Mobile ID

Microsoft Remote Desktop Services (formerly Terminal Server)

Solution guide

Version: 1.0

Swisscom (Schweiz) AG
Security Solutions

Swisscom (Schweiz) AG
Security Solutions

Contents

Swisscom (Schweiz) AG
Security Solutions

1 Introduction

The purpose of this document is to describe how to configure the Microsoft server roles Terminal Services (TS) Gateway and Network Policy Server (NPS) in order to be able to strong-authenticate Remote Desktop Connection (RDP) users with Mobile ID (MID).

1.1 Targeted audience

This integration guide is intended for network administrators and system administrators responsible for implementing and maintaining corporate web services over the Internet.

It's assumed that the reader is familiar with the Swisscom MID service and the related "Mobile ID - Client reference guide", as well as with Windows Server and the RADIUS protocol.

For more information about MID, please refer to [1].
For more information about RADIUS Integration with MID, please refer to [2].

1.2 Terms and abbreviations

Abbreviation	Definition
MID	MobileID is the one-for-all authentication of Swisscom.
RDP	Remote Desktop Protocol is a proprietary protocol developed by Microsoft which allows a user to connect to a remote computer over a network connection, using a graphical interface.
RDC	Remote Desktop Client
RADIUS	Remote Authentication Dial-In User Service is a networking protocol which provides Authentication, Authorization and Accounting for users who connect and use a network service.
TS Gateway	Terminal Services Gateway is a Windows Server service role that allows authorized remote users to connect to resources on an internal corporate or private network from any Internet-connected device.
NPS	Network Policy Server allows to create and enforce organization-wide network access policies for client health and connection request authentication and authorization.
OTP	A One-Time Password is a password that is valid for only one login session or transaction.
PKI	A Public Key Infrastructure is needed to create, manage, distribute, use, store, and revoke digital certificates.
MSISDN	Number uniquely identifying a subscription in a GSM/UMTS mobile network

1.3 Referenced documents

[1] SOAP Client Reference Guide
[2] Mobile ID – RADIUS Integration Guide

2 Overview

This chapter provides the configuration steps and reference to further information for enabling two-factor authentication for RDP by means of using MID.

2.1 Architecture

The following diagram shows the interaction between the main components involved in the authentication process:

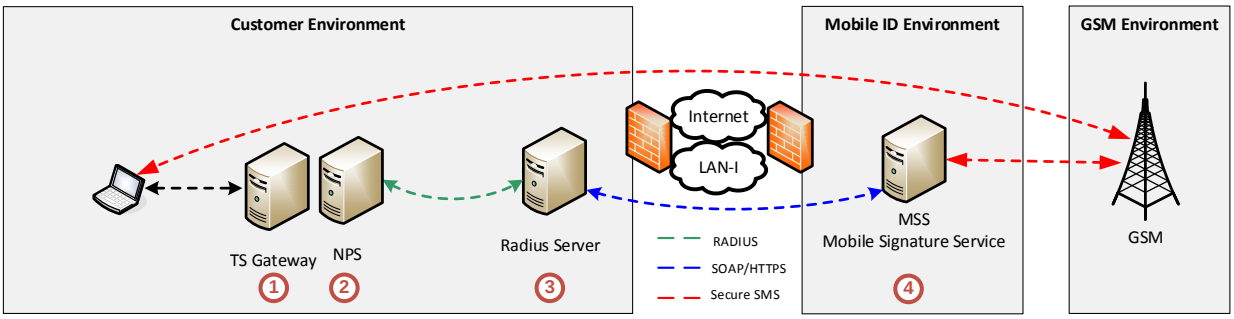


Diagram 1.- System Components

1) TS Gateway – is a Server Role Service that enables the establishment of the RDP connection between the client and the server in the corporate network. A SSL tunnel is established between the RDP client and the TS Gateway.

   TS Gateway encapsulates Remote Desktop Protocol (RDP) within RPC, within HTTP over a Secure Sockets Layer (SSL) connection

2) NPS (Network Policy Server) – is a Server Role Service which enables local and remote network access services and define and enforce policies for network access authentication, authorization and client health. NPS fully supports the Remote Authentication Dial-In User Service (RADIUS) protocol. Deploying NPS as a RADIUS server enables clients to authenticate using strong authentication (OTP).

   NPS will be configured as a RADIUS proxy to forward the connection requests to the RADIUS server offering the MID integration capabilities.

3) RADIUS Server – it translates the RADIUS requests into SOAP calls to the MSS Service. It also maps the Windows credentials to a valid user mobile number (see authentication flow below).

   The Open Source FreeRADIUS can be deployed and configured to accomplish this function.

4) MSS (Mobile Signature Service) – Web Service (XML/SOAP) which accepts mobile signature requests and forwards them to the mobile device through the GSM network.

2.2 Scenario

The following diagram shows the interaction between the involved system components during the two-factor authentication process, which uses the MID as an OTP.

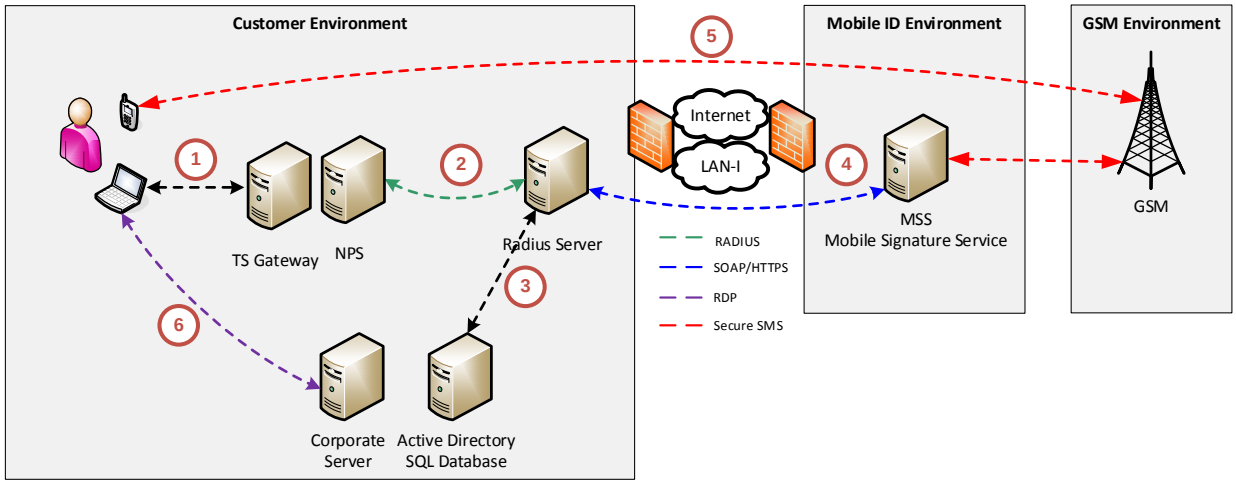


Diagram 2.- Authentication

This diagram shows the authentication process a user who requests RDP access to a server located in the corporate network. The authentication dataflow would be as follows:

1. The client requests a RDP connection to the Corporate Server providing his Windows Credentials to the NPS. The Corporate Server is a host with Remote Desktop enabled.

2. The NPS Server validates the user credentials first and sends a RADIUS authentication request to the MID enabled RADIUS Server afterwards.

3. The MID enabled RADIUS Server verifies the user credentials and maps the username to the user's mobile number by looking it up in Active Directory.

4. The MID enabled RADIUS Server receives the RADIUS request, extracts the necessary information and makes a SOAP call to the MSS, requesting a mobile signature, which will be used to validate the user's identity.

5. The MSS will redirect the request to the user's mobile device over the GSM network. After the user inputs the correct PIN, the response to the mobile signature will be sent to the MSS, which will send a RADIUS Response to the MID enabled RADIUS Server, indicating whether the user was successfully authenticated or not.

6. If the user was granted access – the 2-Factor authentication succeeded – he is able now to connect to the Corporate Server via RDP.

For further information about the RADIUS integration with MobileID refer to [2].

3 Configuration and Best Practices

3.1 Pre-condition

A complete working Windows Server environment is set-up and running. Furthermore, a MID enabled RADIUS server is deployed and configured in the server landscape for translating authentication requests to web service calls to the MID. The Open Source RADIUS Server FreeRADIUS can be easily integrated into a such environment.

For more information on this topic, please refer to [2].

3.2 Deploy Terminal Services Desktop Gateway

TS Gateway is a role service which enables users to connect to resources to an internal corporate or private network from any client running a RDC client.

In order to set up the TS Gateway:

1) On the Server Management Console, go to "Add Roles and Features" and install the "Remote Desktop Services" Role Service and the "Remote Desktop Gateway" Role.
2) The "Network Policy Server" Role Service and the "Web Server" Role (IIS) will be automatically selected and installed as well.

After the installation of the new roles successfully completed, the NPS Server Role has to be configured.

NOTE: in Windows Server 2008 R2, "Terminal Services" has been renamed to "Remote Desktop Services".

3.3 Configuration of the NPS Server

In addition to provide Network Access Protection (NAP), the NPS can be used as a RADIUS Server or as a RADIUS Proxy which will forward the authentication requests to another remote RADIUS server.

The NPS server needs to be configured as a RADIUS Proxy in order for it to forward the incoming RADIUS connections to the MID RADIUS Server.

On the NPS Administration Console (Server Manager - "Tools" - "Network Policy Server"):

1) Under "Templates Management" – "Remote RADIUS Servers" create a new template by selecting "New". Input a new Template Name and the address of the remote RADIUS Proxy, which will be the MID enabled RADIUS Server.
2) In the authentication settings of the new RADIUS Server Template:
    a. Set the authentication port to 1812
    b. Input the Shared Secret
    c. Set the accounting port to 1813
    d. Check the option "Use the same shared secret for authentication and accounting"
    e. Check the option "Forward network access server start and stop notification to this server"
3) About the Load Balancer settings:
    a. In the Load Balancer settings, set the value "Number of seconds before request is considered dropped" to 90.

b. Set the value “Number of seconds between requests when server is identified as unavailable” to 90.

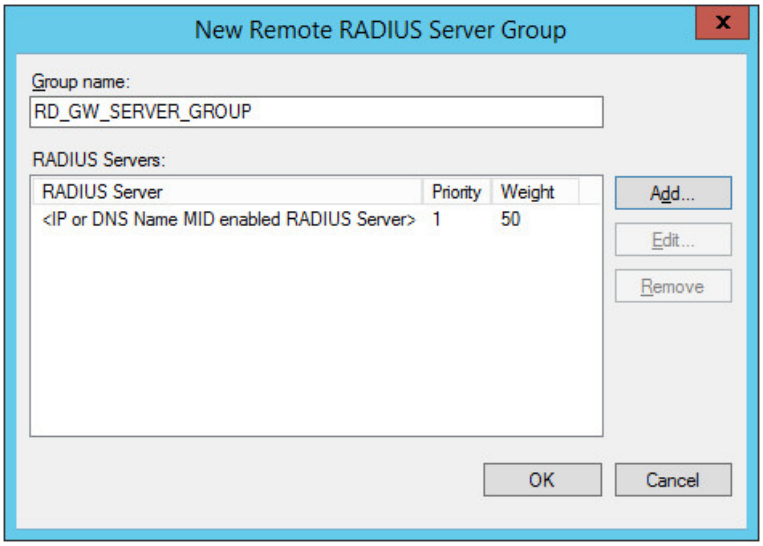
As the MID service requires end-user interaction, it provides no immediate response to the clients. Those clients must be able to set timeouts of at least 90 seconds. In case of retries or fallback, the RADIUS server must be capable to handle those aspects properly.

Following screenshot summarizes the configured settings for the RADIUS Server template:

RADIUS Server settings:

Setting	Value
Address	<IP or DNS Name MID enabled RADIUS Server>
Authentication Port	1812
Request must contain the message authenticator attribute	False
Accounting Port	1813
Forward network access server start and stop notifications to this server	True
Priority	1
Weight	50
Number of seconds without response before request is considered dropped	90
Maximum number of dropped requests before server is identified as unavailable	100
Number of seconds between requests when server is identified as unavailable	90

3) Create a new RADIUS Server Group and give it a name: RD_GW_SERVER_GROUP



4) Add a new Radius Server to the new group.
5) As a RADIUS Server Template, choose the one created in 1).
6) Under “Policies” – “Connection Request Policies”:
   a. Create a new authorization policy and give it a name: RD_GW_AUTHORIZATION_POLICY

b. As “Type of network access server” select “Remote Desktop Gateway”.

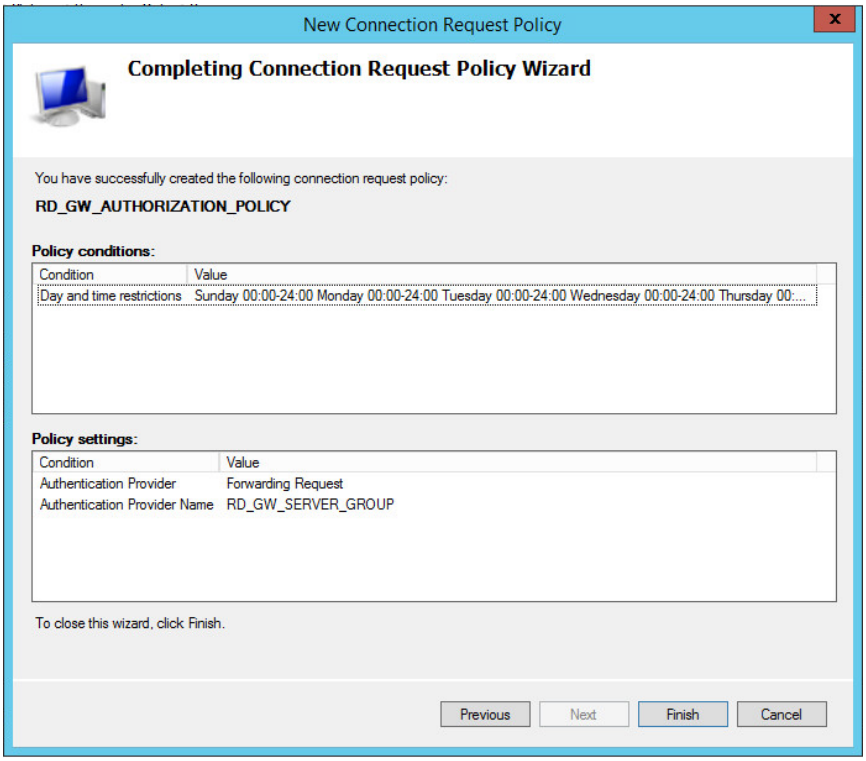
c. Now we have to specify at least a condition in order for the NPS to identify which requests apply this authorization policy to.

   Every network policy must have at least one configured condition. NPS provides many conditions groups that allow you to clearly define the properties that the connection request received by NPS must have in order to match the policy.

   For example, in order to forward all requests to the MID enabled RADIUS server (all the ones with type of network access server matching “Remote Desktop Gateway” as defined in the previous step), we set a “Day and Time Restriction” and select as value all week days, from 00:00 to 24:00.

d. Set “Forward requests to the following remote RADIUS Server Group for authentication” to the group created in 3) - RD_GW_SERVER_GROUP.

Following screenshot summarizes the configured settings for the new Authorization Policy:



7) Make sure that the new created authorization policy comes AFTER the Windows password validation on the list of authorization policies.

3.3.1 Active Directory change

To use the RADIUS service that is provided by NPS, users must have the Dial-in permission assigned. You can set this permission for domain users on a Domain Controller by using Active Directory Users and Computers, or for local users on a member server by using Local Users and Groups.

3.3.2 Relevant configuration changes on the MID enabled RADIUS Server

The RADIUS server must convert the user credentials into a valid MSIDN.

Assuming that FreeRADIUS is the MID enabled RADIUS Server being used, its LDAP module must be used for the mapping of the Windows user ID to a valid MSISDN. The LDAP configuration should just validate the password and lookup the attributes in Active Directory.

Same as before in the Load Balancer settings on the NPS, a configuration change is necessary on the RADIUS server in order to allow longer sessions. Because of the interactive nature of the authentication process, at least 90 seconds are recommended.

3.3.3 Settings on the RDP Client

On the client, on the Remote Desktop Connection dialog:

1) Select “Show Options”
2) Go to “Advanced”
3) Under “Settings” check the option “Use these RD Gateway server settings”
4) In “Server name” input the name of the TS Gateway and exit the configuration window.

The client will try to establish the RDP connection going over the TS Gateway, which is configured to authenticate first with the Windows Credentials and to make a RADIUS authentication request to Mobile ID afterwards, ensuring the two-factor authentication.

3.3.4 Microsoft Technical Guides

TS Gateway Step by Step:

https://technet.microsoft.com/en-us/library/cc771530(v=ws.10).aspx

Remote Desktop Services:

http://technet.microsoft.com/en-us/library/dd640164(v=ws.10).aspx

Configuring the TS Gateway OTP Scenario:

https://technet.microsoft.com/en-us/library/cc731249(WS.10).aspx

Remote Desktop Gateway:

https://technet.microsoft.com/en-us/library/dd983941(v=ws.10).aspx

Configure the TS Gateway Core Scenario:

https://technet.microsoft.com/en-us/library/cc754252(v=ws.10).aspx

Configuring the TS Gateway ISA Scenario:

http://technet.microsoft.com/en-us/library/cc731353(WS.10).aspx