

www.securenvoy.com

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
1.2	GUIDE USAGE
1.3	PRE-REQUISITES
1.4	SUPPORTED TOKEN TYPES
1.5	CONFIGURE THE MICROSOFT SERVER AGENT
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)
1.9	CONFIGURE LOGOUT URL (OPTIONAL)
1.10	CONFIGURE RDWEB ACCESS TEMPLATE (OPTIONAL)
1.11	SINGLE SIGN ON (SSO) - CONFIGURING GROUP POLICY
1.12	SSO - APPLYING GROUP POLICY
1.13	TEST THE TWO FACTOR AUTHENTICATION



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



1.5 Configure the Microsoft Server Agent

Select the SecurEnvoy Servers tab.	SecurEnvoy Server Agent Config - C X
Configure your SecurEnvoy Server 1 IP address and Shared Secret.	This IIS Agent uses RADIUS to comunicate 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"
Once complete, press the Test Server 1. If result returns 'OK', click 'update'.	Server1 IP Address 192.168.99.247 Server1 Shared Secret Test Server Server1 Port 1812 Server2 IP Address Test Server 2 Server2 Shared Secret Test Server 2 Server2 Port 1812
Select the RDWeb & RDGateway tab.	Image: SecurEnvoy Server Agent Config - × SecurEnvoy Servers IIS Authentication RDWeb & RDGateway ADFS
For RD Gateway protection from a direct connection, check the check box for 'Enable 2FA Protection'	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
RD Web Access protection, check the check box for 'Enable 2FA Protection on Default Web Site / RDWeb.	Session Timeout (minutes) 120 Trace RD Web Access FC Enable 2FA Protection on Default Web Site / RDWeb FC Sign RDP Files
To enable RDP file signing, check the check box for 'Sign RDP Files' and select the certificate assigned to your RD Gateway.	Select Certificate To Sign With FE9574C563A0579173CAFC800FF99576C86923C6 CN=WIN2016RDS.RICH.LOCAL Default NetBios Domain Name rich Trace update
Enter your Default NetBios Domain Name	



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

	y	_
Dashboard	Radius	
Domains		
∳†↓ Config		
Gateways	Add New Client	
Radius	P Address Format: xxxxxxxxxx Format: xxxxxxxxxxx Format: xxxxxxxxxxxx Format: xxxxxxxxxxxx Format: xxxxxxxxxxxxx Format: xxxxxxxxxxxx Format: xxxxxxxxxxxx Format: xxxxxxxxxxxx Format: xxxxxxxxxxx Format: xxxxxxxxxxx Format: xxxxxxxxxxx Format: xxxxxxxxxxx Format: xxxxxxxxxx Format: xxxxxxxxxx Format: xxxxxxxxxx Format: xxxxxxxxxx Format: xxxxxxxxxx Format: xxxxxxxxxx Format: xxxxxxxxx Format: xxxxxxxxx Format: xxxxxxxxx Format: xxxxxxxx Format: xxxxxxx Format: xxxxxx Format: xxxxxxx Format: xxxxx Format: xxxxx Format: xxxxx Format: xxxx Format: xxxx Format: xxxx Format: xxx Fo	
2g Users		
II)) NFC	Existing Clients	
Log Viewer	(Click row to edit client)	
Reporting	Name Prosters	
	ND Gateway OCI IVC 189 97,248	
Securitat	Delate Selected	
SecurPesseerd	Hole Cleret List A	
SecuriCE		
(7) Help	Edit 192.168.99.248	
Licence Information CustomeriD: 23020 SecurAccess: 34 of 100	RD Gateway DC Shared Secret *****	
Licence Expires 1st Dec 2019 Version: 9.3.502	Authenticate paracele only Personed Orected by MSS Too Steep paraceles on a separate dialogi. Propried for One Sonje Push. Client must support Access Challenge Default Comm	
© SecurEnvoy 2018 A Shearwater Group plc Comp	ndhùcai. V Allao thea damains	
	retulad	
	Sheet All University All	
	Lipsae -	



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.





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.

File View Help	
Connections Start Page LABCC0 (TESTLAB\administrator) Call Application Pools Sites Default Web Site Default Web Site Default Web Default Web	SecurEnvoy Two Factor Authentication Authentication Timeout (minutes) 360 Timeout on inactivity Timeout after last auth Override recieved hostname with

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.

То

From

Name	Date modified	Туре	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
i readme	21/05/2012 12:47	Text Document	1 KB

> Local Disk (C:) > Program Files (x86) >	SecurEnvoy > Micro	osoft Server Agent → V	VEBAUTHTEMPLATE
Name	Date modified	Туре	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_testsso	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.

📓 Group Policy Management							
<u>File</u> <u>Action</u> <u>View</u> <u>Window</u> <u>Help</u>	<u> </u>						
🔶 📩 📰 🗙 🧟 🛛 🖬							
Group Policy Management Default Domain Policy							
V A Porest: NCH.LOCAL	Scope	Details	Settings Delegation	n			
V RICH.LOCAL	Links						
Default Domain Po	Display	lielce in th	in location:	RICH.LOCAL			
Domain Controllers			domains, and OUs	are linked to th	nis GPO:		
Regions Environmental Action of the second secon					Enforced	Link Enabled	Path
> 🕞 WMI Filters Save Report					No	Yes	RICH.LOCAL
> 👘 Starter GPOs							
> Sites View		,					
Group Policy Modeling New Window from Here							
Delete							
Rename			1.1				
Refresh			aPO can only appl	ly to the followir	ng groups, use	rs, and computers:	
Help							
	AL AL	Inenticate	eo Users				

Navigate to Computer Configuration \rightarrow Policies \rightarrow Administrative Templates \rightarrow System \rightarrow Credentials Delegation

Right click and edit "Allow delegating default credentials"

📓 Group Policy Management Editor —								
File Action View Help								
Tefault Domain Policy [WIN2016DC.RICH.LOCAL] Policy Credentials Delegation Credentials Delegation								
V 🛃 Computer Configuration	Select an item to view its description.	Setting	State	Comment				
Policies		E Allow delegating default credentials with NTLM-only server	Not configured	No				
> 📋 Windows Settings		Allow delegating default credentials	Not configured	No				
🗸 🚞 Administrative Templates: Policy definitions (ADMX files) ı		E Encryption Oracle Remediation	Not configured	No				
> 🧮 Control Panel		E Allow delegating fresh credentials	Not configured	No				
> 🦳 Network		Allow delegating fresh credentials with NTLM-only server a	Not configured	No				
Printers		Allow delegating saved credentials	Not configured	No				
📔 Server		E Allow delegating saved credentials with NTLM-only server a	Not configured	No				
Start Menu and Taskbar		Deny delegating default credentials	Not configured	No				
🗸 🚞 System		E Deny delegating fresh credentials	Not configured	No				
Access-Denied Assistance		Deny delegating saved credentials	Not configured	No				
> 🧰 App-V		Restrict delegation of credentials to remote servers	Not configured	No				
Audit Process Creation								
Credentials Delegation								



Select "Enabled" and click on the "Add servers to the list: Show..." button

Allow delegating default credentials – 🗆 X									
Allow delegating default credentials Previous Setting Next Setting									
O Not Configured	Comment:								^
Enabled									
 Disabled 									× .
	Supported on:	At least Window	vs Vista						^
									~
Options:			Help:						
Add servers to the list:	: Show	above	This policy component This policy achieved by If you enable which the u credentials Windows). The policy R computer re If you disab delegation computer. A behavior m FWlink for R http://go.m	setting applie t (for example setting applie y using a trust le this policy s user's default of are those that becomes effect unning Windo le or do not c of default creat Applications of ight fail authe	es to applic Remote l swhen sec ed X509 co setting, yo credentials t you use v ctive the n ows. configure (dentials is depending entication.	ations u Desktop rver auth ertificate u can sp can be vhen firs ext time by defau not perr upon th For mou inkld=3(ising the C Connection entication or Kerber delegated at logging the user s ult) this po mitted to a his delegat re informa	Cred SSP on). n was ros. servers to I (default on to signs on to signs on to blicy settin any tion ation, see	o a ng, KB.
					OK		Cancel	Арр	y

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

Show	Show Contents — 🗆 X							
Add s	ervers to the list:							
	Value							
1	TERMSRV/WIN2016RDS.RICH.LOCAL							
		ОК	Cance	el 🛛				

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.





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 UsedID and Password



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

 Preload, Realtime and Soft tokens: 	SecurEnvoy Tokenless Authentication Enter Your 6 Digit Passcode
VOICE tokens:	SecurEnvoy Tokenless Authentication
	Login
• Soft Token Push:	Manage My Token



User authenticates successfully and _ 🗆 🗙 ← → Ø https://labdc02.testlab.... is presented with RDWeb 2016: Work Resources eApp and Desktops | Connect to a remote PC Help | Sign out Current folder: / Ì A Paint Calculate - -User launches application from × RDWeb page and selects 'Open' from browser Work Resources App and De oteApp and Desktops Connect to a remote PC Help | Sign out Re Current folder: / Ì A Paint Do you want to open or save cpub-calc-test-CmsRdsh.rdp from labdc02.testlab.local? Open Save 💌 Cancel **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
- 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



www.securenvoy.com

SecurEnvoy HQ, Octagon Point, 5 Cheapside, St Paul's, London, EC2V 6AA E: info@SecurEnvoy.com T: 44 (0) 845 2600010 Company No. 04866711 VAT Number GB 862076128