SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

SecurEnvoy Microsoft Server Agent

Installation and Admin Guide v9.3

SecurEnvoy Microsoft Server Agent Guide

Contents

1.1 Prerequisites

Overview of Installation Files

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.

This agent is only required if you are installing SecurAccess and you need to directly authenticate an application running on an IIS Web Server, Microsoft Remote Desktop Services and SAML claims aware applications configured for SSO with Microsoft ADFS.

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

IIS Pre-Requisites

Supported IIS Versions: -

- 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
- IIS V10 running on Windows 2016

Other Pre-Requisites

It is highly recommended that any protected web server should have SSL (https) enabled.

Microsoft .NET 4.5 is installed.

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

There must be a network connection via RADIUS (UDP Port 1812 - default) between the server with Microsoft Server Agent installed and the SecurEnvoy security server(s).

Note

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

1.2 SecurEnvoy Microsoft Server Agent Install & Configuration for Windows 2008 R2, 2012 R2 and 2016

It is assumed that either Internet Information Services (IIS) and/or Remote Desktop Services (RDS) and/or Active Directory Federation Services (ADFS) are installed as server roles and are 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.

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	✓
Online Push	✓

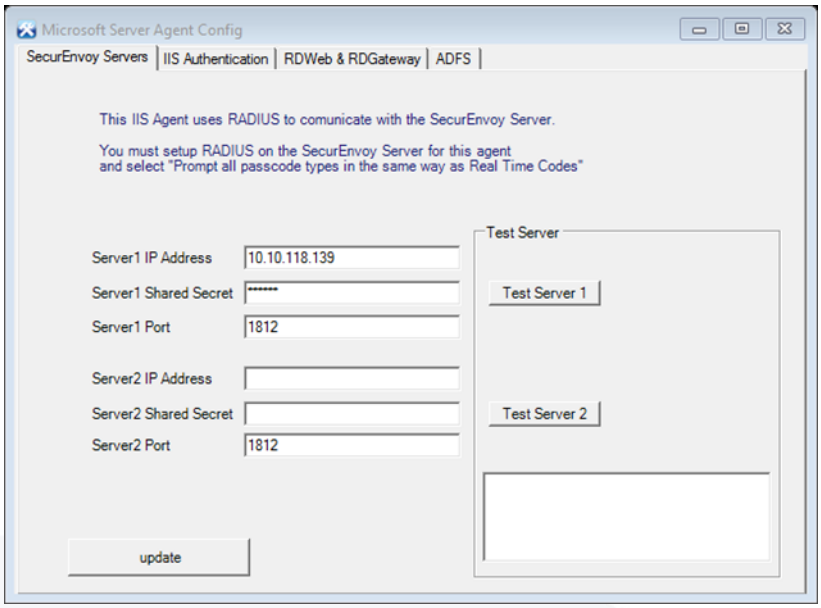
To install the Microsoft Server Agent run "Microsoft Server Agent\setup.exe"
Once installed, the following page is displayed for user input.

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:

Response Code	Meaning
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.

Upgrading SecurEnvoy Microsoft Server Agent

Note

There is no direct upgrade path from the legacy Microsoft IIS Agent. Therefore, if you are running the earlier Microsoft IIS Agent, it is strongly recommended that you uninstall it and then install this agent as it has enhanced security. You can upgrade directly from earlier versions of the Microsoft Server Agent

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 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 from a previous version, 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, please backup files before uninstalling IIS Agent and then install the Microsoft Server Agent.

Note

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

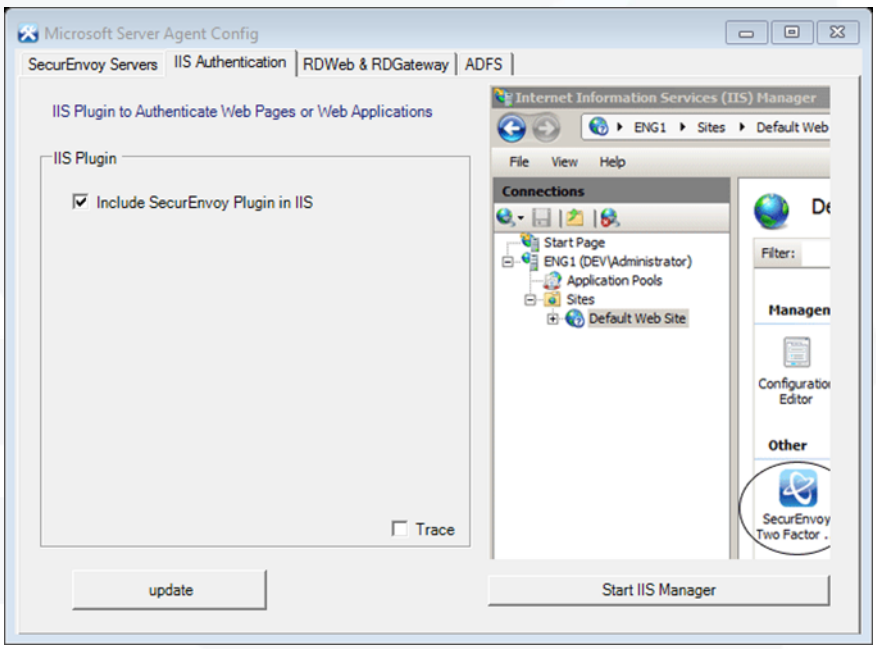
1.3 Internet Information Services Integration Guide

Select the 'IIS Authentication' tab

Tick the "Include SecurEnvoy Plugin in IIS" check box and click on Update.

This will prompt for an IIS reset, please do so.

Once IIS has restarted and click 'Start IIS Manager'



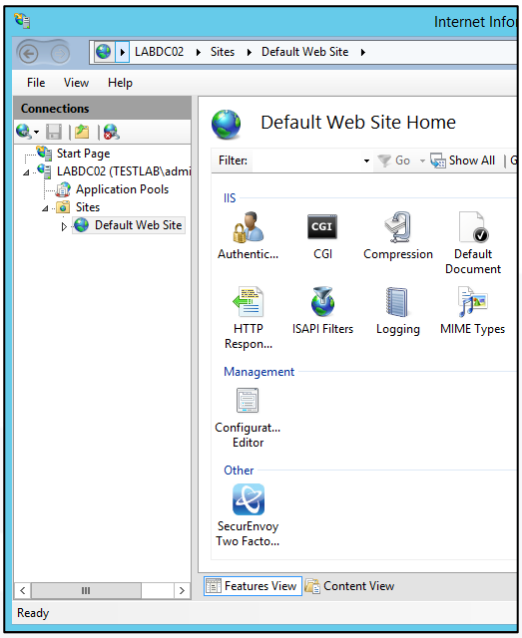
Administration is performed for Windows 2008R2 / Windows 2012R2 / Windows 2016 via Information Services (IIS) Manager (inetmgr).

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

For Windows 2008, Windows 2012 and Windows 2016 deployments

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

Select sites and then navigate to the Default Web Site(s).



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

To enable two factor authentications 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.

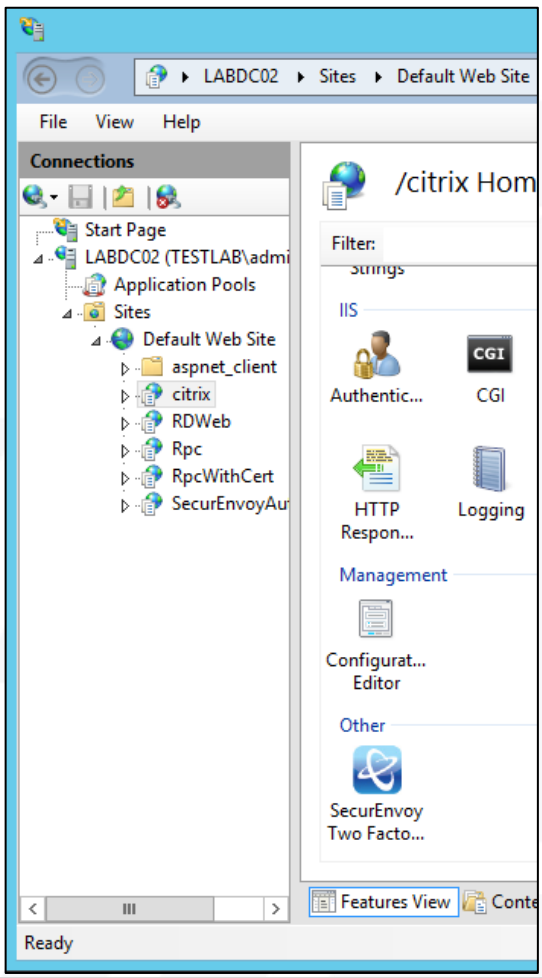
To protect a certain virtual directory, carry out the following: -

For Windows 2008 R2, Windows 2012 R2 and Windows 2016 deployments

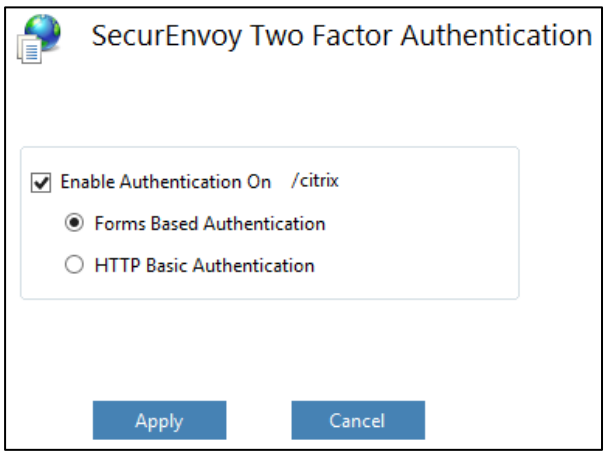
Select Start\Administrative tools\Internet Information Services (IIS) Manager

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 2008 R2, Windows 2012 R2 and Windows 2016 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.

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)"

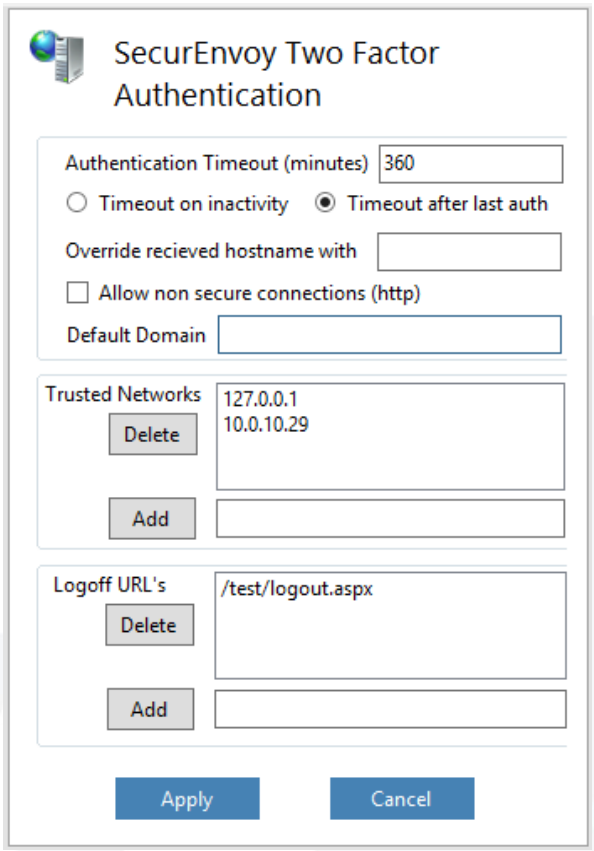
Authentication timeout is the number of minutes from the last successful authentication until the user is prompted for re-authentication. It is recommended that this is set long enough to allow a typical user to complete their session.

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

For Windows 2008 R2, Windows 2012 R2 and Windows 2016 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.

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

Note

Trusted Networks format needs to be one of the following:

Exact IP Address, for example 192.168.1.1

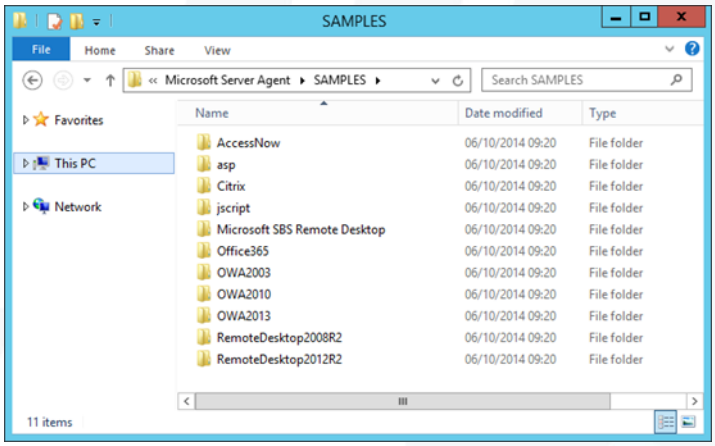
*Wildcard, for example 192.168.1.**

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.

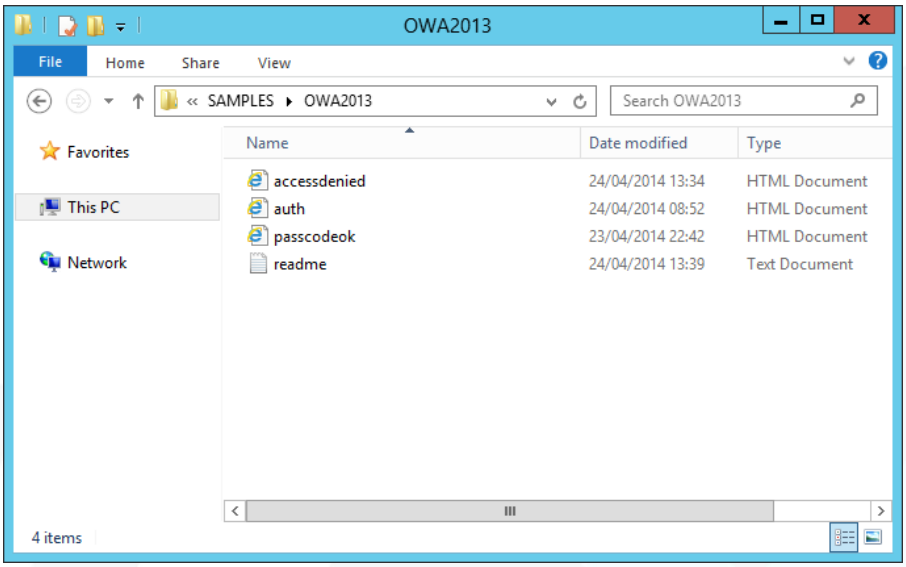
You should use the same Form Action login page defined in your form element. Define hidden input entry fields that match your application logon requirements, substituting $USERID$ and $PASSWORD$ for username and password values.

Example

To configure a Two Factor authentication for Exchange Web mail upon Microsoft Exchange server. Install Microsoft Server Agent upon the Exchange 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\OWA20** as required.



Copy the passcodeok.htm, auth.htm and accessdenied.htm files to:

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

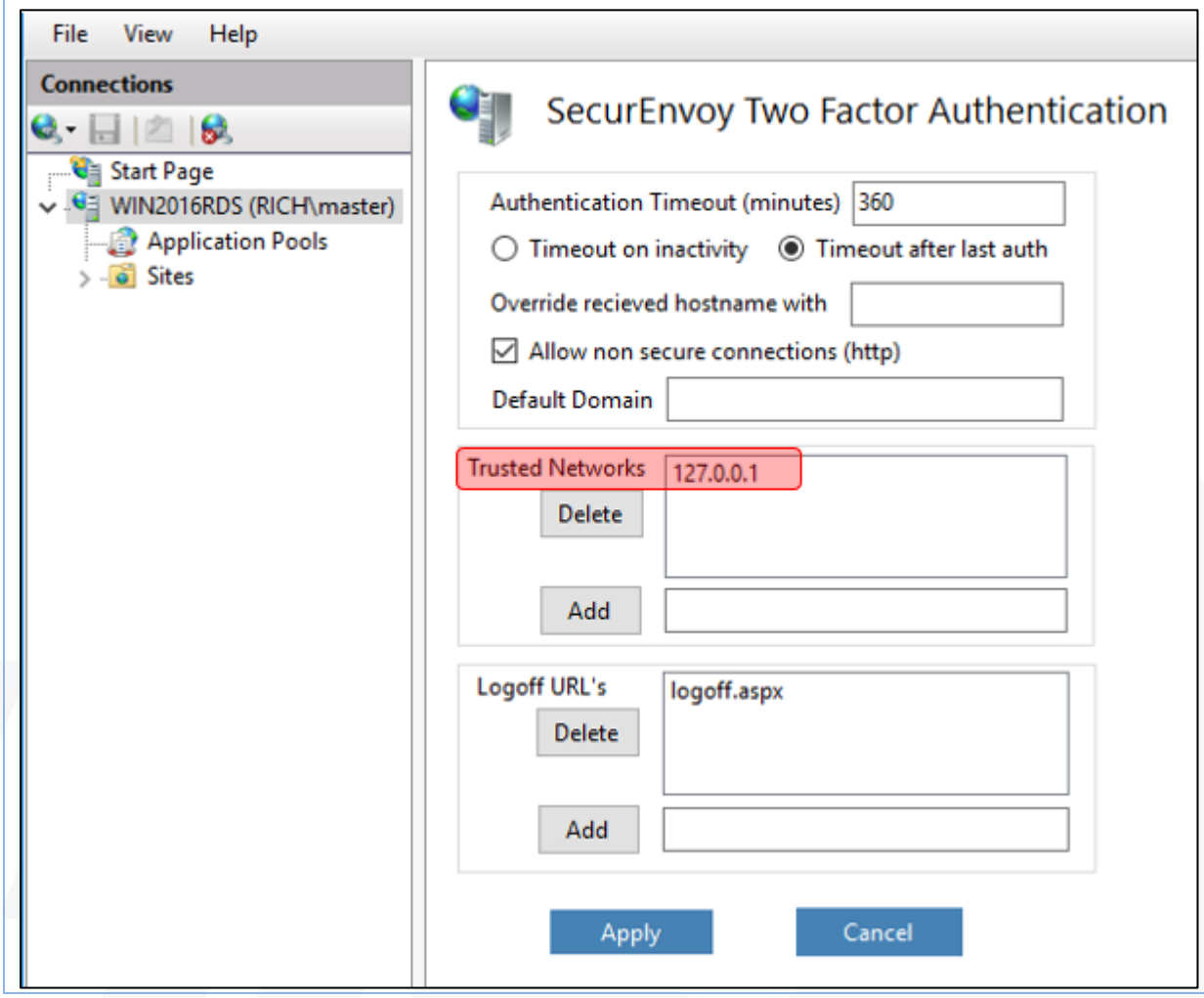
Overwrite the original files.

Note

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

Note

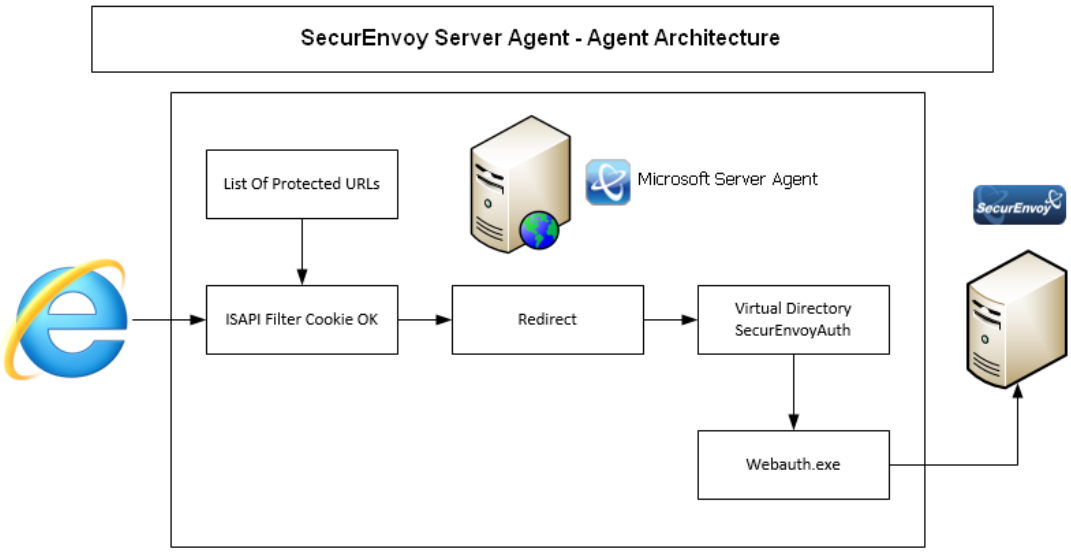
OWA (Outlook Web Access) and ECP (Exchange Control Panel) use the same URL. As such, if you protect OWA with 2FA then access to ECP is also protected with 2FA. If you do not want to protect access to ECP then you can add 127.0.0.1 as a trusted network in the SecurEnvoy Microsoft Server Agent add-in in IIS.



Carry out a test authentication by going to https://servername/owa

Enter UserID, windows password and passcode

IIS Agent Architecture



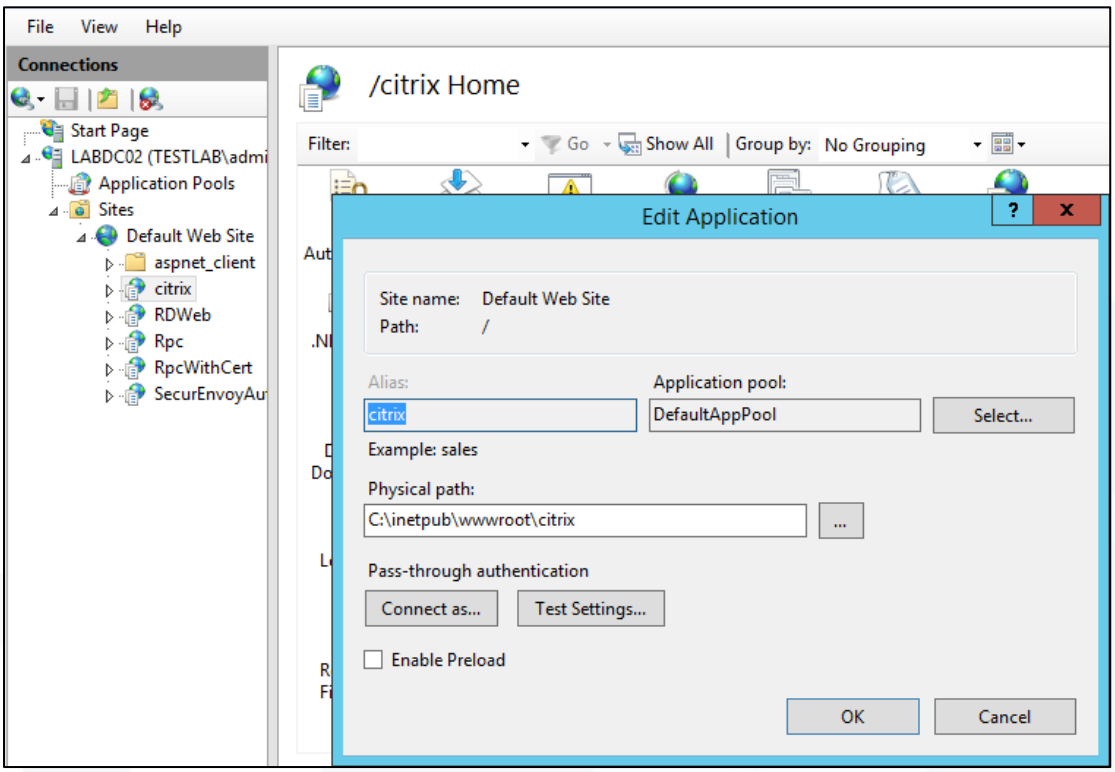
All web URL requests are monitored by the ISAPI filter program webauthfilter. If a protected resource is requested, the filter checks to see if a valid un-tampered cookie is available and that it hasn't timed out. If the cookie is OK then the request is passed on. If the cookie is unavailable or has 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.

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 R2, Windows 2012 R2 and Windows 2016

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

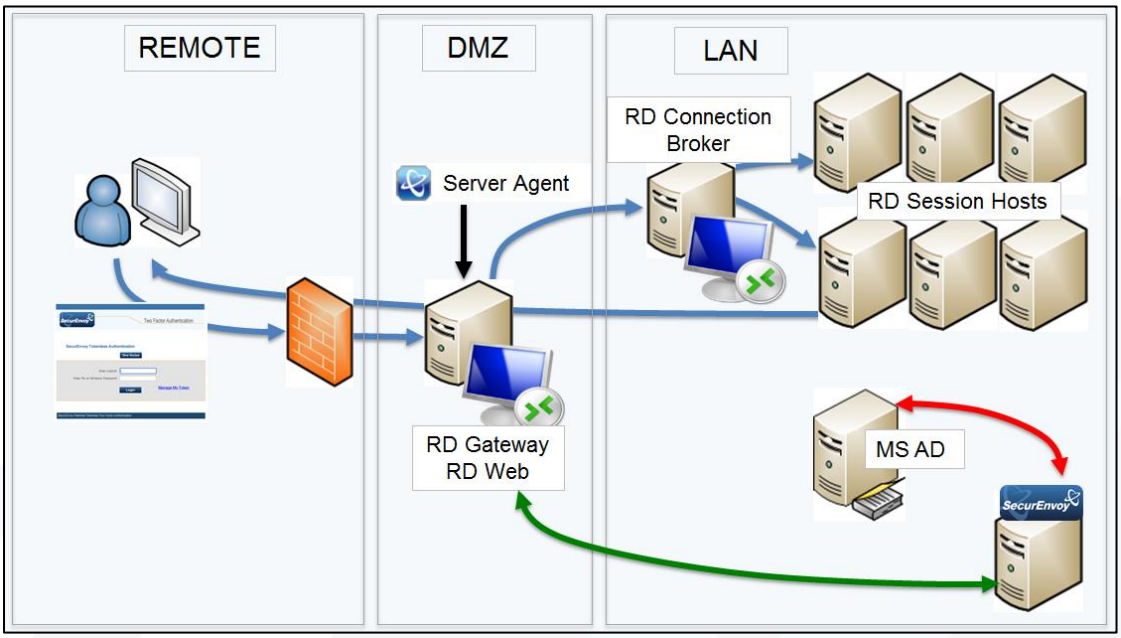
To view the virtual directory application pool, navigate to the required virtual directory and then select "Basic Settings" on the "Action pane" which is located on the right-hand side of the IIS Manager window. The Application pool identity will then be shown, if required the application pool can be changed.

1.4 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

Configure the Microsoft Server Agent for RD Gateway & RD Web Access

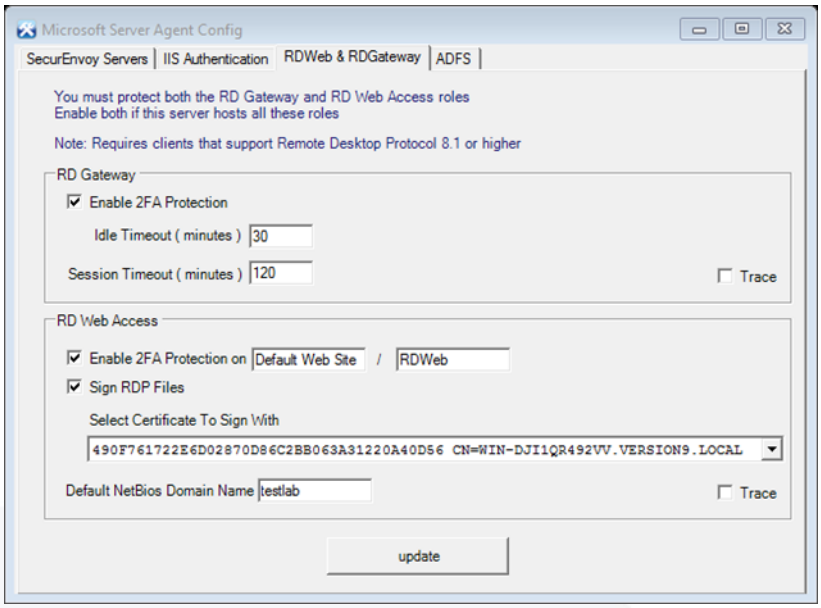
Select the RDWeb & RDGateway tab.

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

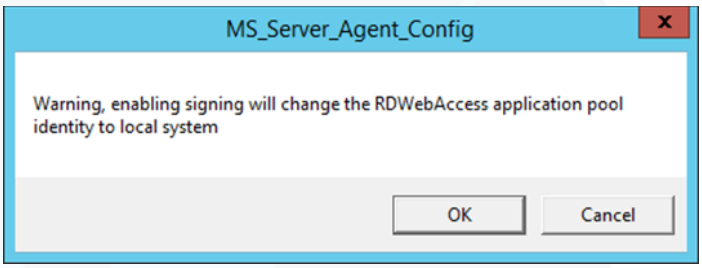
RD Web Access protection, check the check box for 'Enable 2FA Protection on Default Web Site / RDWeb.

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

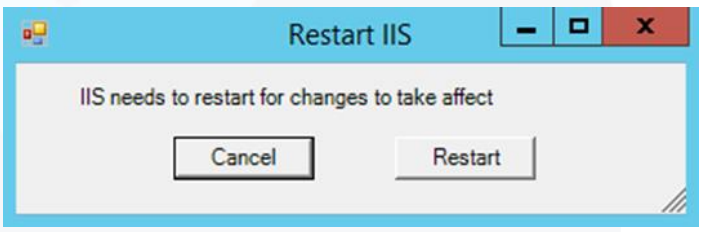


Once prompted for the "Warning, to enable signing will change the RDWebAccess application pool to local system", click 'OK'



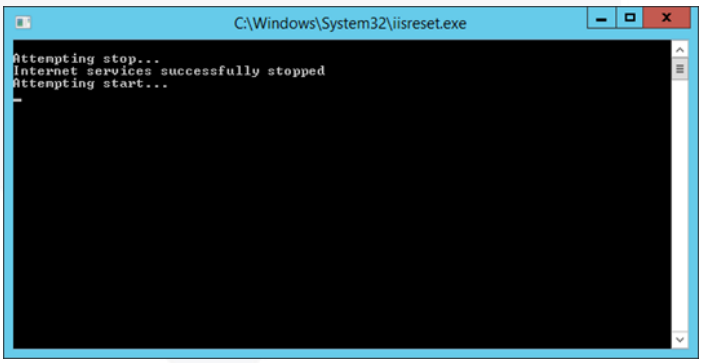
A further warning that "IIS needs to restart for changes to take affect"

Click 'Restart'



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

Click 'Restart



Configure Single Sign On (SSO) for RD Gateway & RD Web Access

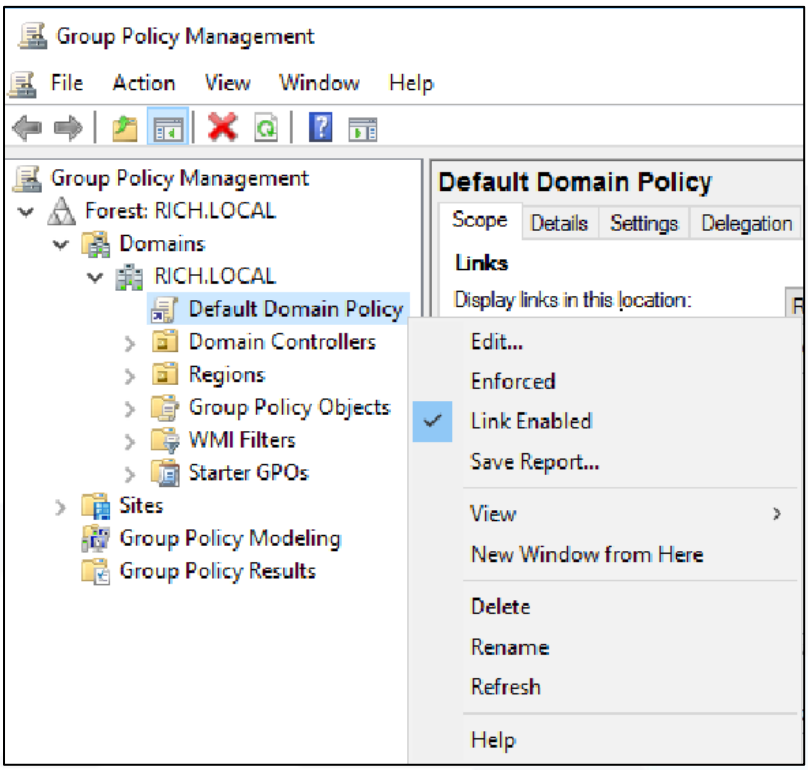
Always take note – our server and domain names are from our internal lab. Yours will be different.

Configuring Group Policy

Log into your Active Directory Domain Controller.

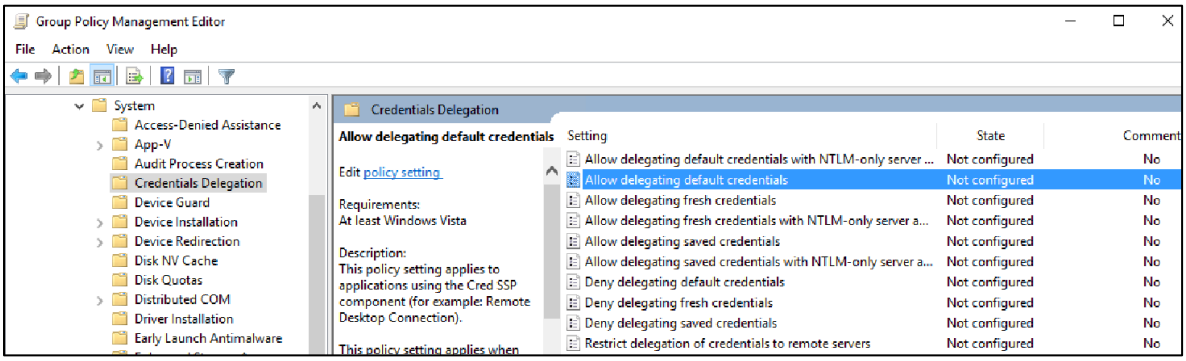
Open Group Policy Management Console (gpmc.msc).

Locate the relevant Group Policy object for your client computers, in this example "Default Domain Policy". Right click it and select edit.

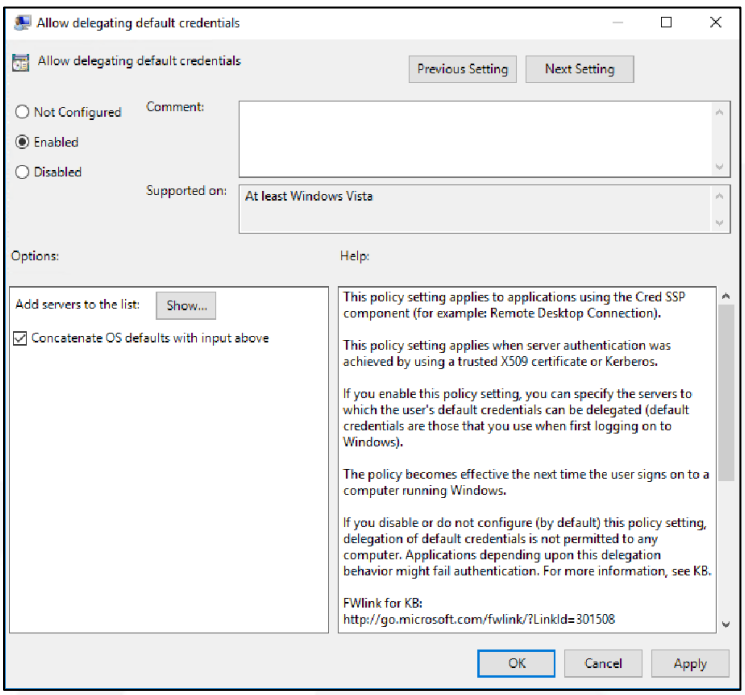


Navigate to Computer Configuration → Policies → Administrative Templates → System → Credentials Delegation.

Right click and edit “Allow delegating default credentials”



Select “Enabled” and click on the “Add servers to the list: Show…” button



Enter the name of the server hosting the Remote Desktop Session Host in the below format.

TERMSRV/host.humanresources.fabrikam.com Remote Desktop Session Host running on host.humanresources.fabrikam.com machine. RECOMMENDED

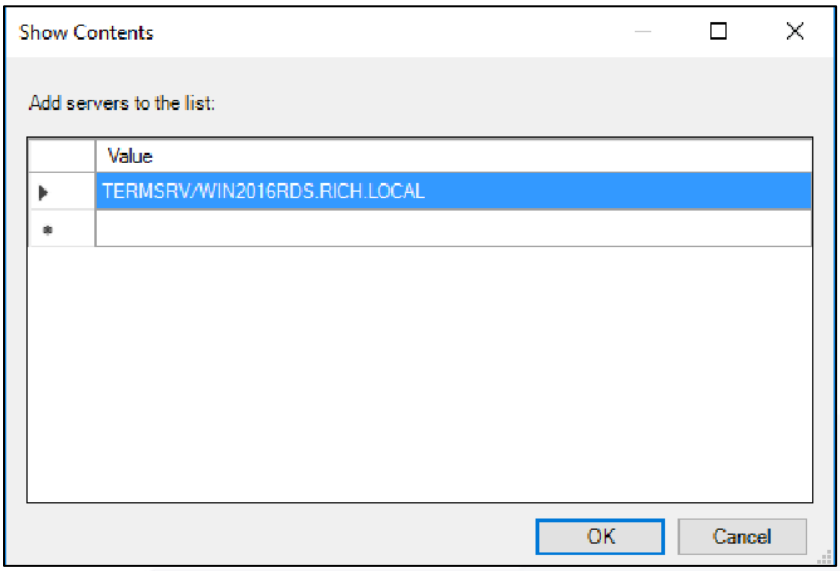
TERMSRV/* Remote Desktop Session Host running on all machines.

TERMSRV/*.humanresources.fabrikam.com Remote Desktop Session Host running on all machines in .humanresources.fabrikam.com

Note: The "Allow delegating default credentials" policy setting can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard character is permitted when specifying the SPN.

For Example:

TERMSRV/WIN2016RDS.RICH.LOCAL



Repeat for all Session host servers in your RDS farm and click on OK.

At the “Allow delegating default credentials” click on “Apply” and “OK”. Close GPMC.

Applying Group Policy

To force the GPO to apply, log into the client machine, open an elevated command prompt and run the gpupdate /force command, as below. However, the GPO will apply dynamically after a pre-defined time.

```
C:\>gpupdate /force
```

Test RD Web Access Two Factor Authentication

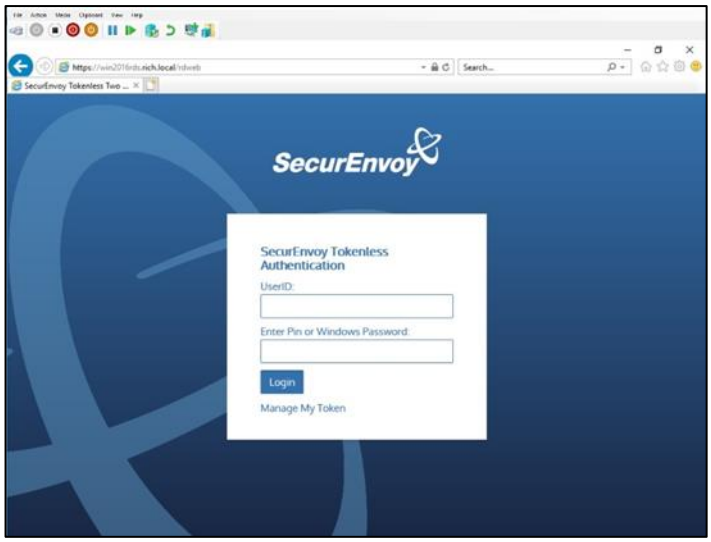
Test the Two Factor Web authentication by opening a browser and going to the URL for the Web server i.e.

https://your_server_name/rdweb

(Don't forget the https)

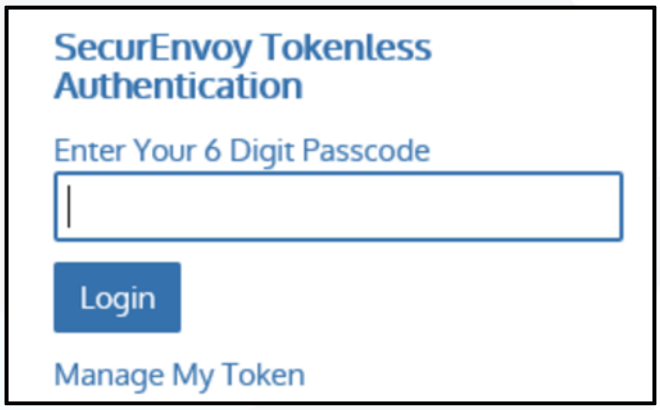
User logon screen is shown.

Enter your UsedID and Password:

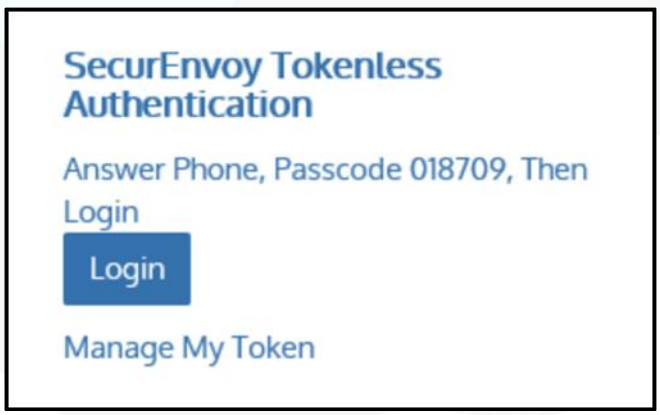


User is then presented with their two-factor authentication type:

- Preload, Realtime and Soft tokens:

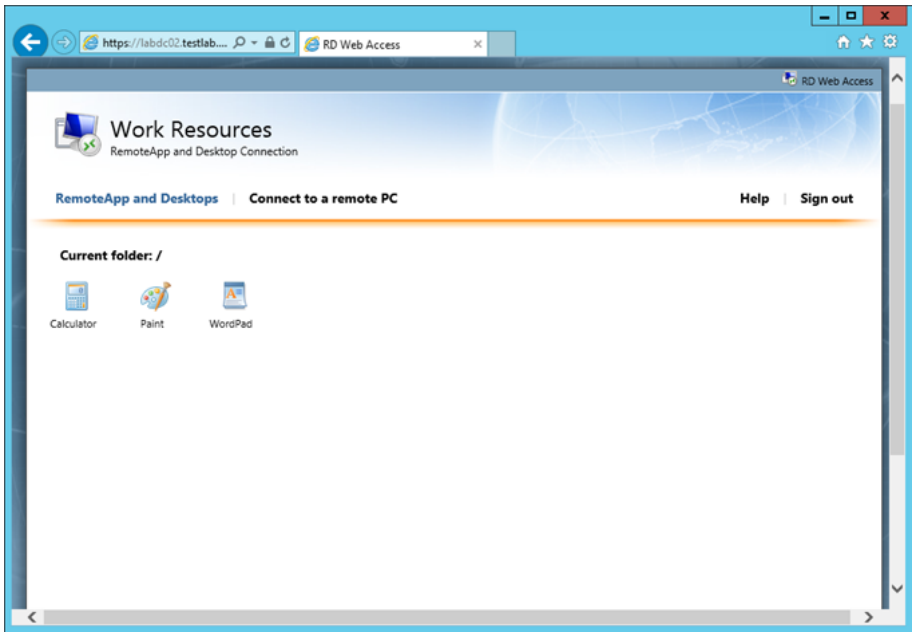


- VOICE tokens:

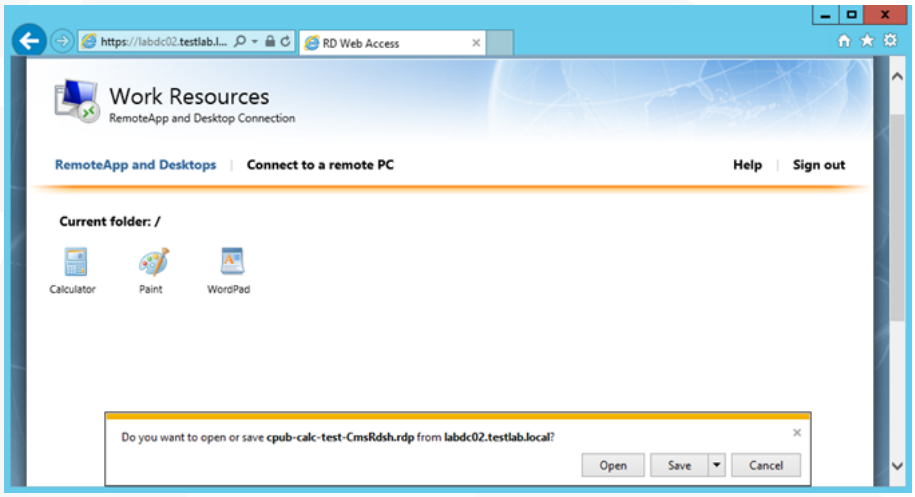


- Soft token Push:

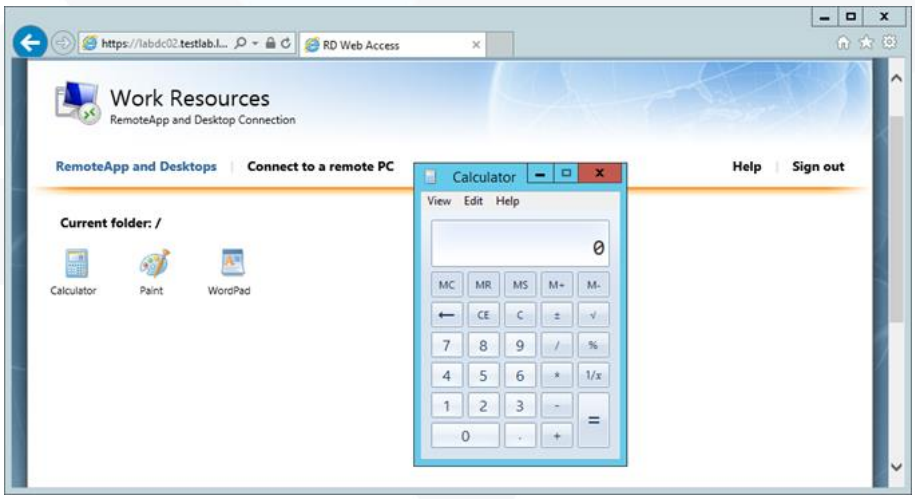
User authenticates successfully and is presented with RDWeb 2012 R2:



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



User is presented with their application



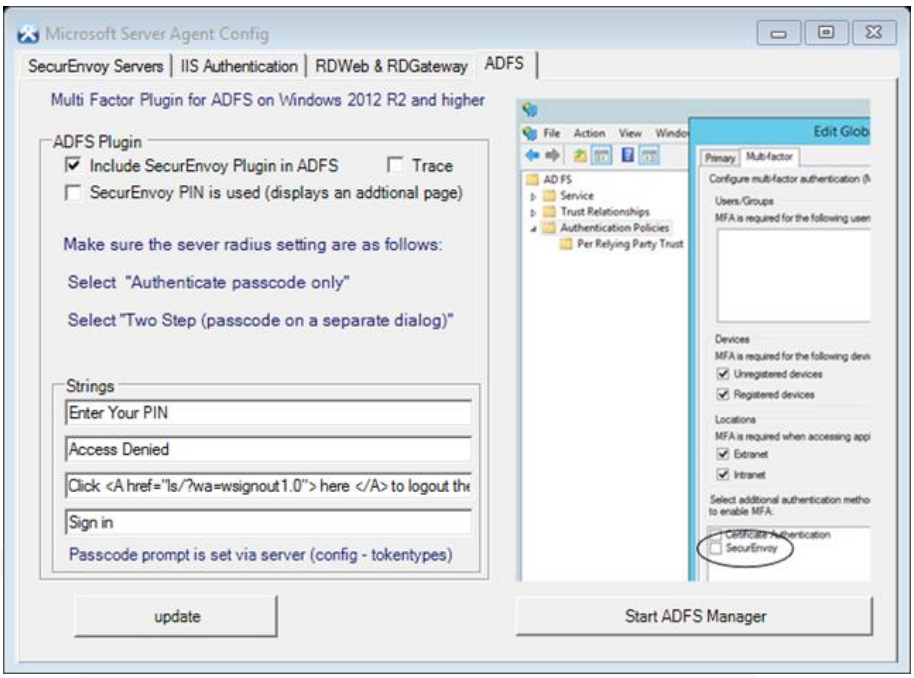
1.5 ADFS v3 or v4 Integration Guide

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.

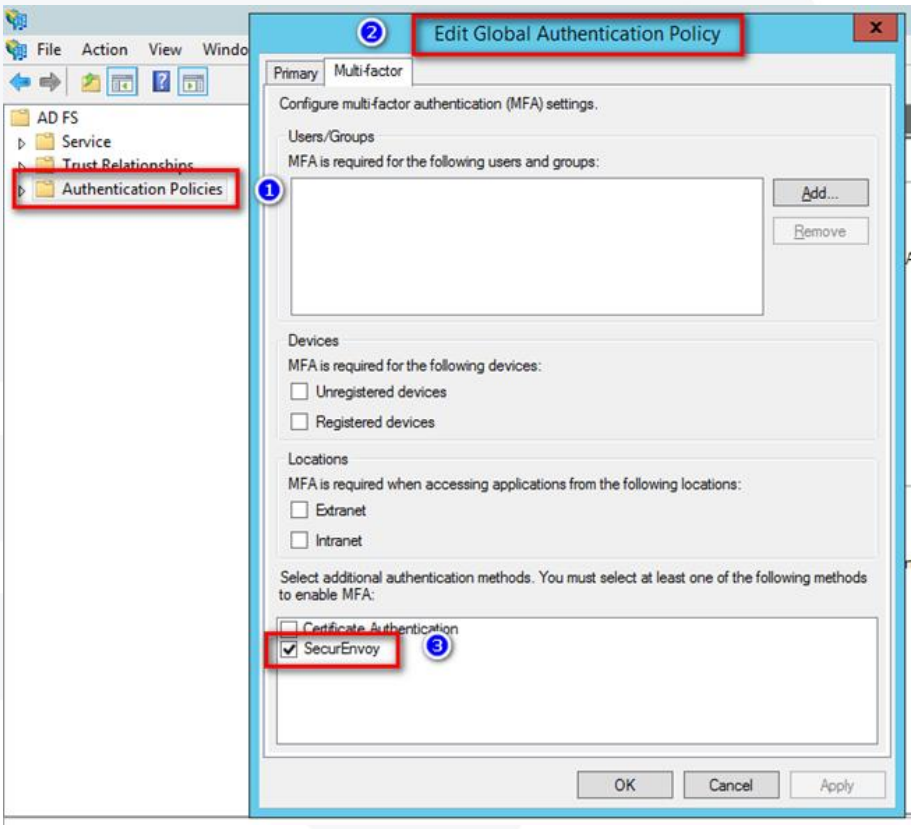
Click 'Update' to apply settings then click 'Start ADFS Manager'.



ADFS V3 (2012R2 Server)

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

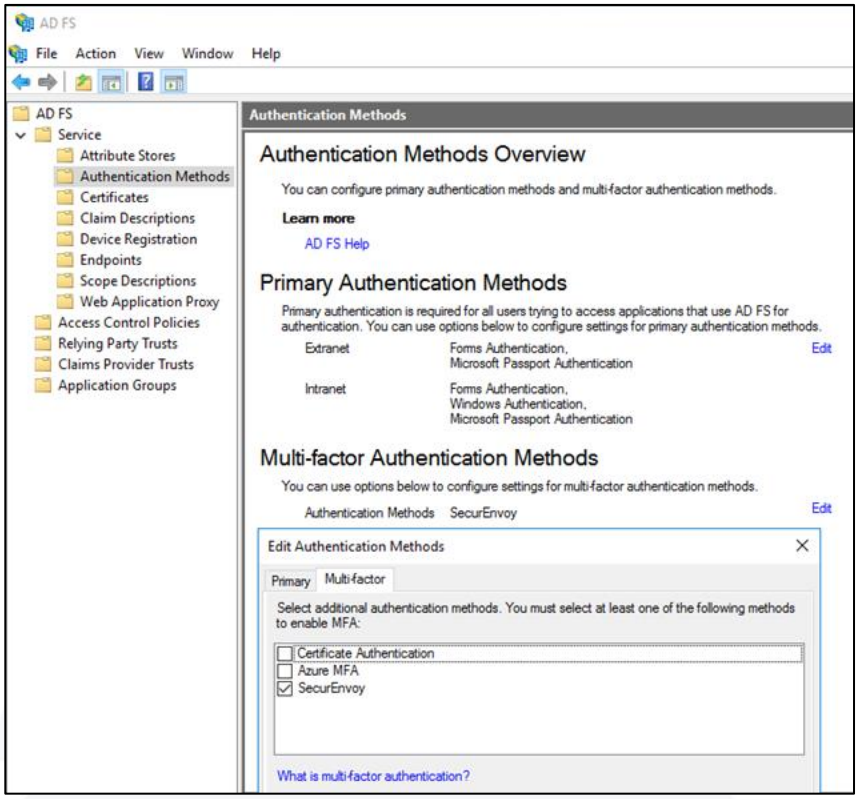
Within additional authentication methods, place a check in the checkbox for 'SecurEnvoy' and click 'OK'.



ADFS V4 (2016 Server)

Once ADFS Manager has launched, select 'Authentication Methods' then click Edit in the Multi-factor Authentication Methods section.

Within Edit Authentications Methods, place a check in the checkbox for 'SecurEnvoy' and click 'OK'.



Test ADFS Two Factor Authentication

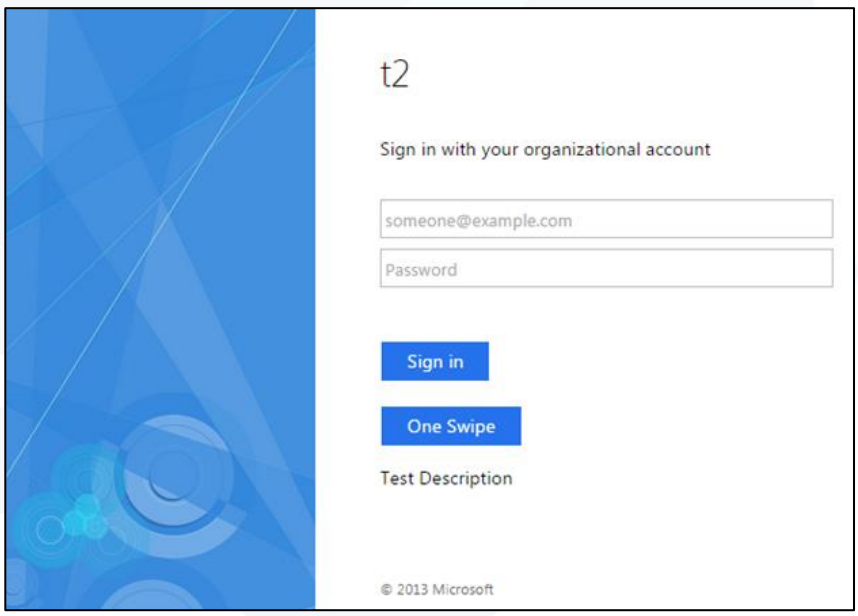
Test the Two Factor Web authentication by opening a browser and going to the URL for the Web server i.e.

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:

Note

If any RADIUS settings in the Agent are changed, including the shared secret, then the Active Directory Federation Service will require a restart in order to apply them.

Please Reach Out to Your Local SecurEnvoy Team...

UK & IRELAND

The Square, Basing View
Basingstoke, Hampshire
RG21 4EB, UK

Sales

E sales@SecurEnvoy.com
T 44 (0) 845 2600011

Technical Support

E support@SecurEnvoy.com
T 44 (0) 845 2600012

EUROPE

Freibadstraße 30,
81543 München,
Germany

General Information

E info@SecurEnvoy.com
T +49 89 70074522

ASIA-PAC

Level 40 100 Miller Street
North Sydney
NSW 2060

Sales

E info@SecurEnvoy.com
T +612 9911 7778

USA - West Coast

Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA - Mid West

3333 Warrenville Rd
Suite #200
Lisle, IL 60532

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA – East Coast

373 Park Ave South
New York,
NY 10016

General Information

E info@SecurEnvoy.com
T (866)777-6211

SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com