SecurEnvoy Microsoft Server Agent

SecurEnvoy Global HQ
Merlin House, Brunel Road, Theale, Reading. RG7 4TY
Tel: 0845 2600010 Fax: 0845 260014 www.SecurEnvoy.com

SecurEnvoy Microsoft Server Agent

Installation and Admin Guide v8.1

© 2016 SecurEnvoy

The SecurEnvoy Security server is the main central component of the SecurEnvoy suite of products. It has direct integration into a LDAP directory server (Microsoft Active Directory, Novell e-Dir, Sun Directory Server and Linux Open LDAP Directory Server) for user information, controls and manages the authentication of SMS passcodes and the subsequent sending of them.

This is a pre-requisite and as such, must be installed before other SecurEnvoy applications will function.

© 2016 SecurEnvoy All Rights Reserved

SecurEnvoy Microsoft Server Agent Installation and Admin Guide v8.1

© 2016 SecurEnvoy

Publisher
SecurEnvoy Publishing

Managing Editor
SecurEnvoy Training Dept

Technical Editors
T Davis Technical Specialist

Cover Designer
SecurEnvoy Marketing

Revision	Date
V1.9 AK	05/3/2012
V2.0 SM	13/05/2013
V2.1 TD	16/1/2014
V2.2 TD	06/10/2014

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Document Version 2.2 Printed: Oct 2014 in United Kingdom.

Contents

1.0 Overview of Installation Files 5
1.1 SecurEnvoy Microsoft Server Agents 5
2.0 SecurEnvoy Microsoft Server Agent Install & Configuration 5
2.1 Agent Architecture 5
2.2 Installing the SecurEnvoy Microsoft Server Agent 5
2.3 Upgrading SecurEnvoy Microsoft Server Agent 7
2.4 SecurEnvoy Microsoft Server Agent Administration 8
3.0 Single Sign on 13
3.1 IIS Agent Architecture 15
3.2 SecurEnvoy Microsoft Server Agent Application Pools 16
4.0 Windows 2012R2 with Remote Desktop Web Gateway Integration Guide 18
4.1 Configure the Microsoft Server Agent 19
4.2 Test the Two Factor Authentication 20
5.0 ADFS v3 22
5.1 Test the Two Factor Authentication 23
6.0 Notes 24

© 2016 SecurEnvoy All Rights Reserved

1.0 Overview of Installation Files

SecurEnvoy Microsoft Server Agent

This agent is only required if you are installing SecurAccess and you need to directly authenticate an application running on an IIS Web Server, or you want to authenticate Microsoft remote gateway.

With this agent, any existing web application can be configured for two factor authentication without the need to modify the application or make any programmatic changes.

1.1 SecurEnvoy Microsoft Server Agents

IIS Pre-Requisites

Supported IIS Versions:-

IIS V6 running on Windows 2003 - all service packs (x32 and x64 bit).
IIS V6.2 running on Windows 2008 SP1-2 (x32 and x64 bit) and R2.
IIS V7 running on Windows 2008 SP1-2 (x32 and x64 bit) and R2.
IIS V8 running on Windows 2012 and R2
It is highly recommended that any protected web server should have SSL (https) enabled.
Microsoft .NET 2.0 is installed

2.0 SecurEnvoy Microsoft Server Agent Install & Configuration

2.2 Installing the SecurEnvoy Microsoft Server Agent

Pre-Requisites: IIS must be installed and running on one of the following: -
Windows 2003
Windows 2008 & R2
Windows 2012 & R2

SecurEnvoy Security Server Version 5.4 or higher is required for this version of SecurEnvoy Microsoft Server Agent.

Microsoft Dot Net v2.0 installed.

There must be a network connection via RADIUS (UDP Port 1812 -default) between the IIS server and the security server(s).

Note

A RADIUS profile must be created upon each authenticating SecurEnvoy Security Server. See Security Server Administration Guide for further details.

© 2016 SecurEnvoy All Rights Reserved

For Windows 2012R2 with Remote Desktop Web Gateway

It is assumed that Remote Desktop Services and is authenticating with a username and password.

Securenvoy Security Server has been installed with the Radius service and has a suitable account that has read and writes privileges to the Active Directory. If firewalls are between the SecurEnvoy Security server, Active Directory servers, and Remote Desktop Services, additional open ports will be required.

Microsoft Server Agent has been installed as per the SecurEnvoy Microsoft Server Agent Installation and Admin Guide:
https://www.securenvoy.com/integrationguides/iis%20agent%20installation%20guide.pdf

Note

You must use SecurEnvoy Microsoft Server Agent 7.3 or higher
You must use SecurEnvoy Security Server version 7.3 or higher
You Must use Remote Desktop Client 8.1 or higher

The following table shows what token types are supported.

Token Type Supported	
Real Time SMS or Email	✓
Preload SMS or Email	✓
Soft Token Code	✓
Soft Token Next Code	✓
Voice Call	✓
One Swipe Push	✓
One Swipe QRCode	✓

© 2016 SecurEnvoy All Rights Reserved

To install the Microsoft Server Agent run "Microsoft Server Agent \setup.exe"

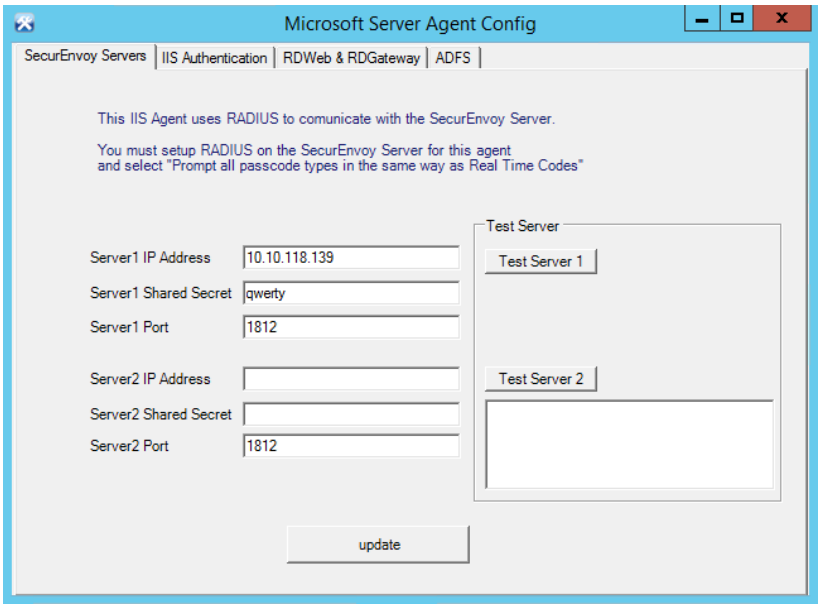
The following page is displayed for user input.

When prompted; enter up to two security servers (note these two security servers must have a RADIUS profile created upon each.)

If only one security server is required, blank the second server entry.

The "Test Server" button allows a RADIUS communication test to see if the Security server is reachable.

Make sure all the security server names you enter can be resolved and reached. It is recommended to start a CMD window and PING all security servers that will be entered.



Response codes are shown below:

OK	All settings are correct
Error, Shared Secret Does Not Match the Server	Shared secret mismatch
Error, Connection Timed Out	IP address or Port issue

This completes the Microsoft Server Agent installation.

2.3 Upgrading SecurEnvoy Microsoft Server Agent

Note

If you are running the earlier Microsoft IIS Agent, it is strongly recommended you upgrade as this agent has enhanced security

If you are upgrading from version 5.3 or earlier the agent communications protocol has changed from http (port 80 TCP) to RADIUS (port 1812 UDP). Make sure any firewalls between the Server Agent and the Security server allow the radius ports 1812 UDP. Next

© 2016 SecurEnvoy All Rights Reserved

setup the IP address of this agent in the security server's radius settings (when upgrading you will be prompted for the security server's radius settings).

To upgrade the Microsoft Server Agent, please complete the following:

Backup the seiis.ini file resides under C:\windows\.

If you have changed the login web templates, you should backup the WEBAUTHTEMPLATE directory.

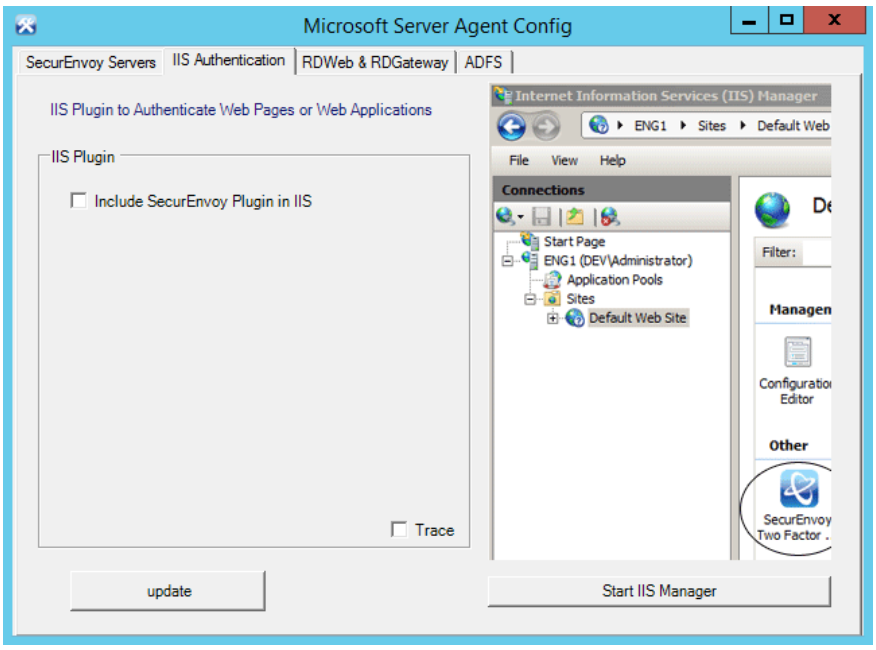
Install the new Microsoft Server Agent over the existing install by running setup.exe. If you have an existing Microsoft IIS Agent, you can upgrade and directories will be preserved.

> **Note**
>
> ***Upgrading will automatically preserve your current settings and a backup of any custom login templates will be created for you. If you have enabled the ADFS plugin, it is recommended that you uncheck "Include SecurEnvoy Plugin in ADFS" in Microsoft Server Agent Config before uninstalling or upgrading.***

> **Note**
>
> ***Do NOT un-install the existing Microsoft Server Agent or you will lose your configuration settings***

2.4 SecurEnvoy Microsoft Server Agent Administration

Select the 'IIS Authentication' tab and click 'Start IIS Manager'



© 2016 SecurEnvoy All Rights Reserved

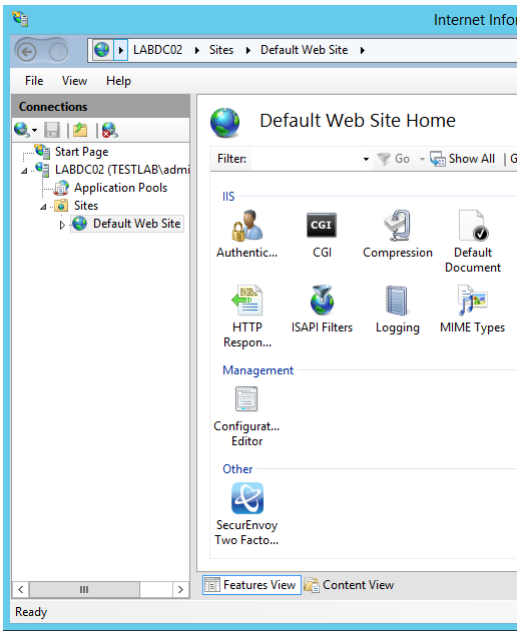
Administration is performed on Windows 2003 via Microsoft's Management Console (MMC) or for Windows 2008R2 / Windows 2012R2 via Information Services (IIS) Manager.

To enable the Agent and protect the whole web site carry out the following: -

For Windows 2008 & Windows 2012 deployments

Select Start\Administrative tools\Internet Information Services (IIS) Manager

Select sites and then navigate to the web site(s) that you wish to protect.



Double click the SecurEnvoy Icon, the screen below is shown. Enable the Microsoft Server Agent by checking the box "Enable authentication On" and select the "Protect all resources" click apply.

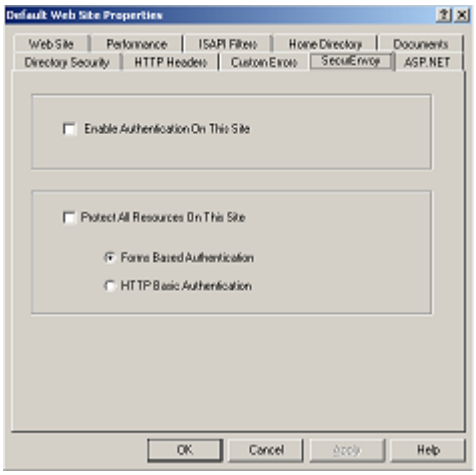


For Windows 2003 deployments

Select Start\Programs**SecurEnvoy**\IISConfig MMC.

Right click the web site that you wish to protect.

Select the **SecurEnvoy** Tab
You should see the following screen:



Enable Microsoft Server Agent by checking the box "Enable Microsoft Authentication" and select the "Protect all resources" Click OK.

© 2016 SecurEnvoy All Rights Reserved

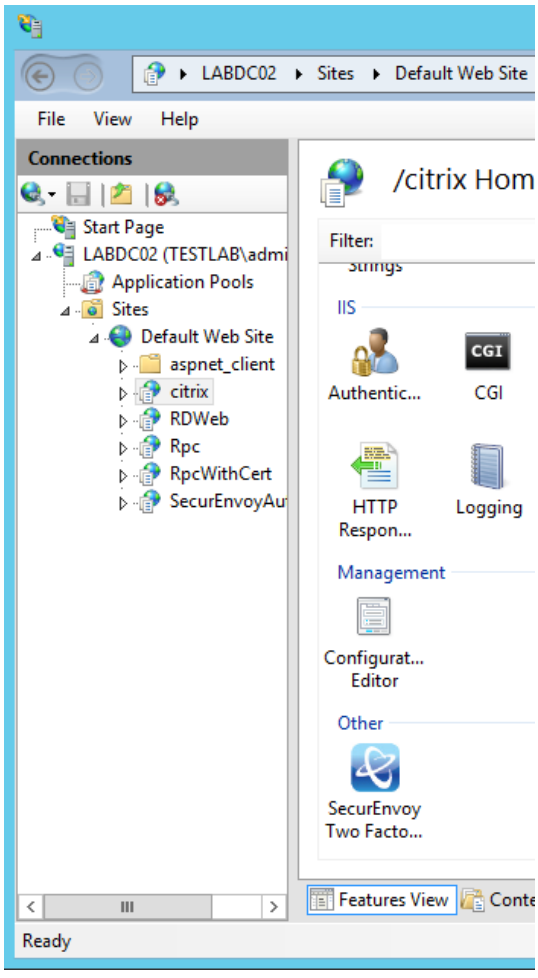
To enable two factor authentication to this server select "Enable Authentication". If you require the whole web to be protected enable the check box "Protect all resources on this server". If you wish a more granular approach to only protect certain resources upon the IIS web server leave this box unchecked and apply protection for each required resource. The protection can be applied at a virtual server or a virtual directory.

To protect a certain virtual directory carry out the following: -

For Windows 2008 & Windows 2012 deployments

Select Start\Administrative tools\Internet Information Services (IIS) Manager

Select sites and then navigate to the web site(s) that you wish to work with. Select the virtual directory, you will then see a SecurEnvoy Icon displayed in the "Features View window".

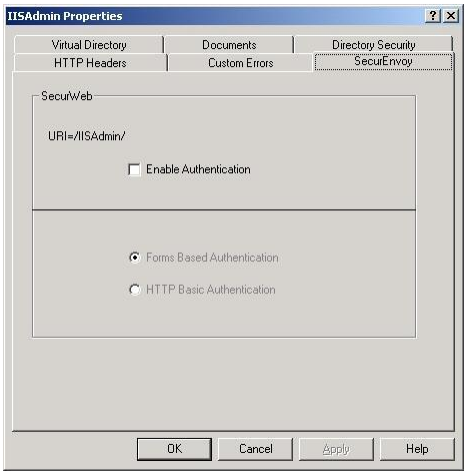


Double click the SecurEnvoy Icon; the following screen will be displayed.

For Windows 2003 deployments

Select Start\Programs**SecurEnvoy**\IISConfig MMC.

Select Web sites and then navigate to the web site that you wish to work with.
To protect a web resource (a Directory, Virtual Directory or Page) select the resource and right click it and then select properties and the **SecurEnvoy** Tab and enable the check box.



Check the "Enable Authentication" box to enable authentication on this resource and any directories or pages inside it.

There are two ways to carry out a two-factor authentication with IIS, the first is to use a form based logon, and the second is to use a HTTP basic auth. The basic auth will provide a pop up authentication screen for the web browser.

© 2016 SecurEnvoy All Rights Reserved

For Windows 2008 & Windows 2012 deployments



Check the "Enable Authentication" box to enable authentication on this resource and contents within.

There are two ways to carry out a two-factor authentication with IIS, the first is to use a form based logon, and the second is to use a HTTP basic auth. The basic auth will provide a pop up authentication screen for the web browser.

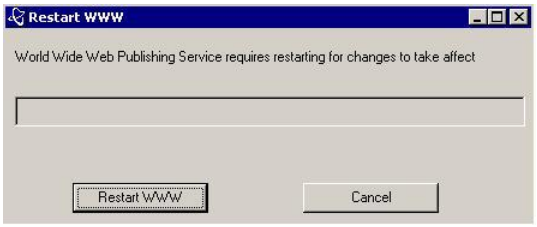
Click "Apply"

Follow prompts for restarting the IIS web server.

For Windows 2003 deployments

Click Ok

When complete the configuration will prompt for the World Wide Web publishing service to be restarted.



Note

If using HTTP Basic Authentication then Microsoft LDAP password must be used as the pin. See Config Section of Security Server Admin Guide for further details. In addition, the protected resource must be set to basic only authentication and have a default domain listed for the authentication. This will then allow a single sign on solution from a two-factor authentication to the application. In addition, "Passcode prompt is on a separate dialog (requires Access Challenge) must be disabled from within the Radius tab for Basic HTTP Authentication to work correctly.

If this server doesn't have SSL (https) enabled it is recommended that a server certificate is added and SSL is enabled on this server, See Appendix A. If however you don't wish to add a server certificate and are willing to risk session cookies being intercepted as they are sent down a non-encrypted connection, then you can check the box "Allow Non Secure Communications (http)"

Authentication timeout is the number of minutes from the last successful authentication until the user is prompted for re-authentication. It is recommended that this is set long enough to allow a typical user to complete their session.

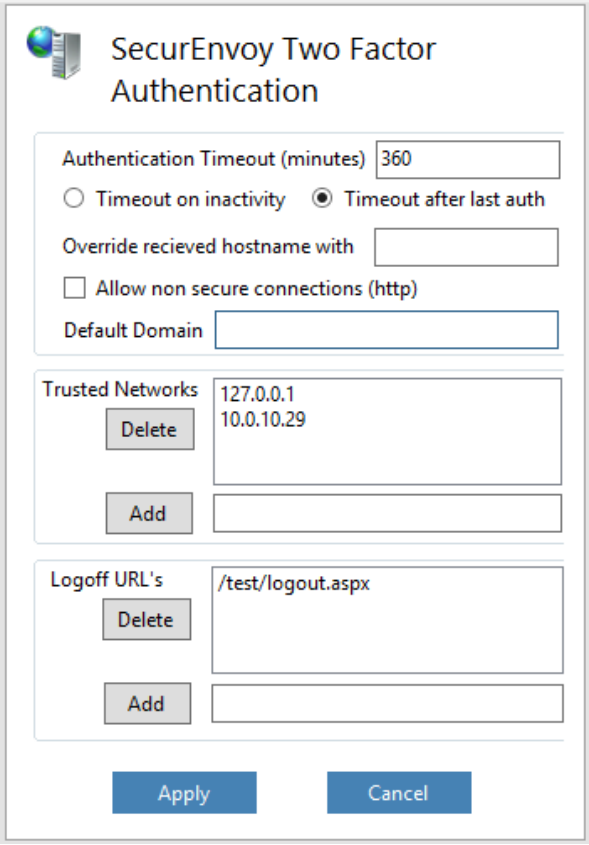
© 2016 SecurEnvoy All Rights Reserved

To change the global parameters for the IIS the Agent carry out the following: -

For Windows 2008 & Windows 2012 deployments

Select Start\Administrative tools\Internet Information Services (IIS) Manager

Select the physical machine, and then double click the SecurEnvoy Icon, the following screen will appear.



The following parameters can be changed:

Authentication timeout in minutes, select from inactivity timeout or timeout after authentication

Override Hostname information
Allow http connectivity

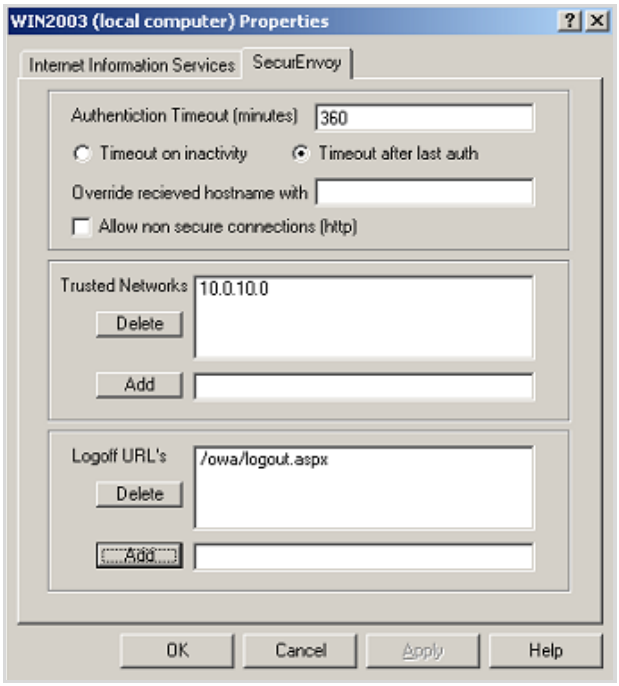
Trusted Networks, networks and single machines that are trusted and do not require a 2FA can be entered here.

Logoff URL's, existing application logoff URL's can be entered and these will then be called when the browser is closed or user logoff's.

For Windows 2003 deployments

Select Start\Programs**SecurEnvoy**\IISConfig MMC.

Select the physical machine, and right click and then select properties, the following screen will appear.



Select the **SecurEnvoy** Tab

The following parameters can be changed:

Authentication timeout in minutes, select either inactivity timeout or timeout after authentication

Override Hostname information
Allow http connectivity

Trusted Networks, networks and single machines that are trusted and do not require a 2FA can be entered here.

Logoff URL's, existing application logoff URL's can be entered and these will then be called when the browser is closed or user logoff's.

Domain and passcode parameters are controlled within the RADIUS profile upon the SecurEnvoy Security Server.

© 2016 SecurEnvoy All Rights Reserved

Note

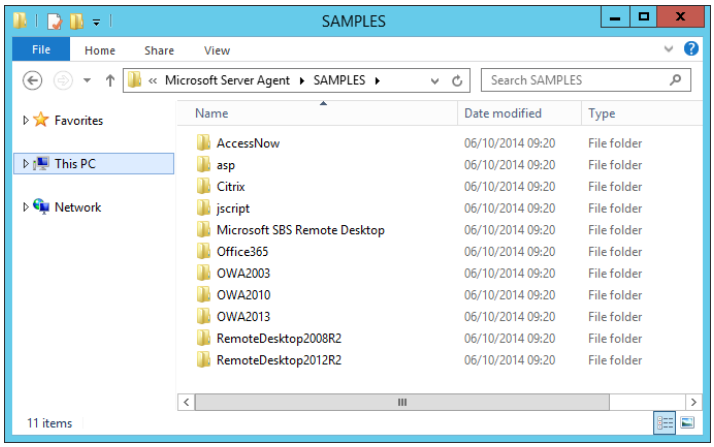
Trusted Networks format needs to be one of the following:
Exact IP Address, for example 192.168.1.1
*Wildcard, for example 192.168.1.**

3.0 IIS Single Sign on

Any application that makes use of IIS basic authentication (Not Integrated Windows authentication), users will be automatically signed into the application after a 2FA with either HTTP Basic or Form based authentication enabled.

To facilitate a simple sign on solution, SecurEnvoy has included a number of pre-configured templates for the majority of mainstream applications.

Navigate to Program Files\SecurEnvoy\Microsoft Server Agent\Samples directory; there will be a number of pre-configured applications.



Select the one that is correct for your environment.

Select the correct application and then copy the passcodeok.htm file to:

C:\Program Files\SecurEnvoy\Microsoft Server Agent\WEBAUTHTEMPLATE

Overwrite the original file.

Note

It is recommended to either rename or backup the original Passcodeok.htm file prior to this process.

Note

*For **SSO** with form based logon. If no available passcodeok.htm file exists in samples directory for your specific application. Simply create a new passcodeok.htm file and map the form elements required for authenticating. See existing sample passcodeok.htm files for reference.*

You should use the same Form Action login page defined in your form element. Define hidden input entry fields that match your application logon requirements, substituting $USERID$ and $PASSWORD$ for username and password values.

© 2016 SecurEnvoy All Rights Reserved

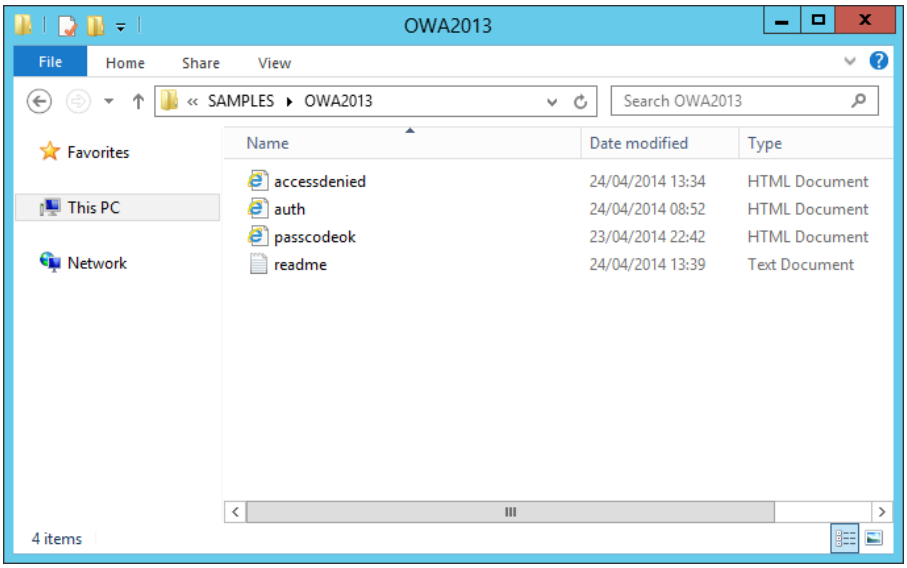
Example

To configure a Two Factor authentication for Exchange Web mail upon Microsoft Exchange 2013 server.

Install Microsoft Server Agent upon the Exchange 2013 Front end server.

1. Click – start – programs – SecurEnvoy – IIS Config MMMC
2. Expand MMC tree to show default web site
3. Right mouse click default web site, select properties, select the SecurEnvoy tab, click "Enable SecurAccess authentication upon this server", click OK
4. Click restart WWW
5. Navigate to Exchange virtual directory, right mouse click and select SecurEnvoy tab, check enable authentication, check Forms based authentication, click OK
6. Click restart WWW

Navigate to Program Files (x86)\SecurEnvoy\Microsoft Server Agent\Samples\OWA2013



Copy the passcodeok.htm, auth.htm and accessdenied.htm files to:
C:\Program Files\SecurEnvoy\Microsoft Server Agent\WEBAUTHTEMPLATE

Overwrite the original files.

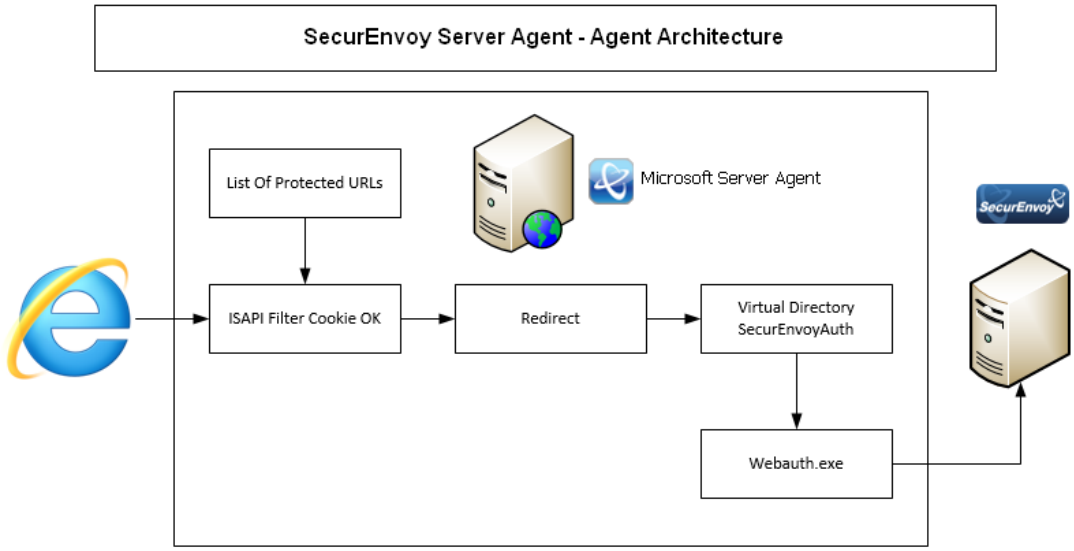
Note

It is recommended to either rename or backup the original Passcodeok.htm, auth.htm and accessdenied.htm files prior to this process.

Carry out a test authentication by going to https://*servername*/owa
Enter UserID, windows password and passcode

© 2016 SecurEnvoy All Rights Reserved

3.1 IIS Agent Architecture



All web URL requests are monitored by the ISAPI filter program webauthfilter. If a protected resource is requested, the filter checks to see if a valid un-tampered cookie is available and that it hasn't timed out. If the cookie is OK then the request is passed on. If the cookie is unavailable or has timed out the ISAPI filter redirects the request to SecuEnvoyAuth/webauth.exe. This program requests a UserID, Pin and Passcode and sends it to the security server for authentication. If the security server returns AUTH OK then webauth.exe creates a valid cookie and redirects the request back to the original page.

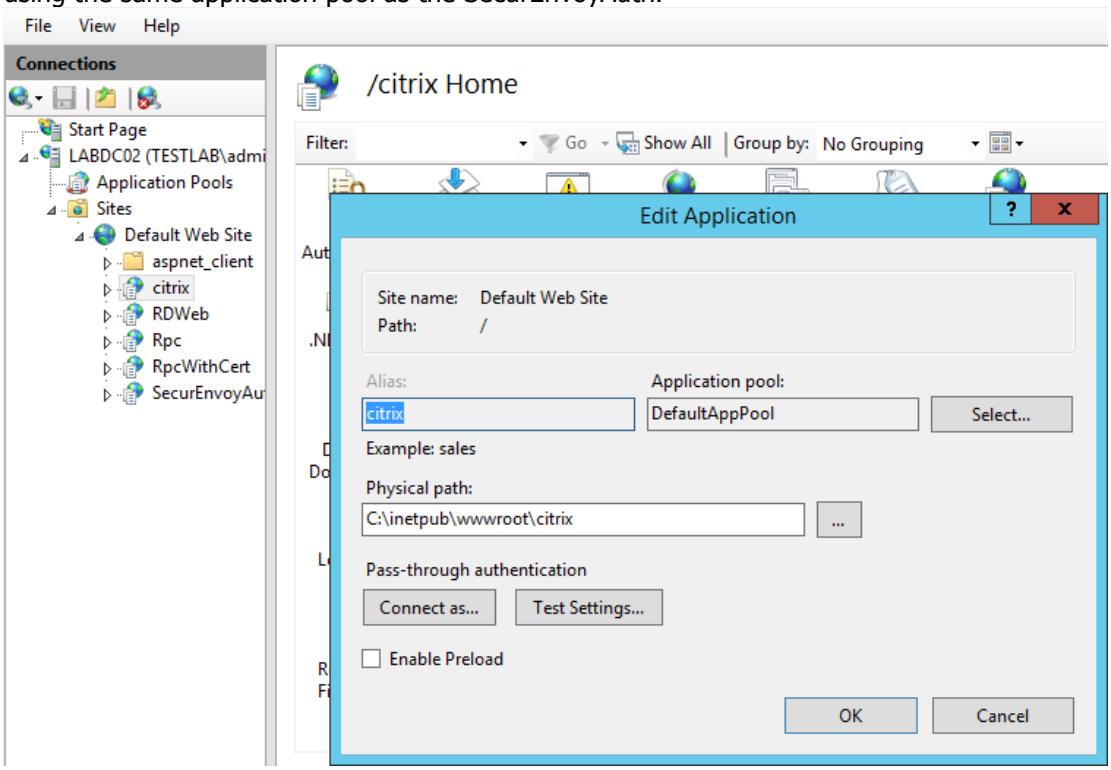
© 2016 SecurEnvoy All Rights Reserved

3.2 SecurEnvoy Microsoft Server Agent Application Pools

To allow successful use of the Microsoft Server Agent, the web site or virtual directory (application) that requires protecting uses the correct "Application pool".

For Windows 2008 & Windows 2012

Within Internet Information Services (IIS Manager) navigate to the Application pools, by default SecurEnvoy will be within the Default App pool. Make sure the virtual directory is using the same application pool as the SecurEnvoyAuth.



Note

SecurEnvoy auth pool must run under the same application pool as the application being protected

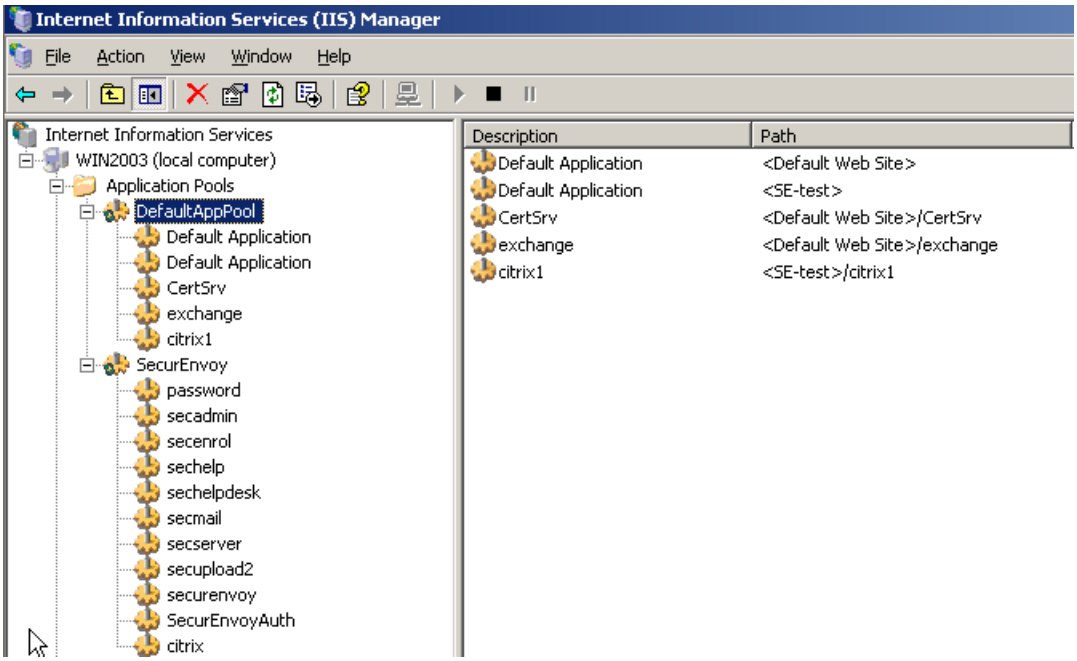
To view the virtual directory application pool, navigate to the required virtual directory and then select "Basic Settings" on the "Action pane" which is located on the right hand side of the IIS Manager window.

The Application pool identity will then be shown, if required the application pool can be changed.

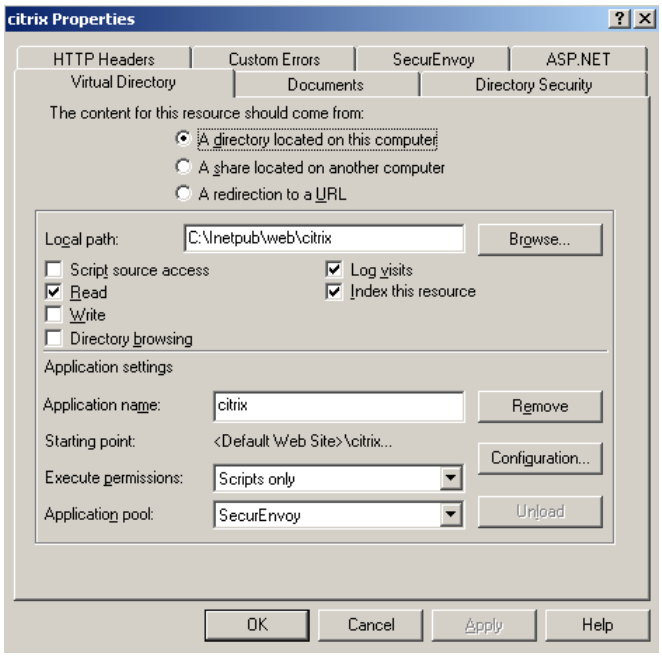
© 2016 SecurEnvoy All Rights Reserved

For Windows 2003

Within Internet Information Services (IIS Manager) navigate to the Application pools, by default SecurEnvoy will be within the Default App pool. Make sure the virtual directory is using the same application pool as the SecurEnvoyAuth.



Depending upon deployment the SecurEnvoyAuth may reside in a different application pool. See below: In this example the SecurEnvoyAuth resides within the SecurEnvoy Application pool.



To protect a virtual directory (application), this virtual directory must use the same application pool as SecurEnvoy.

Navigate to the virtual directory then select properties.

In the Application Pool drop down menu, select the pool SecurEnvoy.

Click OK when complete.

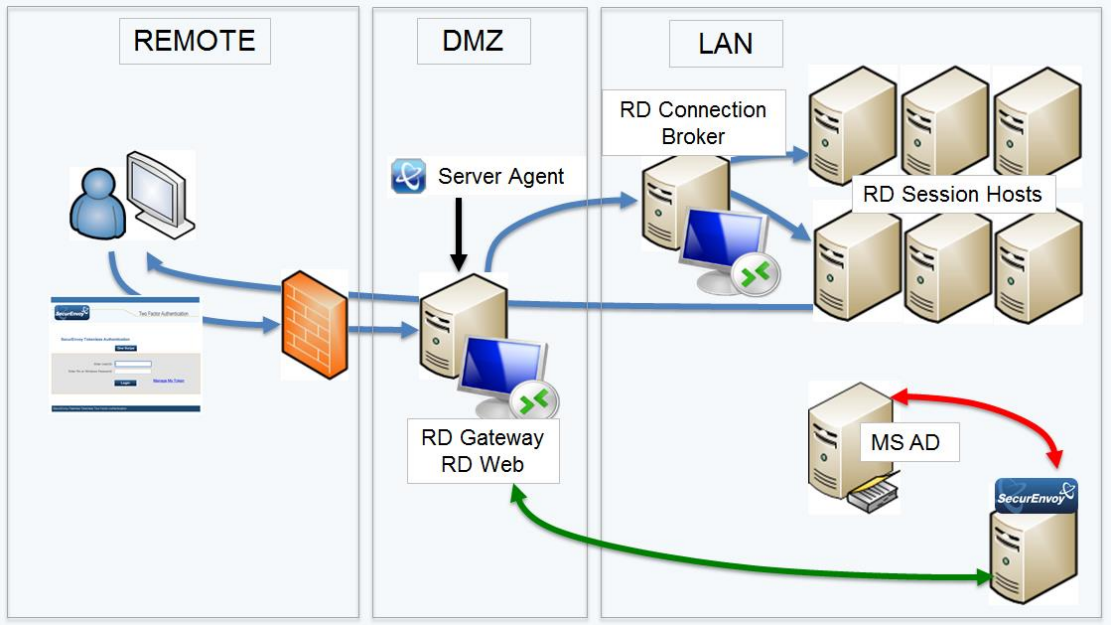
© 2016 SecurEnvoy All Rights Reserved

4.0 Windows 2012R2 with Remote Desktop Web Gateway Integration Guide

This section describes how to integrate a Windows 2012 R2 Remote Desktop Web (RDWeb) Gateway installed with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Microsoft Windows 2012 R2 Remote Desktop provides Web based Secure Application Access to the internal corporate network.

Connections to Remote Desktop must be made from a browser and not directly from a terminal server client.



Note

This document relates only to RDWeb access. If you want to authenticate Remote Desktop Client connections as well you will need to install Windows Login Agent on the Terminal Server hosts instead of this solution: see http://www.securenvoy.com/integrationguides/Windows%20Login%20Agent.pdf

© 2016 SecurEnvoy All Rights Reserved

4.1 Configure the Microsoft Server Agent

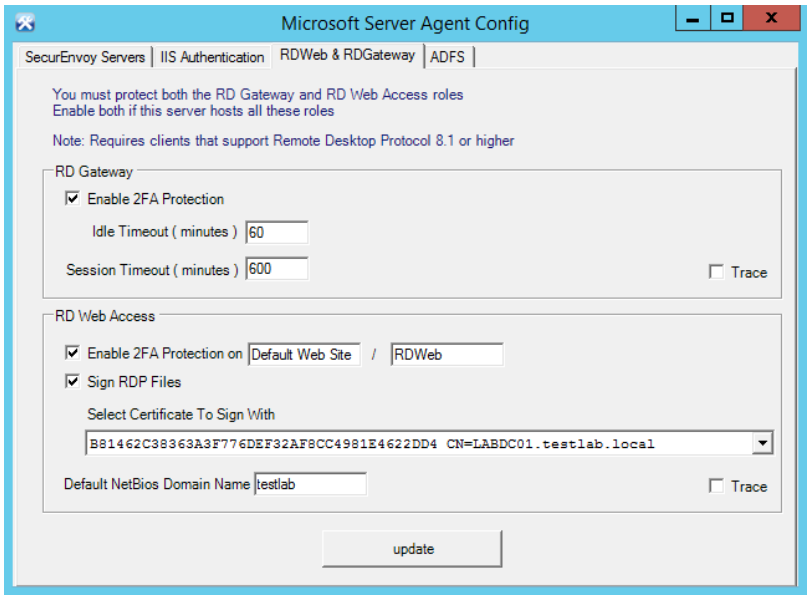
Select the RDWeb & RDGateway tab.

For RD Gateway protection from a direct connection, check the check box for 'Enable 2FA Protection'

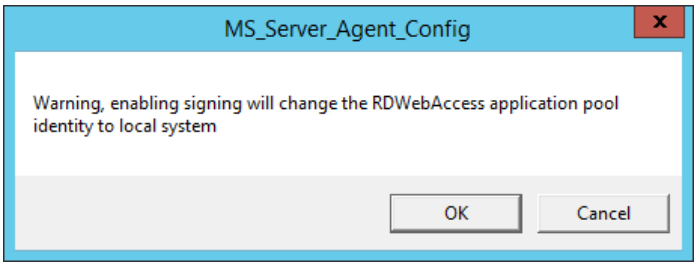
RD Web Access protection, check the check box for 'Enable 2FA Protection on Default Web Site / RDWeb.

To enable RDP file signing, check the check box for 'Sign RDP Files' and select the certificate assigned to your RD Gateway.

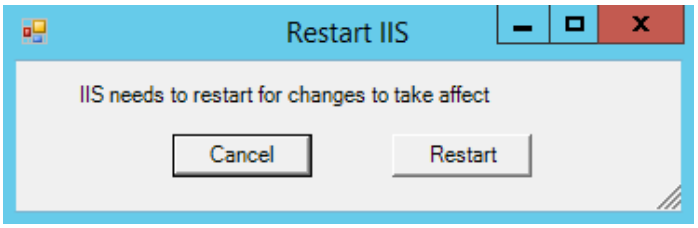
Enter your Default NetBios Domain Name



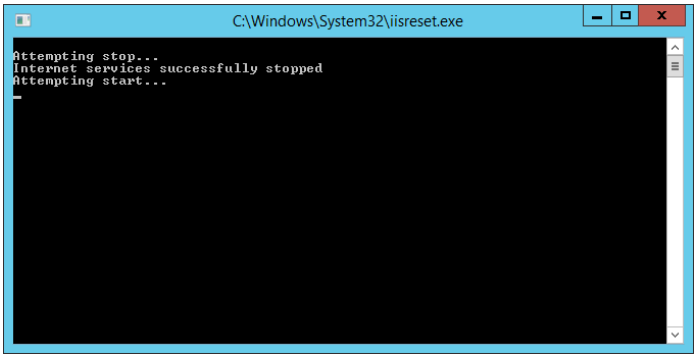
Once prompted for the "Warning, to enable signing will change the RDWebAccess application pool to local system", click 'OK'



A further warning that "IIS needs to restart for changes to take affect" Click 'Restart'



Wait for iisreset.exe to perform a stop and restart of the entire web server



© 2016 SecurEnvoy All Rights Reserved

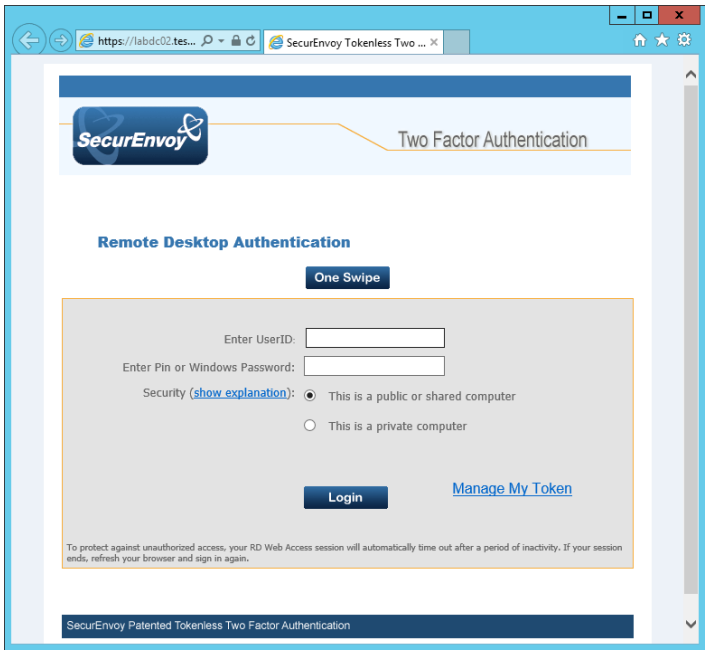
4.2 Test the Two Factor Authentication

Test the Two Factor Web authentication by opening a browser and going to the URL for the Web server i.e.

https://your_server_name/rdweb (Don't forget the https)

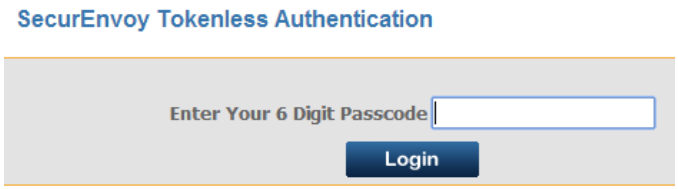
User logon screen is shown.

Enter your UsedID and Password:

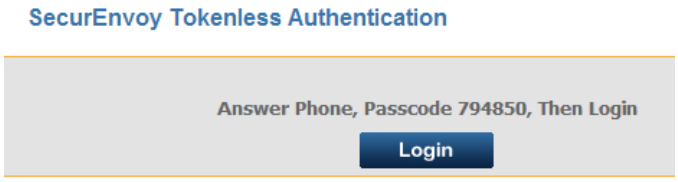


User is then presented with their two factor authentication type:

- Pre load, Realtime and Soft tokens:



- VOICE tokens:

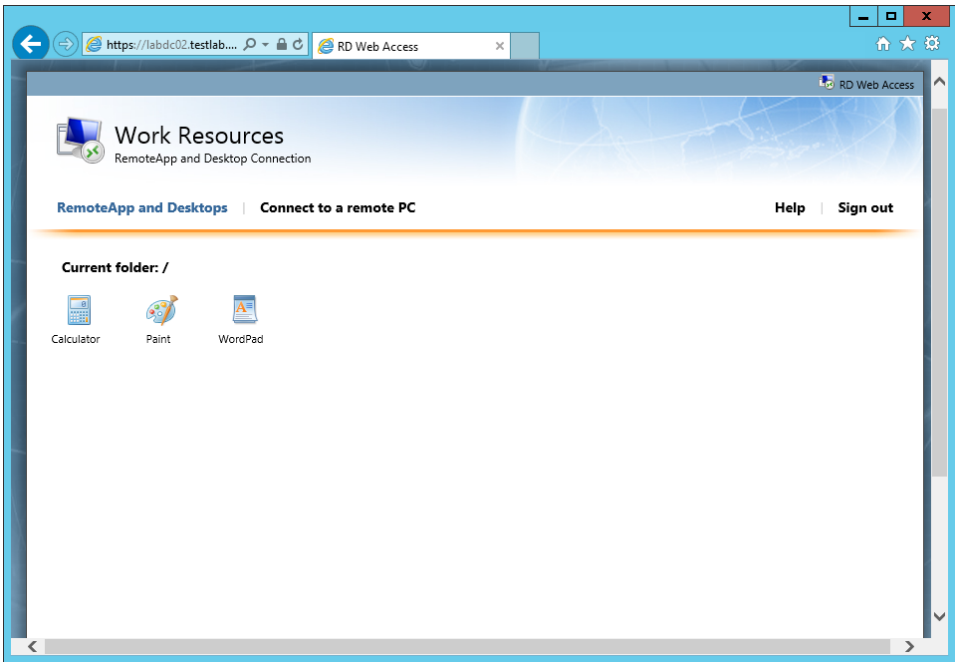


- One Swipe:

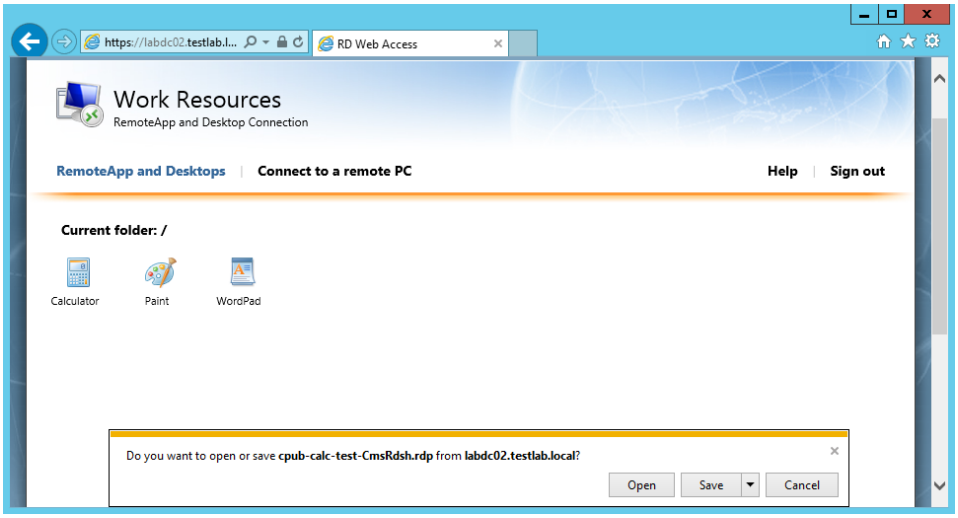


© 2016 SecurEnvoy All Rights Reserved

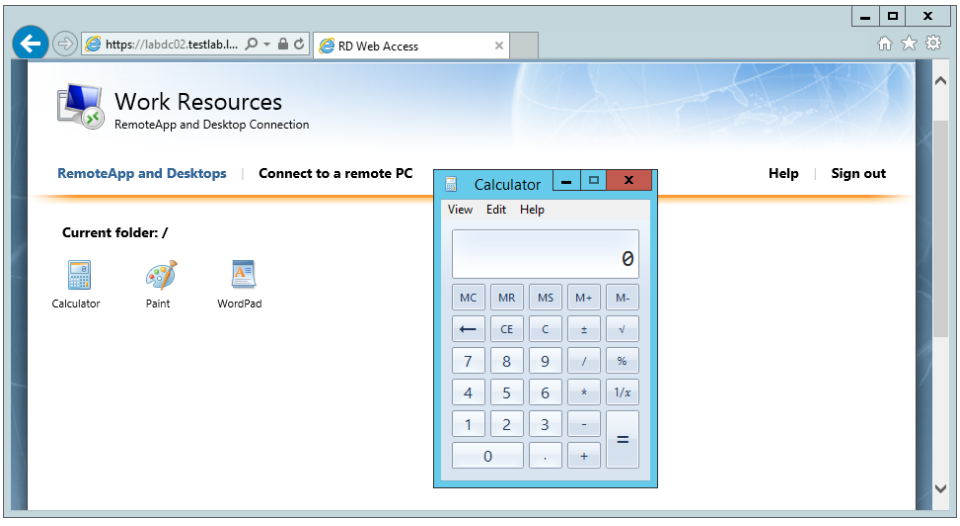
User authenticates successfully and is presented with RDWeb 2012 R2:



User launches application from RDWeb page and selects 'Open' from browser



User is presented with their application



© 2016 SecurEnvoy All Rights Reserved

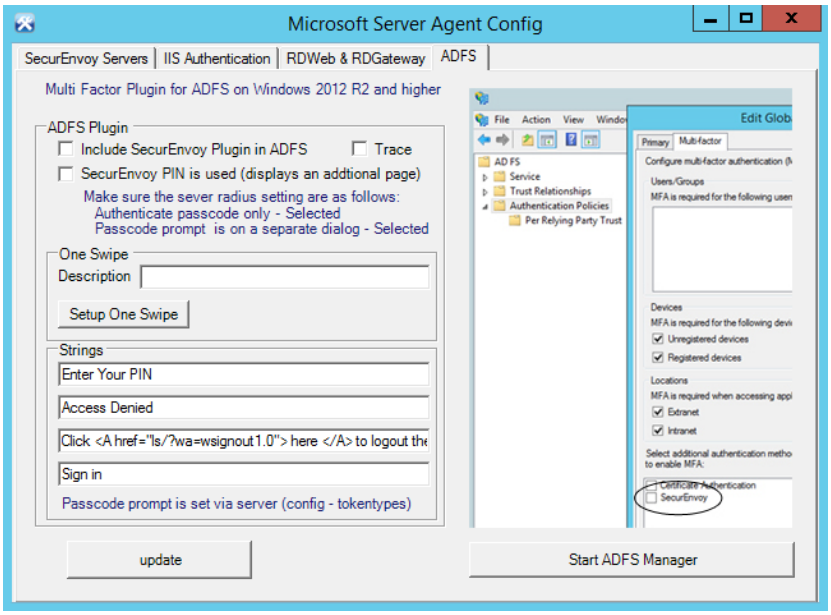
5.0 ADFS v3

Select the ADFS tab.

Place a check in the checkbox for 'Include SecurEnvoy Plugin in ADFS'.

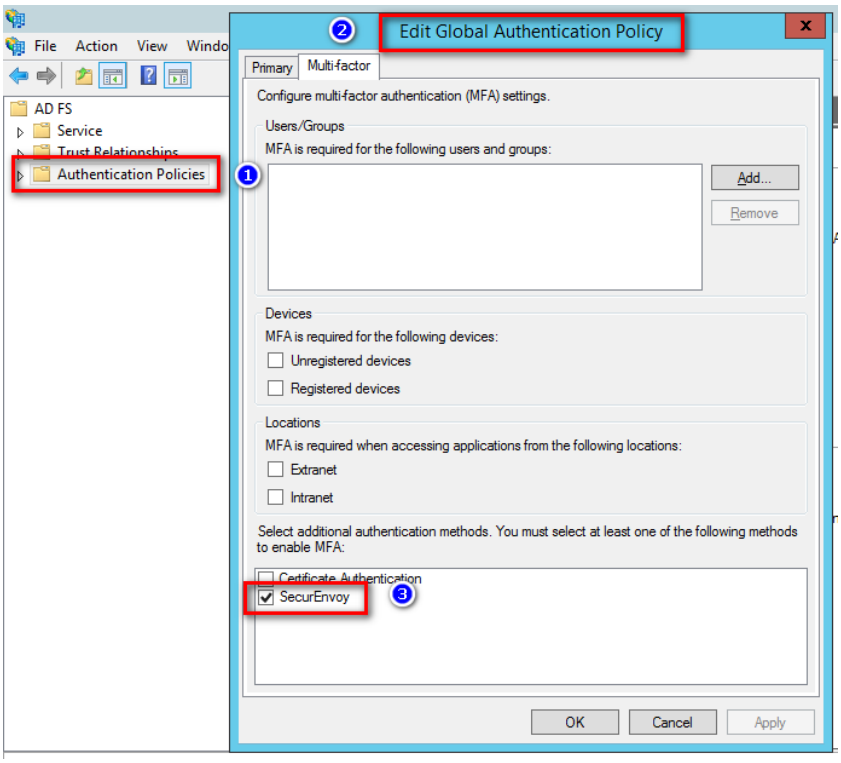
Place a check in the checkbox for 'SecurEnvoy PIN is used', if you wish to use SecurEnvoy's built in PIN management.

Click 'Update' to apply settings then click 'Start ADFS Manager'.



Once ADFS Manager has launched, select 'Authentication Policies' then click 'Edit Global Authentication Policy'.

Within additional authentication methods, place a check in the checkbox for 'SecurEnvoy' and click 'OK'.



© 2016 SecurEnvoy All Rights Reserved

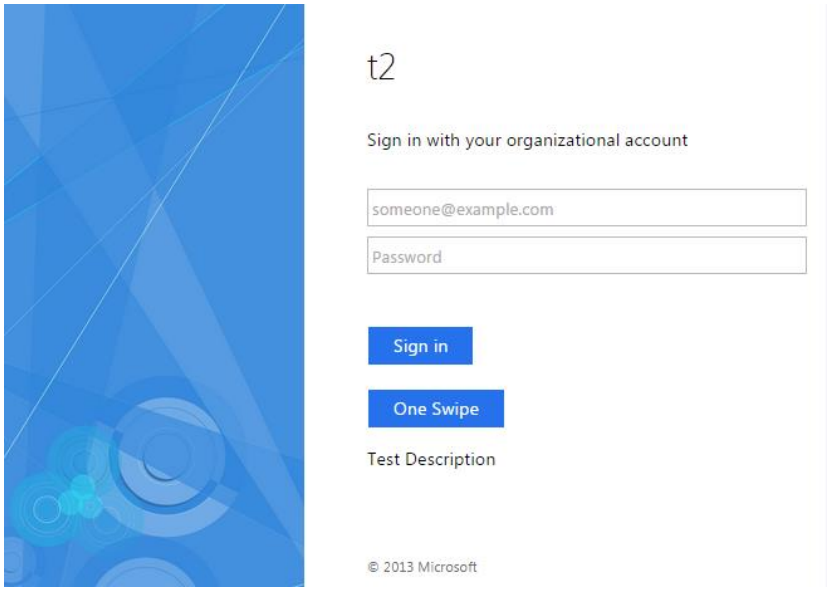
5.1 Test Two Factor Authentication

Test the Two Factor Web authentication by opening a browser and going to the URL for the Web server i.e.

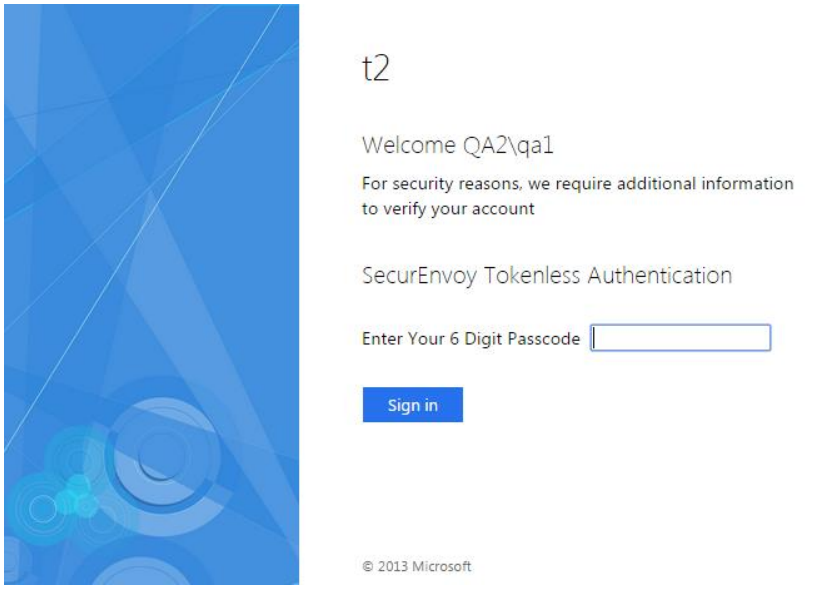
https://your_server_name/rdweb (Don't forget the https)

User logon screen is shown.

Enter your UsedID and Password:



User is then presented with their two factor authentication type:



© 2016 SecurEnvoy All Rights Reserved

6.0 Notes

© 2016 SecurEnvoy All Rights Reserved