Ivanti Patch for Windows® Servers

Agent Quick Start Guide

ivanti

Copyright and Trademarks

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 © 2006 - 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.

Document Information and Print History

Document number: N/A

Date	Version	Description
October 2006	Shavlik NetChk Agent 5.8	Initial release of the **Shavlik NetChk Agent Quick Start Guide**.
April 2007	Shavlik NetChk Agent 5.9	Updated info on setting up a distribution server.
January 2008	Shavlik NetChk Agent 6.0	Added agent policy information.
June 2009	Shavlik NetChk Agent 7.0	Updated for version 7.0.
April 2010	Shavlik NetChk Agent 7.5	Updates for agent interface changes, add asset and power management, other miscellaneous changes.
September 2010	Shavlik NetPt Agent 7.6	Rebrand from NetChk Agent to NetPt Agent.
March 2011	Shavlik NetPt Agent 7.8	Update with minor interface changes.
October 2011	VMware vCenter Protect Agent 8.0	Update product branding and UI references for 8.0
September 2012	Vmware vCenter Protect 8.0.1	Update product name and version, update cover graphics.
May 2013	Shavlik Protect 9.0	Rebrand to Shavlik Protect. Navigation pane and menu changes. Add agent overview and cloud sync information. Remove references to Agent Manager.
April 2014	Shavlik Protect 9.1	Update Web links and remove references to legacy files.
September 2015	Shavlik Protect 9.2	Minor updates for user interface changes.
April 2017	Ivanti Patch for Windows® Servers 9.3	Rebrand to Ivanti. Remove references to AV.

PREPARING TO USE AN AGENT

Welcome

This document provides a roadmap of tasks you must perform when preparing to use an agent with Ivanti Patch for Windows® Servers. For more detailed information see the help system or the *Ivanti Patch for Windows® Servers Administration Guide*.

What is an Agent?

Ivanti Patch for Windows® Servers Agent is an agent service. The agents 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.

Depending on how they are configured, when installed on a machine an 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 for policy updates and download the new policy immediately
- Receive policy updates from the cloud
- Report the results to the console either directly or through the cloud

How Do I Configure and Use an Agent?

All agents are configured on the Ivanti Patch for Windows® Servers console and then installed on the desired machines one of three ways: by pushing them from the console, by installing them from the cloud, or by manually installing them on individual machines. You can configure several unique agent policies and install different agent policies on different machines.

The remainder of this guide describes the steps you must perform to configure and install your agents.

(Optional) Set 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 few reasons for using a distribution server, including:

- If some of your agents do not have Internet access and therefore will not be able to download the latest scan engines, XML data files, and patch files from the default Web sites. 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 Web sites. You must make the custom patches available by manually copying the patches to one or more distribution servers.

If your agent machines are able to access the Ivanti Patch for Windows® Servers console to download all necessary files, then you can skip this section. You may, however, elect to use one or more distribution servers anyway in order to speed the download process or to simply take some pressure off your console machine.

To set up a distribution server:

1. On the Ivanti Patch for Windows® Servers main menu select **Tools > Options > Distribution Servers**.
2. Click **New** and configure the distribution server.

   In the top half of the **Distribution Servers** dialog, be sure to specify a location and authentication method that all the agents can use when accessing the server. The lower half of the dialog is used to specify how the console will connect to and synchronize with 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 agents when accessing the data (**UNC** vs. **Anonymous HTTP** vs. **Authenticated HTTP**).
3. Click **Save**.

4. Update the distribution server with the latest patches, scan engines, and XML data files by synchronizing the server with the files contained on the console.

   - Create a scheduled synchronization entry.

     A. In the **Add scheduled sync** box in the top pane, select **All engines, definitions, and patch downloads**.

     B. In the top pane, select the distribution server you want to synchronize with the console.

     C. Click **Add scheduled sync**.

     D. Specify when you want the synchronization to occur.

     E. Click **Save**.

     F. (Optional) You might also consider configuring Patch for Windows® Servers to automatically download the scan engines and data files prior to the scheduled synchronization. To do this, select **Tools > Options > Downloads** and see the **Schedule automatic downloads** area.

   - (Optional) Perform a manual synchronization. This initiates a synchronization right now so you don't have to wait for the next scheduled interval.

     A. Make sure you have the latest files on the console by selecting **Help > Refresh Files**.

     B. Select **Tools > Options > Distribution Servers**.

     C. In the **Schedule automatic synchronization** pane, select one or more scheduled synchronization entries.

     D. Click **Run now**.

     This will immediately copy all appropriate files from the console to the specified distribution server.

Create and Configure an Agent Policy

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



There are many different features and capabilities you can enable within an agent policy. This example will illustrate how to configure an agent policy that contains all available features. In order to keep things relatively simple the default settings will be used wherever possible. Please see the online Help system for complete information on customizing a Patch for Windows® Servers Agent policy.

Create a New Agent Policy

1. On the main menu select **New > Agent Policy**.
2. Type a unique name for the policy.

On the General Settings Tab

1. If you elected to use a distribution server, in the **Engine, data, and patch download location** area, choose **Distribution Server** and then specify the distribution server you configured earlier.
2. If the agent machines must authenticate themselves to a proxy server when accessing the Internet, in the **Internet proxy credentials** box specify the necessary credentials.
3. If you want agents to be able to check in via the cloud, or if you want to install agents via the cloud, enable the **Sync with the Protect Cloud** check box (see page 10).

   This check box is only available if your console is registered with Protect Cloud. For more information, in the online Help system see **Administration > Protect Cloud Synchronization > Protect Cloud Sync Options**.

On the Patch Tab

This example shows how to configure a regularly scheduled patch task to run following Microsoft's Patch Tuesday (the second Tuesday of each month).

1. Click **Add a Patch Task**.
2. Type a name for the task (for example, *Monthly Patch Scan*) and then click **Save**.
3. On the **Schedule** tab, choose **Once per month** and in the associated boxes specify the *Second Wednesday*.

On the Asset Tab

This example shows how to configure a software and hardware asset scan that is performed every Sunday at 12:00 pm.

1. Click **Add an Asset Task**.
2. Type a name for the task (for example, *Weekly Asset Scan*) and then click **Save**.
3. In the **Schedule** area, choose **Days**, enable the **Sunday** check box, and clear all other daily check boxes.

On the Power Tab

This example shows the power management options that are available. It will not have you save a power task in the agent policy. You should not implement a power task unless you are certain you want to restart your machines, shut down your machines, or put them into a sleep or hibernate state.

1. Click **Add a Power State Task**.
2. Type a name for the power task (for example, *Temporary Power Task*) and then click **Save**.
3. In the **Power State Template** area, click **New**.
4. On the **Power State Template** dialog, click the **Power action** box and review the power state options that are available.

   You can use the power template to:

   - Put machines directly into a sleep state (for overnight energy savings)
   - Put machines directly into a hibernate state (for overnight energy savings)
   - Shut down machines (for weekend and holiday energy savings)
   - Restart machines (for maintenance purposes)
   - Restart machines and then put them into a sleep state (for maintenance and for overnight energy savings)
   - Restart machines and then put them into a hibernate state (for maintenance and for overnight energy savings)
   - Restart machines and then shut them down (for maintenance and for weekend and holiday energy savings)
5. Click **Cancel**.

   You do not want to save this new template, just review the available options.
6. Click **Delete** and then confirm the deletion.

   You do not want to save this power task in this example.

Save the Agent Policy

Click **Save and update Agents**. You can review the agent policy by selecting it from within the **Agent Policies** list in the navigation pane.

AGENT INSTALLATION OPTIONS

Installation Option 1: Use the Console to Install Agents on the Target Machines

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

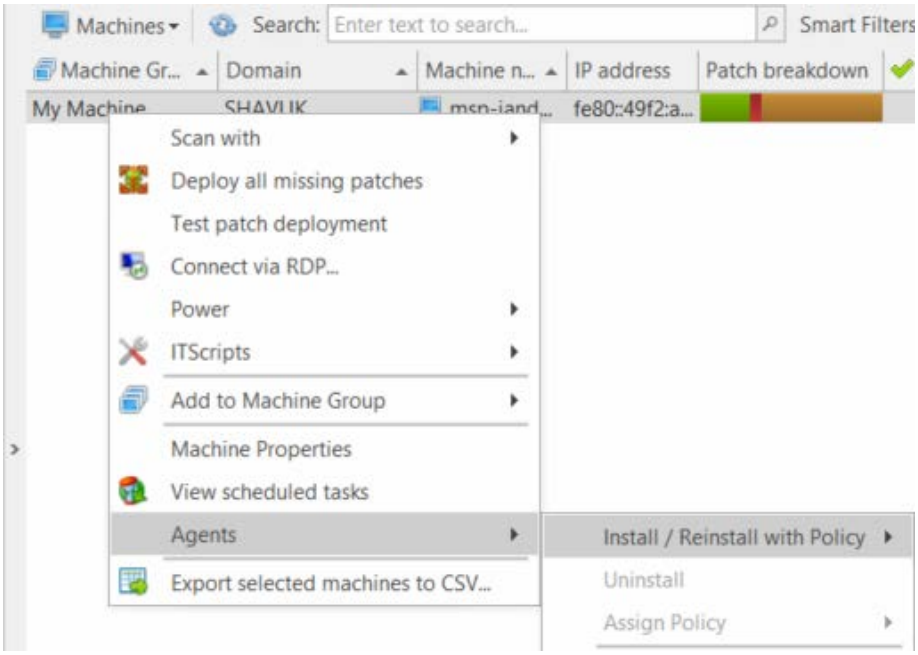


You can use the console to "push install" the agent to connected target machines. In order to perform the push install, each target machine must be online and have an active network connection to the console during the installation process. This connection is required in order to exchange security information that will be used to establish an encrypted link for all future communication between the console and its agents.

Note: Installing an agent on a distribution server machine is a special case. The machine's SYSTEM account must have read access to the distribution server folder. See **Administration > Using Distribution Servers > Configuring System Account Permissions** in the online Help system for details.

For Machines That Have Been Previously Scanned

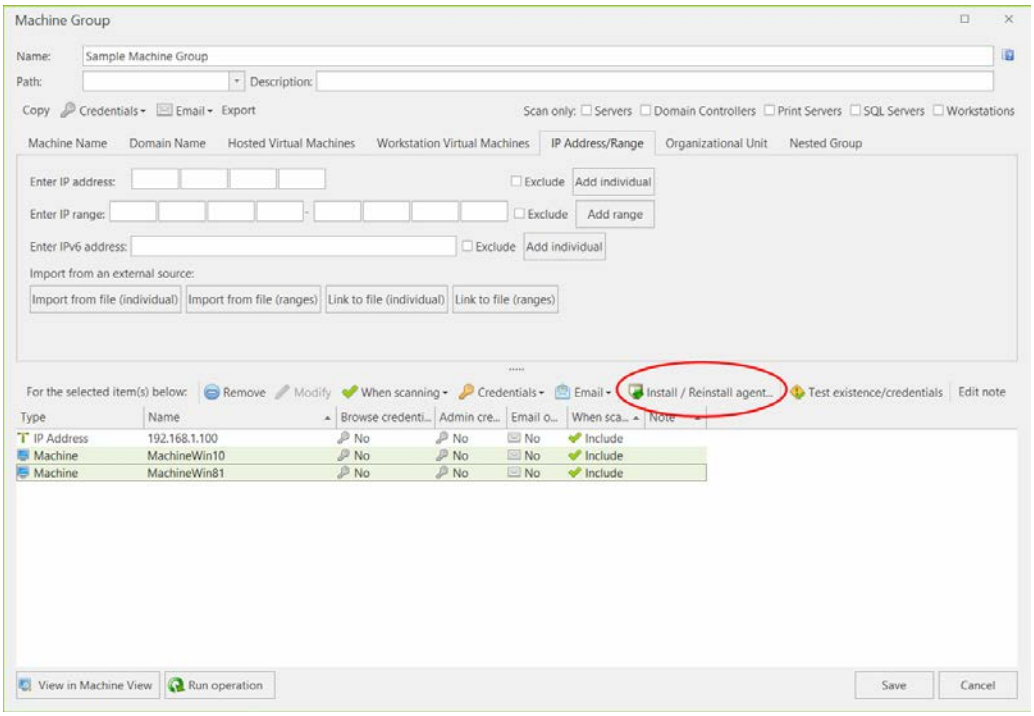
1. Go to either Machine View or Scan View.
2. Right-click the desired machines, select **Agents > Install/Reinstall with Policy** and then select the desired agent policy. For example:



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, specify credentials for the machines, and then use the **Install / Reinstall agent** button to install an agent policy on those machines. The caveat is that the machines must be online and

connected to the network. If the console cannot make a connection to a machine the agent installation will fail for that machine.



What Happens During the Installation Process

The following occurs when you push install an agent to a machine:

- The Operations Monitor is displayed and shows the status of the installation request.
- Once the agent is successfully installed on a target machine, the agent is automatically started on the machine.
- After an agent is installed on a machine, that machine becomes a managed machine and the status can be checked using Machine View. You'll have to wait until the next time the agent checks in with the console, but once that occurs the **Agent State** column will indicate that the machine contains an agent.

Installation Option 2: Installing an Agent from the Cloud

If you are using Protect Cloud synchronization, you have the ability to install an 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.

There are two basics steps to a cloud-based installation:

1. You (the administrator) must log on to the Protect Cloud service, create an agent key, and then email the key to the users of each target machine.
2. The user on each target machine will follow the email instructions to install and register the agent.

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



Requirements

- The target machine must have Internet access
- The Ivanti Patch for Windows® Servers console must be registered with Protect Cloud (**Tools > Options > Protect Cloud Sync**)
- There must be at least one policy that is configured to allow synchronization with Protect Cloud (see the **Sync with the Protect Cloud** check box on the agent policy **General Settings** tab)
- 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 Procedure

From Your Web Browser

1. Go to http://protectcloud.shavlik.com and log on to your account.

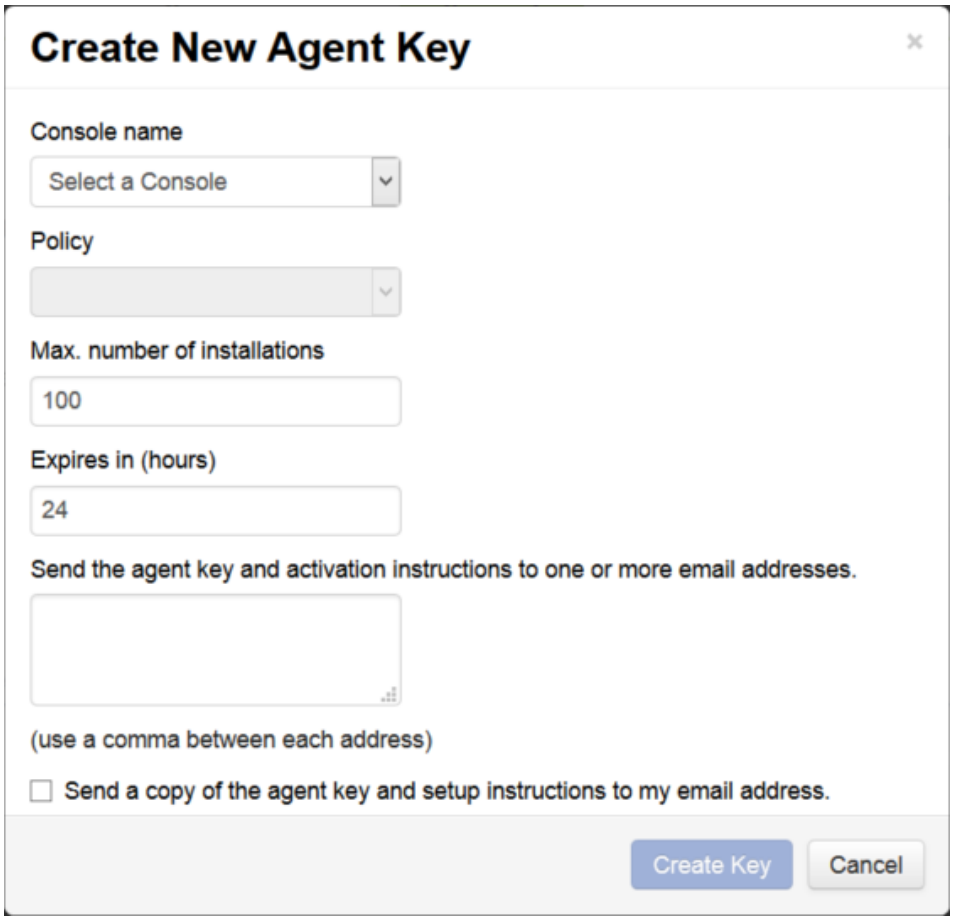
   If you don't already have an account, click **Register** to quickly setup an account.

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 a license 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.



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 (via **Tools > Edit database description**) 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 (see the agent policy **General Settings** tab).
Max. number of installations	Specify the maximum number of agent installations you will allow to be performed using this agent key. **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.
Send the agent key and activation instructions to one or more email addresses	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 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 email message that contains the agent key and the installation instructions.
3. Use the instructions to install and register the agent.
4. Wait for the agent registration process to complete; this may take 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.

Installation Option 3: Manually Installing Agents

You must manually install an agent on machines that are guarded by a firewall. You do this by copying the agent installation files to the desired machines and then running the agent installation wizard on each machine.

Requirements

- The target machines must be able to communicate with the console.
- You must configure at least one agent policy before manually installing an agent.
- You must specify how the agent will authenticate itself to the console during the registration process. See **Administration > Configuring Program Options > Agent Options** in the online Help system for details.
- Installing an agent on a distribution server machine is a special case. The machine's SYSTEM account must have read access to the distribution server folder. See **Configuring System Account Permissions** in the Help system 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** directory.

2. Copy the .exe file to the desired target machines.

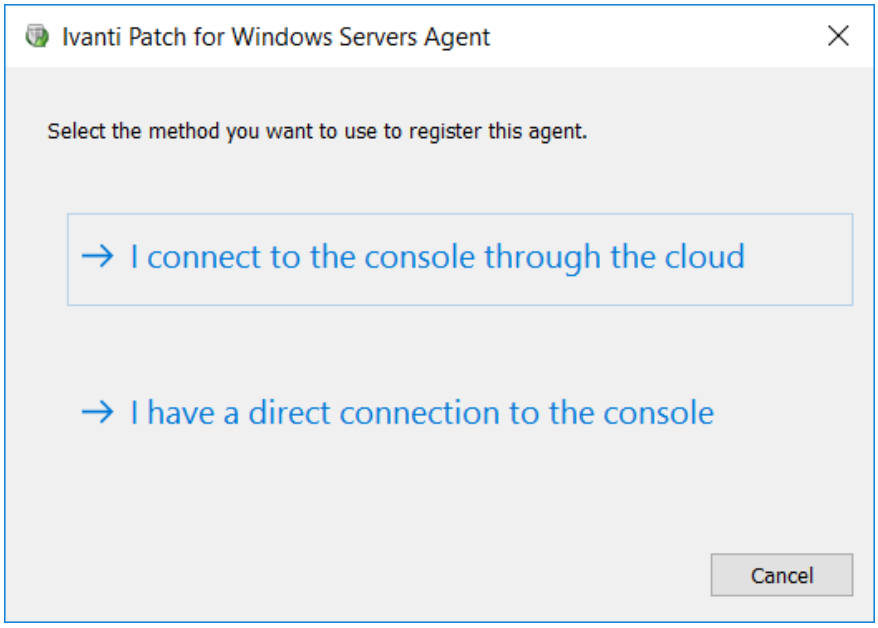
   You can distribute this file using Active Directory, or you can simply copy it to a physical media such as a CD or USB flash drive and manually distribute it to the desired machines.

   Note: When distributing this file you may choose to create an installation script that automatically passes all necessary information to the installation wizard. See **Agents > Using an Agent > Creating and Using a Manual Installation Script** in the online Help system for details.

3. Log on to the target machine using an administrator account.

4. Double-click the file named **STPlatformUpdater.exe**.

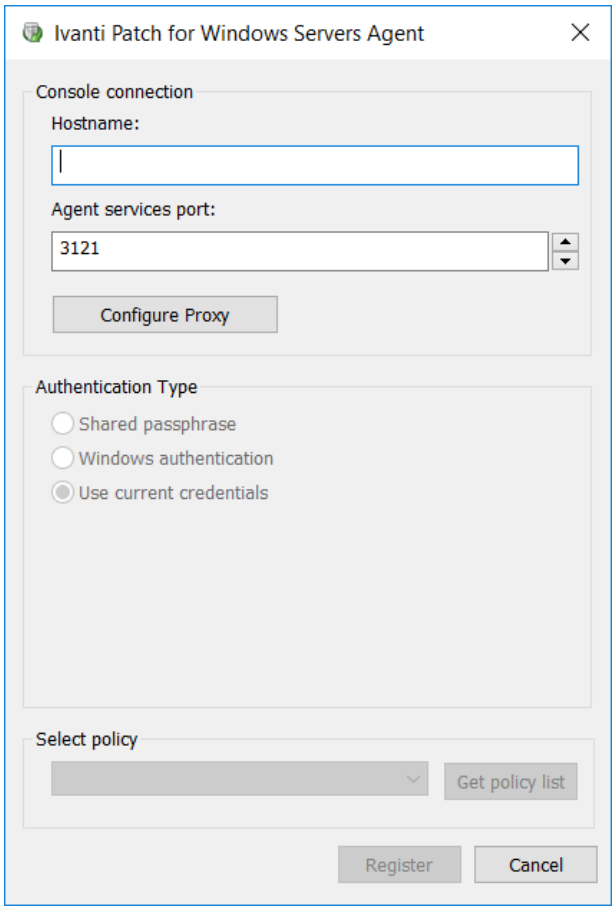
The agent is installed. When the installation is complete the **Ivanti Patch for Windows® Servers Agent** dialog is displayed.



5. Click **I have a direct connection to the console**.

Note: The **I connect to the console through the cloud** button is used if you are installing the agent using the Protect Cloud service.

The following dialog is displayed.



6. Type 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.

     Note: 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. For more details, in the online Help system see **Configuring Proxy Server Settings**.

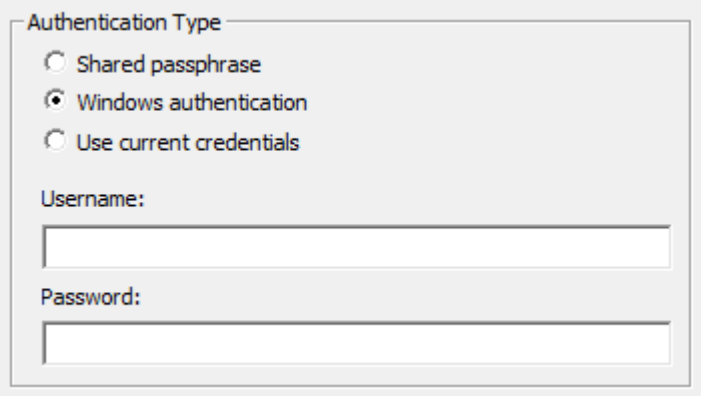
   - **Authentication Type**: You must choose the authentication method dictated by the **Tools > Options > Agents** dialog.

     - 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

7. On the **Agent Registration** dialog, click **Register**.

8. On the **Agent Setup Wizard** dialog, click **Finish**.

When the installation process is complete the agent will be started automatically.

Installation Option 4: Using a Manual Installation Script

When manually installing an 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.

Note: 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*).
- **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.

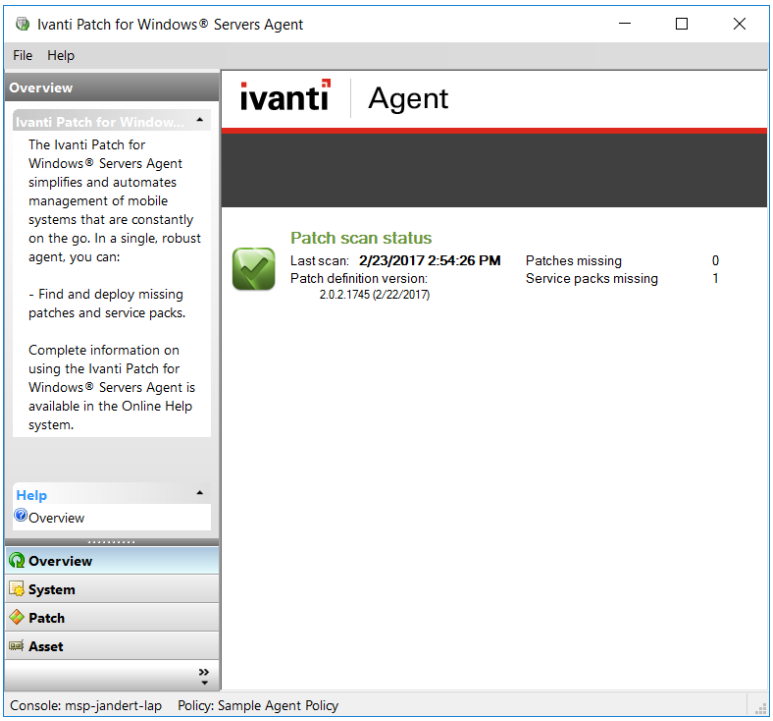
USING AN AGENT ON A MACHINE

The users of each agent machine can, if you permit, control many of the 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 Agent > Ivanti Patch for Windows Servers Agent**
- Tap or click the Ivanti Patch for Windows® Servers Agent program icon on the desktop
- Double-click the Ivanti Patch for Windows® Servers Agent icon that resides in their machine's system tray



A window similar to the following is displayed:



If users want information on how to use the client program they can simply click **Help > Contents** from the main menu.