Authentication with Windows 2012 R2 Server with Remote Desktop Web Gateway

Authenticate with Push only (SSO) and native RDP connections that don't visit RDWeb.

© 2016 SecurEnvoy Ltd. All rights reserved

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	Lime Tree Gate Crockford Lane Basingstoke Hampshire RG24 8WH	
Dorian Tomkins	dtomkins@securenvoy.com	

Index

1. Document Purpose 3
2. Supported Authentication Types 4
3. Prerequisites 5
4. Configure Microsoft's Network Policy Server for SecurEnvoy Push 6
5. Configure SecurEnvoy Security Server 8
6. Test connectivity to the Remote Desktop Applications 9
7. Notes 10

© 2016 SecurEnvoy Ltd. All rights reserved Confidential

1. Document Purpose

Windows 2012 R2 Server with Remote Desktop Web Gateway Maintaining SSO with SecurEnvoy Push technology.

This document is one of two integration guides that describes how to integrate a Windows 2012 R2 RDGateway.

Advantages

- Supports Microsoft's Password SSO. If you authentication to RDWeb with a password, you don't need to re-enter this password when the RD client connects to RDGateway.

- RDP clients of any version can directly connect to RDGateway without the need to first visit RDWeb.

Disadvantages

- Only supports Oneswipe Push tokenless type and cannot fail back to a manual entering an offline passcode. The user must have their phone online for this approach.

Note

This document relates only to RDGateway via Network Policy Server and Push technology.

Review the "Windows Logon Agent" guide if you want to authenticate Remote Desktop Client connections on the Terminal Server Hosts.

The equipment used for the integration process is listed below:

Microsoft Windows Server 2012 R2
Installed roles:
Remote Desktop Services

SecurEnvoy
SecurAccess Server software release v8,1,502

© 2016 SecurEnvoy Ltd. All rights reserved

2. Supported Authentication Types

The following table shows what token types are supported.

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

© 2016 SecurEnvoy Ltd. All rights reserved

3. Prerequisites

It is assumed that Remote Desktop Gateway has already been configured to authenticate a password via Network Policy Services (NPS).

Securenvoy Security Server has been installed with the Radius service and has a suitable account that has been setup and verified to work with OneSwipe Push.

Note

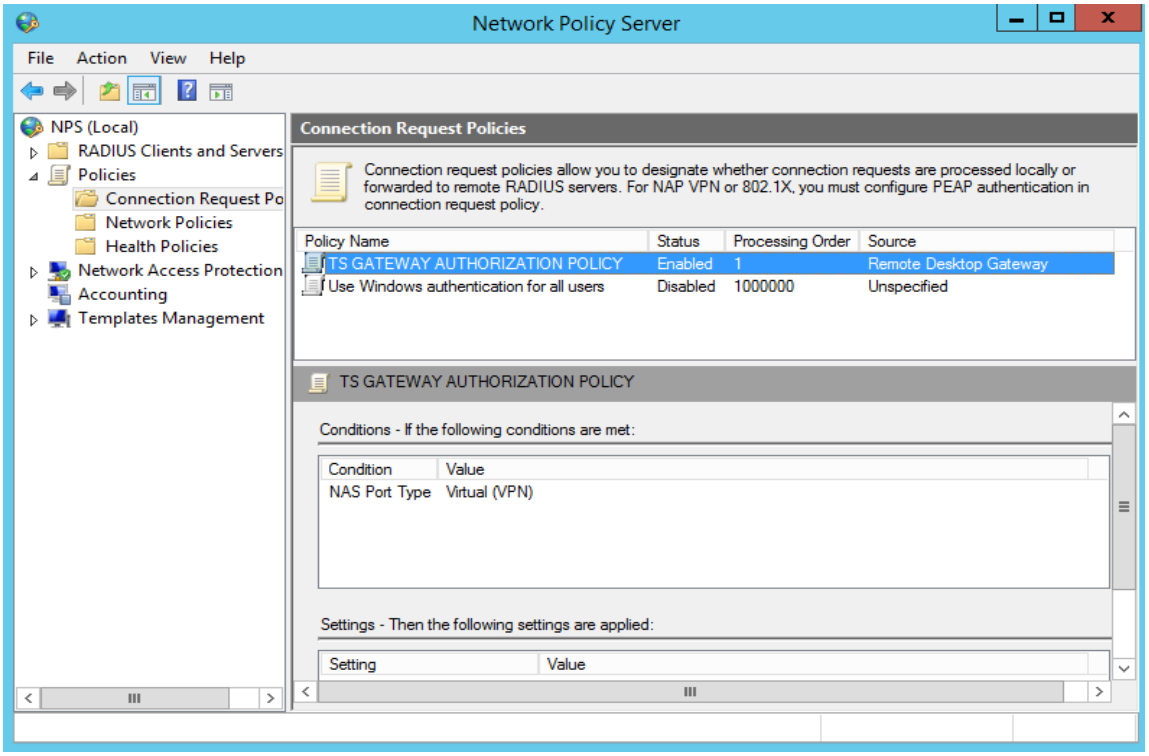
You must use SecurEnvoy Security Server version 8.1.502 or higher
You Must use Soft Token Push ONLY!

Microsoft NPS is a Radius service and will use port 1812 by default. If you install SecurEnvoy server on the same host it is recommended you set the Radius port to 51812 - If available.

© 2016 SecurEnvoy Ltd. All rights reserved

4. Configure Microsoft's Network Policy Server for SecurEnvoy Push

From your RDS Server -> Launch Network Policy Server.



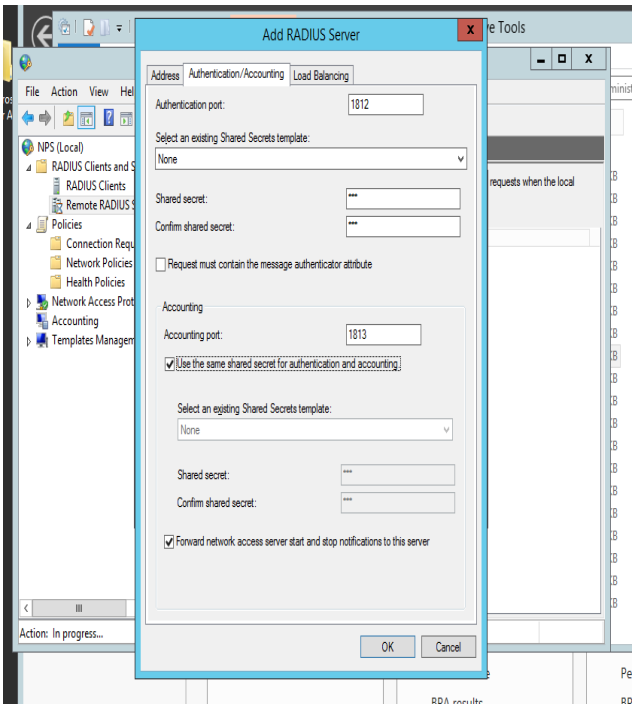
Expand "RADIUS Clients and Servers -> Right Select: Remote RADIUS Server -> New.

Enter the Group Name: "SecurEnvoy" and select "Add".

Address tab:
Select: Verify -> enter the IP Address of your SecurEnvoy Security Server Admin.
Select: "Resolve" and then select "Ok".

Authentication/Accounting tab:
Authentication Port "1812" or 51812 if the SecurEnvoy server is on the same host.

Enter the "Shared Secret" and "Confirm Shared Secret".



© 2016 SecurEnvoy Ltd. All rights reserved

Load Balancing tab:

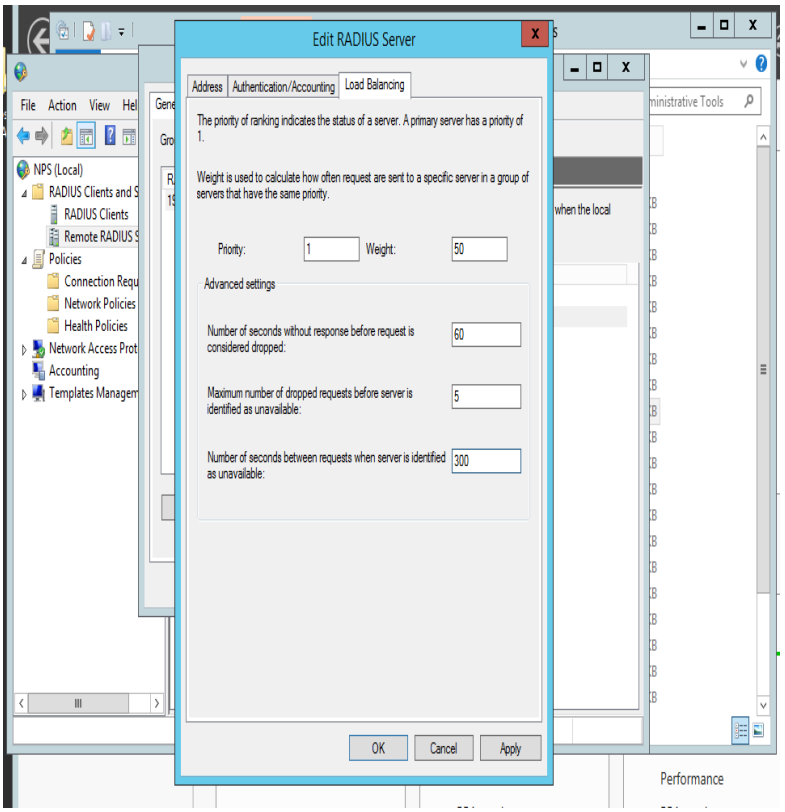
- Priority = 1
- Weight = 50

Number of seconds without response before request is considered dropped: = 60

Maximum number of dropped requests before server is identified as unavailable = 5

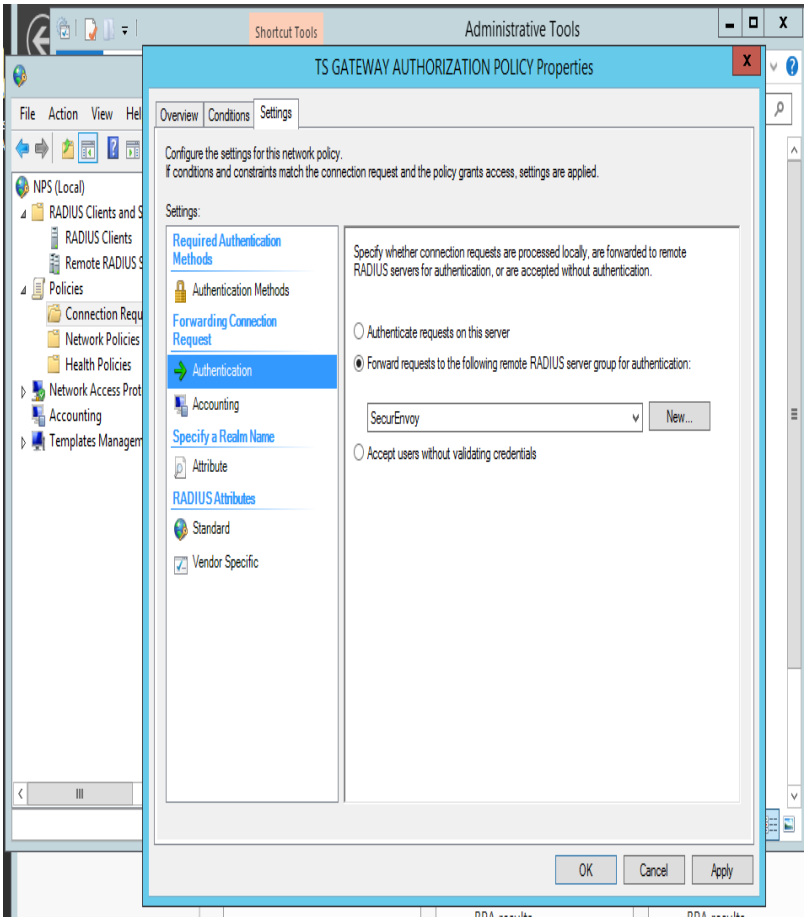
Number of seconds between requests when server is identified as unavailable = 300

Select: "Ok"



© 2016 SecurEnvoy Ltd. All rights reserved

Expand Polices -> Select: Connection Request Polices -> Right select: "TS GATEWAY AUTHORIZATION POLICY" and then select "Properties"



Settings tab

Select: Forward Connection Request -> Authentication

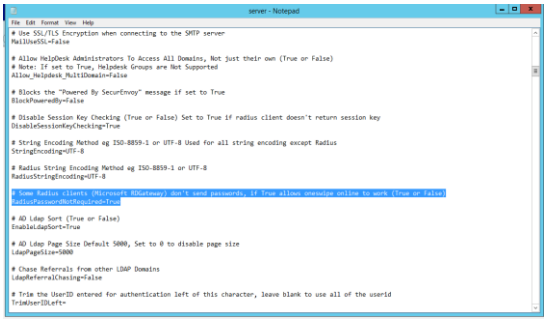
Check: "Forward requests to the following remote RADIUS server group for authentication".

From the drop-down list select "SecurEnvoy profile - > and then select "Ok"

5. Configure SecurEnvoy Security Server

From the SecurEnvoy Security Server Admin -> Launch "File Explorer" and navigate to C:\Program Files (x86)\SecurEnvoy\Security Server.

Edit the Server.ini file and check that the below line exists and its value is set to "True".



# Some Radius clients (Microsoft RDGateway) don't send passwords, if True allows oneswipe online to work (True or False)
RadiusPasswordNotRequired=True

Close and save the Server.ini file.

Launch "Security Server Admin"

© 2016 SecurEnvoy Ltd. All rights reserved

Radius tab

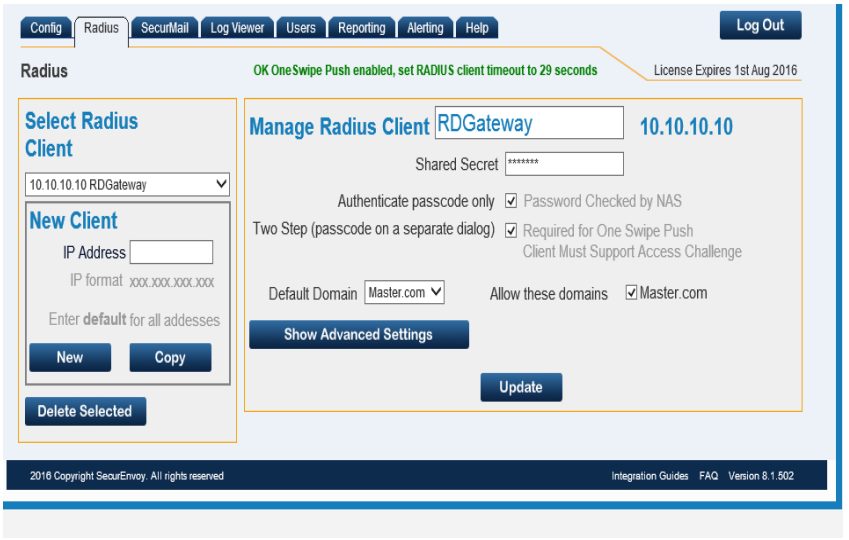
Configure a "New Client" pointing this to your RDS server IP Address.

Enter in the matching Shared Secret.

Check: "Authentication passcode only".

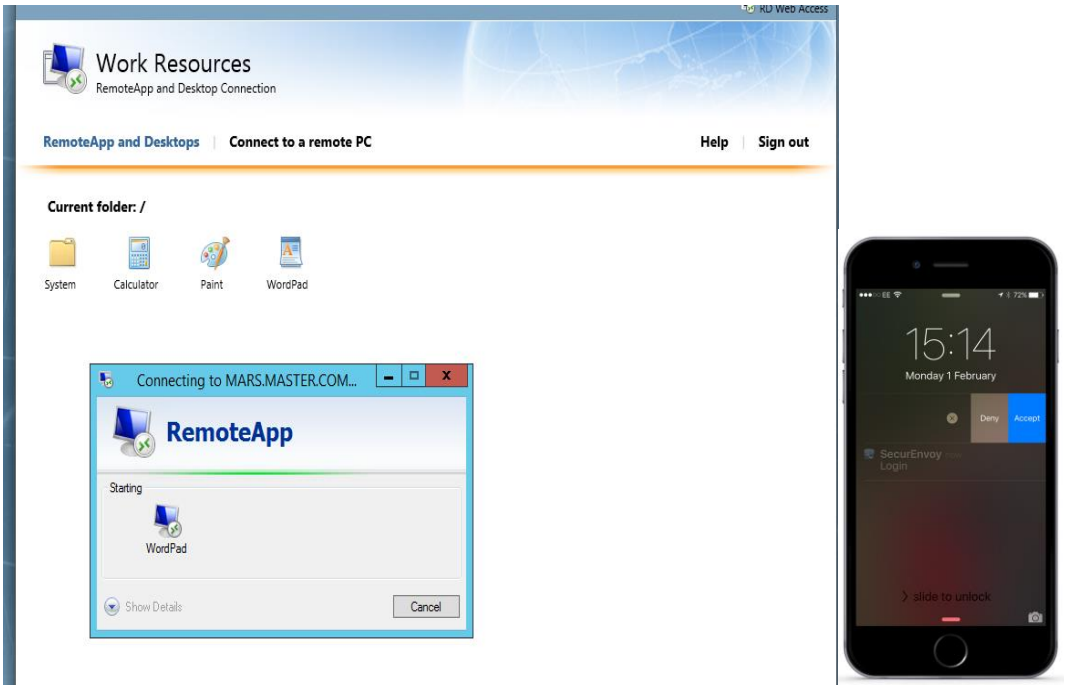
Check: "Passcode prompt is on a separate dialog".

Select: "Update".



6. Test connectivity to the Remote Desktop Applications

Test that a User authenticates successfully and is presented with OneSwipe Push:



7. Notes

© 2016 SecurEnvoy Ltd. All rights reserved