



# External Authentication with Windows 2016 Server with Remote Desktop Web Gateway with Single Sign On

**Authenticating Users Using SecurAccess  
Server by SecurEnvoy**

# Remote Desktop Web Gateway 2016

## Contents

1.1	SOLUTION SUMMARY .....	3
1.2	GUIDE USAGE .....	3
1.3	PRE-REQUISITES.....	3
1.4	SUPPORTED TOKEN TYPES .....	4
1.5	CONFIGURE THE MICROSOFT SERVER AGENT.....	5
1.6	CONFIGURE A RADIUS CLIENT IN SECURENVOY SECURACCESS SERVER FOR MS RDS. ....	6
1.7	CONFIGURE THE MICROSOFT SERVER AGENT FOR THE DEFAULT WEBSITE (OPTIONAL) .	7
1.8	CONFIGURE THE MICROSOFT SERVER AGENT FOR RDWEB (OPTIONAL) .....	8
1.9	CONFIGURE LOGOUT URL (OPTIONAL).....	9
1.10	CONFIGURE RDWEB ACCESS TEMPLATE (OPTIONAL) .....	9
1.11	SINGLE SIGN ON (SSO) - CONFIGURING GROUP POLICY .....	10
1.12	SSO - APPLYING GROUP POLICY .....	12
1.13	TEST THE TWO FACTOR AUTHENTICATION .....	13

## 1.1 Solution Summary

SecurEnvoy's SecurAccess MFA solution offers Two Factor Authentication for remote access solutions, such as Microsoft Remote Desktop Services 2016.

The software used for the integration process is listed below:

### Remote Desktop Services

Microsoft Windows Server 2016

Microsoft Internet Information Services v10

### SecurEnvoy

SecurEnvoy SecurAccess Release v9.3.502

SecurEnvoy Microsoft Server Agent Release v9.3.502

## 1.2 Guide Usage

The information in this guide describes the configuration required for integration with SecurEnvoy and common to most deployments. It is important to note two things:

- Every organization is different and may require additional or different configuration.
- Some configuration may have other methods to accomplish the same task than those described

## 1.3 Pre-requisites

The following conditions are required to set up SecurEnvoy's MFA Solution:

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/en-gb/support>

## 1.4 Supported Token Types

Token Type	Supported
Soft Token App	✓
Soft Token App Next code (Auto Resync)	✓
SMS Preload Code	✓
SMS Three Code	✓
SMS Day Code	✓
SMS Realtime	✓
SMS Preload	✓
Email Three Code	✓
Email Day Code	✓
Email Realtime	✓
Voice Call	✓
OneSwipe Push	✓

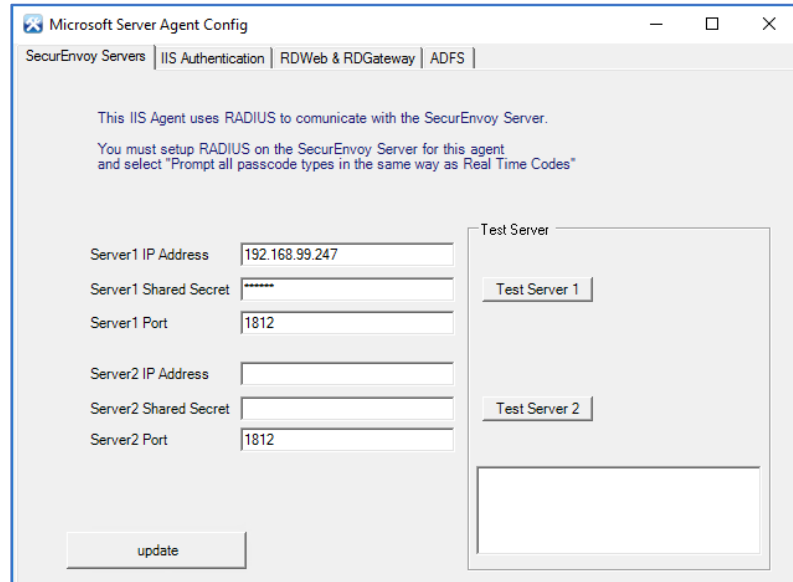
## 1.5 Configure the Microsoft Server Agent

Select the SecurEnvoy Servers tab.

Configure your SecurEnvoy Server 1 IP address and Shared Secret.

Once complete, press the Test Server 1.

If result returns 'OK', click 'update'.



Microsoft Server Agent Config

SecurEnvoy Servers | IIS Authentication | RDWeb & RDGateway | ADFS

This IIS Agent uses RADIUS to communicate with the SecurEnvoy Server.

You must setup RADIUS on the SecurEnvoy Server for this agent and select "Prompt all passcode types in the same way as Real Time Codes"

Server1 IP Address: 192.168.99.247

Server1 Shared Secret: \*\*\*\*\*

Server1 Port: 1812

Server2 IP Address: [ ]

Server2 Shared Secret: [ ]

Server2 Port: 1812

Test Server

Test Server 1

Test Server 2

update

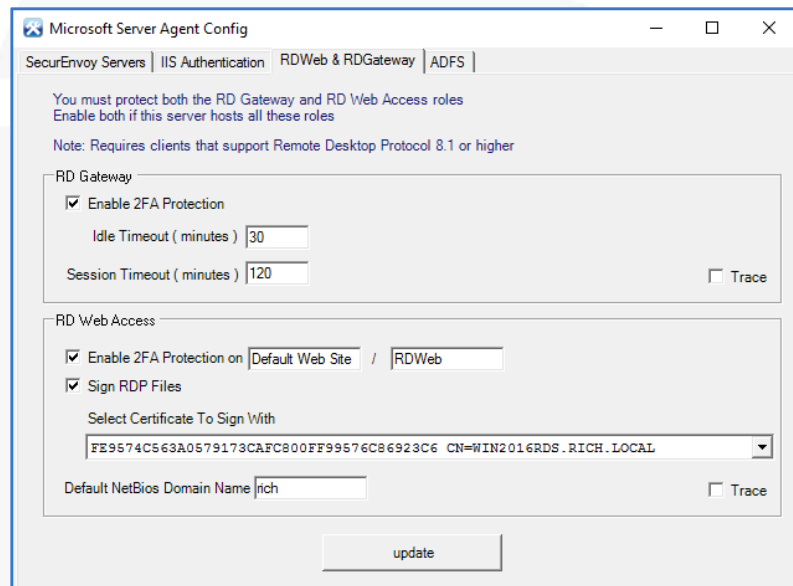
Select the RDWeb & RDGateway tab.

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



Microsoft Server Agent Config

SecurEnvoy Servers | IIS Authentication | RDWeb & RDGateway | ADFS

You must protect both the RD Gateway and RD Web Access roles. Enable both if this server hosts all these roles.

Note: Requires clients that support Remote Desktop Protocol 8.1 or higher

RD Gateway

Enable 2FA Protection

Idle Timeout ( minutes ) 30

Session Timeout ( minutes ) 120  Trace

RD Web Access

Enable 2FA Protection on Default Web Site / RDWeb

Sign RDP Files

Select Certificate To Sign With

FE9574C563A0579173CAFC800FF99576C86923C6 CN=WIN2016RDS.RICH.LOCAL

Default NetBios Domain Name rich  Trace

update

## 1.6 Configure a RADIUS client in SecurEnvoy SecurAccess Server for MS RDS.

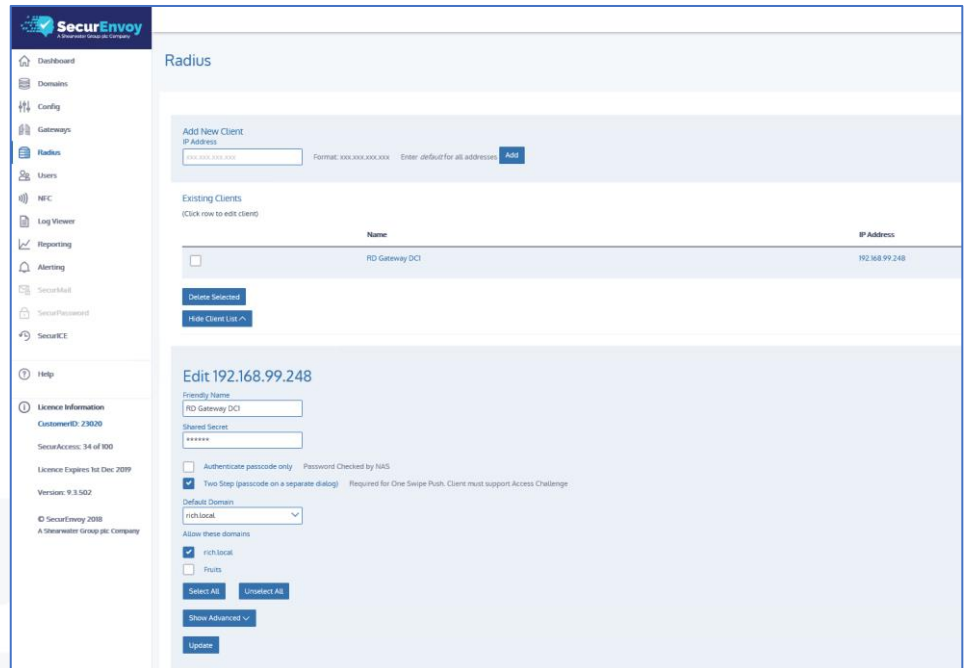
Open the SecurEnvoy SecurAccess Admin console

Navigate to the RADIUS tab

Enter the IP address of the Microsoft Remote Desktop Services server and click on Add

Type in a Friendly Name so that you can easily identify the server and the same shared secret that was entered into the Microsoft Server Agent in the previous step

Click on Update



**SecurEnvoy**  
A Shearwater Group plc Company

Dashboard  
Domains  
Config  
Gateways  
**RADIUS**  
Users  
NEC  
Log Viewer  
Reporting  
Alerting  
SecurMail  
SecurPassword  
SecurICE  
Help

License Information  
CustomerID: 23620  
SecurAccess: 34 of 100  
License Expires 1st Dec 2019  
Version: 9.3.502  
© SecurEnvoy 2018  
A Shearwater Group plc Company

### Radius

Add New Client  
IP Address:  Format: xxx.xxx.xxx.xxx Enter default for all addresses **Add**

Existing Clients  
(Click row to edit client)

Name	IP Address
<input type="checkbox"/> RD Gateway DCI	192.168.99.248

**Delete Selected**  
**Hide Client List**

### Edit 192.168.99.248

Friendly Name:   
Shared Secret:   
 Authenticate password only Password Checked by NAS  
 Two Step (password on a separate dialog) Required for One Swipe Push. Client must support Access Challenge.  
Default Domain:   
Allow these domains:  
 rich.local  
 Fruits  
**Select All** **Unselect All**  
**Show Advanced**  
**Update**

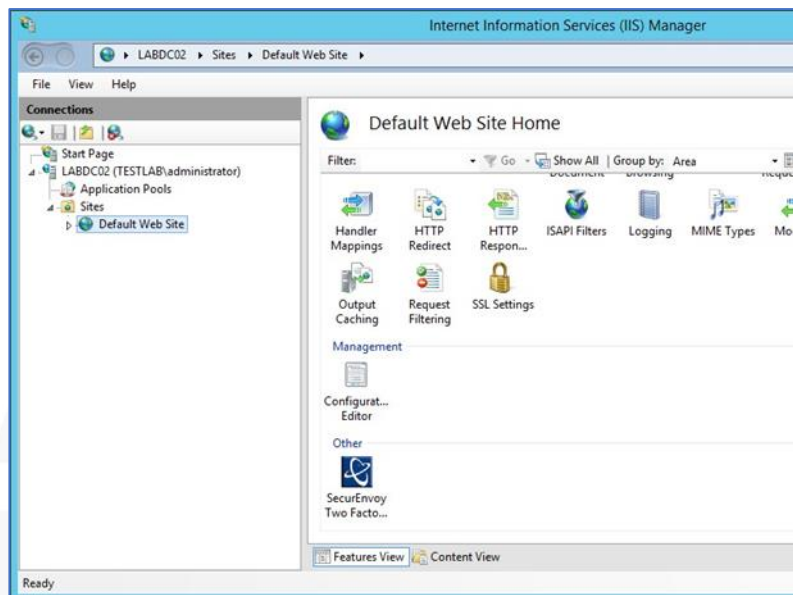
## 1.7 Configure the Microsoft Server Agent for the Default website (optional)

### Note

This section of the guide is for manual configuration of the RD Web Access and is not required, if you have used the Microsoft Server agent in section 1.1.

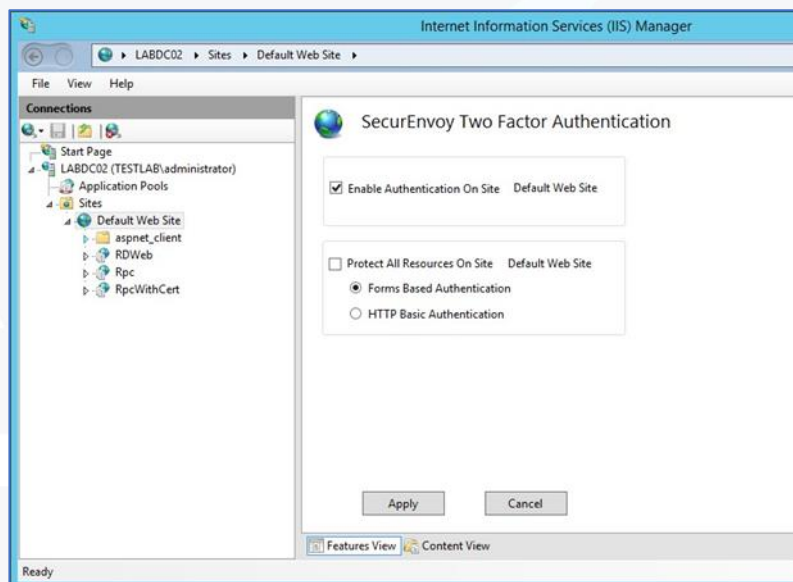
Launch the IIS management interface, either from “Start”, “Administration Tools” or from the Server Manager

Expand the sites list on the navigation pane and select “Default Web Site”, then scroll down the centre panel and press the “SecurEnvoy Two Factor” icon.



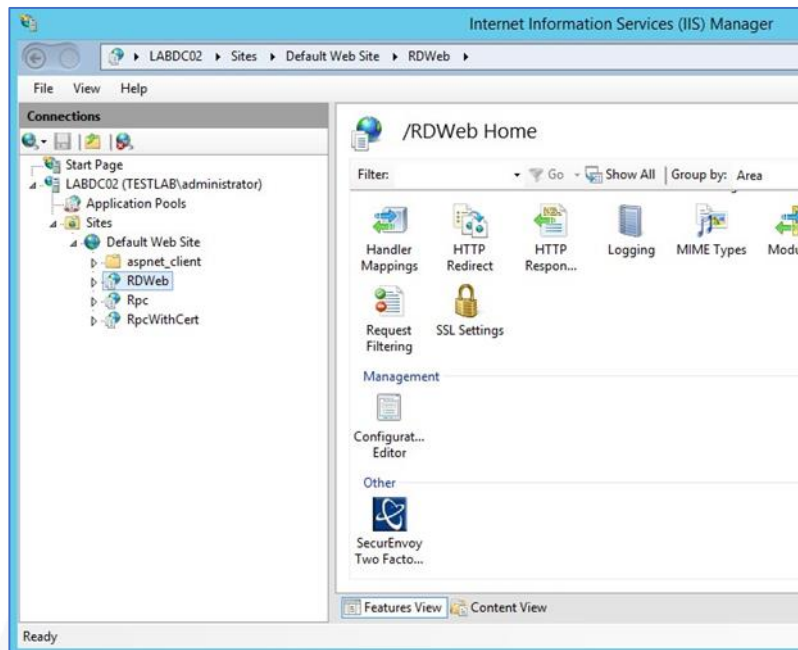
Enable the tick box to “Enable Authentication On Site Default Web Site”

Click “Apply” when complete.

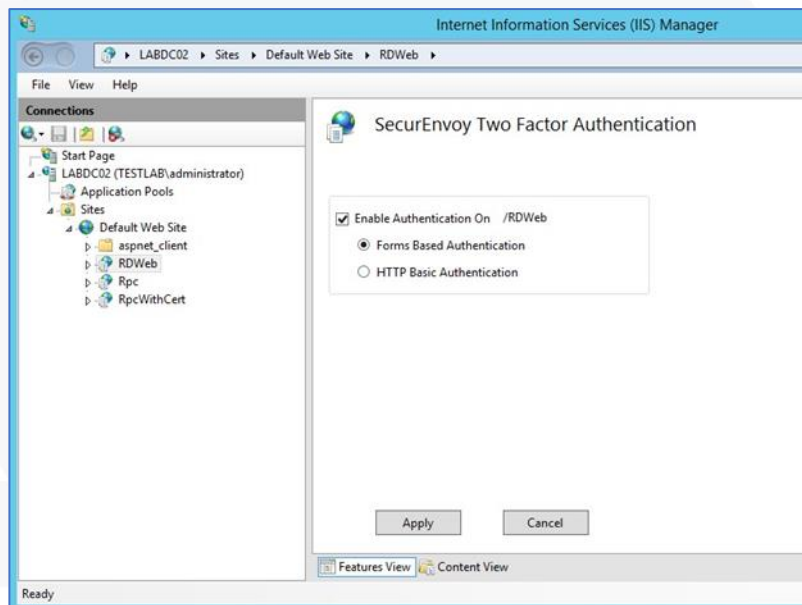


## 1.8 Configure the Microsoft Server Agent for RDWeb (optional)

Select the virtual web site you want to protect. For RDWeb select “RDWeb”, scroll down the centre panel and select “SecurEnvoy Two Factor”



Select the tick box “Enable Authentication On /RDWeb”  
 Select “Form Based Authentication” (The Default)  
 Click “Apply” to finish  
 Cancel restart IIS when prompted.



### Note

The virtual directory SecurEnvoyAuth is automatically set to the application pool “RDWebAccess”. This must be maintained for correct operation.



## 1.9 Configure Logout URL (Optional)

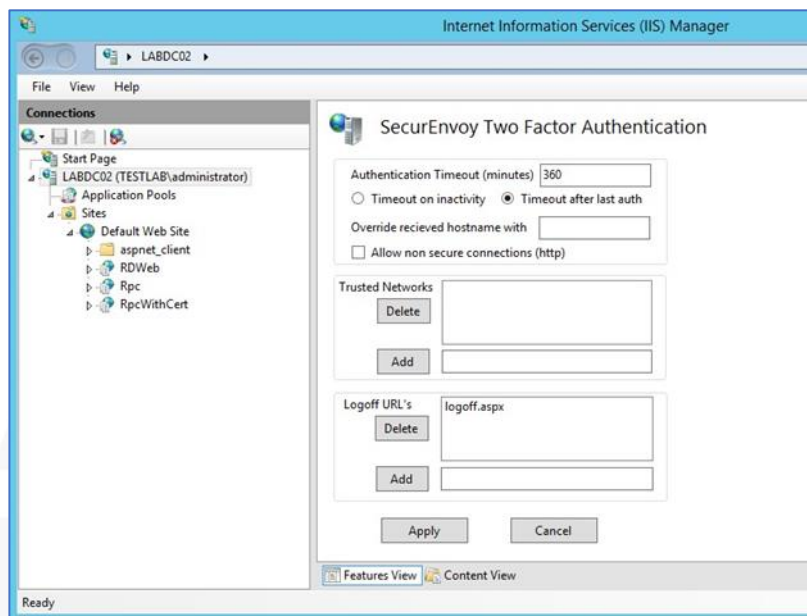
In the Navigation pane, select top level host name (the 2nd line down).

Scroll down the centre panel and press the “SecurEnvoy Two Factor” icon.

Setup your required inactivity timeout.

Add the logout URL logoff.aspx

Restart IIS when prompted.



## 1.10 Configure RDWeb Access Template (optional)

Copy the contents of RDWeb2012R2&2016 (C:\Program Files (x86)\SecurEnvoy\Microsoft Server Agent \SAMPLES)

to

C:\Program Files (x86)\SecurEnvoy\Microsoft Server Agent\WEBAUTHTEMPLATE, backing up existing files.

From

Name	Date modified	Type	Size
accessdenied	11/12/2018 17:00	HTML Document	7 KB
auth	11/12/2018 16:59	HTML Document	7 KB
passcodeok	21/08/2014 13:51	HTML Document	2 KB
readme	21/05/2012 12:47	Text Document	1 KB

To

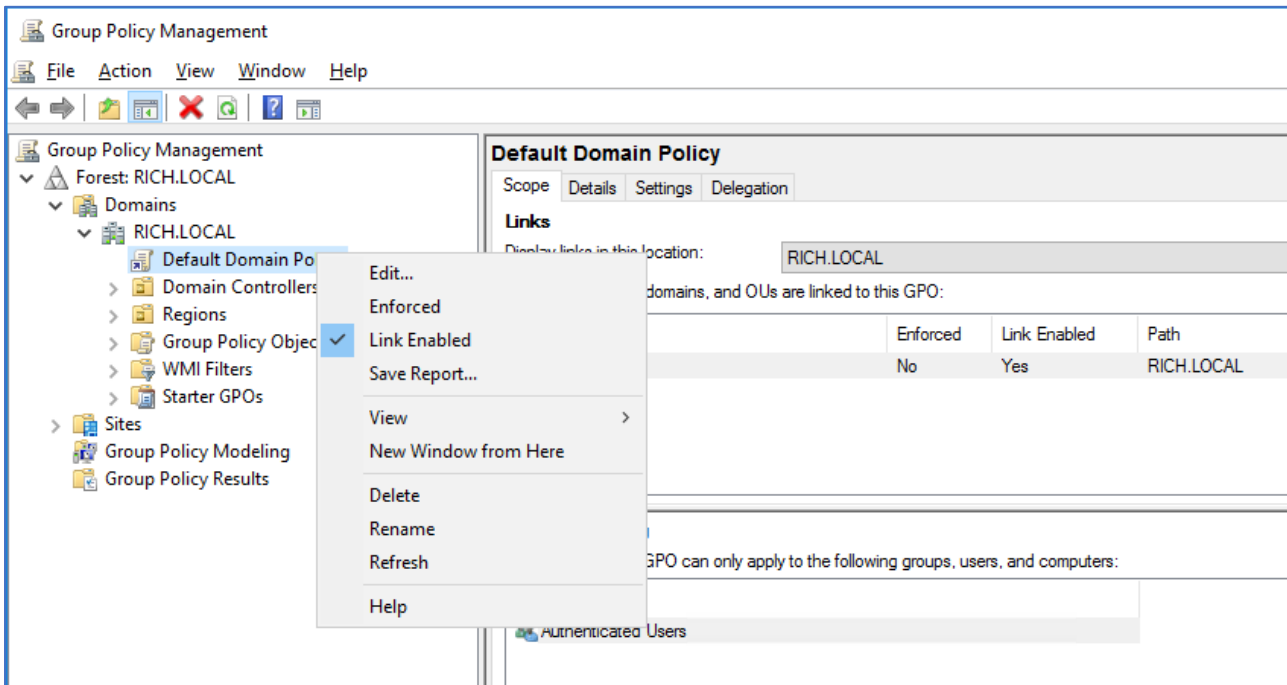
Name	Date modified	Type	Size
accessdenied	11/12/2018 17:00	HTML Document	7 KB
accessdeniedbasic	06/07/2017 12:01	HTML Document	3 KB
auth	11/12/2018 16:59	HTML Document	7 KB
error	06/07/2017 12:01	HTML Document	3 KB
logout	06/07/2017 12:01	HTML Document	3 KB
passcodeok	21/08/2014 13:51	HTML Document	2 KB
passcodeok_testss0	06/07/2017 12:01	HTML Document	2 KB
realtime	06/07/2017 12:01	HTML Document	4 KB
redirecthttps	06/07/2017 12:01	HTML Document	3 KB

## 1.11 Single Sign On (SSO) - Configuring Group Policy

Log into your Active Directory Domain Controller.

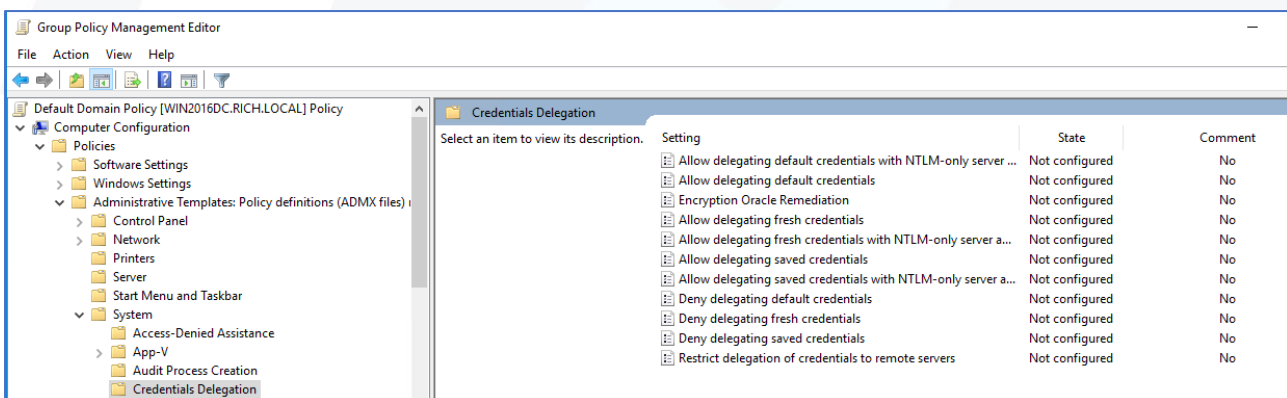
Open Group Policy Management Console (gpmc.msc).

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

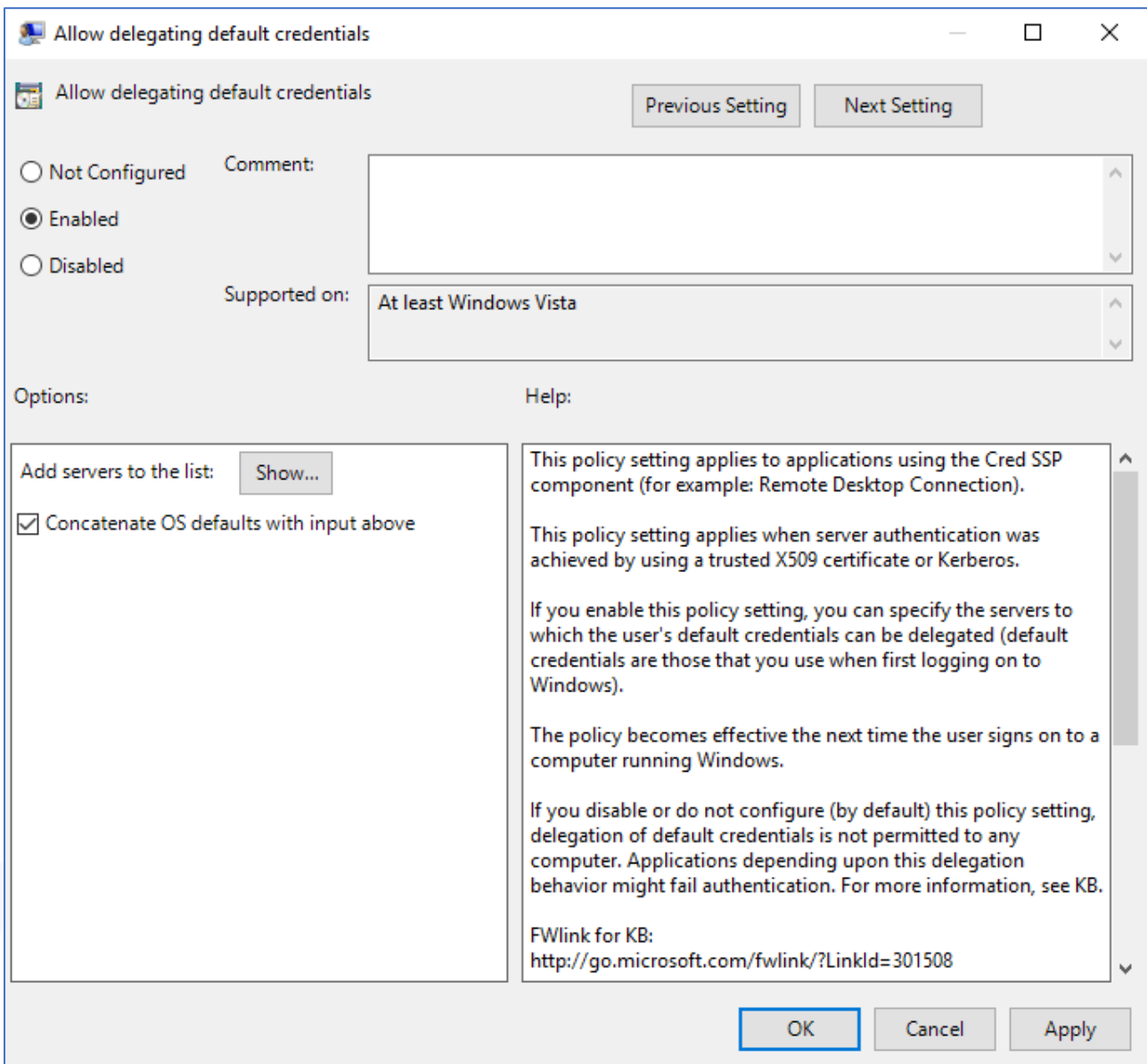


Navigate to Computer Configuration → Policies → Administrative Templates → System → Credentials Delegation

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

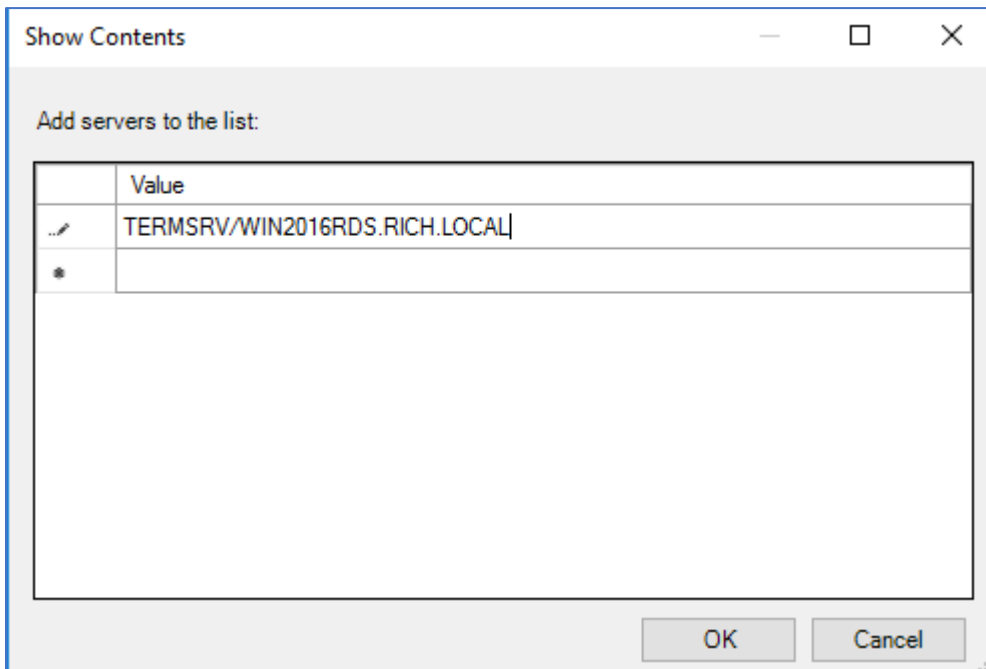
TERMSRV/\* Remote Desktop Session Host running on all machines.

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 and then again on OK at the next screen.

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

## 1.12 SSO - 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_
```

## 1.13 Test the Two Factor Authentication

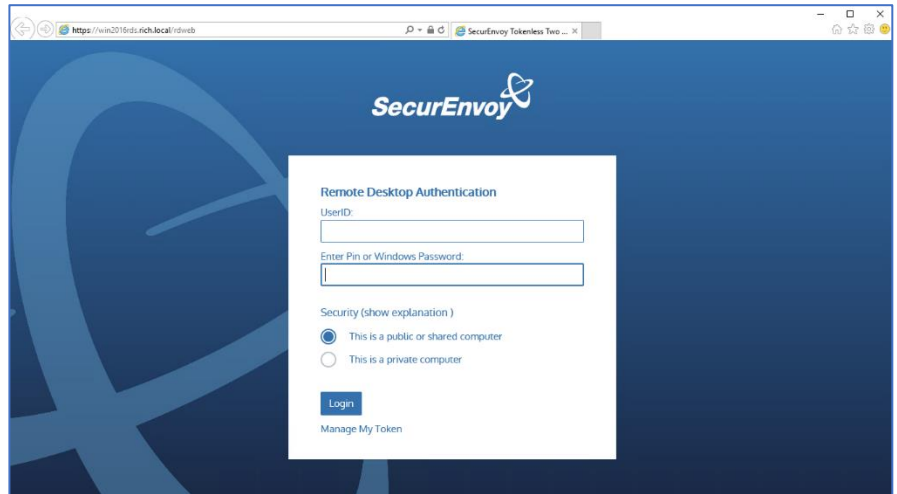
Test the Two Factor Web authentication by opening a browser and going to the URL for the Web server i.e.

`https://your_server_name/rdweb`

(Don't forget the https)

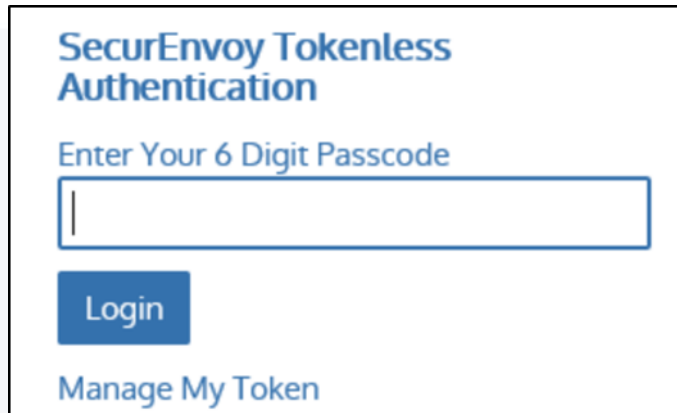
User logon screen is shown.

Enter your UserID and Password

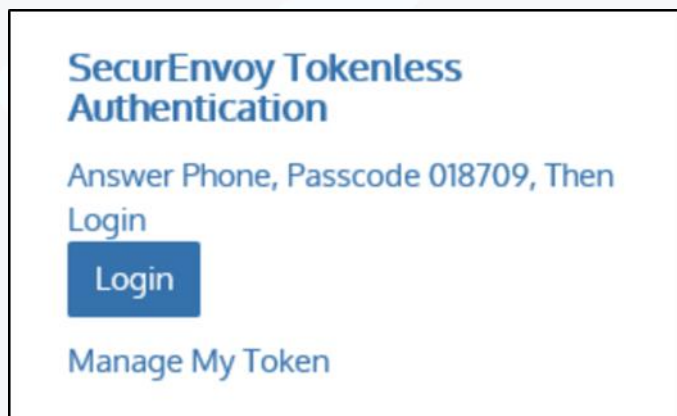


User is then presented with their two-factor authentication type:

- Preload, Realtime and Soft tokens:



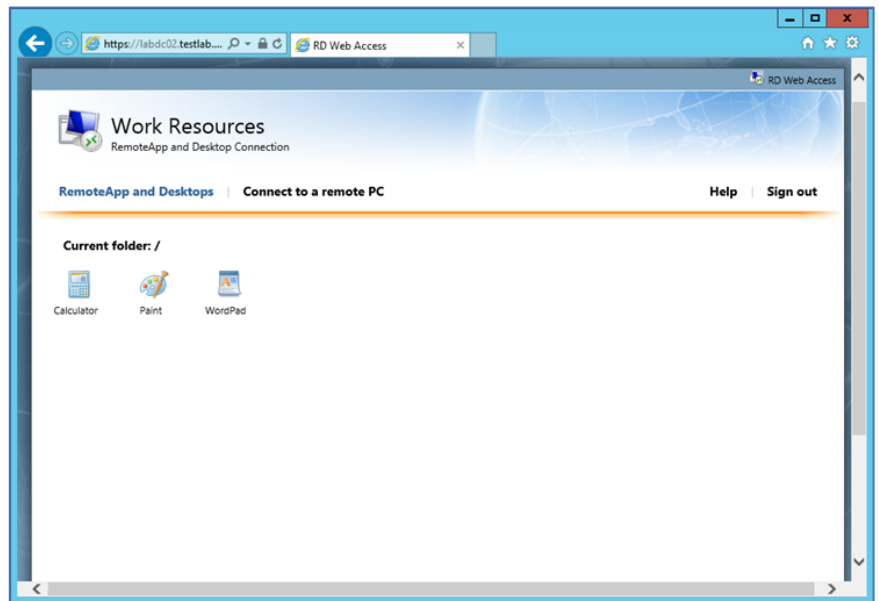
- VOICE tokens:



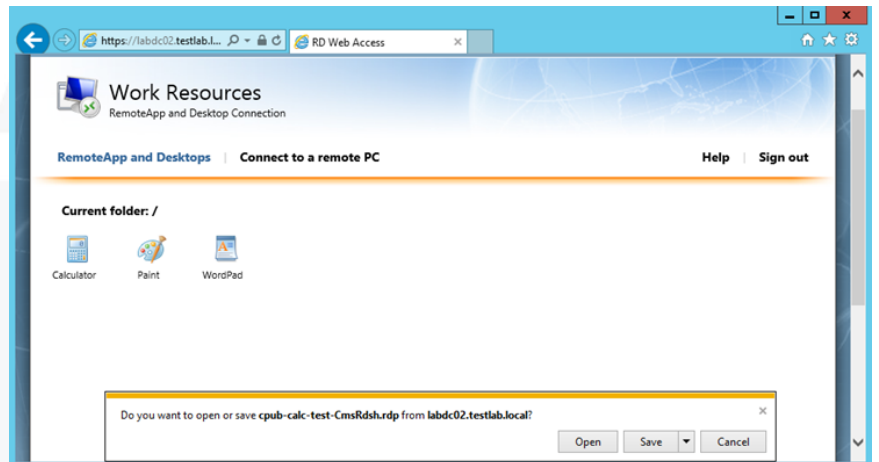
- Soft Token Push:



User authenticates successfully and is presented with RDWeb 2016:



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



**Note**

Configure your domain name within seiis.ini (C:\Windows):

# Default Domain Name to use if no domain information is included in this UserID (leave blank if not required)  
 DefaultDomain="yourdomain"

This will allow your users to logon to RD Web Access without specifying the domain name:  
 domain\UserID

# Please Reach Out to Your Local SecurEnvoy Team...



## UK & IRELAND

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

### Sales

E [sales@SecurEnvoy.com](mailto:sales@SecurEnvoy.com)  
T 44 (0) 845 2600011

### Technical Support

E [support@SecurEnvoy.com](mailto:support@SecurEnvoy.com)  
T 44 (0) 845 2600012



## EUROPE

Freibadstraße 30,  
81543 München,  
Germany

### General Information

E [info@SecurEnvoy.com](mailto:info@SecurEnvoy.com)  
T +49 89 70074522



## ASIA-PAC

Level 40 100 Miller Street  
North Sydney  
NSW 2060

### Sales

E [info@SecurEnvoy.com](mailto: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](mailto:info@SecurEnvoy.com)  
T (866)777-6211



## USA - Mid West

3333 Warrenville Rd  
Suite #200  
Lisle, IL 60532

### General Information

E [info@SecurEnvoy.com](mailto:info@SecurEnvoy.com)  
T (866)777-6211



## USA - East Coast

373 Park Ave South  
New York,  
NY 10016

### General Information

E [info@SecurEnvoy.com](mailto:info@SecurEnvoy.com)  
T (866)777-6211



A Shearwater Group plc Company

[www.securenvoy.com](http://www.securenvoy.com)