currently assigned this policy as follows: • If an agent machine is online and configured to listen for policy updates, the updated policy will be pushed out to that machine immediately. • If an agent machine is online but is not configured to listen for policy updates, the updated policy will be pushed out the next time the agent checks in with the console. • If an agent machine is not currently online, the updated policy will be pushed out the next time the agent checks in with the console. The Agent Policy Editor will be closed.
Cancel	Indicates you want to exit the Agent Policy Editor without saving your most recent changes. A "*Do you want to save your changes?*" prompt will appear that gives you a second chance to save your changes. If you click **Yes** the policy will be saved and the associated agents updated (the same as **Save and Update Agents**). If you click **No** the Agent Policy Editor will be closed without saving your changes.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

About Service Pack Groups

Ivanti Patch for Windows® Servers provides the ability for agents to use a service pack group to deploy a particular set of service packs.

Example 1: Suppose Company A has a patch approval process under which they've certified four service packs as being mandatory for their organization. They do not want to deploy any patches, just the four service packs. They also want to be able to receive compliance reports. By creating a service pack group they can deploy only the specified service packs and receive a variety of deployment reports.

Example 2: Suppose you identify a certain service pack as being critical for your organization. You can create a service pack group that contains just this service pack. When your agents perform a deployment, the only service pack that will be deployed will be the service pack defined in the group.

For information on implementing and using service pack groups, see Creating and Editing a Service Pack Group and Creating and Configuring a Patch Task.

Notes About Service Pack Groups

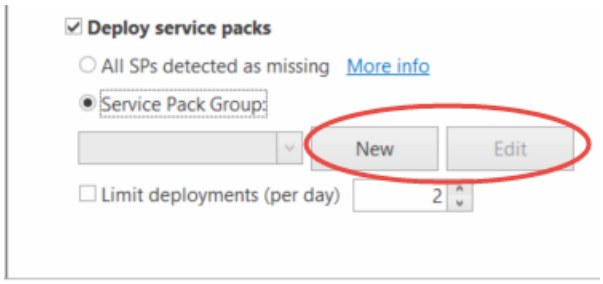
- Service pack groups apply only to agents and not to agentless deployments.
- Agent-based service pack deployments are tracked the same way as any other agent activity. See Monitoring Agents for details.
- If an agent machine is missing multiple service packs, only one service pack will be installed at a time. Ivanti Patch for Windows® Servers Agent will begin by initiating the download of all missing service packs. Operating system service packs are downloaded at a higher priority, but whichever service pack is available first is the one that is first installed. After that service pack is successfully installed, the machine is restarted, rescanned, and the process is repeated until all service packs are deployed or until the daily limit is reached.
- The downloads occur in the background using idle bandwidth not being used by other applications on the agent machine. Foreground tasks such as Web browsing are not affected by the service pack download process.
- The number of service packs that can be deployed in one day is defined by the **Limit deployments (per day)** option on the agent patch task.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating and Editing a Service Pack Group

To create a new service pack group or edit an existing service pack group:

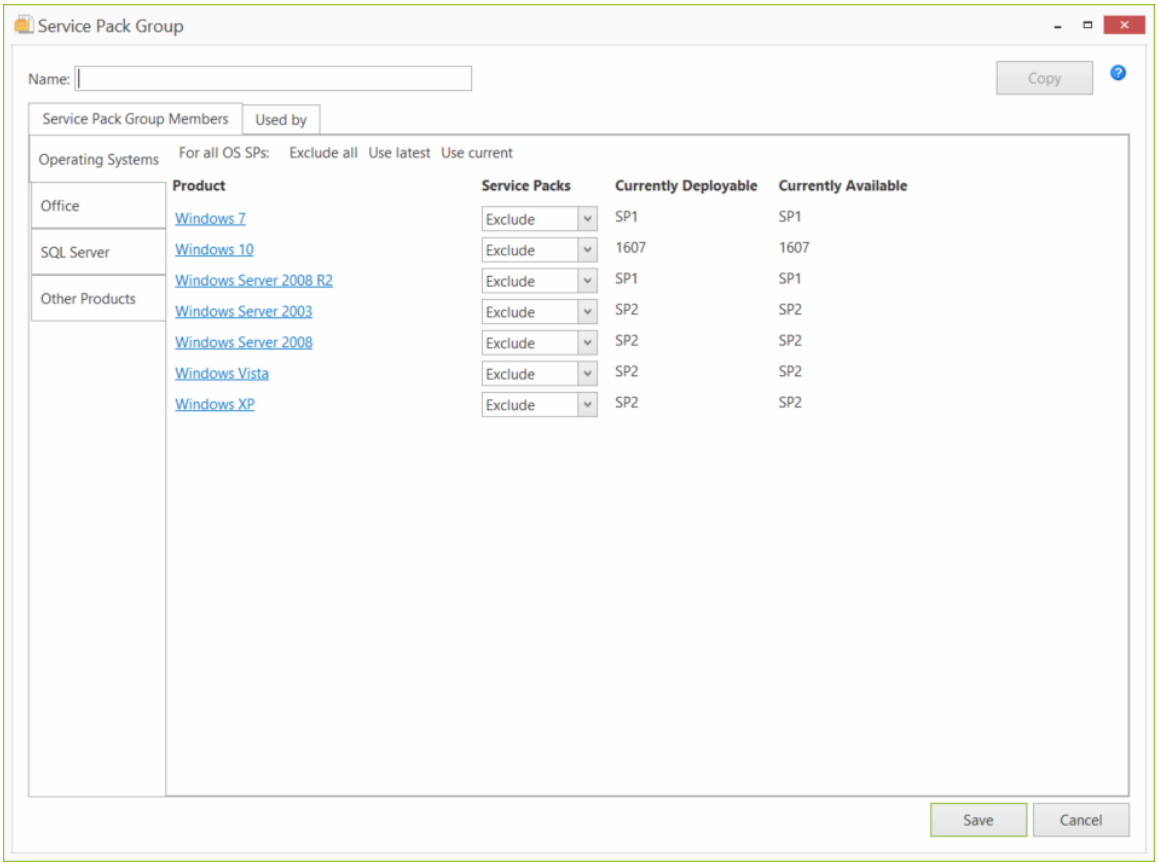
1. From within an agent patch task, enable **Deploy service packs**.
2. Enable **Service Pack Group** and then click either **New** or **Edit**.



Other options for creating a new service pack group is to select **New > Service Pack Group** from the main menu. Another option for editing an existing service pack group is to double-click the group from within the **Service Pack Groups** list. You can also use this list to copy or delete a service pack group.

This will display the **Service Pack Group** dialog.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Be careful when editing an existing service pack group. Any modifications you make will affect any patch task that references the service pack group. Also, if you edit and save a service pack group that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console.

Name	Type a name that you would like to assign to this service pack group.
Copy	Makes a copy of the service pack group. Type a new name for the group and then click **OK**.
	Displays Help information about this dialog.
Service Pack Group Members	This tab enables you to add service packs to this group. The available service packs are separated into four product categories that are represented by the tabs shown along the left side of the dialog. For each product category you can: • **Exclude all**: Excludes every service pack in the product category. This is the default value.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

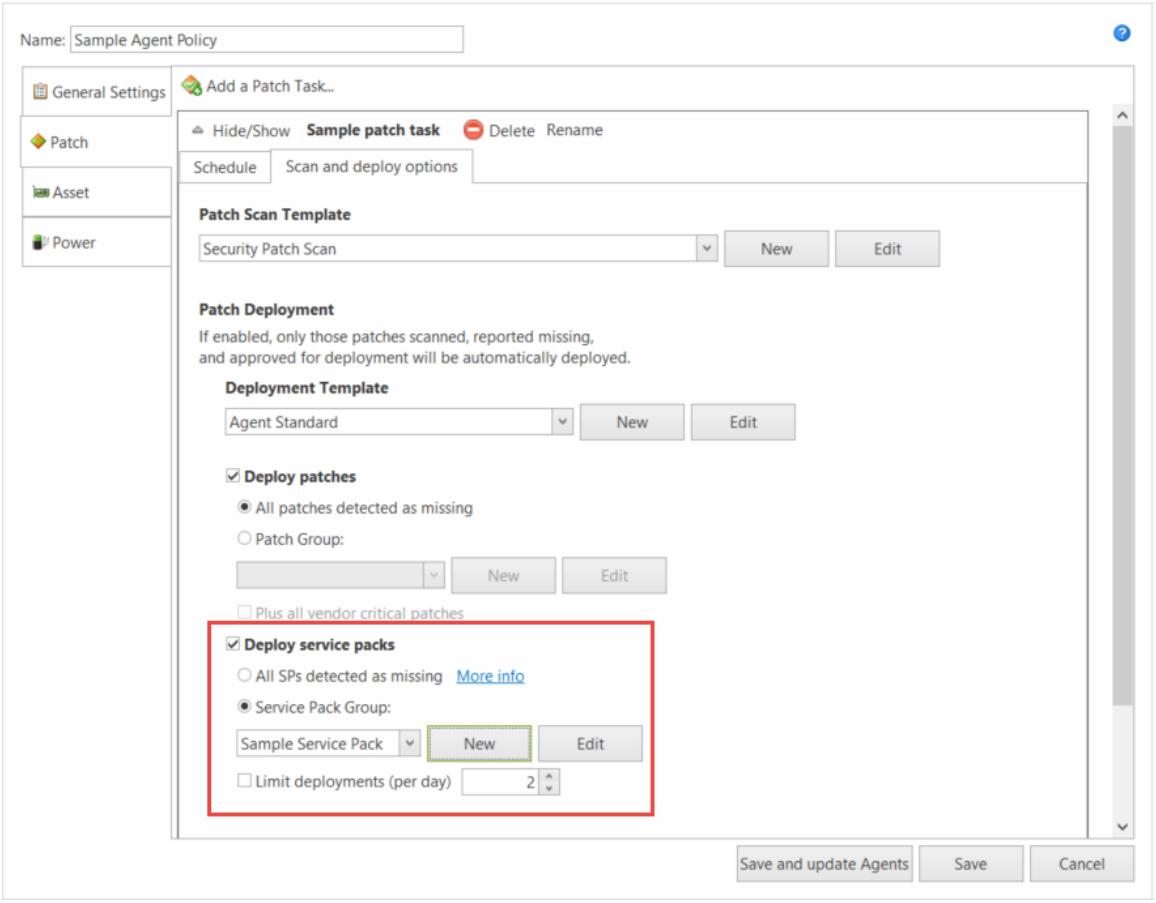
	• **Use latest**: Sets all service packs in the category to **Latest**. This means that the latest service pack available for a product always will be deployed. The advantage to this setting is that if a new service pack becomes available it will be the one that is automatically deployed. • **Use current**: Sets the value to the service pack that is currently available for each product. This value will not change if a new service pack becomes available. You can also manually set the service pack value for each individual product.
Used By tab	This tab shows you the agent policies that are currently using this service pack group. This is important to know if you are considering modifying the group, as it tells you what other areas of the program are affected.

IMPORTANT! If a new product becomes available, the product will be added to the appropriate product category the next time the Ivanti Patch for Windows® Servers XML files are refreshed. Keep in mind that the default value for any new product service packs will be **Exclude all**. If you want the new product's service pack to be included in the group you must revisit the service pack group and update the product service pack setting.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Using a Service Pack Group

A service pack group is used within an agent patch task to specify exactly which service packs should be deployed. For more information, see Creating and Configuring a Patch Task.

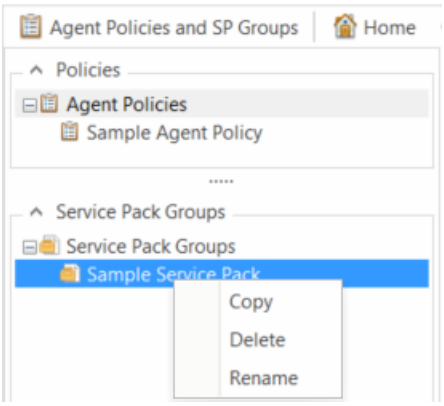


Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Copy, Delete, or Rename a Service Pack Group

To copy, delete, or rename an existing service pack group:

1. In the navigation pane select **Agent Policies and SP Groups**.
2. Right-click an existing service pack group and then select the desired menu item.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

ITScripts and Windows PowerShell™ Overview

Windows PowerShell™ is a task automation framework. It is built on Microsoft .NET Framework and provides administrators the ability to quickly and easily perform management tasks on Windows machines and applications. The ITScripts function of Ivanti Patch for Windows® Servers supports the use of PowerShell 4.0 and WinRM 2.0, enabling you to execute a variety of scripts on the console and on remote target machines. It also enables you to start a Windows PowerShell session between the console and a selected machine.

HOW-TO INFORMATION

For information on how to perform ITScripts tasks, see:

- Creating an ITScripts template
- How to Execute a Script
- Monitoring an ITScript
- ITScripts Results View

WHY USE WINDOWS POWERSHELL SCRIPTS?

PowerShell scripts enable you to perform a wide variety of administrative tasks on the machines in your organization -- from the most rudimentary task to highly advanced and complex operations. You might want to search your target machines for a particular type of data, gather and read log files, install software, create a report, determine the status of a service, read the registry, etc. PowerShell scripts are a great way to automate repetitive tasks across a large number of machines.

WHY USE Ivanti Patch for Windows® Servers TO RUN SCRIPTS?

The advantages to running scripts in Ivanti Patch for Windows® Servers include:

- Scripts execute against the machines and machine groups you have already defined in Ivanti Patch for Windows® Servers
- Use the machine and machine group credentials you have already entered in Ivanti Patch for Windows® Servers
- Scripts execute in the background
- Script execution can be run immediately or scheduled to run in the future
- Scripts are executed in parallel against the target machines and usually complete in a fraction of the time that it would take to run them serially (and you can control the level of parallelism)
- Script output is captured to files that you can review at your convenience

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- Status of script execution is displayed within Ivanti Patch for Windows® Servers
- You can open the result files directly from Ivanti Patch for Windows® Servers
- Your scripts can be parameterized, and different sets of parameters can be saved in a template or provided when you start the script or schedule it for execution
- Scripts can use the PowerShell remoting features, allowing the broadest set of capabilities provided by Windows PowerShell

MANY PREDEFINED SCRIPTS ARE AVAILABLE

The ITScripts function comes with a number of predefined scripts. The most basic scripts are free and are used to perform various utility tasks. The more advanced scripts perform more complicated tasks and can be used only if you have either a Ivanti Patch for Windows® Servers Advanced license or a separately purchased add-on license key.

You can use the Script Catalog Manager to view the predefined scripts that are available to you.

CREATE AND IMPORT CCUSTOM SCRIPTS

If you have a Ivanti Patch for Windows® Servers Advanced license or a separately purchased add-on license key, you can import custom scripts that you created or that were created by someone you trust, such as a member of the ITScripts Community Site. Any custom scripts you import will appear in the Script Catalog Manager along with the predefined scripts. Custom PowerShell modules are also supported. You can create and import modules containing cmdlets, providers, functions, variables, and aliases that you can use in your other custom scripts. For more information, see Creating a Custom Script.

TARGET TYPES

Ivanti Patch for Windows® Servers provides several target types for executing scripts. The target type indicates what the target machine requires when executing a script. The target type is set by the script author using the scriptType element and cannot be altered by Ivanti Patch for Windows® Servers. A script can only be run in one mode. In all cases the script engine runs on the Ivanti Patch for Windows® Servers console.

- **Console:** The script runs only against the console and not against a set of target machines. For example, you might use a Console script to query or modify Active Directory.
- **Any:** The script is run against selected target machines or machine groups **without** the services of WinRM (PowerShell remoting). The PowerShell client on the console communicates with the target machines by using other Windows remoting services such as remote registry service, remote Windows file sharing, WMI services, etc. The scripts will be run in parallel, not one machine at a time.

  You do not need to install any additional software on the target machines when executing scripts of this type. The only ports required are the ports required by the Windows services being used.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **WinRM Remoting:** The script runs against the target machine using WinRM (PowerShell remoting). The WinRM service must be enabled and configured on the target machine. This mode provides full PowerShell capabilities and is typically faster and more efficient. Instead of the console performing the tasks, the commands issued by the console will be performed on the target machine by the PowerShell remoting service.

  For the full list of target machine requirements when using WinRM Remoting (PowerShell remoting), see ITScripts Requirements.

- **ESXi Hypervisor:** The script runs against an ESXi Server or a vCenter Server. This type of script may use VMware vSphere PowerCLI. VMware vSphere PowerCLI lets you automate all aspects of vSphere management, including network, storage, VM, guest OS and more. Scripts of this type only run against machine groups that contain ESXi servers. If the machine group contains any other machines, they will be ignored when this script executes. For information on creating a machine group that contains ESXi servers, see Adding Virtual Machines Hosted by a Server.

You can use the Script Catalog Manager to identify the target type that will be used by a script.

SECURITY CONSIDERATIONS

Ivanti Patch for Windows® Servers provides a number of security features when using the ITScripts function.

- Only scripts that are signed by authorities that you trust can be imported to the Script Catalog Manager and made available for use.

  Scripts created by Ivanti will be signed by Ivanti. If you create a custom script you must sign it using your own certificate and you will accept all liability for use of that script.

- Ivanti Patch for Windows® Servers will use the credentials that are already associated with your machine groups to run the scripts.

- Only those scripts that you approve will be available within the Ivanti Patch for Windows® Servers interface.

- Scripts are not encrypted. This enables you to inspect and review the scripts before they are run.

VIRTUAL MACHINE CONSIDERATIONS

Scripts can be executed on online virtual machines but not on offline virtual machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

ITScripts Requirements

License Requirements

The ITScripts features that are available to you depend on your license key. To determine your license level, select **Help > About Ivanti Patch for Windows® Servers**.

ITScripts features available with a Ivanti Patch for Windows® Servers Standard license

- Access to free scripts created by Ivanti
- Execute scripts against target machines
- Execute scripts from the console
- Create PowerShell Templates

ITScripts features available with a Ivanti Patch for Windows® Servers Advanced license

- Access all predefined scripts provided by Ivanti
- Import your own custom scripts
- Import custom scripts written by others, such as those on the ITScripts Community Site
- Import scripts that use custom PowerShell modules
- Execute custom scripts on the console (target type = Console)
- Execute custom scripts on the console against target machines (target type = Any)
- Execute predefined and custom scripts on the target machine (target type = WinRM Remoting)
- Execute predefined and custom scripts against ESXi Servers and vCenter Servers (target type = ESXi Hypervisor)
- Schedule scripts

Script Requirements

There are two basic requirements for using a script within Ivanti Patch for Windows® Servers:

- The script must contain metadata that uniquely identifies it and describes its functionality and input parameters
- The script must be signed by an authority that is trusted by the machine that the console is running on

See Creating a Custom Script for more information on these and other script requirements.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Console Requirements

- Microsoft .NET Framework 4.6.1 or later
- Windows PowerShell 4.0 or later: Windows PowerShell is a command-line shell and scripting language that is designed for system administration and automation
- Operating System: All operating systems that support the Ivanti Patch for Windows® Servers console will also support PowerShell 4.0
- A Ivanti Patch for Windows® Servers Advanced license must be available in order to access the more advanced features of the ITScripts function
- When using PowerShell Remoting: On the **Tools > Options > ITScripts** tab you should verify the TCP port to use, and you should select the credential to use if it is necessary for Ivanti Patch for Windows® Servers to temporarily add a target machine to the console's TrustedHosts list when executing a WinRM script.

Target Machine Requirements When Using PowerShell Remoting or Opening a PowerShell Prompt

For additional details see **about_Remote_Requirements** in the PowerShell Help system.

- Windows PowerShell 3.0 or later
- The Microsoft .NET Framework 2.0 SP2
- Windows Remote Management 2.0 (WinRM 2.0) or later: Working in conjunction with Windows PowerShell, WinRM allows scripts to be invoked on remote machines.

  Although WinRM is automatically included in Windows 7, Windows Server 2008 R2, and Windows Server 2008 R2 - Core, it is not enabled by default on any of these operating systems.

  TIP: The **winrm quickconfig** command is an easy method for enabling the protocol and setting up the default configuration.

- Windows Server 2008 SP2, Windows Server 2003 SP2, Windows Vista SP2, and Windows XP SP3: You must download and install WinRM 2.0 on target machines using these operating systems (see KB968929 for information).
- TCP port 5985: This is the default port that must be configured on your organization's firewall to allow the WinRM protocol. You can use a different port if it is defined in the WinRM listener.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- Credentials must be provided for the target machines. You cannot execute scripts using your current logon credentials.
- Administrator Requirements: Administrator privileges (Run As Administrator) are required in order to perform some remoting operations.
- User Requirements: To establish a remote connection and run remote commands, the current user must be a member of the Administrators group on the remote computer. Or, the current user must be able to provide the credentials of an administrator.
- Windows Network Location: To enable remoting on client versions of Windows, such as Windows 7, the current Windows network location must be Domain or Private ("Home" or "Work"). If the network location is Public, Windows PowerShell cannot create the required firewall exception for WS-Management communication.
- Configuration Requirements: To configure Windows PowerShell to receive remote commands, at a PowerShell command prompt type **enable-psremoting**.
- Secure Connection Requirements: If you want to use a secure connection you must do the following on the console and on each target machine:
  - Console: Enable the **Use SSL** check box on the **Tools > Options > ITScripts** tab. On that same tab you should also choose the secure TCP port to use.
  - Target machine: Each target machine must contain a signed certificate and a WinRM HTTPS Listener.

Target Machine Requirements When NOT Using PowerShell Remoting

You do not need to install any additional software on the target machines. The script is run against selected target machines or machine groups **without** the services of WinRM (PowerShell remoting). The PowerShell client on the console communicates with the target machines by using other Windows remoting services such as remote registry service, remote Windows file sharing, WMI services, etc. The only ports required are the ports required by the Windows services being used.

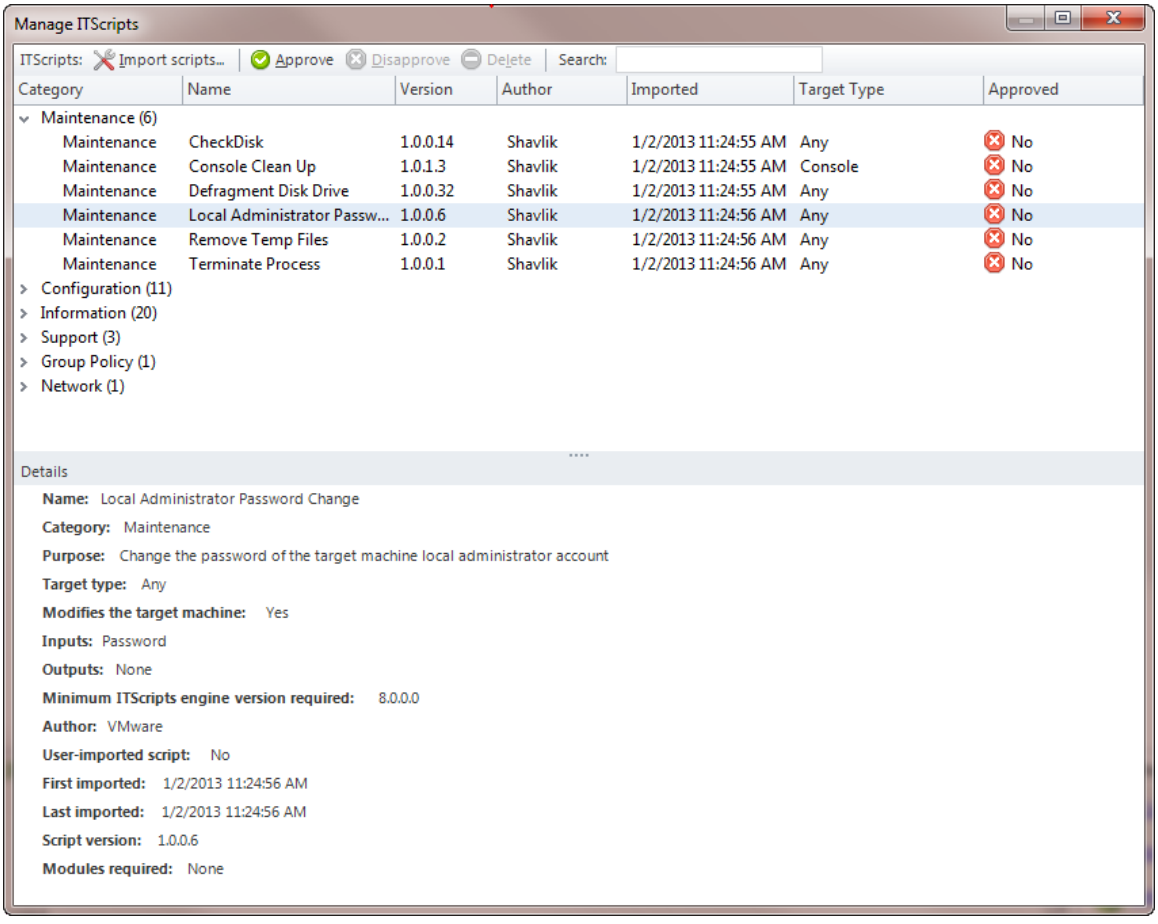
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Managing ITScripts

The Script Catalog Manager displays the scripts that are available and specifies which scripts are approved for use within your organization. Only those scripts that you approve will be available in other areas of the Ivanti Patch for Windows® Servers interface. You can use the Script Catalog Manager to:

- View the list of all currently available scripts (predefined scripts and custom scripts)
- Import new custom scripts that you have created or that were created by a trusted member of the ITScripts Community Site (requires a Ivanti Patch for Windows® Servers Advanced license)
- Approve, disapprove, and delete scripts
- Display details about an individual script

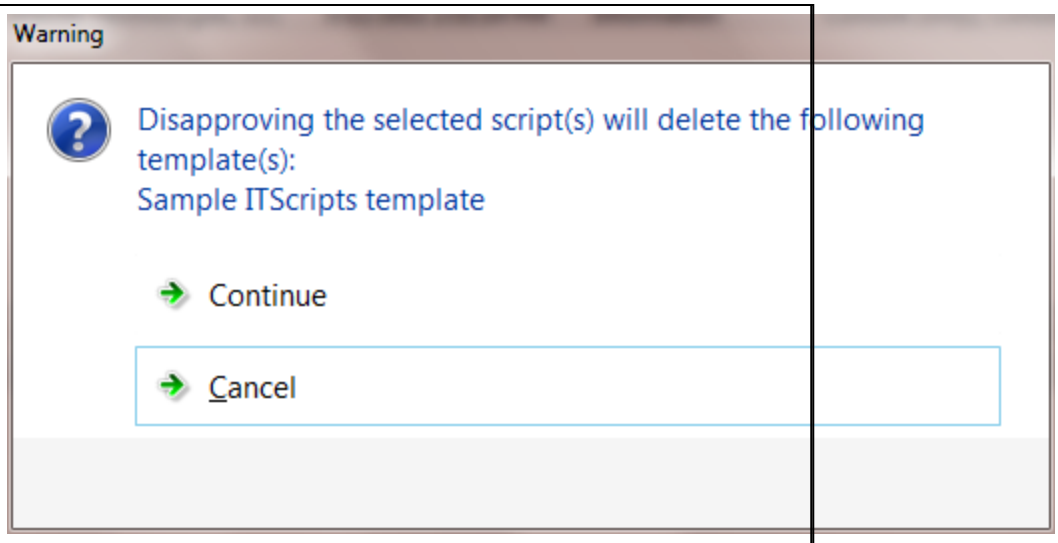
To access the Script Catalog Manager, select **Manage > ITScripts**. The program will automatically download and import the latest scripts available from Ivanti. When the process is complete the available scripts are displayed in the **Manage ITScripts** dialog.



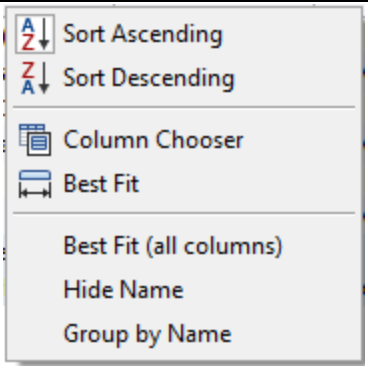
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Import scripts	Import custom scripts that you created or that were created by someone you trust. This button is available only if you have Ivanti Patch for Windows® Servers Advanced. In order to import a script the script must: • Be digitally signed by an authority that you trust • Contain metadata that uniquely identifies it and describes its functionality and input parameters If you are importing a script that was created by a third party your process should be as follows: • Download the script to an accessible location • Review the script for accuracy and for security issues • Re-sign the script with your own certificate or by someone you trust • Import the script into the Script Catalog Manager A console must trust the authority that issued the certificate in order to import or execute the script on that console. If you import user scripts on one console, they will also appear on other consoles that are using the same database. If the other consoles don't trust the signer, however, they will not be able to execute the scripts.
Approve	Approves the selected script(s) for use within the program.
Disapprove	Disapproves the selected script(s). The scripts will still be displayed in the dialog but they will not be available for selection elsewhere in the program. If you attempt to disapprove a script that is currently being used by an ITScripts template, a warning dialog is displayed. Verify that the script and the template are not needed before continuing.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	
Delete	Deletes the selected script(s) from the Script Catalog Manager. Only custom scripts can be deleted.
Search	You can easily search for scripts contained in the top pane. All searches are performed using the Search tool.  To initiate a search you type the item you want to find and then press **Enter**. Only those scripts matching the search criteria are displayed; all other scripts are hidden. **Tips for Using the Search Tool** • The Search tool works only on the information currently visible in the pane. • All partial matches are displayed. For example, if you search for scripts named *Test*, any script with "test" in its name will be considered a match (e.g. TestScript1, Contest, etc.). • The use of wildcards in the Search tool is not allowed.
Column headers	• You can reorder the columns by clicking and dragging the column headers to new locations. For example, if you want category information to be displayed in the first column, simply click on the **Category** column header and drag it to the first column. • You can right-click within a column header and perform a number of additional actions.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	
Details	Displays the metadata that describes the selected script.

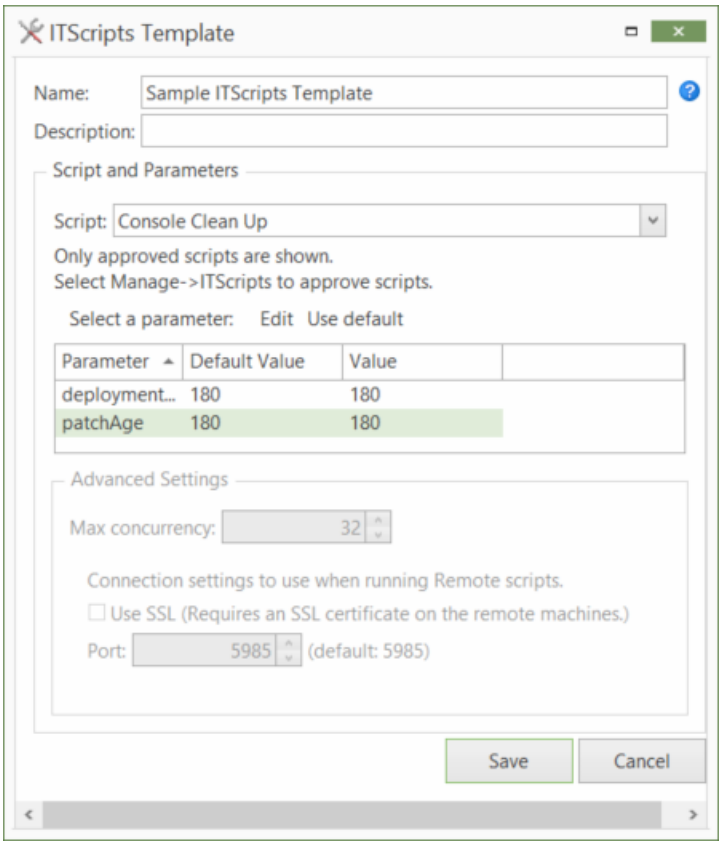
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating an ITScripts Template

An ITScripts template is used to define how a particular script should be executed. The template specifies:

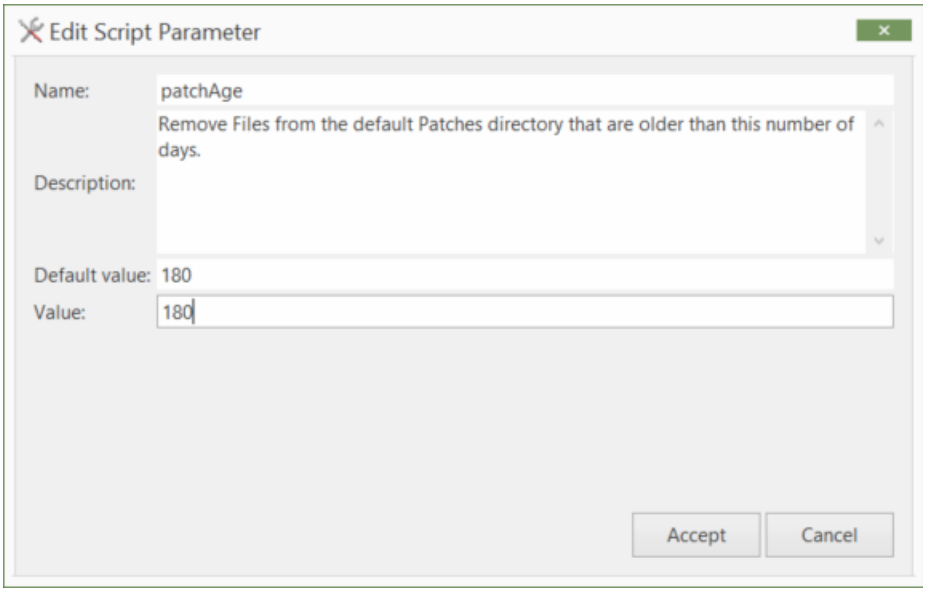
- Which script to execute
- The values of the input parameters used by the script
- The maximum number of machines the script may run on simultaneously (concurrency)

Ivanti Patch for Windows® Servers allows you to create any number of custom ITScripts templates. To create a new ITScripts template, from the main menu select **New > ITScripts Template**. The **ITScripts Template** dialog will appear.



Name	The name that you wish to assign to this template.
Description	A description of the template.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Script	Select the script you want this template to run. Only approved scripts contained in the Script Catalog Manager are available for selection. The Script Catalog Manager will also provide detailed information about each script.
Parameters	Displays the input parameters used by the script and the parameter values that will be used by the template. To modify a parameter value, double-click the parameter or select the parameter and click **Edit**. The **Edit Script Parameter** dialog is displayed. The modified parameter value only applies to the template; the value in the original script is unchanged. Also, string values must be contained within quotes (for example, "*"); numeric values do not require quotes. 
Max concurrency	This option does not apply to scripts whose target type = Console. Specifies the maximum number of target machines you will allow the script to run on at one time. Valid values are 1 - 256. One suggestion is to set this value to four times the number of CPUs on the console machine. (Example: If you have an eight core machine the **Max concurrency** value should be 32.) Your network speed and bandwidth should also be taken into consideration when setting this value.
Use SSL	This option is only available for scripts whose target type = WinRM Remoting. If you want the console to contact the target machines using an SSL connection, enable this check box. This value is initially set on the **Tools > Options > ITScripts** dialog but you can override that value here.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Port	This option is only available for script whose target type = WinRM Remoting. Enables you to specify the port used by the console when contacting the target machines. The default value is as follows: • If you are NOT using SSL the default value is 5985 • If you ARE using SSL the default value is 5986 This value is initially set on the **Tools > Options > ITScripts** dialog but you can override that value here.

To save the template, click **Save**. To close the dialog without saving the changes, click **Cancel.**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

How to Execute a Script

All scripts can be executed using an ITScripts template. You can also execute a script directly without a template if the script does not require input parameters or if you want to use the default parameter values.

You can initiate the execution of a script from several different areas of the interface.

A console must trust the authority that issued the certificate in order to import or execute the script on that console. If you import user scripts on one console, they will appear on other consoles that are using the same database. If the other consoles don't trust the signer, however, they will not be able to execute the scripts.

FROM THE HOME PAGE

You can use the home page to execute a script on any of the four pre-defined groups (**My Machine**, **My Domain**, **My Test Machines**, **Entire Network**) or on a custom machine group.

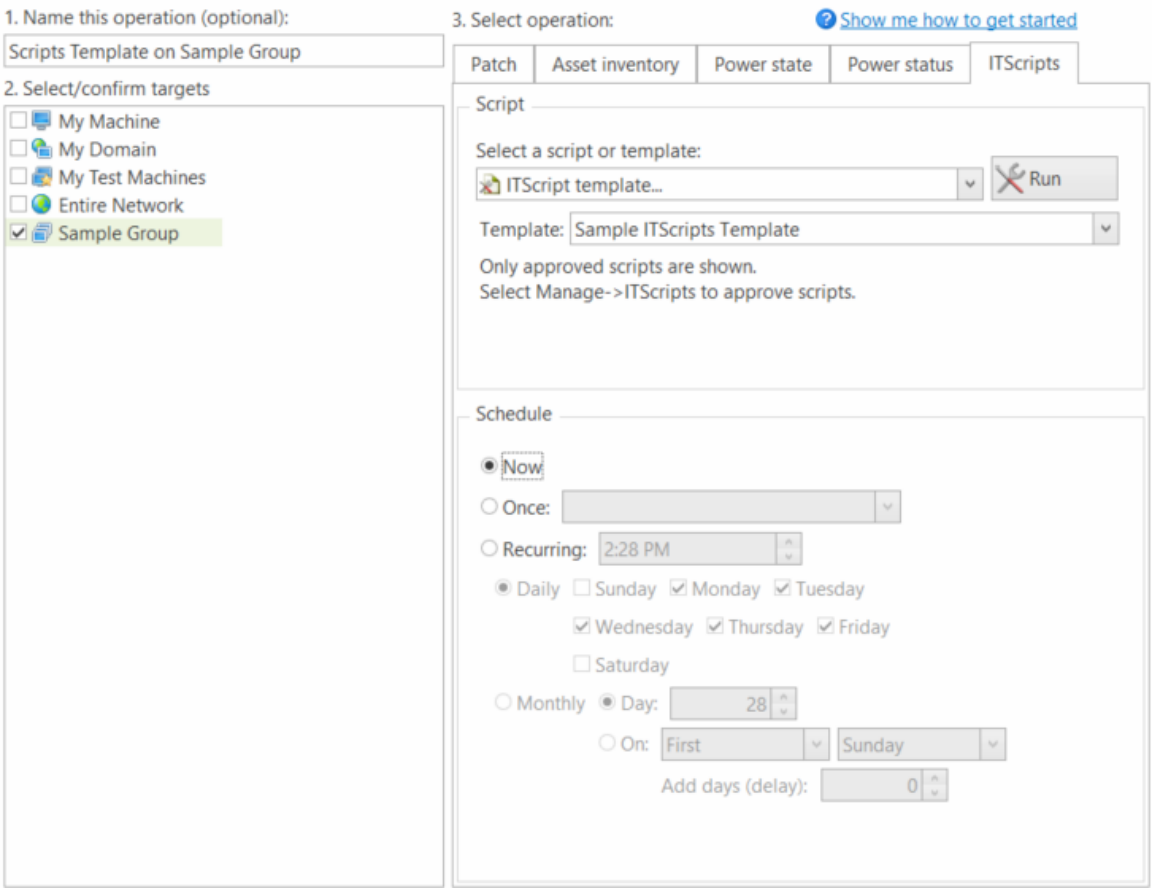
1. Type a name for the operation you are about to perform.

   One suggestion is to specify which machines are affected and the purpose of the operation (for example, *Sample Group GetRebootTime*). You may wish to include other identifiers such as the template being used, if it is a regularly scheduled operation or an out of band task, etc. A maximum of 80 characters can be used for the name.

   A date and time stamp will be automatically appended to the name. If you do not specify an operation name, the date and time stamp will be used as the name.

2. Select the desired machine group(s).

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



3. On the ITScripts tab, select how you want to execute the script.
    - **ITScript:** When this option is selected, additional fields are displayed that let you:
        - Choose the script you want to execute (scripts defined as target type = Console are not available here)
        - Edit any parameters associated with the script
    - **ITScript template:** When this option is selected, this area lets you choose the template you want to use when executing the script.
4. Select when you want to execute the script (**Now**, **Once**, or **Recurring**).
5. Click either **Run** or **Schedule**.
    - **Run:** This is the button name if **Now** is your selected scheduling option. This will immediately begin executing the script on the machines in the machine group(s). The Operations Monitor is used to track the progress of the script.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See Scheduling Scripts and Monitoring a Scheduled Script for more details.

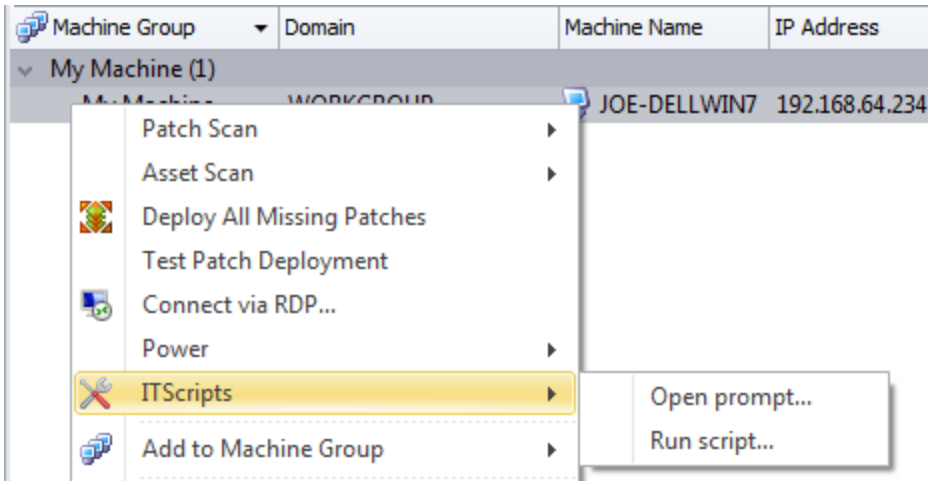
You can review the results of the script using ITScripts Results View.

FROM MACHINE VIEW OR SCAN VIEW

You can execute a script from within Machine View or Scan View by using right-click commands.

1 Select one or more machines.

2. Right-click the machine(s), select **ITScripts**, and then specify how you want to execute the script.



- **Open prompt:** Enables you to start a Windows PowerShell session with the selected machine. For details see Opening a PowerShell Prompt.

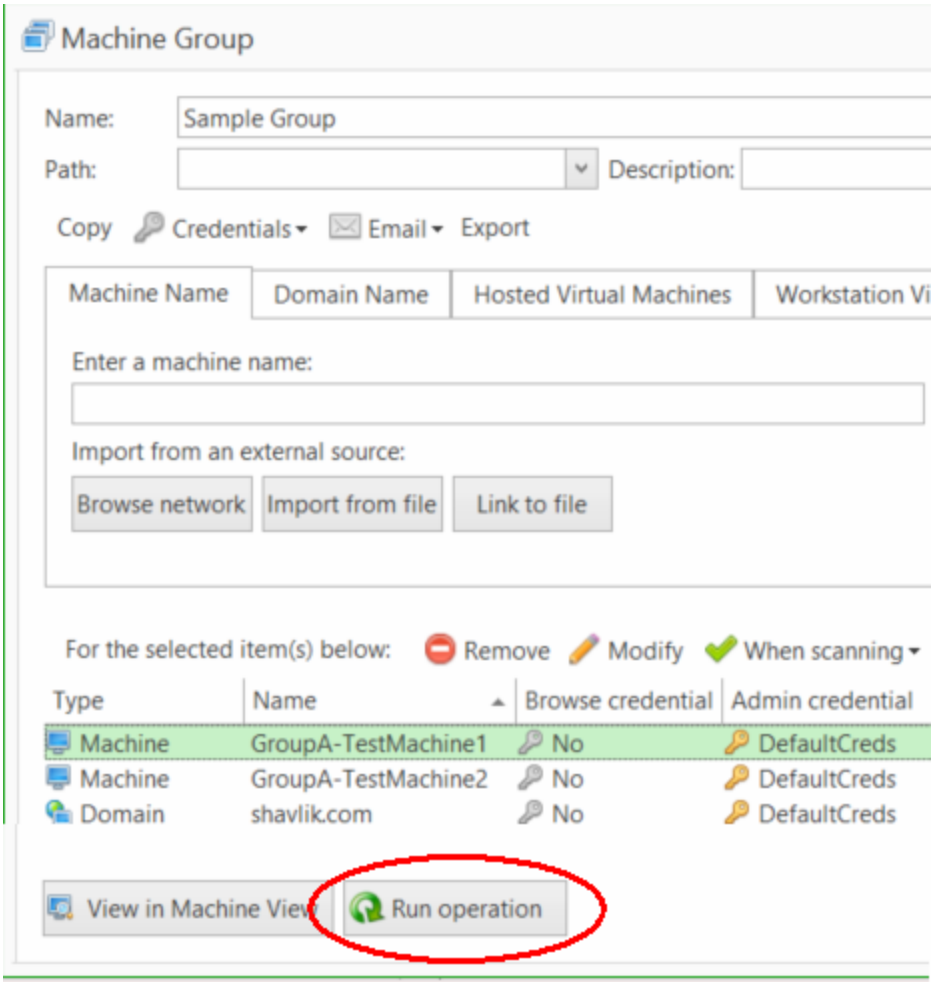
- **Run script:** Opens the Run Operation dialog, which enables you to run a script with or without a template.

FROM A MACHINE GROUP

1 In the **Machine Groups** pane select the desired machine group.

2. Within the machine group dialog click **Run Operation**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



3. On the **Run Operation** dialog, select when and how you want to execute the script.
   - **ITScript:** When this option is selected, additional fields are displayed that let you:
     - Choose the script you want to execute (scripts defined as target type = Console are not available here)
     - Edit any parameters associated with the script
   - **ITScript template:** When this option is selected, this area lets you choose the template you want to use when executing the script.
4. Click either **Run** or **Schedule**.
   - **Run:** This is the button name if **Now** is your selected scheduling option. This will immediately begin executing the script on the machines in the machine group. The Operations Monitor is used to track the progress of the script.

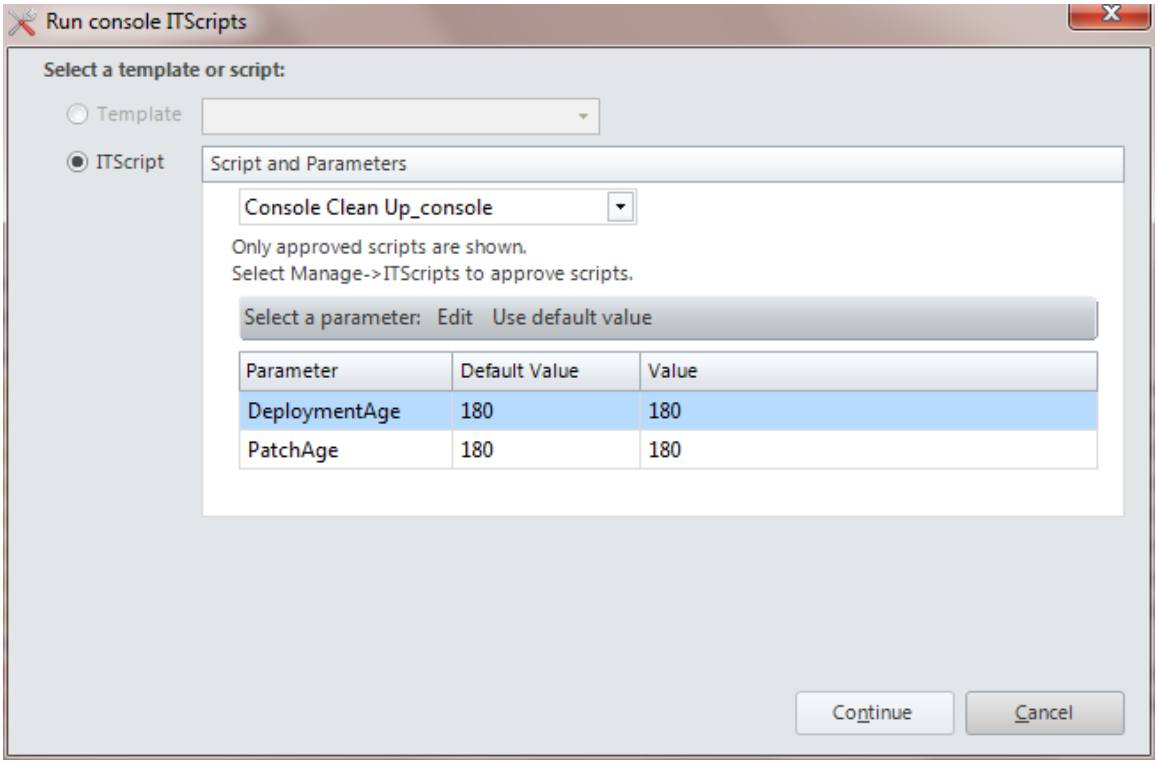
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See Scheduling Scripts and Monitoring a Scheduled Script for more details.

You can review the results of the script using ITScripts Results View.

FROM THE TOOLS > RUN CONSOLE ITSCRIPTS MENU

The **Tools > Run console ITScripts** command enables you to select and run Console mode scripts. These are scripts that are designed to run only on the console machine and not against target machines. The **Run console ITScripts** dialog is displayed.



This dialog enables you to run a console-only script with or without a template.

- If you choose a template you will execute the associated script using predefined parameter values.
- If you choose to run the script directly without a template you have the ability to modify the values of any input parameters associated with the script.

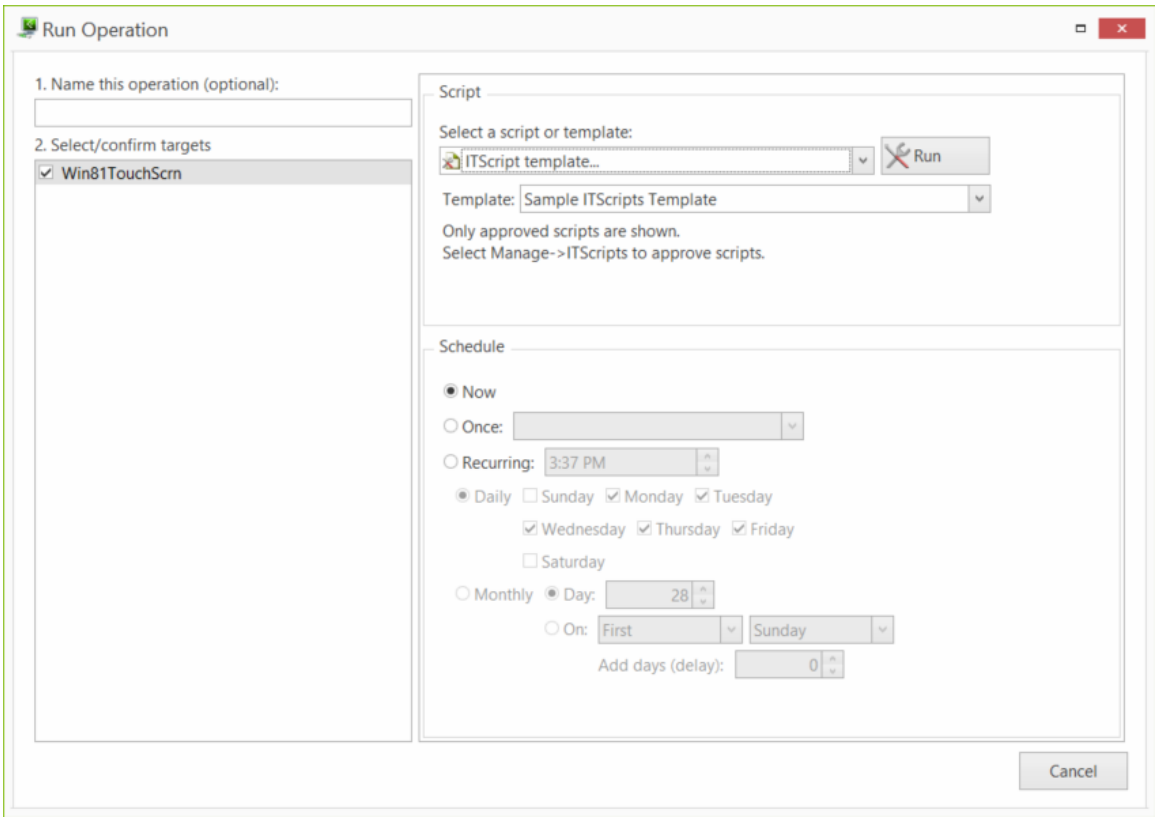
After making your selections, click **Continue** and use the Run Operation dialog to specify when the Console mode script should be run.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Scheduling Scripts Using the Run Operation Dialog

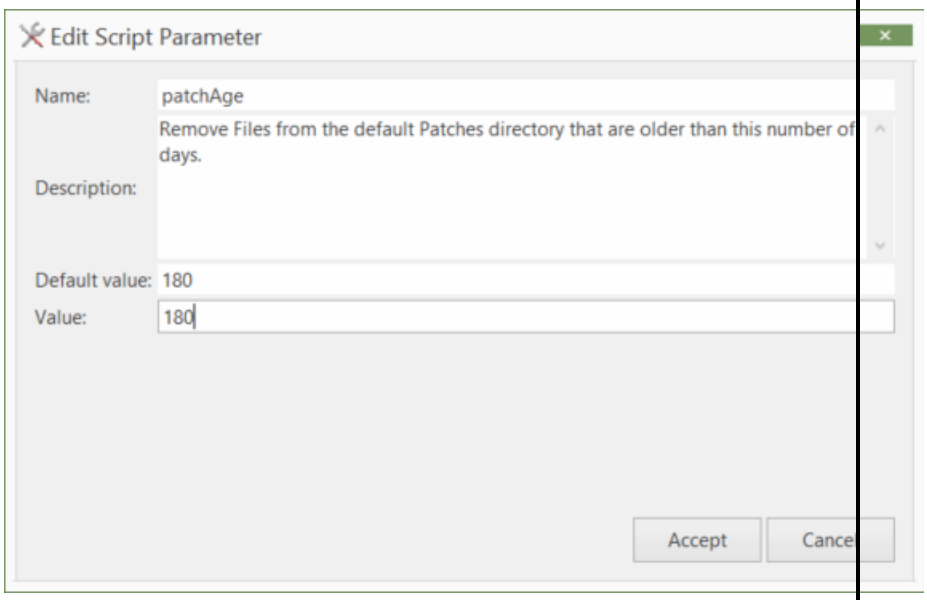
When you initiate a script operation the **Run Operation** dialog is displayed. This dialog enables you to specify if the operation should run now or be scheduled for a future time or date.

Make sure you assign credentials for all machines involved in the operation.



Name this operation (optional)	Enables you to provide a unique name for the operation. By default, the name of the machine group used to initiate the operation and the current date/time will be used. The name is displayed in the Results pane.
Select/confirm targets	This list is a reminder of the machines and machine groups that will be affected by the operation. If the wrong machines or groups are listed, click**Cancel**and re-initiate the operation using the correct targets.
Select a script or template	Enables you to select the ITScript or ITScript template you want to use when performing the operation.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• If you choose to run a script using a template you will execute the script using predefined parameter values. The template also defines the maximum number of machines the script may run on simultaneously (concurrency). • If you choose to run the script directly without a template you have the ability to modify the values of any input parameters associated with the script. All approved scripts of type **Any, WinRM Remoting, or ESXi Hypervisor** are available for selection. The Script Catalog Manager will also provide detailed information about each script. To run a script of type Console see Using the Run console ITScripts dialog. • Any input parameters used by the script will be displayed. To modify a parameter value, double-click the parameter or select the parameter and click **Edit**. The **Edit Script Parameter** dialog is displayed. String values must be contained within quotes (for example, "*"); numeric values do not require quotes. 
Schedule	There are three scheduling options: • **Now** runs the operation as soon as the **Run** button is clicked. • **Once** indicates that the operation will be run once at the day and time selected.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

	• **Recurring** allows an administrator to regularly schedule operations at a specific time and using a specified recurrence pattern. For example, using this option, an operation could be run every night at midnight, or every Saturday at 9 PM, every weekday at 11 PM, or at any other user selected time and interval. You can also use the **Recurring** option to schedule an operation in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a script operation to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by one day.

When the desired options are selected, click **Run** (if **Now** is selected) or **Schedule** (if **Once** or **Recurring** is selected).

- **Run:** The operation is initiated immediately and the **Operations Monitor** is displayed.
- **Schedule:** The operation is scheduled on the console machine. See Monitoring a Scheduled Script for details.

  If scheduled credentials are not currently assigned the **Scheduled Console Scans/Operations Credential** dialog is displayed. You must assign a shared credential to perform a schedule action. You can use the **Set scheduler credential** button on the **Scheduled Console Tasks** dialog to view and modify which credential is being used as the scheduler credential.

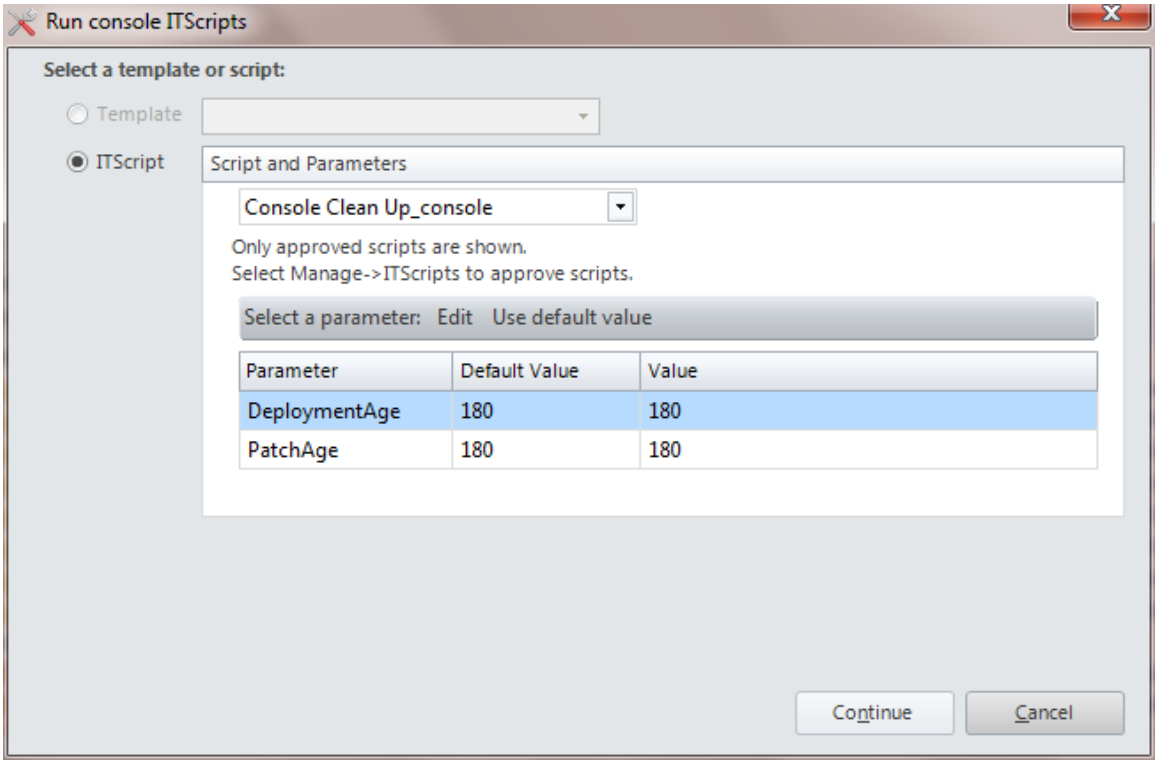


The scheduled credentials are only used to schedule the operation on the console machine. The scheduled credentials are (typically) different from the machine-level credentials that are used to perform the actual operations on the target machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

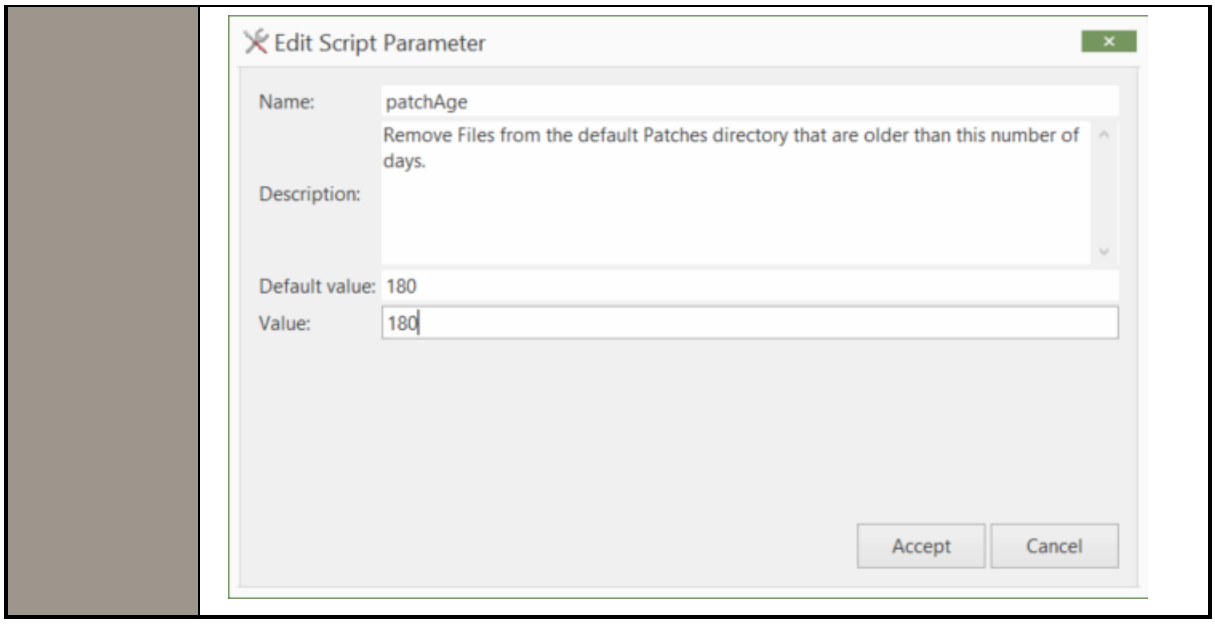
Using the Run console ITScripts Dialog

The **Run console ITScripts** dialog enables you to select and run those scripts that are designed to run only on the console machine (and not against target machines). You access this dialog by selecting **Tools > Run console ITScripts**.



Template	If you choose to run a console-only script using a template you will execute the script using predefined parameter values.
Script	If you choose to run a script directly without a template you have the ability to modify the values of the input parameters associated with the script. All approved console-only scripts contained in the Script Catalog Manager are available for selection. The Script Catalog Manager will also provide detailed information about each script.
Parameters	Displays the input parameters used by the script and the parameter values that will be used by the template. To modify a parameter value, double-click the parameter or select the parameter and click **Edit**. The **Edit Script Parameter** dialog is displayed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

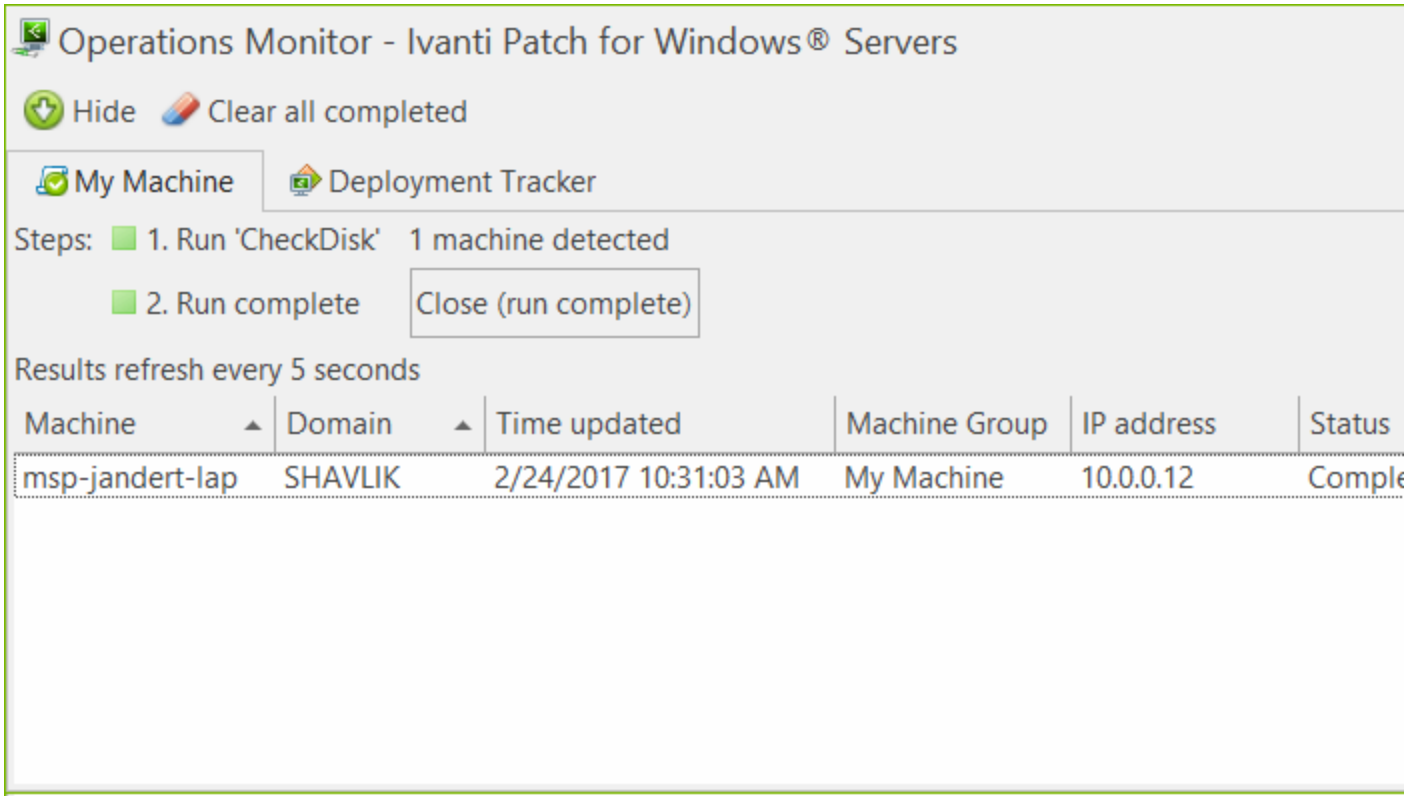


To execute the selected script, click **Continue**. To close the dialog without initiating a script, click **Cancel.**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Monitoring the Execution of a Script

The Operations Monitor is automatically displayed whenever a script is executed. It shows the steps involved in the process and the progress of each step.



Using the Operations Monitor you can:

- Remove the active tab by clicking **Close**. Any other tabs on the Operations Monitor will remain open.
- Close the Operations Monitor by clicking **Hide**. No tabs are removed from the Operations Monitor. Select **View > Operations Monitor** to reopen the window.
- Remove the active tab and all other tabs with completed tasks by clicking **Clear All Completed**.

To view the results of the script, see ITScripts Results View.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Monitoring a Scheduled Script

When you click **Schedule** on either the home page or the **Run Operation** dialog, a scheduled task is created on the console that will launch the script at the appointed day and time. To view the scheduled task, select **Manage > Scheduled Console Tasks**.

The Scheduled Console Tasks Manager uses the services of the Microsoft Task Scheduler to schedule and initiate each task. If you prefer, you can view the tasks within the Microsoft Scheduler by accessing the **Task Scheduler** dialog on your Windows console machine and then expanding the **Task Schedule Library > LANDESK > Protect** tree.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

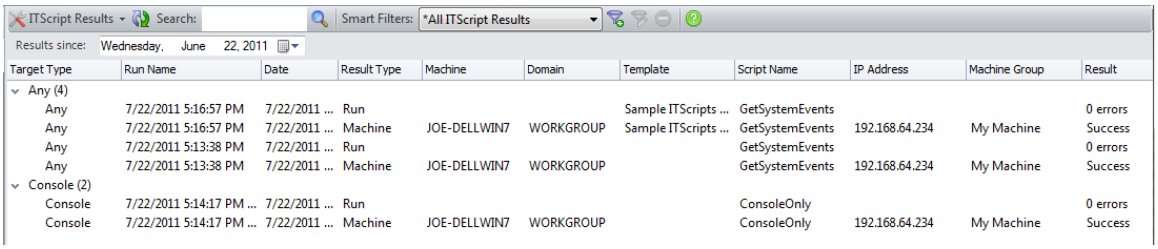
ITScripts Results View

ITScript Results View provides a way to view the results of all scripts that have been run from Ivanti Patch for Windows® Servers. It displays all results that have ever been reported to the console, providing a complete historical record for your organization.

When a script is executed on one or more target machines the results are automatically reported to the console. ITScript Results View is accessed from the main menu by selecting **View > ITScript results**.

You can adjust the amount of information that is displayed by using the **Results since** option, the Smart Filter, or the **Search** option. By default, all script results that have been reported to the console within the last 30 days will be displayed.

ITScript Results View will be empty if you view it immediately after installing the program or if no script results have been reported to the console. This is because there is no script information in the database to display.



Target Type	Identifies the mode that was used when the script was run. • **Console:** The script was run on the Ivanti Patch for Windows® Servers console only and not against a set of target machines. • **Any:** The script was run on the console against selected target machines or machine groups without the services of WinRM (PowerShell remoting). • **WinRM Remoting:** The script was run against the target machine(s) using WinRM (PowerShell remoting). • **ESXi Hypervisor:** The script was run against ESXi Servers and/or vCenter Servers.
Run Name	Identifies the name specified in the **Name this operation** box when the script was run. (See How to Execute a Script and Scheduling Scripts Using the Run Operation Dialog.)
Date	Identifies the date and time that the script was run.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Result Type	Identifies whether the line of output shows run results or machine results. • Run results contain output information related to the execution of the script. • Machine results contain the output that was created when the script was run against the selected machine.
Machine	Identifies the machine that the script was run against.
Domain	Identifies the domain to which the machine is assigned.
Template	Identifies the ITScripts template that was used to initiate the script.
Script Name	Identifies the name of the script that was run.
IP Address	Identifies the IP address of the machine.
Machine Group	Identifies the machine group that the machine was selected from (machines can belong to more than one group).
Result	Provides a short summary or status. For detailed result information you must view the result output file.

For additional information, see:

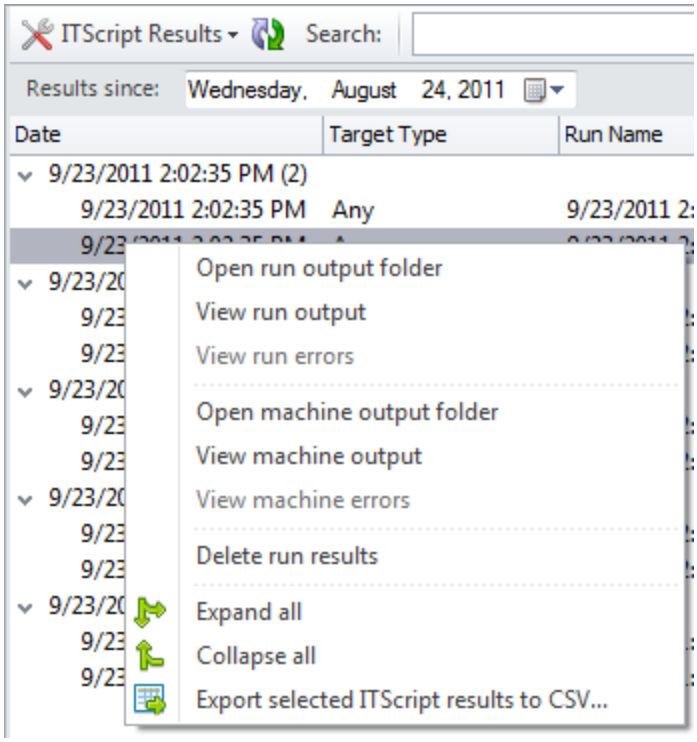
- Performing Actions on Script Results
- Searching for Script Results
- Using the Script Result Smart Filter

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing Actions on Script Results

Right-Click Menu

You can right-click on any result entry within ITScripts Results View and perform a number of different actions.



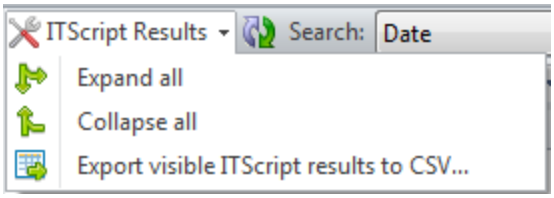
Run Results vs Machine Results

- **Run** results contain execution information about the script (when the script was run, whether the script was successful, etc.). It also contains output for each of the machines scanned by the script.
- **Machine** results contain the output that was created when the script was run on a particular machine.

All results are located in the following directory: **C:\ProgramData\LANDESK\Shavlik Protect\ITScriptsOutput**

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Command Descriptions

Open run output folder	This command is available only if **Result Type = Run** and if the run generated an output file. The command uses Windows Explorer to open the output folder associated with this run. The output folder contains a sub-folder for each machine that was in the run. Within each machine sub-folder is a text file that contains the machine output.
View run output	This command is available only if **Result Type = Run**and if the run generated an output file. It displays a text file containing output information related to the execution of the script.
View run errors	This command is available only if **Result Type = Run**and if the run generated an error file. It displays a text file containing the errors that occurred when the script was executed. For example, if a machine could not be resolved and a connection error occurred, that error would be displayed here.
Open machine output folder	This command is available only if **Result Type = Machine** and if an output file or an error file was generated. The command uses Windows Explorer to open the output folder associated with this machine. The output folder contains the machine output text file and/or the machine error text file.
View machine output	This command is available only if **Result Type = Machine**and if an output file was generated. It displays the output that was created when the script was run on the selected machine.
View machine errors	This command is available only if **Result Type = Machine** and if an error file was generated. It displays a text file containing the errors that occurred when the script was executed on the selected machine.
Delete run results	Deletes all output for the selected run (both the run output files and the machine output files).
Expand all	Expands all result trees. This can also be accomplished using the **ITScript Results > Expand all** menu. 
Collapse all	Collapses all script result trees in the top pane. This can also be accomplished using the **ITScript Results > Collapse all** menu.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Export selected ITScript results to CSV	Export information about the selected script results to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program. The **ITScript Results > Export visible ITScript results to CSV** menu command is similar except that it exports all results in the right pane rather than just selected results.

Double-Click Shortcut

You can double-click any result entry to immediately view its results. If there are multiple result types available for an entry the program will choose either the output file or the error file first, and if neither of these are available it will display the output folder.

Keyboard Shortcuts

The following keyboard shortcuts are available:

- **Ctrl+A**: Selects all script results.
- **CTRL+click**: Multiple script results can be selected by holding down the CTRL key while selecting script results.
- **SHIFT+click**: A contiguous group of script results can be selected by holding down the SHIFT key while selecting the starting and ending script results in the list.
- **SHIFT+PAGE UP**: Selects a range of script results from the one currently selected to the top of the table.
- **SHIFT+PAGE DOWN**: Selects a range of script results from the one currently selected to the bottom of the table.
- **CTRL+HOME:** Moves the focus to the first cell in the table.
- **CTRL+END**: Moves the focus to the last cell in the table.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Searching for Script Results

You can easily search for specific results contained in the Script Results View. All searches are performed using the Search tool.



To initiate a search you type the item you want to find and then press **Enter**. Only those scripts matching the search criteria are displayed; all other scripts are hidden.

Tips for Using the Search Tool

- The Search tool works only on the information currently visible in the pane. The **Results since** option can be used to adjust the amount of information displayed within the pane.
- If a Smart Filter is applied, only script results matching BOTH the search criteria and the smart filter criteria are displayed.
- All partial matches are displayed. For example, if you search for scripts named *Get*, any result with "get" in its name will be considered a match (e.g. GetServicesAsCSV, GadgetScript, etc.).
- A semicolon (;) can be used to concatenate multiple search terms into one search string. For example, specifying "console;any" will return all items containing either of the two terms.
- The use of wildcards in the Search tool is not allowed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Using the Script Result Smart Filter

Information displayed in the list can be easily filtered to narrow the focus to only those script results of interest. One way to do this is by using the Smart Filter.



The Smart Filter contains several default filters. You can also define your own custom filters.

The **Results since** option can be used to adjust the amount of information displayed within the pane prior to using the Smart Filter.

Default Filters

The Smart Filter contains several default filters that are identified by a leading asterisk. Default filters cannot be modified or deleted. The default filters include the following:

- ***All ITScript Results**: All script results are displayed.
- ***Today:** Only those script results that were generated today are displayed.
- ***Last 30 Days:** Only those script results that were generated within the last 30 days are displayed.
- ***Last 60 Days:** Only those script results that were generated within the last 60 days are displayed.
- ***Last 90 Days:** Only those script results that were generated within the last 90 days are displayed.

Custom Filters

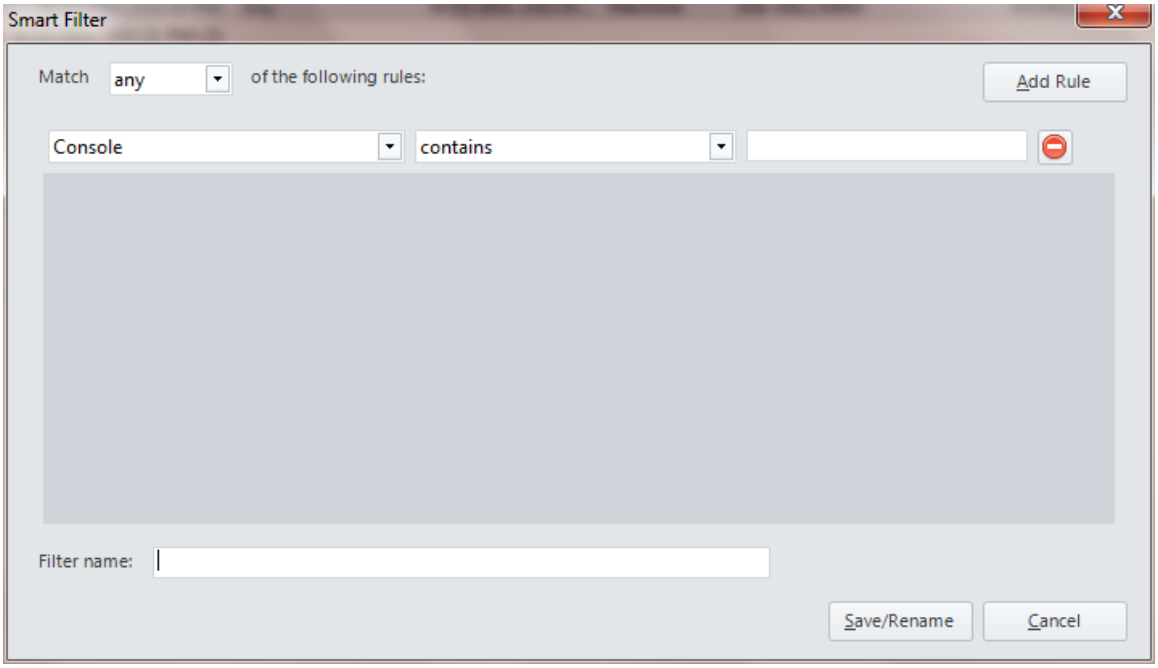
You can create your own custom filters. This is a powerful tool that enables you to specify exactly which results you want displayed. Each custom filter is comprised of one or more rules. You can define as many rules in a filter as needed.

To create a new filter:

1. Click the Create a New Smart Filter icon ( ).

   The **Smart Filter** dialog is displayed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



2. Specify which rules in the filter must be matched.
   - **All**: Only those events that match all the rules in the filter will be displayed.
   - **Any**: Events that match at least one rule in the filter will be displayed.
3. Define one or more rules.

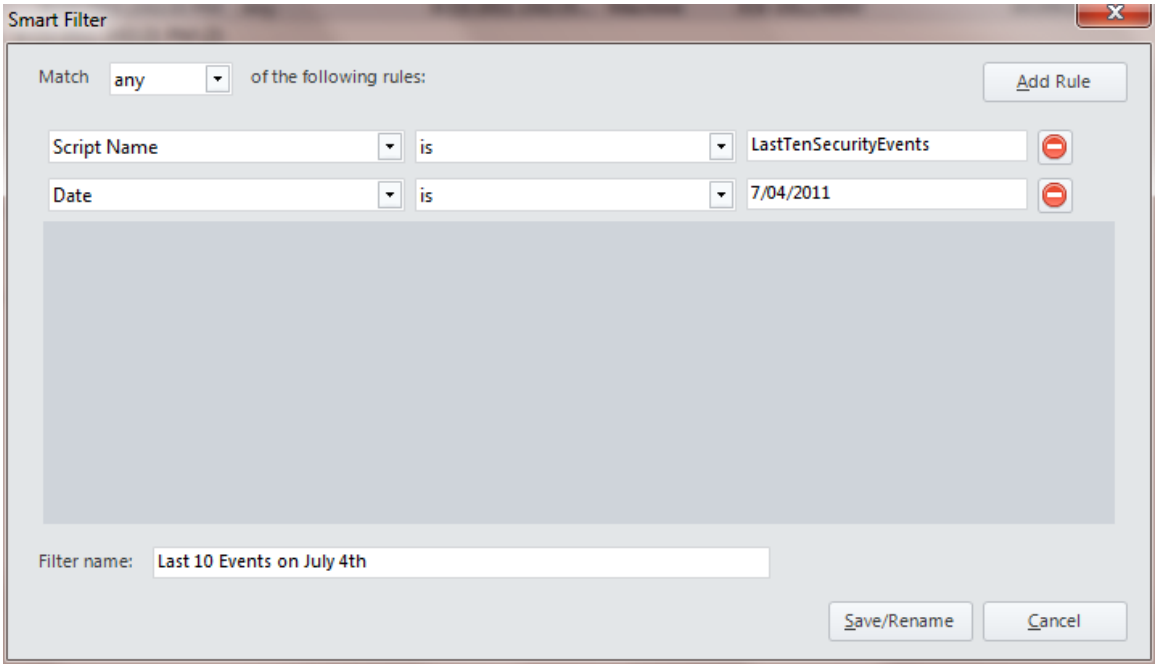
   To define a rule, select an option in each of the first two logic boxes and then type the criteria in the third box. To add another rule simply click **Add Rule**.

   If you define a rule that does not make sense (for example, "Script Name is greater than 3") the rule will simply be ignored.
4. Type a name for the filter.
5. When you are finished defining your custom filter, click **Save/Rename**.

Example

Assume you want to see the security events that occurred on your target machines on a specific date. You simply create a filter similar to the following:

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



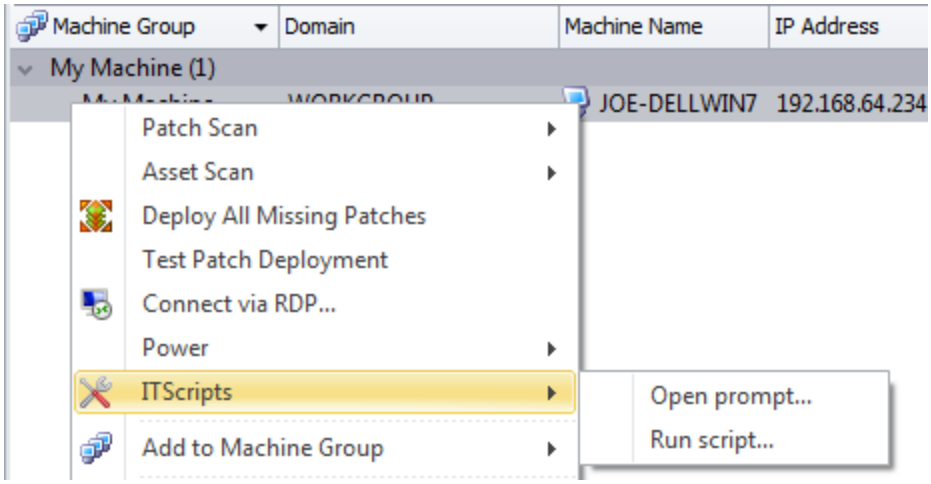
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Opening a Windows PowerShell Prompt

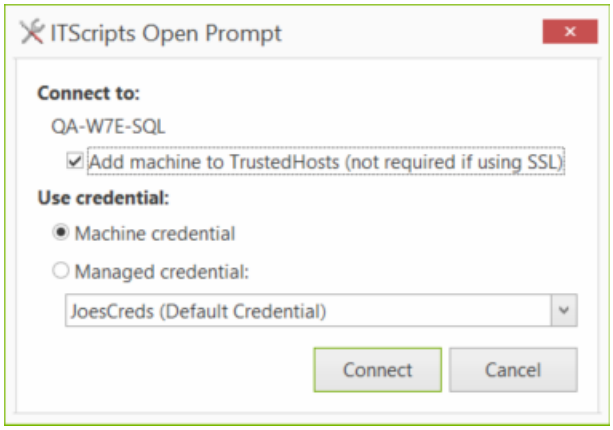
The target machine must meet all PowerShell Remoting requirements; for details see ITScripts Requirements.

You can start a Windows PowerShell session with any single target machine. Doing so will enable you to execute PowerShell commands as an administrator on the target machine.

From either Machine View or Scan View, simply right-click the desired machine and select **ITScripts > Open prompt**.

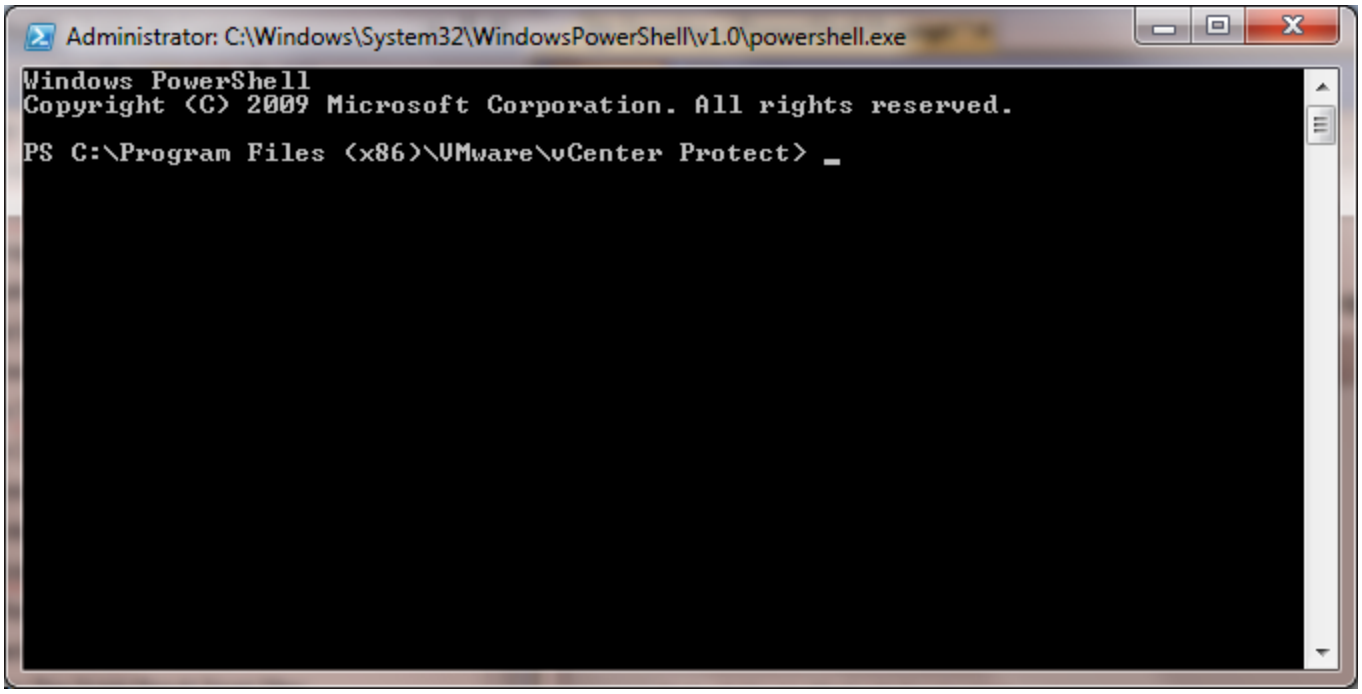


You will need to provide the necessary credentials on the **ITScripts Open Prompt** dialog in order to make the connection. For credential information see Defining Credentials.



After making the connection the Windows PowerShell prompt is displayed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating a Custom Script

If you have a Ivanti Patch for Windows® Servers Advanced license, or if you are using Ivanti Patch for Windows® Servers Standard and have a license for the Advanced ITScripts add-on, you can create and import your own scripts that will completely integrate into the Ivanti Patch for Windows® Servers environment. When creating a custom script there are a few basic guidelines you must follow, such as:

- The script must contain metadata that uniquely identifies it and describes its functionality and input parameters
- The script must be signed by an authority that is trusted by the machine that the console is running on
- The script can use any number of variables and functions that are provided by Ivanti and that are designed for use with Ivanti Patch for Windows® Servers

For complete details on creating a custom script, please refer to *Guidelines for Creating Custom Patch for Servers Scripts*, a document available on our website.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Understanding RDP

The Microsoft Remote Desktop Protocol (RDP) provides the ability to remotely manage Windows-based machines over a network connection. RDP capabilities are supported in Ivanti Patch for Windows® Servers, enabling you to use stored machine credentials to quickly connect the Ivanti Patch for Windows® Servers console to a target machine. With Remote Desktop you can access the target machine's programs, files, and resources as if you were physically sitting in front of the machine. For a complete list of the features of Remote Desktop, please visit any number of sites on the Web.

For information on using the Remote Desktop feature, see the following topics:

- RDP Requirements
- How to Initiate a Remote Desktop Connection

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

RDP Requirements

Before attempting a Remote Desktop connection, please confirm that you meet the following requirements.

- The Ivanti Patch for Windows® Servers console must have network access to the target machine.
- The RDP port specified by Ivanti Patch for Windows® Servers must be the same as the RDP port specified by the target machine.

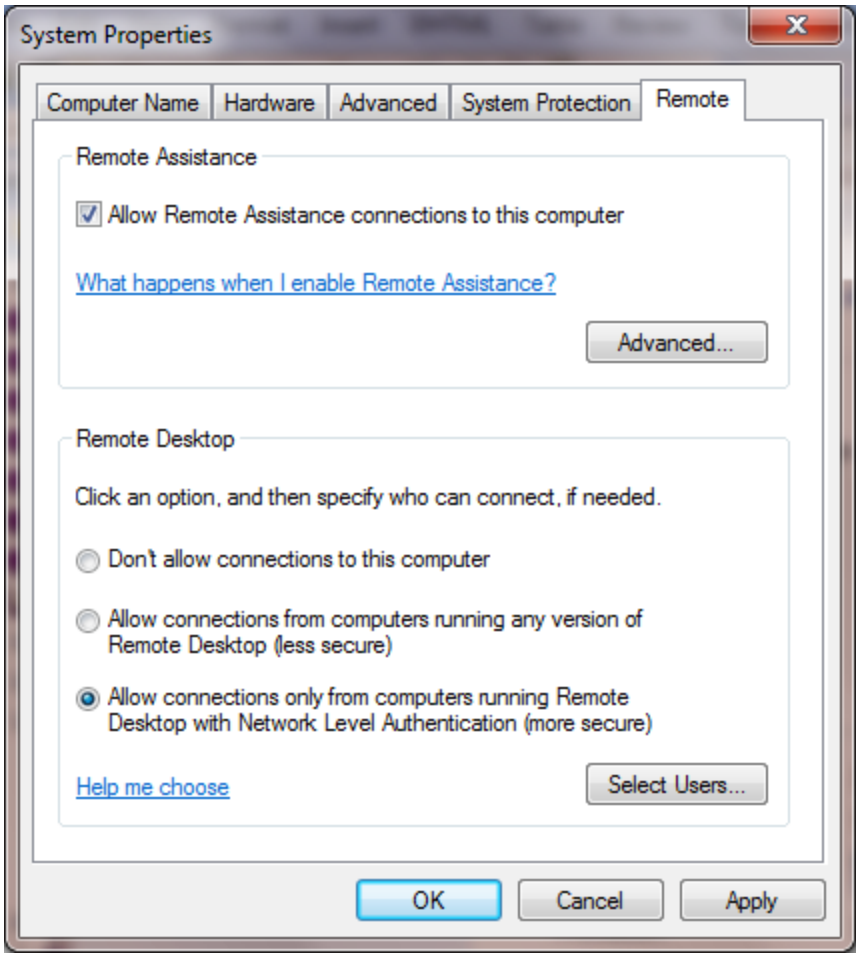
  If the target machine is not using the default RDP port (3389), use the **Machine Properties** dialog to match the port value specified on the target machine.
- The target machine must be powered on; it cannot be in sleep or hibernation mode.
- You must have access to a user account on the target machine.
- The target machine must be configured to allow Remote Desktop Connection.

  a) On the target machine, right-click the **Computer** icon and choose **Properties**.

  b) Select the more secure connection option when possible.

  Windows XP machines may not support Network Level Authentication and may require the less secure option. All other operating systems supported by Ivanti Patch for Windows® Servers should support the more secure option.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



- You must have permission to connect to the target machine.

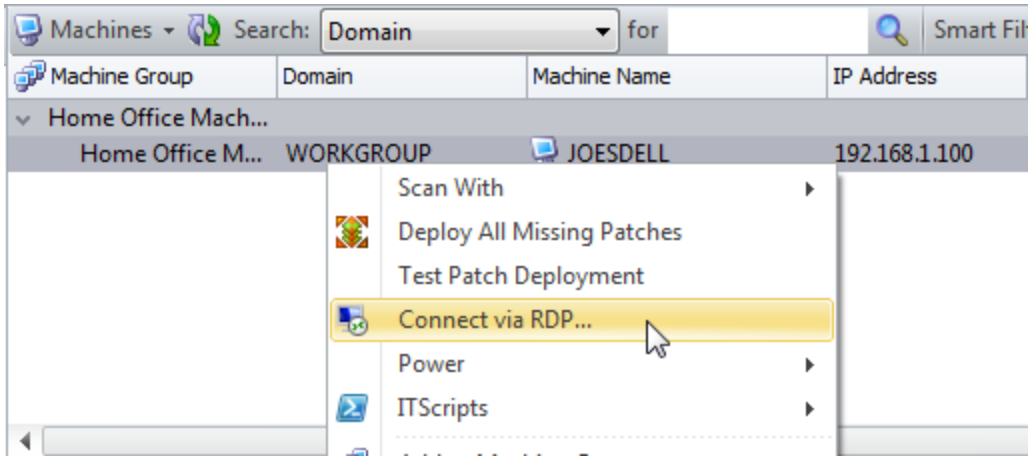
  For permission to connect, you must be on the list of users. On the **System Properties** dialog (shown above), click **Select Users** and add the name of the user.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

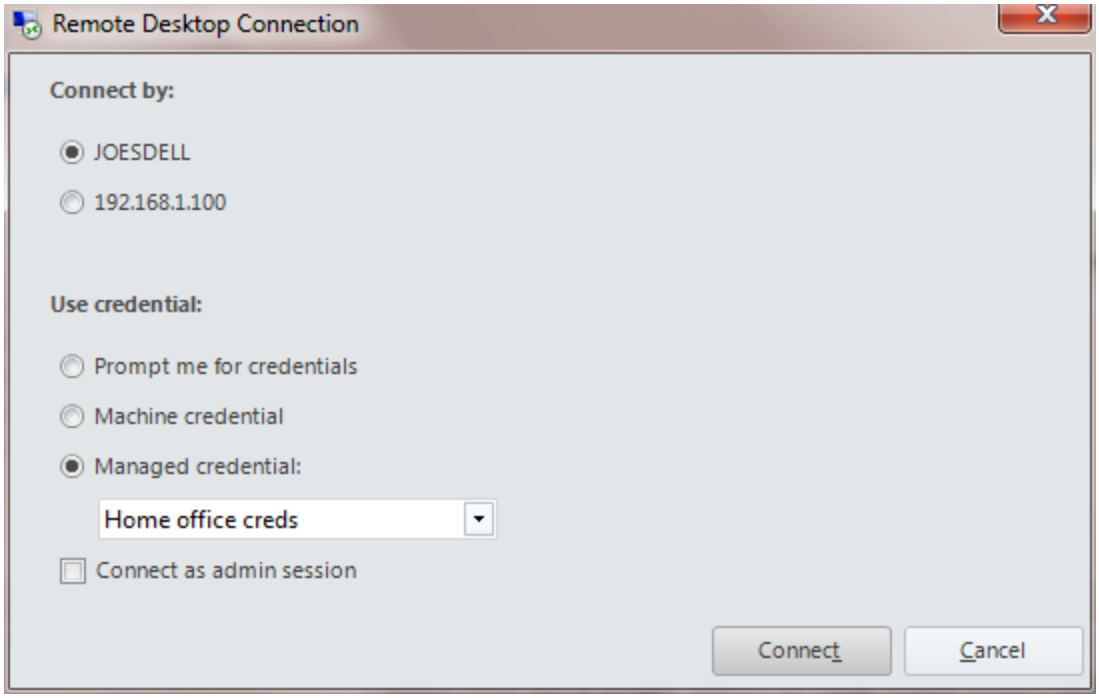
How to Initiate a Remote Desktop Connection

A Remote Desktop connection can be initiated from either Machine View or Scan View by using the right-click menu.

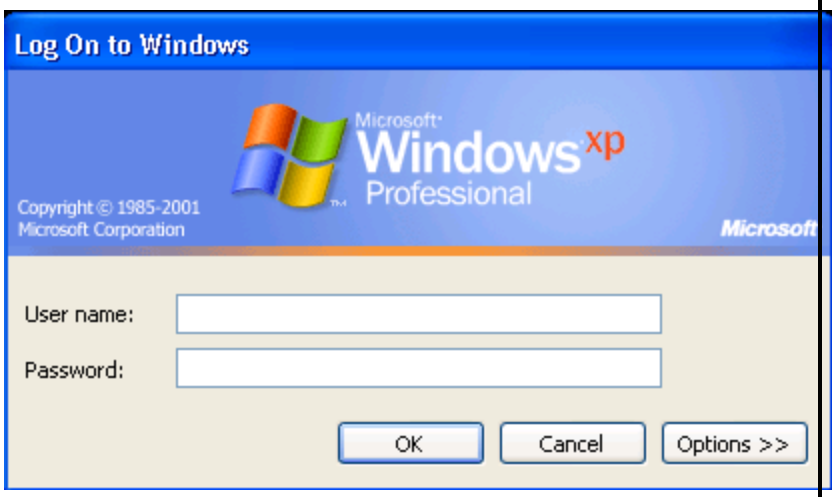
1. Select the desired target machine.
2. Right-click the machine and then select **Connect via RDP**.



3. Use the **Remote Desktop Connection** dialog to specify how you will make the connection.



Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Connect by	You can make the connection using either the machine name or the IP address. Both options should work equally well. If your scan information is old and you cannot depend on the IP address you may want to use the host name. If your organization is experiencing DNS issues and cannot properly resolve the host name you should use the IP address.
Use credential	You must specify which credential to use when making the RDP connection. • **Prompt me for credentials:** Will display a separate dialog that you can use to provide the user name and password credentials. This is a good option to use for rogue machines for which you do not have predefined credentials.  • **Machine credential:** Will use the credential assigned on the **Machine Properties** dialog. This is a convenient option for machines you have previously assigned credentials. • **Managed credential:** Enables you to choose which credential to use when making the connection. This is the preferred option for those machines that use your managed credentials. See Managing Credentials for more information. If the credential you choose does not work and you are unexpectedly prompted for credentials, check to see if the user name contains *.\Administrator*. Some newer operating systems translate this term to *consolemachinename\Administrator*and the credentials will be rejected. The solution is to use *Administrator* rather than *.\Administrator*.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Connect as admin session	If enabled, specifies that the remote connection will be made to the "session 0" session of the server (the target machine). Session 0 is required to perform certain administrative tasks on some Windows operating systems.
Connect	To initiate the RDP connection, click **Connect**.
Cancel	To cancel without making the connection, click **Cancel**.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Assigning Aliases to the Console

WARNING! Accidentally changing or deleting existing entries on the **Console Alias Editor** dialog may cause problems when your agents attempt to contact the console or when your agentless machines attempt to report deployment status messages. Only qualified system administrators should modify existing names or IP addresses.

TIP: The most common time to use this tool will be during an upgrade from an earlier version of Ivanti Patch for Windows® Servers.

There are two primary uses for the **Console Alias Editor** tool.

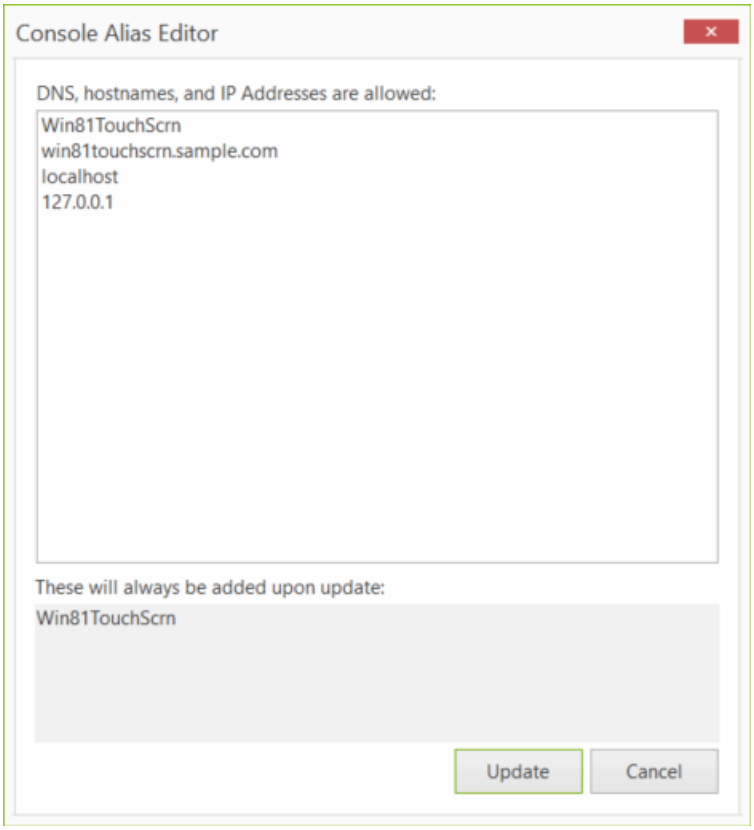
- **Agent check-in:** When an agent checks in with the Ivanti Patch for Windows® Servers console it must verify that the machine it contacted is a trusted machine. It does this using the trusted names and IP addresses contained in the certificate that is exchanged between the agent and the console. If you assign the console machine to a new domain or give it a new common name or IP address, any existing agents that recognize the console by its old name or address will no longer trust the console machine. To get around this issue you simply identify the old console names or addresses as trusted aliases. This is done using the **Console Alias Editor** tool.
- **Patch deployment pingback:** Patch deployments to your agentless machines can be monitored using the Ivanti Patch for Windows® Servers Deployment Tracker. In order for your agentless machines to send status messages to the console they need to know the valid name or IP address of the console. The valid names and IP addresses are defined using the **Console Alias Editor** and are passed to the machines when a patch deployment is initiated from the console.

This menu command is not available to users assigned the **Report Only** role.

1. Select **Tools > Console alias editor**.

   The **Console Alias Editor** dialog is displayed. It will contain the names and IP addresses currently used to identify the console machine.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



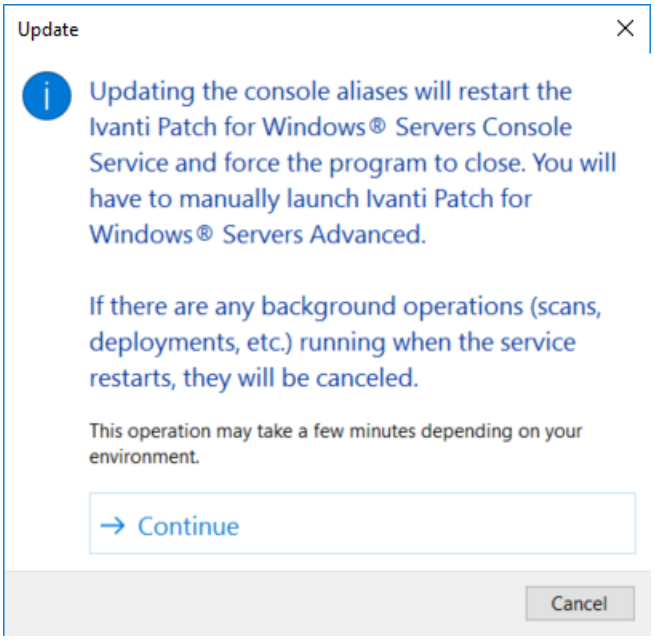
2. Type the name or IP address that you want to use as an alias for the console machine.

   You can specify IP addresses using either an IPv4 or IPv6 format.

3. Click **Update**.

   The **Update** dialog is displayed.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



In order to update the console aliases the console service must be restarted and Ivanti Patch for Windows® Servers must be closed and then manually restarted.

IMPORTANT! The agents will not recognize a new alias until after they check-in with the restarted console. The check-in must be initiated by an agent either manually using the agent client program or via a scheduled check-in; a check-in command issued from the console to an agent will not update the console certificate.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Migration Tool

Ivanti provides a Migration Tool that is used to migrate your existing Ivanti Patch for Windows® Servers console to a new machine. The Migration Tool simplifies the migration process. The tool captures core and user data from your existing console and rewrites it into a new Ivanti Patch for Windows® Servers installation.

The most common reasons for migrating a Ivanti Patch for Windows® Serversconsole to a new machine are:

- Migrate off an operating system that is no longer supported by the latest version of Ivanti Patch for Windows® Servers
- Migrate off an operating system that has been marked for end-of-life (Windows XP, Windows Server 2003, etc.)
- Migrate from a 32-bit architecture to a 64-bit architecture
- Migrate to better, faster hardware

To launch the Migration Tool, select **Start > Ivanti Patch for Windows® Servers > Migration Tool**.

For complete information on how to access and use the Migration Tool, please see the *Migration Tool User's Guide* available at: www.ivanti.com/en-US/support/product-documentation.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Using the API Feature

The API feature is meant for advanced users who want to perform tasks beyond those available through the Ivanti Patch for Windows® Servers user interface. The feature exposes the Ivanti Patch for Windows® Servers API stack, enabling you to execute API-level calls from the command-line or from a PowerShell console. You can use the API feature to:

- Interact with different systems in your environment

  You are now able to integrate your patching and power state processes with items such as vulnerability scanners, SQL Server consoles and orchestrators such as Chef, vRealize or Puppet.

- Perform actions that you can't with the Ivanti Patch for Windows® Servers user interface

  This can be actions such as suspending nodes, starting and stopping services at certain points, restarting machines in a specific order, etc.

- Script a sequence of complex events that contain dependencies

  Using PowerShell, you can script out interesting and complicated workflows. You can include checks within the script to make sure that everything goes according to plan. For example, you might patch one machine in a cluster and make sure that everything goes according to plan before proceeding with the other machines in the cluster.

For complete information on how to access and use the API feature, please see the *Ivanti Patch for Windows® Servers API Quick Start Guide* available at: www.ivanti.com/en-US/support/product-documentation.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

What is the Issue?

Ivanti Patch for Windows® Servers uses a self-signed SHA-2 root certificate to issue the console, agent and scheduler certificates used within the product. Some security tools, however, may see the self-signed certificate as a medium level security risk. To be clear, Ivanti Patch for Windows® Servers does **not** have a certificate security issue, but these tools have no way of determining that information. If you want to stop the Ivanti Patch for Windows® Servers certificate from being flagged as a warning, you have the option to use a trusted certificate authority (CA) from your own PKI infrastructure to issue a replacement root certificate for Ivanti Patch for Windows® Servers.

This section describes the tasks you must perform if you wish to replace the default Ivanti Patch for Windows® Servers root certificate with a certificate that is issued by your own CA.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Overview of the Solution

A process is available for you to use your own CA to generate a new authority certificate and replace the default self-signed root certificate created by Ivanti Patch for Windows® Servers. The authority certificate that you generate will in turn be used to issue console, agent and scheduler certificates for Ivanti Patch for Windows® Servers.

Major steps in the process

Here are the major steps for using your own CA to issue a new certificate:

1. Issue a new sub-authority certificate from your CA.

   For details on performing this step, see How to Issue a New Certificate.

   - If your CA is accessible over the network, you can use your local system facilities to create the new certificate. If you are using a Microsoft CA infrastructure, use the Subordinate Certificate Authority certificate template when creating the certificate.
   - If your CA is on a disconnected network, you will use the STMgmt command-line tool to request and then accept the new sub-authority certificate.

2. Let the new certificate work its way through Ivanti Patch for Windows® Servers.

   For details on this step, see Let the New Certificate Percolate Through the System.

3. Commit the new sub-authority certificate.

   For details on performing this step, see Commit the New Sub-Authority Certificate.

4. Test and verify that new console, scheduler and agent certificates are in place.

   For details on performing this step, see Testing for and Verifying the New Certificate.

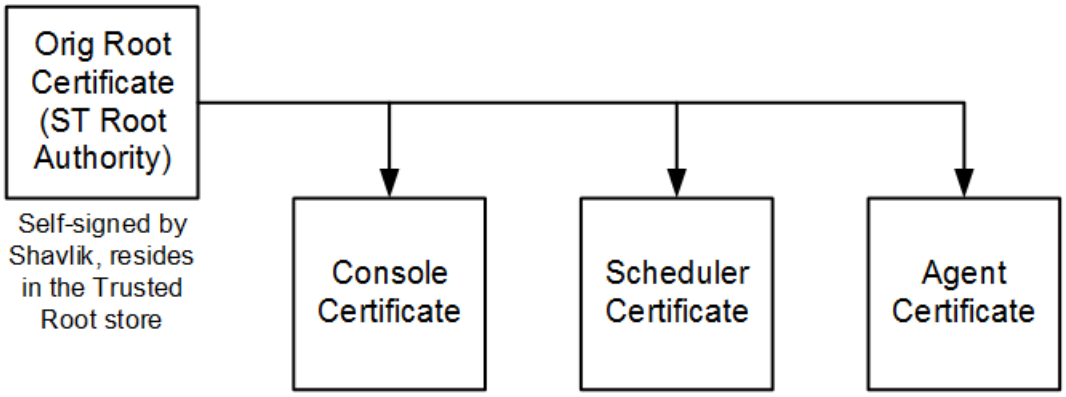
Before and after views of your certificate environment

The following diagrams illustrate the state of the Ivanti Patch for Windows® Servers certificates as originally installed and after using your own CA to issue new certificates.

As originally installed with Ivanti Patch for Windows® Servers

Here is the relationship of the certificates after initially installing Ivanti Patch for Windows® Servers. The console, scheduler and agent certificates are all issued by the self-signed root certificate.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

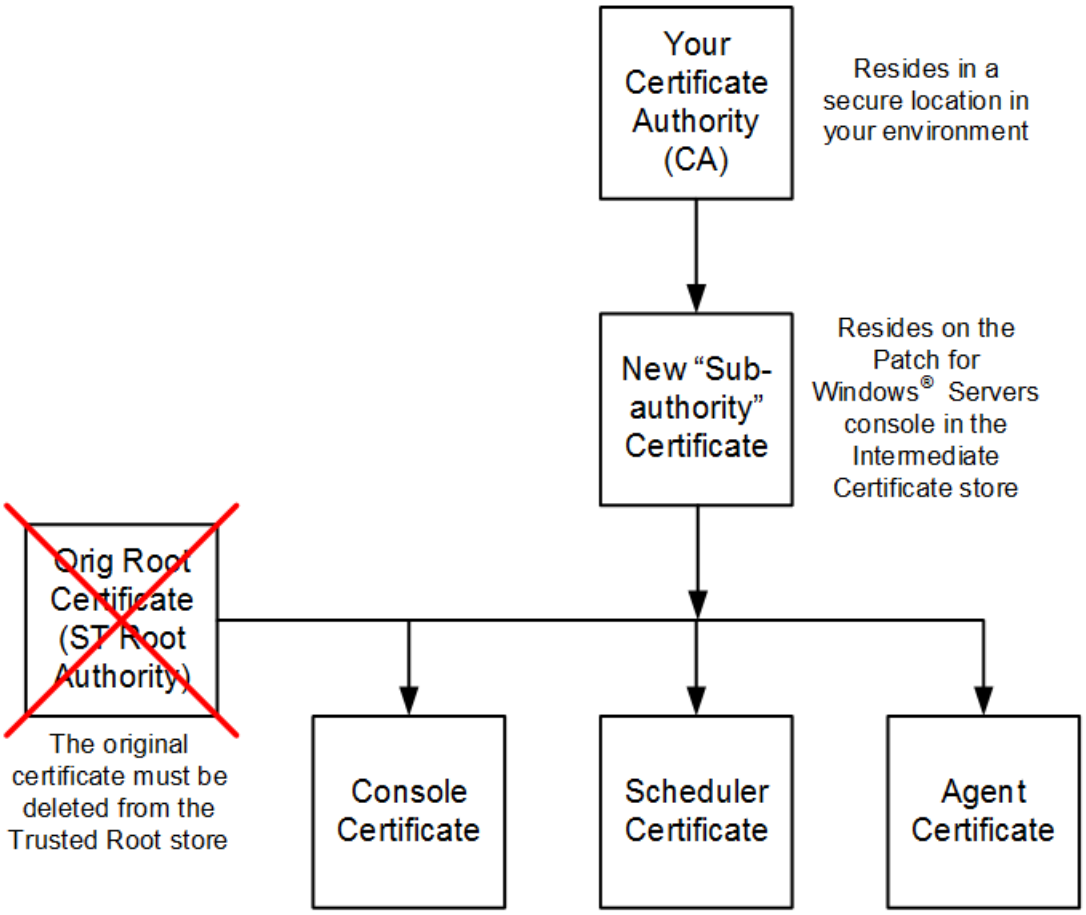


- The console certificate resides on the Patch for Windows® Servers console in the computer account Personal store.
- The scheduler certificates reside in the /ProPatches/Scheduler directory.
- On agent machines, the console certificate and the agent certificate reside in the Shavlik Protect Agent store.

After using a trusted CA to issue a new authority certificate

Here is the relationship of the certificates if you choose to issue a replacement certificate using your own CA. In Ivanti parlance, the new certificate that is issued by your CA is known as a *sub-authority*. A total of four unique certificates will be issued during the entire process. Your CA will issue a sub-authority certificate, and the sub-authority certificate will in turn issue a console certificate, a scheduler certificate and (if you use agents) an agent certificate. Multiple scheduler and agent certificates may exist, one for each scheduler and one for each agent you install.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



- The console certificate resides on the Patch for Windows® Servers console in the computer account's Personal store.
- The scheduler certificates reside in the /ProPatches/Scheduler directory.
- On agent machines, the console certificate and the agent certificate reside in the computer account's Shavlik Protect Agent store.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Requirements and Exceptions

This section identifies the requirements you must meet if you choose to use your own CA to generate a new authority certificate.

You cannot use a server SSL certificate (such as a wild card certificate) as your sub-authority certificate.

Requirements of the New Sub-Authority Certificate

- Must have a basic constraints extension

  The extension indicates that the certificate is able to issue other certificates. You may choose to specify that the parameter length is 0 (meaning that certificate cannot be used to create an issuing certificate). For more information, see RFC 5280.

- Must have KeyCertSign and CrlSign key usage extensions
- Must have an associated private key on the Ivanti Patch for Windows® Servers console machine
- Must be located in the computer account's Intermediate Certification Authorities certificate store on the console machine

Exceptions

When you configure your environment to work with a third-party CA, the console will no longer automatically update an expiring root certificate. Ivanti Patch for Windows® Servers will provide a warning when the certificate is nearing its expiration date, but it will be up to the local administrator to manually create the new certificate using their own CA.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Step 1: How to Issue a New Certificate Using Your Own CA

The specific actions you take to issue a new sub-authority certificate depends on your environment.

Option A: If your CA is accessible over your network

1 Close Ivanti Patch for Windows® Servers.

2. Use your local system facilities to issue the new certificate from your CA.

   Make sure the certificate meets all of the requirements.

3. Save the new certificate to the console machine's Intermediate Certification Authorities store.

4. On the console, open an administrator command prompt window and change to the Ivanti Patch for Windows® Servers installation directory.

   The default installation directory is: **C:\Program Files\LANDESK\Shavlik Protect**.

5. Using the STMgmt command-line tool, issue the **select_subauthority -thumbprint <thumbprint>** command to specify that the new certificate should act as the sub-authority certificate.

   Example: `stmgmt.exe -select_subauthority -thumbprint 3e656d7ca744c131c2daba3e4fb4e8731784824e`

   Be sure to include the -thumbprint argument, which indicates to Ivanti Patch for Windows® Servers that it should use the certificate as the sub-authority certificate. One method for getting the thumbprint is to:

   (a) Copy the thumbprint from the new certificate into an application such as Notepad.

   (b) Remove any spaces and special characters.

   (c) Save the file in an ANSI-encoded format.

   (d) Paste the thumbprint character from the Notepad file into the **select_subauthority** command.

   For information on using STMgmt, type the following from an administrator command prompt on the console machine:

   ```
   C:\Program Files\LANDESK\Shavlik Protect>stmgmt
   ```

6. See Let the Certificate Percolate Through the System for information on whether you need to wait 30 days before committing to the new certficate.

Option B: If your CA is not accessible over your network (the CA is offline or in a disconnected network)

1 On the console, open an administrator command prompt window and go to the Ivanti Patch for Windows® Servers installation directory.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

The default installation directory is **C:\Program Files\LANDESK\Shavlik Protect**.

2. Using the STMgmt command-line tool, issue a **request_subauthority -of <requestfile>** command to create a sub-authority certificate request.

   Example: `stmgmt.exe -request_subauthority -of samplerequestfilename.req`

   This is the request to issue the new Ivanti Patch for Windows® Servers sub-authority certificate. It creates all the information necessary for a CA to issue a certificate and save it to a file. This file is a PKCS10 certificate request and it will be used to generate the certificate on the CA.

3. Transport the file to the CA.
4. Have your CA issue the new sub-authority certificate and save it to a file.

   Make sure the certificate meets all of the requirements.

5. Transport the file to the console machine and save it to a local directory.
6. Using the STMgmt command-line tool, issue an **accept_subauthority -if <issuedcert>** command.

   Example: `stmgmt.exe -accept_subauthority -if sampleresponsefilename.cer`

   This command does several things. It:

   - Accepts the new certificate that was generated from the trusted CA
   - Binds it back to the private key on the console
   - Specifies that Ivanti Patch for Windows® Servers should use the certificate as the sub-authority certificate
   - Manages the installation of the new certificate

7. See Let the Certificate Percolate Through the System for information on whether you need to wait 30 days before committing to the new certficate.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Step 2: Let the New Certificate Percolate Through Ivanti Patch for Windows® Servers

After the new certificate has been issued by your CA and specified as the sub-authority certificate, the certificate is said to be in a pending state. The next step is to let the pending certificate work its way through Ivanti Patch for Windows® Servers.

30 day waiting period

There is a 30 day period during which the pending certificate will be distributed to your agent machines. Here's how it works:

1. Your agents will check in during this 30 day period.
2. The agents will receive a copy of the new certificate.
3. The certificate will be stored in the Intermediate store on the agent machine.

The agents will not use the pending certificate just yet, but they will have it in their possession for when the transition to the sub-authority certificate is made permanent. The pending certificate is made permanent when the system automatically issues a commit command after 30 days. If problems occur during the 30 day period, you may need to manually perform the commit.

For information about the commit process, see Commit to the New Sub-Authority Certificate.

Bypassing the 30 day waiting period

The system will wait for 30 days before it automatically commits to the new sub-authority certificate, and it does this regardless of whether you have any agents. If you do not have agents and you want to commit to the new certificate without waiting the 30 days, you can do so by manually issuing the commit command. For information about the commit process, see Commit to the New Sub-Authority Certificate.

There are other reasons you may choose to manually issue the commit command. If you have forced your agents to check in and you are certain they have all received the new certificate, you can manually issue the commit command and move forward without waiting for the 30 day waiting period to expire. Or, problems may occur that prevent the commit command from being issued automatically. For more information, see Commit to the New Sub-Authority Certificate.



Be careful when forcing agents to check in. Some agents may not receive the check-in request if they are not listening, are offline or are cloud agents.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Step 3: Commit the New Sub-Authority Certificate

Automatic commit process

If you have agents and everything has gone according to plan, after 30 days all of your agents should have checked in, received the new certificate and the system will have automatically committed to the new sub-authority certificate. See the section below titled **What happens after the commit is issued?** for more information.

Manual commit process

You may choose to manually issue the commit command for the following reasons:

- If you do not have agents, you can manually force the commit without waiting for 30 days.
- If there are agents and the system has not automatically committed to the new certificate after 30 days (or as defined by Ivanti Patch for Windows® Servers internal optimization from the maintenance task), evaluate why the commit has not occurred.



Stmgmt.exe -commit_authority will tell you which machine names it expects to fail when you perform the commit.

There are a number of outstanding issues, errors or warnings that may have occurred that are preventing the commit from happening automatically. The most likely reason is an agent-related problem, such as one or more orphaned agents that have not checked in (and never will). Your options are to (1) figure out a way to get those agents to check in, (2) delete the machines from Machine View, (3) flag the machines to uninstall their agents (even if a machine never checks in to receive the uninstall command, the fact that Ivanti Patch for Windows® Servers has indicated that the agent should be uninstalled is enough to get past the error/issue with that machine), or (4) you can manually issue the commit and permanently orphan those agent machines.

Test mode

You can use the test mode in the **commit_authority** command to tell you about potential problems with performing the commit. The command is: `stmgmt.exe -commit_authority -test`

By analyzing this information you can make an educated decision on whether to perform the commit. In some circumstances you may choose to force the commit and purposely orphan certain problem machines.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

To force the commit

Use the following command: `stmgmt.exe -commit_authority -force`

If you force the commit and you do have agents that haven't checked in that you want to keep, you will need to reinstall the agent on those machines (the agent will be unable to use the configuration information created by the console and will most likely fail to check in).

What happens after the commit is issued?

When the commit command is issued, the system will stop using the original self-signed certificate and will begin using the new sub-authority certificate. In particular, the following actions will occur:

- A new console certificate will be automatically issued from the sub-authority certificate and saved to the computer account's Personal store on the console machine.
- A new scheduler certificate will be issued whenever the Ivanti Scheduler is installed or an agentless deployment using the Ivanti Scheduler is performed.
- A new agent certificate will be automatically issued whenever a new agent is installed or when an existing agent's certificate needs to be reissued. The process should have very little affect on your network performance.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

IAVA Overview

When you purchase the Government Edition of Ivanti Patch for Windows® Servers you will receive a license key that enables you to use the Information Assurance Vulnerability Alert (IAVA) Reporter. The IAVA-specific files are automatically installed when Ivanti Patch for Windows® Servers is installed.

IAVA XML File

The IAVA Reporter provides a cross reference of the existing XML patch file supplied by Ivanti and the IAVA XML file compiled by the U.S. Government. There is typically a two week gap between the time a new patch is released (by Microsoft or other vendors) and the time the patch is included in the IAVA XML file.

There are two different ways to get the latest version of the IAVA XML file:

- By selecting **Help > Refresh files** on the Ivanti Patch for Windows® Servers console.
- By downloading the file from http://content.ivanti.com/data/iadata.cab. Place this file into the appropriate folder where the Ivanti Patch for Windows® Servers folder is installed. For example:

  C:\Program Data\LANDESK\Shavlik Protect\Console\DataFiles

See also:

- Creating an IAVA Report
- Performing an IAVA Patch Scan

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Creating an IAVA Report

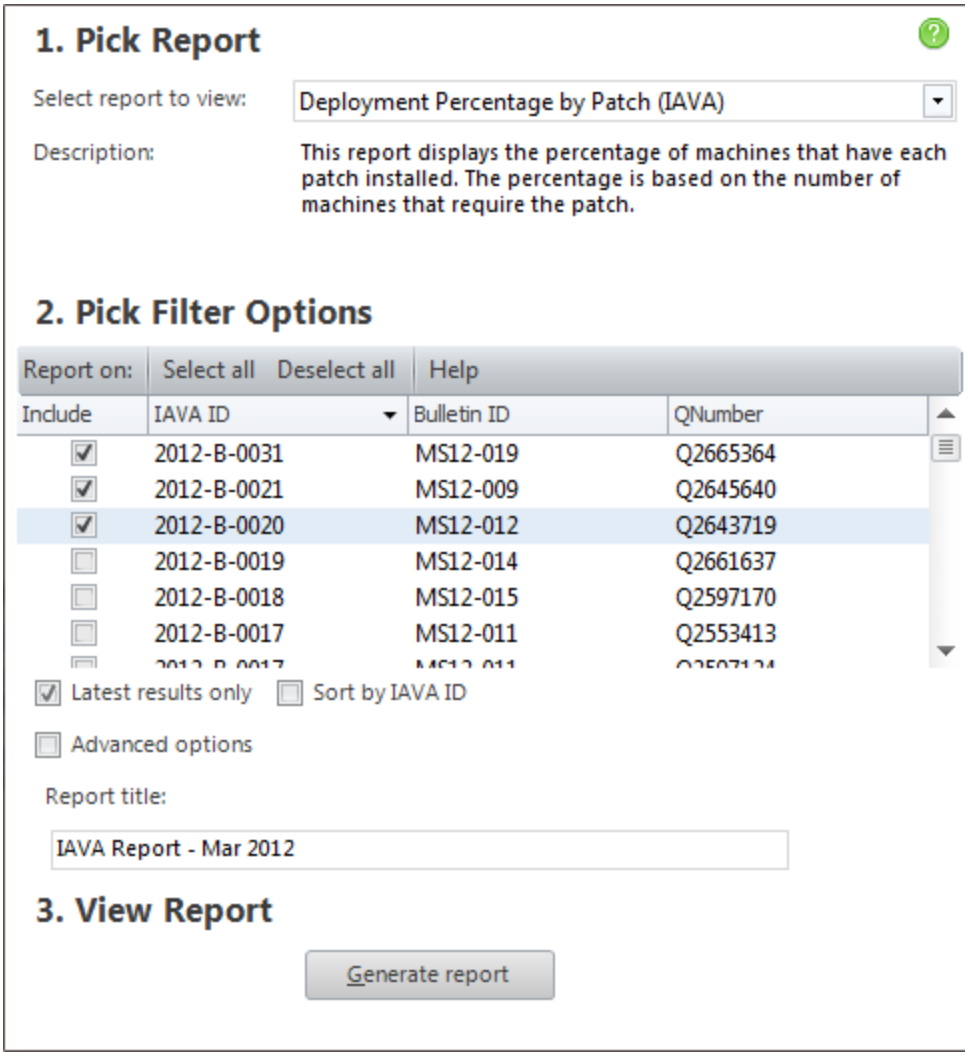
With the IAVA Reporter you can create a number of different IAVA reports using existing data in the Ivanti Patch for Windows® Servers database.

1. Open the **Reports** dialog using the **Tools > Create report** menu.
2. In the **Select report to view** box, select the IAVA report you want to generate.

   The IAVA reports are at the bottom of the Patch Reports section.

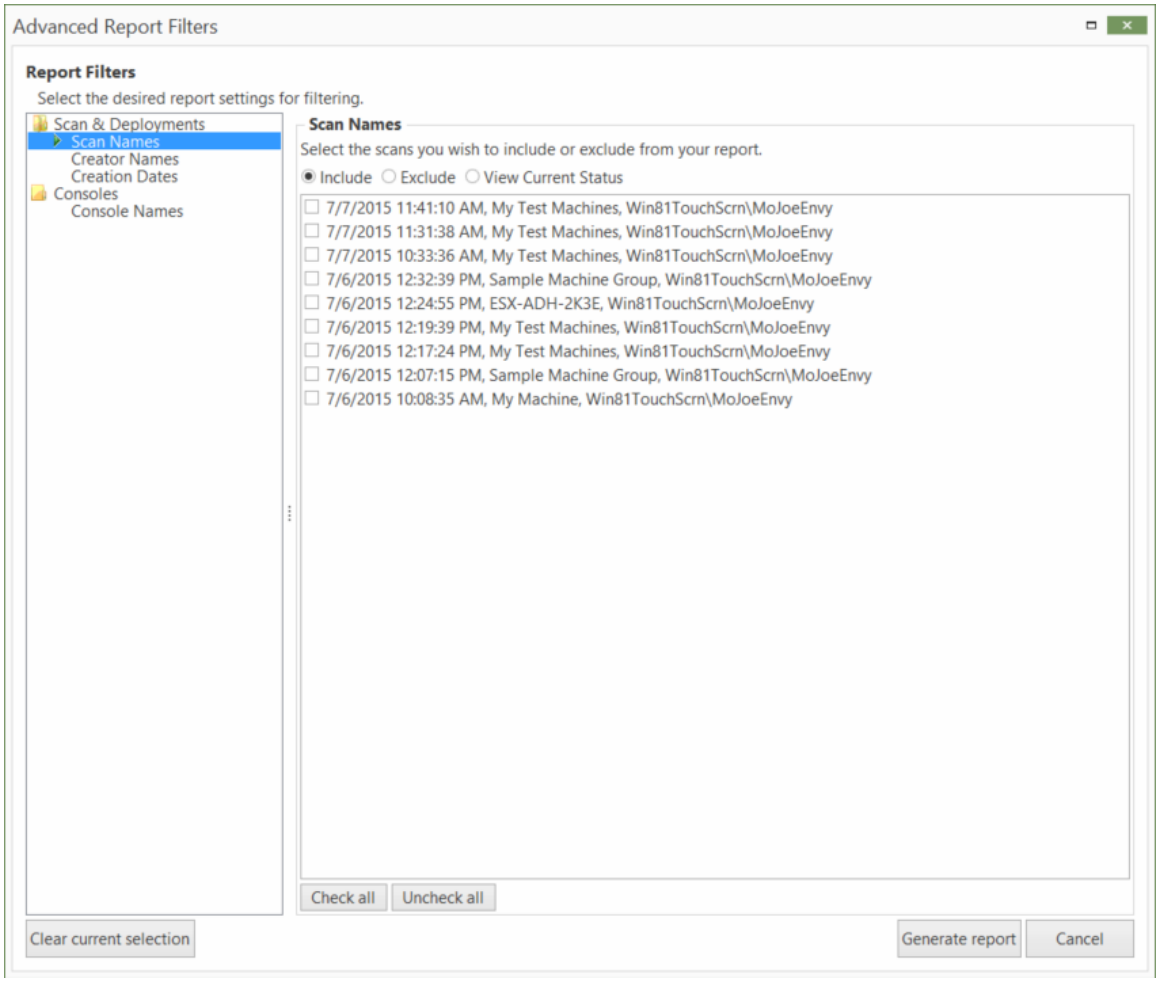
   - **Deployment Percentage by Patch (IAVA):**Displays the percentage of machines that have each patch installed. The percentage is based on the number of machines that require the patch.
   - **Detailed Summary (IAVA):** Shows a summary of the scan, plus it provides a list that shows each machine that was scanned and detailed information about each machine.
   - **Machine Status by Patch Count (IAVA):** Displays the number of machines in groups based on the number of missing patches.
   - **Patch Status Detail (IAVA):** Provides detailed information about each patch discovered by the scan.
3. Select the specific patches to report on, or select all patches.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



4. Select the desired report customization options:
   - The **Latest results only** check box enables you to view the current status by limiting the report to the most recent scan results for all machines.
   - The **Advanced options** check box will let you filter the results to specific scans, deployments, consoles, or machines.

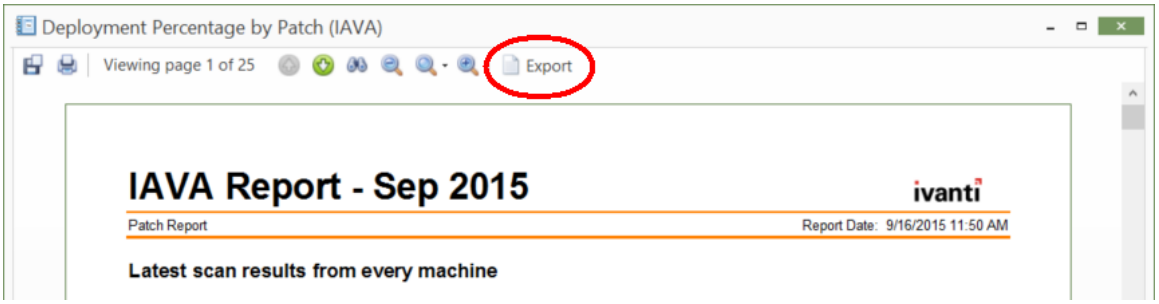
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.



- **Sort by IAVA ID:** Sorts the report results by IAVA number (lowest to highest)

5. In the **Report title** box, type a descriptive title.
6. Click **Generate report**.

The report that is generated can be exported to a variety of different formats by clicking the **Export** button.



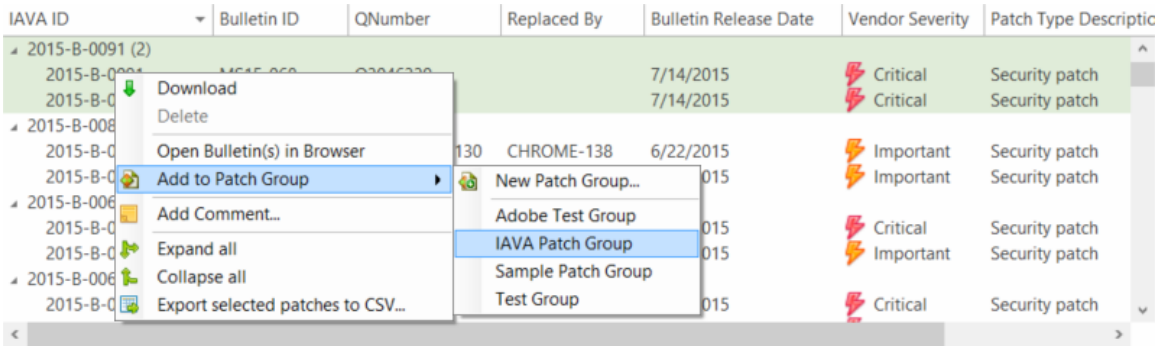
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Performing an IAVA Patch Scan

Another common use of the reporting tool is to create a patch group that contains one or more patches that are of particular interest. You then specify the patch group within a Ivanti Patch for Windows® Servers patch scan template and use the template to scan your machines on a regular basis.

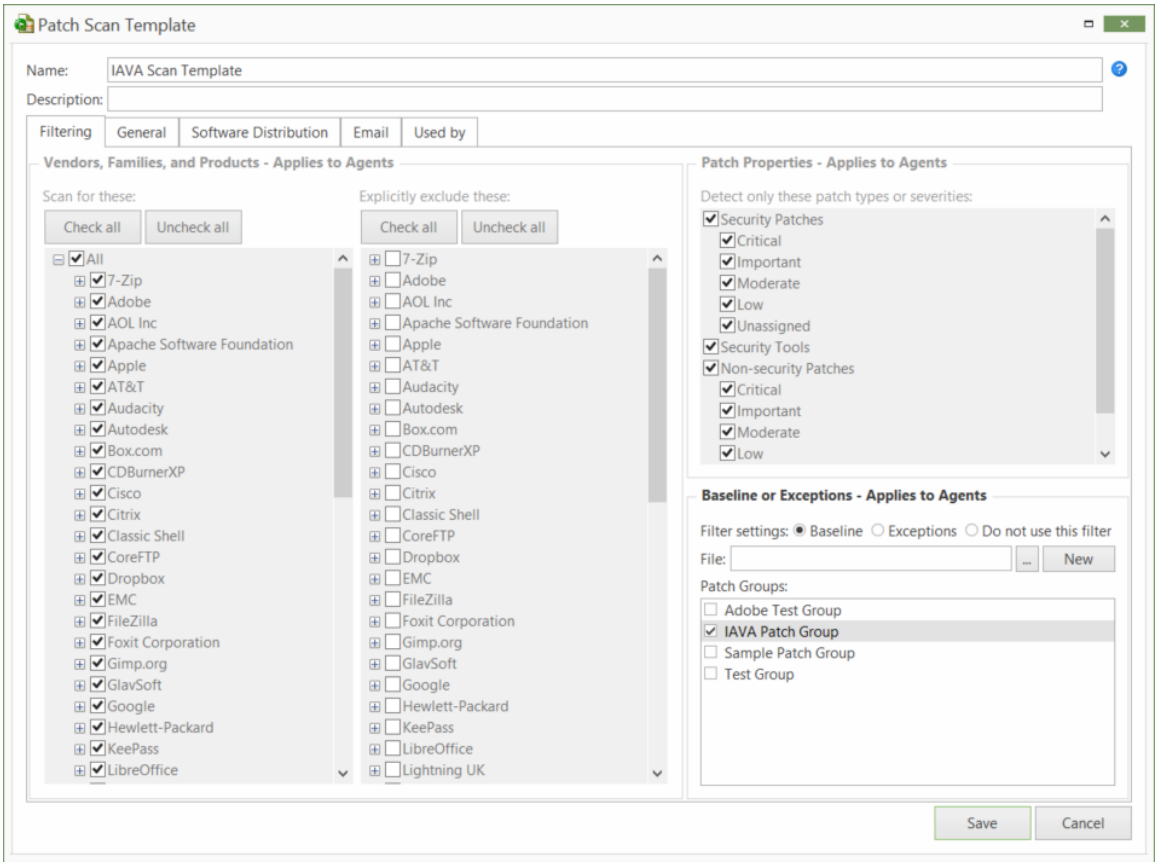
1. Create a patch group that contains the patch or patches you would like to scan for (or deploy).

   To do this, select either **View > Patches** or **New > Patch Group** and then use a Smart Filter to narrow the focus to only those patches of interest. You can then click the **IAVA ID** column header to sort the remaining patches by their IAVA ID. After selecting the desired patches, use the right-click menu to add the patches to a new or existing patch group.



2. From the main menu select **New > Patch Scan Template**.
3. On the **Patch Scan Template** dialog, type a name for the new template.
4. On the **Filtering** tab, in the **Baseline or Exceptions** area, choose **Baseline**.
5. Select the patch group you created earlier.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

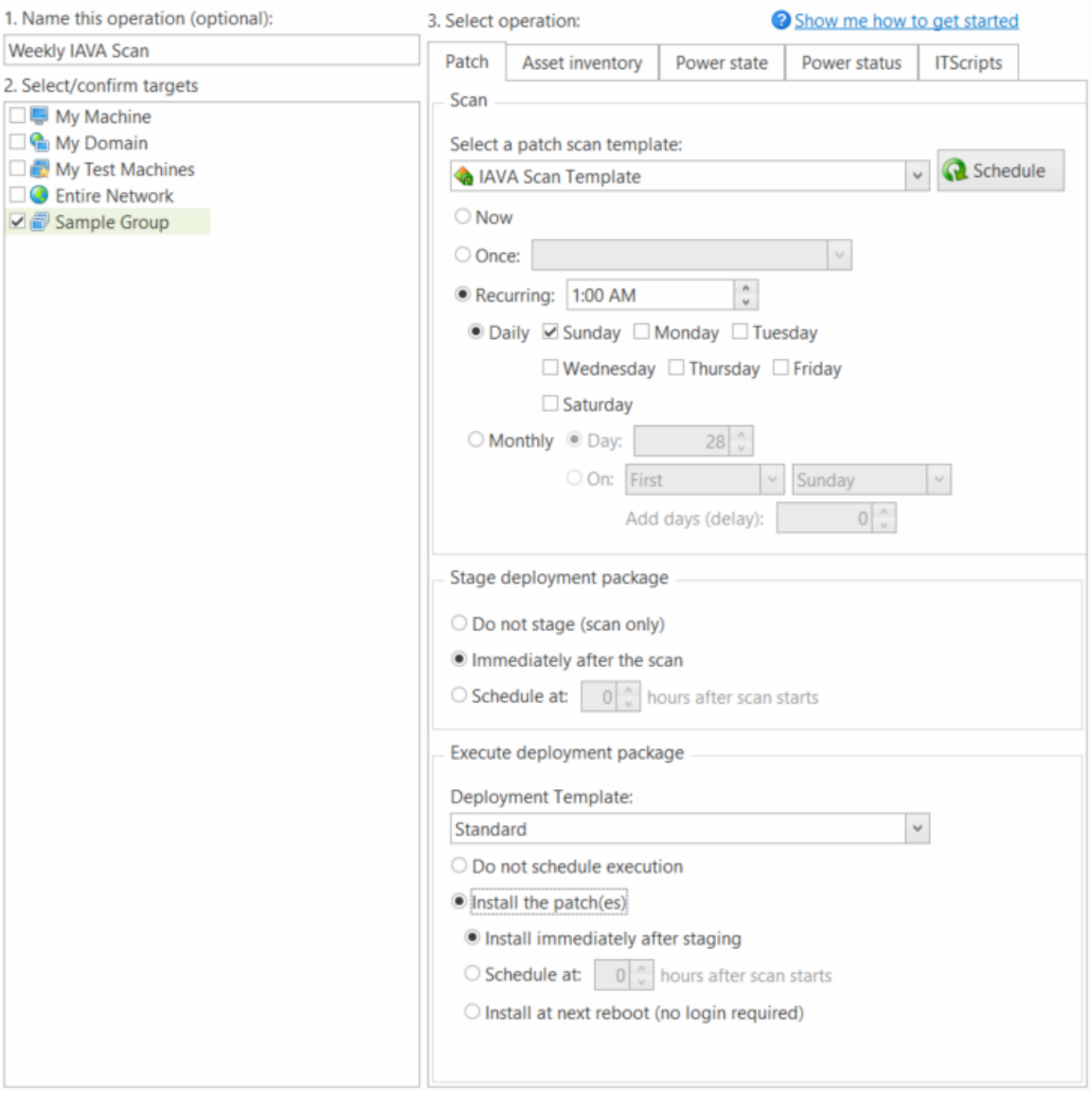


6. In the **Patch Properties** area, specify the type of patches you want to scan for.

   You must specify all patch types contained in your patch group. For example, if you selected all IAVA patches when you created the patch group, you should enable the **Non-security Patches**, **Security Patches**, and **Security Tools** check boxes.

7. Save the scan template.
8. On the home page, in the **Select/confirm targets** area, select the machine group you want to scan.
9. On the **Patch** tab, select the patch scan template you just created.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

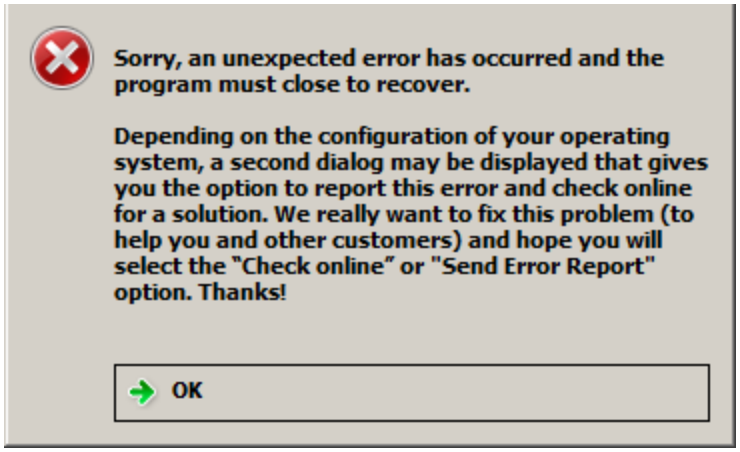


10. Schedule the scan to occur at the desired date and time.
11. (Optional) If you want to automatically deploy the patches in the patch group, select the desired deployment options in the **Stage deployment package** and **Execute deployment package** areas.
12. Click **Schedule**.

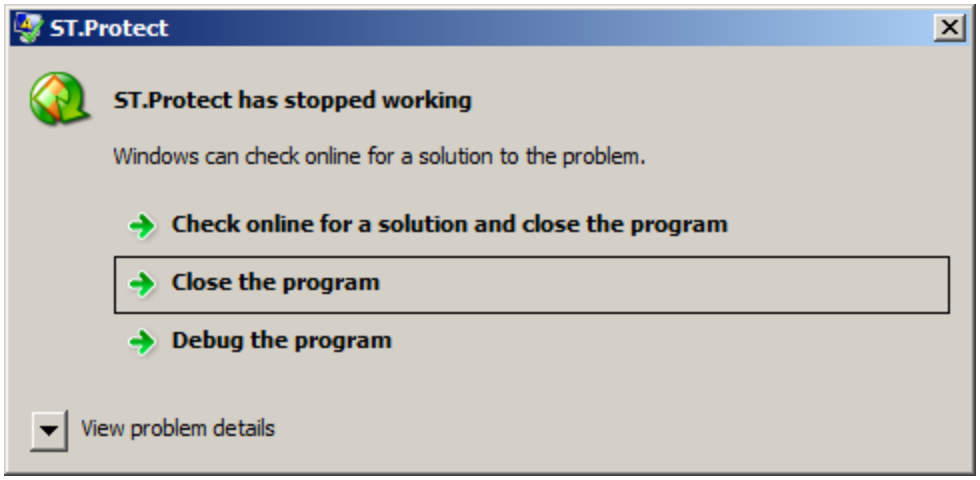
Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Reporting Errors and Checking for Possible Solutions

If an error occurs that requires the program to close in order to recover, an error dialog will be displayed.



If your operating system is configured to allow the capture and reporting of errors, after you click **OK** a second dialog will be displayed. This dialog gives you a couple of error reporting options.



Check Online for a Solution

This dialog gives you the option to send information about the error to Ivanti and to receive a possible solution to the problem. Ivanti recommends selecting the **Check online for a solution and close the program** option. This option will:

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

- Send information about the problem to Ivanti so the problem can be researched and fixed.
- Query an online database for a possible solution to the problem. If a solution exists it will be displayed on the console machine in a separate dialog.

Privacy and Security Concerns

Only information pertaining to the specific problem will be sent to Ivanti; no personal, machine, or network information is collected or sent. The information is sent anonymously and the process will not impact your network.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Obtaining Support

For technical assistance with Ivanti Patch for Windows® Servers, please refer to one of the following support options:

- Browse the Ivanti Community Site at https://community.ivanti.com
- View video tutorials on the Ivanti Help Channel on YouTube
- View product documentation at https://www.ivanti.com/en-US/support/product-documentation
- Open a support request at http://support.shavlik.com/CaseLogging.aspx
- Phone Technical Support at 1-866-407-5279 or +1-651-407-5279
- Email: support@scriptlogic.com
- Web: www.scriptlogic.com/support
- Phone: 1-561-886-2450

If you ever have a question or issue with Ivanti Patch for Windows® Servers that requires help from our Technical Support staff, please see How Do I Collect Data for Tech Support before opening a support request or calling.

Copyright © 2017 , Ivanti. All Rights Reserved. Terms of Use.

Index

.

.drs file 519

6

64-bit operating systems 21

64-bit version of the program 28

A

Action Center (Windows) 608

Activating the program 45

Active Directory 95

Active function pane 52

Address book 559

Administering roles 182

Administrator privileges 44

Advanced edition 19

Advanced report filter 571

Affected machine count 465

Agent 599

- Agent-based solution 595, 597
- Agent client program 629
- Agent cloud 614
- Agent commands 623
- Agent installation - manual 608
- Agent installation errors 622
- Agent installation options 605, 608
- Agent installation script 620
- Agent licenses 601

Agent listens 635

Agent log 635

Agent maintenance tasks 628

Agent monitoring 626

Agent on distribution server 524

Agent policies 634

Agent process 601

Agent proxy options 635

Agent uninstalling 632

Agent:When to use 597

Agent configuration 634

Asset task 649

General settings 635

Patch task 640

Power task 652

Agent options 509

Agent patch deployment process 640

Agent service pack deployment process 640

Agent Standard template 341

AgentInstaller.msi 608

Agentless solution 595

Agents managed from the cloud 545

Aggregate database 520, 570, 586

Alias (console) 704

Always reboot 348

API feature 708

Approved patches 195, 644

Archive Items list 54

Arrival options 519

Asset management 16, 397

Hardware asset scan 402, 472

Software asset scan 402, 471

Virtual asset scan 402

Asset scan 405

Asset scan template 402

Asset task 649

Assigning an agent policy 623

Assigning user roles 183

Asynchronous tasks 21, 221

Automatic synchronization 534

Automatically deploy patches 238

Automatically download patches 511

Automatically sending e-mail 561

B

Background tasking 221, 490

Backup files for uninstall 346

Bandwidth throttling 640, 655

Baseline patches 247, 276-277

Best practices 348

BIOS 418

Browse active directory 95

Browse credentials 154

Bugtraq 223

Built-in Administrator account 232, 399

Bulletin ID 465

Bulletin release date 465

Bulletin Title 465

Button tray 52

C

CAB file 223

Cancel deployment 339

Cancel task 368

Central console 578

Central Policy Manager 578

Certificates

- Agent 710
- Console 710
- Scheduler 710
- Sub-authority 711

Charts 60

Check-in interval 601, 636

Check for new data files 640

Checkpoint/restart 646

Client program 629

Cloud agents 545

- Cloud agent requirements 547
- Installing cloud agents 614

Collect data for Tech Support 203

Column chooser 289

Column filter 449

Command-line 68, 620

Comment 467

Community site 728

Concurrency 671

Configuration options 498
Connection limit 215
Connection timeout 504
Console alias editor 704
Console credentials 154
Console maintenance 477
Console Tasks Manager 493
Consoles (multiple) 578, 593
Context-sensitive Help 67
Copy but do not install 330
Copy speed 346
Creating
  Creating a custom XML file 371
  Creating a patch group 277
  Creating a patch scan template 247
  Creating an agent policy 634
  Creating favorites 172
  Creating machine groups 71
Credential best practices 154
Credentials
  Browse credentials 154
  Credentials Manager 163
  Default credentials 163
  Defining credentials 159
  Merge credentials 164
  Multiple administrator issue 179
  Precedence 168
  Requirements for deploying to VMs 324

Scheduler credential 494
Sharing credentials 161
Supplying credentials 154
Criticality 469
Criticality level for machines 487
CSV file 470
Current patch status 466
Currently assigned role 187
Custom
Custom Actions 249, 356
Custom bulletin 377
Custom criticality 487
Custom filter 269
Custom patch 379
Custom Patch File Editor 371
Custom patch process 370
Custom product 373
Custom reports 565
Custom scripts 697
Custom XML 371, 393
Customizing column headers 287
CVEID 223

D

Data files 564
Data rollup 579-580
Data rollup operations 519
Database description 64
Database maintenance 538

Database setup 33
Database sharing 532
db_owner role 30
Default credentials 163
Default patch scan template 256
Definition download source 511
Deploying patches 318
Deploying all patches 319
Deploying one patch 318
Deploying to multiple machines 321
Deploying to virtual machines 324
Deploying with an agent 640
Deploying service packs 328
Deploying SPs from the console 328
Deploying SPs with an agent 640
Deployment
Automatic deployment 333
Cancelling a deployment 339
Deploymen prerequisites 313
Deployment configuration 330
Deployment history 340
Deployment results 338
Deployment seats 51
Monitoring a deployment 336
Scheduling a deployment 330
Staging a deployment 333
Deployment template 341-342
Deployment Tracker 365

Detailed patch information 306
DFS replication 532
Dialog 349
Disable networking 324
Disable supersedence 504
Disable Sysprep 325
Disconnected console configuration 586
Configuring the central console 590
Configuring the remote console 591
Disconnected network mode
Activating a disconnected console 45
Managing data files and missing patches 564
Putting a console into disconnected mode 563
Discovery filter 159
Display icon in system tray 635
Display options 500
Display the file size confirmation dialog 502
Distributed Policy Manager 578
Distributed Policy Service 578
Distribution server status report 532
Distribution servers 521
Configuring 524
Deployment template tab 358
IP addresses 536
Recommended with threat task 635
Synchronizing 532
Update distribution server 584
Domains 90

Download 309

Download directory 511

Download file name 465

Download individual patches 310

Download method 465

Download non-English patches 310

Downloading patches 309

Duplicate virtual machines 215

Dynamic product detection 221

E

E-mail feature 558

E-mail operations 517

E-mail tab 354

Editions of the program 19

Effectively installed patches 229

Email feature 558

- Address book 559
- Automatically sending email 561
- Manually sending email 562

Enable automatic e-mailing 517

Enable e-mailing 517

Enable passphrase in manual agent installs 509

Enumerating machines 224

EOL notification 49

EOL products 453

EOL report 565

Error codes 284

Error messages 622

ESX Server 101

ESXi Hypervisor 111

Event history 477

Excluding machines 108

Executive Summary link 291

Executive summary report 291

Expiring certificate 477

Explicitly installed patches 228

Export data rollup settings 519

Export machine group 78

Exporting Reports 572

F

F1 67

Favorites 172

File download options 511

File locations 564

File version 226

Filter

- Column filter 449
- Filter Patches 247
- Filtering Machine View 295
- Filtering machines 78, 295
- Filtering Patch View 269
- Filtering reports 571

Find user 184

Firewall 399

Folder path 72

Force reboot 348

Foreign language support 310

Found patch count 465

FQDN 87

Friendly name 159

Full Asset Scan template 402

G

Generate MBSA-formatted output 504

Global thread pool 504

Global thread pool override 251

Government edition 19

Green initiative 414

GUI 60

H

Hardware asset scan 402

Hardware asset summary 472

Help system 67

hf7b.xml 223, 564

hfcli.exe 68

Hibernate requirements 417

Hibernate state 432

History 243, 340

Home page 60

Hosted virtual machines 100

How-to tutorials 209

How do I . . . ? 60

HTTP proxy 39

Hypervisor 111

Hypervisor requirements 113

I

IAVA 719

Ignoring machines 108

Import data rollup settings 519

Import from file 88, 91, 94

Import machine group 61

Importing patch definitions 44

Installation log (agent) 622

Installation logs 203

Installing

- Installing agents 605, 608
- Installing agents manually 608
- Installing the program 32
- Installing the Scheduler 498
- Installing third-party applications 283

Interactive logon: Do not require CTRL+ALT+DEL 417

Interface 52

Intermediate Authority store 716

Internet 554

Internet Explorer 554

IP address 93

IPv6 93

ITScripts

- Community site 662
- Concurrency 671
- Creating a custom script 697
- Executing 675
- Licensing 664

Metadata 697
Open PowerShell prompt 695
Operations Monitor 684
Options 556
Output 688
Overview 661
Parameters 671
PowerShell modules 662
Requirements 664
Results View 686
Scheduling 679
Script Catalog Manager 667
Secure connection requirements 664
SSL 556
Target types 662
Template 671
TrustedHosts list 557
WinRM Remoting 663
Ivanti Agent 599
Agent policy 634
Assigning an agent policy 623
Icon 627
Installing 605, 608
Maintenance 628
Monitoring 626
Preparing 603
Uninstalling 632
Ivanti Scheduler 498, 507

K

Kerberos 37

Keyboard shortcuts 300

L

Language for countdown dialog 350

Language for patches 310

License information 51

License refresh 61

Linking text files 109

Listener 556

Listening agent 635

Listening port 635

Local machine credentials 154

Local system account 154

Localized help 67

Log files 497

- Agent log files 635
- Console log files 552
- Event log 338
- Installation logs 203
- Scheduler log 338
- Version log 49

Logging on to a server 103

Logging options 552

M

Machine account credentials 40

Machine criticality 487

Machine group 71, 77
Add by IP 93
Add by OU 95
Add domain 90
Add machine by name 87
Add virtual machine 99
Excluding machines 108
Linking files to 109
Nested group 98
Machine properties 483
Machine View 446
Accessing Machine View 447
Filtering information 295
Machine group information 293
Navigating Machine View 448
Performing actions on patches 469
Searching for machines 294
Viewing hardware summaries 472
Viewing patch summaries 465
Viewing software summaries 471
Machines not scanned 284
Maintenance tasks for agents 628
Maintenance window 645
Manage items 482
Managing custom XML files 393
Manual agent installation script 620
Manually installing agents 608
Manually sending e-mail 562

Menu commands 61

Metadata 697

Microsoft Knowledge Base 223

Microsoft Scheduler 507

Microsoft Scheduler 2.0 495

Migration Tool 707

Missing patch count 465

Mitre.org 223

Monitoring

- Asset scans 411
- Monitoring agents 626
- Monitoring deployments 336
- Patch scan 241
- Power task 438

MSST-001 249

Multiple administrators 175

Multiple consoles 578

Multiple users 630

My Domain 60, 69

My Machine 60, 69

My Test Machines 70

N

Navigating the interface 52

Nested group 98

Network Interface Card (NIC) 418

Network isolation 324

Never reboot 348

Newsfeed 53

Non-English patches 310

Non-security patches 246

NTFS 21

Nullpatch.exe 249

O

Obtaining the software 28

Offline virtual machines 99, 210

Online Help 67

Open prompt (script) 674

Operations

- Data rollup 519
- Database maintenance 538
- Definition download source 511
- Email 517
- Patch download source 511

Operations Monitor 490

Options 498

- Agent options 509
- Data rollup options 519
- Database maintenance options 539
- Display options 500
- Distribution servers 524
- Email options 517
- ITScripts options 556
- Logging options 552
- Notification and warning options 502
- Patch options 504
- Protect Cloud options 550

Proxy options 554
Scan options 504
Scheduling options 507
Snapshot maintenance options 542
Organizational Unit 95
Original patch status 465

P

Passphrase 509, 611
Patch
Directory on target machine 484
Effectively installed 229
Explicitly installed 228
Patch agents 597
Patch deployment 318
Patch download source 511
Patch group 276-277
Patch Info tab 306
Patch list 582, 585
Patch management program 19
Patch scan 233
Patch scan results 284
Patch scan template 245
Patch status 225
Patch supersedance 227
Uninstalling 369
Patch breakdown 453
Patch count 456
Patch data file 223

Patch deployment 312
Canceling a deployment 339
Deploying one or more patches 318
Deploying service packs from the console 328
Deploying service packs with an agent 640
Deploying to multiple machines 321
Deployment prerequisites 313
Deployment process (agents) 640
Monitoring deployments 336
Staging deployments 333
Patch download directory 511
Patch download source 511
Patch drive path 484
Patch groups 278
Patch Information tab
Machine View 306
Patch View 273
Scan View 306
Patch language files 310
Patch management 16
Patch release date 465
Patch scan 233
Patch scan results 284
Patch status 225
Patch summaries 301, 465
Patch task 640
Patch Tuesday 239
Patch type 466

Patch updated 465
Patch View 257
Accessing Patch View 257
Filtering Patch View 269
Navigating Patch View 258
Searching Patch View 268
Path box 71
Performing actions on machines 298
Performing actions on patches 271, 469
Permissions
Offline hosted VM permissions 214
System account permissions 529
VM template permissions 217
PKI infrastucture 709
Policy agent 634
Port 135 399
Port 3389 699
Port 443 103
Port 5985 665
Port 9 418
Port requirements 26
Post-deploy reboot 350
Power management 414
Hibernate 432
How to initiate 424
Power requirements 417
Power status scan 440
Restart 437

Shutdown 436
Sleep 432
Wake-on-LAN 434
Power state template 419
Power status scan 440
Power task 652
PowerCli 663
PowerShell (see "ITScripts") 661
PowerShell prompt 695
Pre-deploy reboot 348
Predefined scan templates 246
Predictive patch 515
Prerequisites 29
Product improvement program 63
Program Functions 54
ProPatches folder 487
Protect Cloud 545
Enabling Protect Cloud synchronization 549
Installing cloud agents 614
Protect Cloud requirements 547
Protect database 32
Proxy options 554
Proxy server 554

Q

QNumber 465
Quiet mode 346

R

Randomize scheduled time 642

Reboot options 348, 350
Reboot when needed 350
Recent Items list 54
Refresh files 63
Refresh license 63
Registering 45
Remote console 578
Remote Desktop (RDP)
Initiating a connection 701
RDP port 484
Remote Desktop overview 698
Remote Desktop requirements 699
Remote dialog 347
Remote scripts 661
Remote Tasks Manager 495
Remove temp files 346
Replaced by 465
Report filtering 569, 571
Report Gallery 569
Reporting errors 726
Reports 565
Automatically sending reports 561
Custom reports 565
Manually sending reports 562
Scheduling 574
Requirements 21
Agent requirements 21
Asset scan requirements 399

Hypervisor requirements 113
Patch scan requirements 231
Port requirements 26
Power management requirements 417
System requirements 21
Restart now 424, 437
Result View (ITScripts) 686
Results importer 36
Results list 54
Right-click menu 298
Role-based administration 182
Rollback of patches 369
Rollup console 579
Routers 418
Run on boot 642
Run Scan dialog 238

S

SafeReboot 348, 350
Scan credentials 154
Scan history 243
Scan options 504
Scan results 284
Asset scan results 413
Hardware asset scan results 472
Patch scan results 284
Software asset scan results 471
Virtual machine scan results 284
Scan summary 291

Scan template 245
Scan View 284
Scan/Deployment history 243, 340
Scanning
  Scan history 243
  Scanning domains 233
  Scanning machines 233
  Scanning overview 230
  Scanning prerequisites 231
  Scanning the local machine 233
  Scheduling scans 238
  Vendor severity scanning 247
Scanning engine 223
Scans database 32
Schedule reboot 351
Scheduled Console Tasks Manager 493
Scheduled Remote Tasks Manager 495
Scheduled scans 172, 409, 495
Scheduled Tasks Manager 495
Scheduler credential 494
Scheduler Lifetime 507
Schedulers 498, 507
Scheduling
  Scheduling a report 574
  Scheduling asset scans 409
  Scheduling ITScripts 679
  Scheduling options 507
  Scheduling patch deployments 330

Scheduling patch scans 238
Scheduling power tasks 430
Script Catalog Manager 667
Script for manual agent installation 620
Scripts (also see "ITScripts") 661
Search machine groups 75
Search tool 268, 294
Secure connection requirements (scripts) 664
Security Patch Scan 245-246
Security Patch Scan template 246
Send Tracker status 346
Service pack group 655
Service packs
Deploying service packs from the console 328
Deploying service packs with an agent 640
Downloading from the console 309
Severity 307
SHA-2 709
Shared credentials 161
Shortcut on desktop 32
Show Charts button 60
Show informational items 500
Show main newsfeed sidebar 500
Show main toolbar 500
Show only items created by me 500
Show Run Now dialog 504
Show Start Page button 52
Shut down now 424, 436

Shutdown IIS Server 346

Shutdown SQL Server 346

SID (security identifier) 21

Simple file sharing 232

Sleep requirements 417

Sleep state 432

Smart filters 269, 295

SMTP server 517, 558

Snapshot 361

Snapshot maintenance 542

Software 28

Software asset scan 402

Software asset summary 471

Software distribution 250, 283

SQL Server maintenance 540

SQL Server notes 30, 40

SSL 526

- Distribution server 524
- Remote scripts 556, 671

Staging patch deployments 333

Standard deployment template 341

Standard edition 19

Starting the program 44

Statistics 60

Status report 532

STCatalogUpdate 41

STExec role 40

STMgmt command-line tool 714

STPlatformUpdater 608
STServiceHost.exe.config 39
Sub-authority certificate 711
Submit a feature request 61
Subnet-directed broadcast 418
Supplying credentials 154
Support 728
Synchronizing agents (check in) 635
Synchronizing agents using VMware Go 545
Synchronizing distribution servers 532
Sysprep 325
SYSTEM account 154, 529
System requirements 21

T

Take ownership 538
  Database maintenance 538
  Scheduled console tasks 493
Technical Support 203, 728
Temp files 346
Templates
  Asset scan template 402
  Creating a scan template 247
  Default scan template 256
  Deployment template 341
  ITScripts template 671
  Power state template 419
  Predefined scan templates 246
  Virtual machine template 211

Test Machines group 70
Test Patch Deployment tab 491
Testing patch deployment 316
Third-party applications 282-283, 322
Timeouts 504
Today's deployments 340
Today's Items list 54
Today's scans 243
Tracker 365
Trial edition 19
Trial license 46
Troubleshooting agents 622
TrustedHosts list 557
Tutorials 209

U

UAC 232, 399
Unattended console 582, 584
UNC share 511
Uninstalling agents 632
Uninstalling patches 369
Update agent settings 635
Update files 61, 511
Use backup server 358
Use only the browse list 504
Use vendor as backup 358
Used By tab
    Asset scan template 402
    Deployment template 363

Patch scan template 247
Power state template 419
User criticality 465
User interface 60
User roles 183

V

Validating custom XML 391
vCenter server 100, 103, 111
Vendor file name 465
Vendor severity 465
Vendor severity scanning 247
Vendor website location 511
Version information 49, 226
Version log 49
View current status 570
View usage (credentials) 163
Viewing custom patches 395
Viewing favorites 174
Virtual asset scan 402
Virtual environments 221
Virtual Inventory feature 111
Virtual Machine Standard deployment template 341
Virtual machines
Connection limits 214
Duplicates 215
Network isolation 324
Offline workstations 104
Roadmap of tasks 219

Snapshots 361
Viewing in machine group 107
Virtual machine notes 214
Virtual machine overview 210
Virtual machine template 211
VirtualMachine.Interact 215
VirtualMachine.Provisioning 217
VirtualMachine.State 215
VMware ESX server 103
VMware permissions
Adding hosted VMs to a group 100
Changing power state of offline VM 214
Managing snapshots 214, 217
VMware tools 325
VPN tunnels 599

W

Wake-on-LAN 434
Wake-on-LAN requirements 417
Welcome 16
What's new 20
Windows Action Center 605, 608
Windows Firewall 399
Windows Security Center 605
Windows Vista 26, 154, 231
WinRM 661
Winrm quickconfig command 664
WMI 399
WoL requirements 417

WUScan 246

X

XML file (custom) 371

XML patch data file 223