THALES

SafeNet Agent for NPS 3.0.1

INSTALLATION AND CONFIGURATION GUIDE

Document Information

Product Version	3.0.1
Document Part Number	007-013942-002, Rev. B
Release Date	January 2021

Trademarks, Copyrights, and Third-Party Software

Disclaimer

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

PREFACE

This document describes how to install and configure the SafeNet Agent for Network Policy Service (NPS).

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with Microsoft's Network Policy Service (NPS).

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

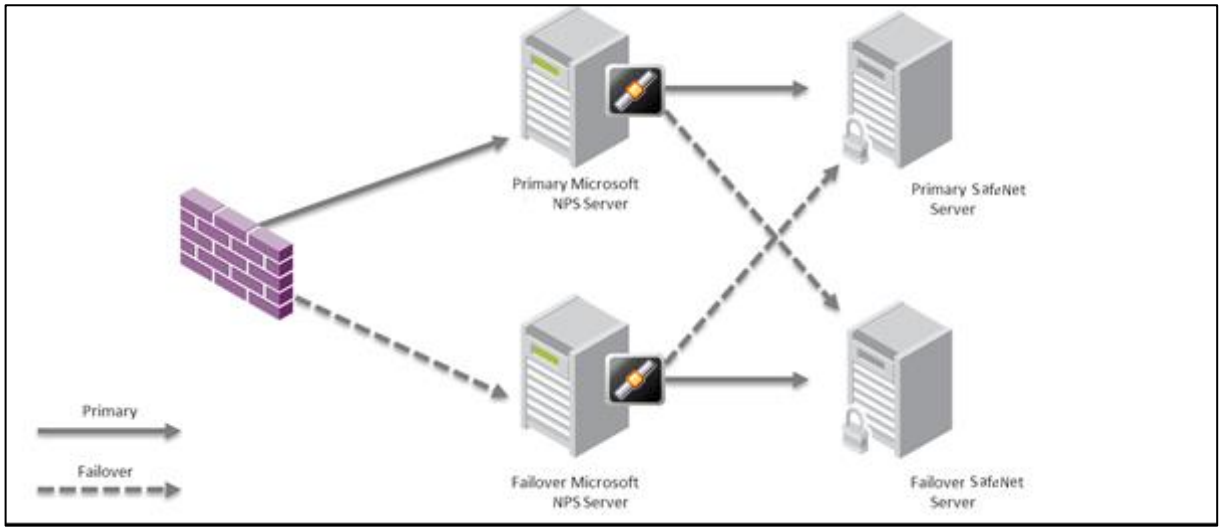
Overview

The SafeNet server uses the NPS Remote Authentication Dial-In User Service (RADIUS) components of the Windows Server.

To enable SafeNet server to accept RADIUS authentication requests, complete the following:

> Install the Windows NPS component.

> Install the SafeNet Agent for NPS on the machine hosting the NPS.



RADIUS requests received by the NPS from devices such as VPNs, firewall and other RADIUS Clients are passed to the SafeNet server via the agent.

> **NOTE:** The SafeNet Agent for NPS must be installed on the same server as the Microsoft NPS. We recommend installing SAS PCE/SPE on a different server. The agent can be configured for failover to an alternate SAS PCE/SPE server.

Logging with Push OTP

When logging to a website supporting the Push OTP function, the user enters the Username, leaves the password field empty, and clicks the login button. The user will then receive a prompt on their MobilePASS+ app, to accept or reject the logon request. On accepting the logon request, the user is logged in to the website.

System Requirements

Prerequisites

> Microsoft .NET Framework 4.5.2 (or above) must be installed on the same computer as the SafeNet Agent for NPS.

Operating Systems

The SafeNet Agent for NPS is supported on the following operating systems:

> Windows Server 2012 R2 (64-bit)

> Windows Server 2016 (64-bit)

> Windows Server 2019 (64-bit)

Authentication Management Platforms

> SafeNet Authentication Service PCE/ SPE 3.9.1 and above

> SafeNet Trusted Access (earlier, SAS Cloud)

Authentication Protocols

The SafeNet Agent for NPS supports the following authentication protocols:

> PAP

> CHAP

> MS-CHAP-v2

The following restrictions apply when working in Challenge/Response mode:

> Tokens in Challenge/ Response mode are supported only for PAP.

> GrIDSure tokens are supported only for PAP and MS-CHAP-v2.
MS-CHAP-v2 requires SAS 3.9.1 or later.

NOTE: To use GrIDSure with the SafeNet Agent for NPS, the user must utilize an external GrIDSure Service (for example SafeNet Self Service Portal).

Push OTP

The SafeNet Agent for NPS supports the Push OTP function when working with MobilePASS+.

NOTES:

1. High Push OTP utilization can lower the authentication throughput in the NPS.
2. To use PUSH OTP, ensure that the NPS Agent Server can connect with the SafeNet PUSH Service. If you are using a proxy with the NPS Agent Server, add IP address of the SafeNet PUSH Service in the proxy.

Supported Environment

The SafeNet Agent for NPS supports Push OTP with the following components:

- **Authenticator**: MobilePASS+
- **Management Platform:** SAS PCE/SPE 3.9.1 and later

NOTE: Push OTP is not currently supported for SAS PCE/SPE.

Configuring RADIUS Client with Push OTP

When using Push OTP, we recommend the following settings in the RADIUS Client:

Multiple NPS servers (backup/ failover)	Timeout: 60 seconds Retries: 1
Single NPS server	Timeout: 20 seconds Retries: 3

Release Notes

The Customer Release Notes (CRN) document provides important information about this release that is not included in other customer documentation. It is strongly recommended that you read the CRN to fully understand the capabilities, limitations, and known issues for this release.

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet Agent for NPS users and security officers, the key manager administrators, and network administrators. It is assumed that the users of this document are proficient with security concepts.

All products manufactured and distributed by Thales are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

Document Conventions

This section describes the conventions used in this document.

Command Syntax and Typeface Conventions

This document uses the following conventions for command syntax descriptions, and to highlight elements of the user interface.

Convention	Description
bold	The bold attribute is used to indicate the following: > Command-line commands and options (Type **dir /p**.) > Button names (Click **Save As**.) > Check box and radio button names (Select the **Print Duplex** check box.) > Window titles (On the **Protect Document** window, click **Yes**.) > Field names (**User Name:** Enter the name of the user.) > Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) > User input (In the **Date** box, type **April 1**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
Double quote marks	Double quote marks enclose references to other sections within the document. For example: Refer to "**Error! Reference source not found.**" on page **Error! Bookmark not defined.**.
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>] [a | b | c] [<a> | <b> | <c>]	Square brackets enclose optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task. Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.
{ a | b | c } { <a> | <b> | <c> }	Braces enclose required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

Notifications and Alerts

Notifications and alerts are used to highlight important information or alert you to the potential for data loss or personal injury.

Tips

Tips are used to highlight information that helps to complete a task more efficiently.

> **TIP:** This is some information that will allow you to complete your task more efficiently.

Notes

Notes are used to highlight important or helpful information.

> **NOTE:** Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss.

> **CAUTION!** Exercise caution. Contains important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

> ****WARNING** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.**

Related Documents

The following document(s) contain related or additional information:

> SafeNet Agent for NPS v3.0.1: Customer Release Notes

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click the **REGISTER** link.

Telephone Support

The support portal also lists telephone numbers for voice contact (Contact Us).

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.

CHAPTER 1: Configuring Network Policy Service

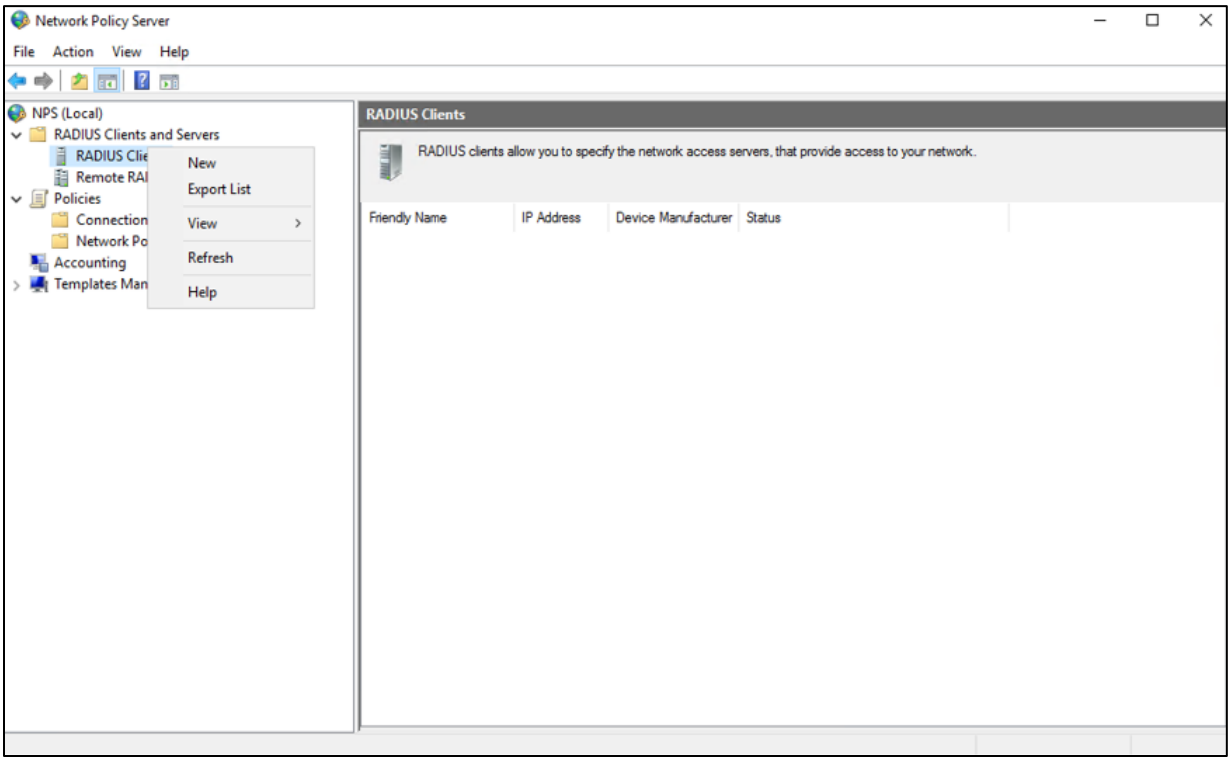
Configuring NPS for RADIUS Clients

RADIUS clients include any network access devices/ servers or software that requires authentication from the SafeNet server.

> **NOTE:** To work with SafeNet Agent for NPS, the **Network Policy and Access Services** role must first be added to Windows using the **Windows Server Manager**.
> Refer Microsoft documentation for details.

To configure SafeNet Agent for NPS for RADIUS clients:

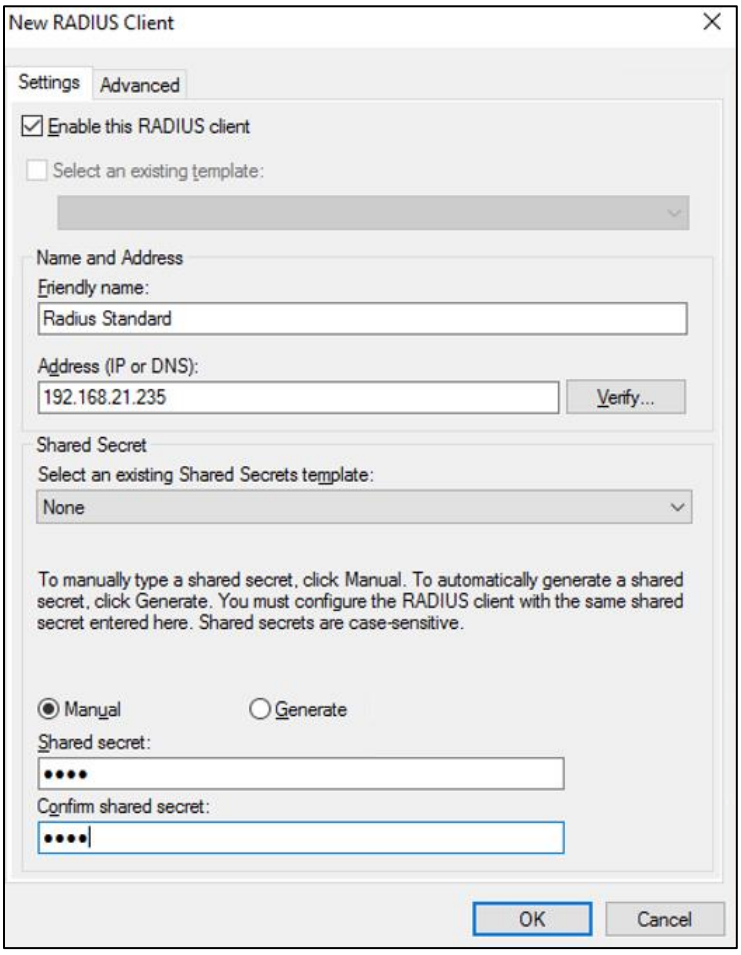
1. Select **Start > Administrative Tools > Network Policy Server.**
2. In the left pane:
   a. Double-click **RADIUS Clients and Servers**.
   b. Right-click **RADIUS Client** and select **New**.



(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

3. On the New RADIUS Client window, complete the following fields:

Enable this RADIUS Client	Select this check box.
Friendly name	Enter a name for the remote client (for example, **SSL VPN Authentication**).
Address (IP or DNS)	Enter the IP address of the remote client.
Vendor name	Select **RADIUS Standard**.
Shared Secret	Select **Manual** and enter the shared secret value.
Confirm shared secret	Re-enter the shared secret value to confirm.



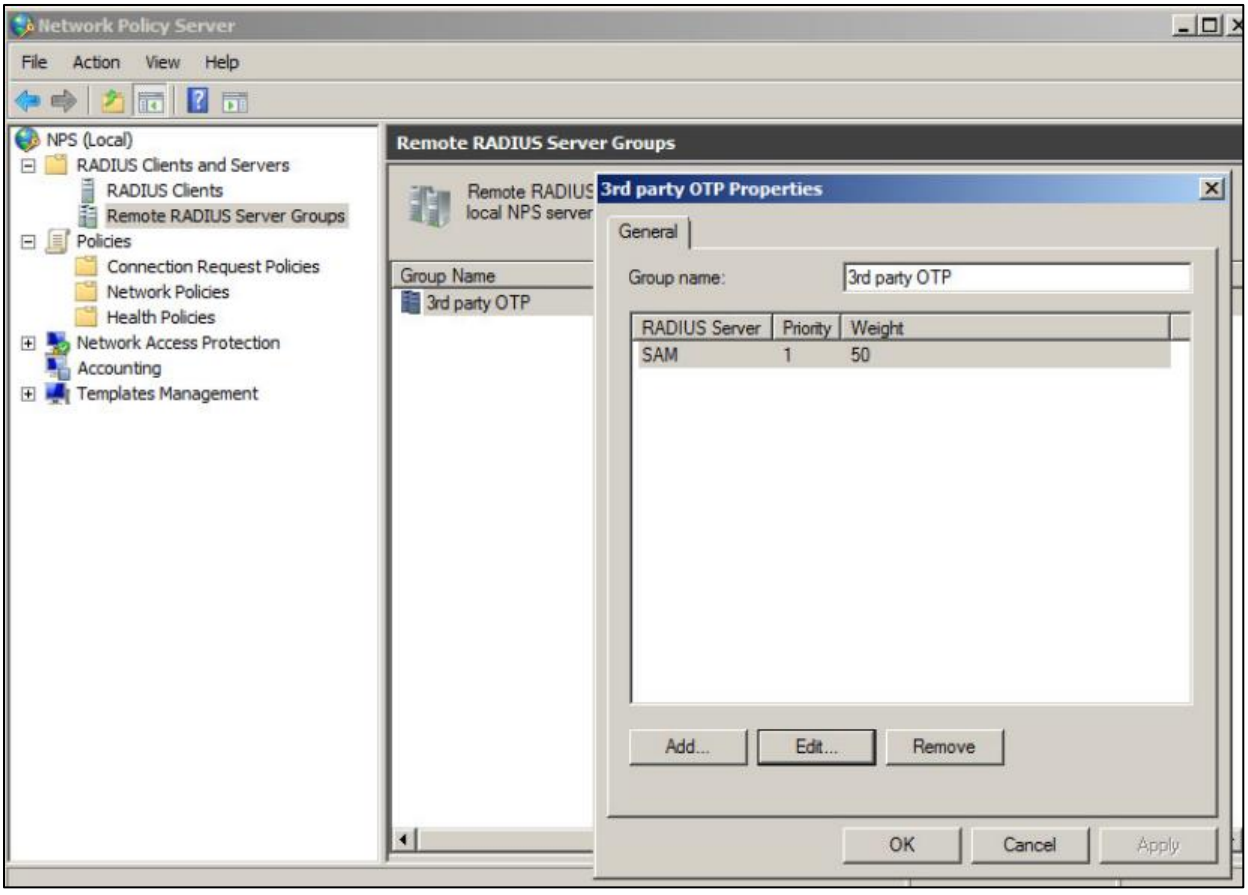
(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

4. Click **OK**.
5. Restart Network Policy Server.

Configuring NPS for Remote RADIUS Server Groups

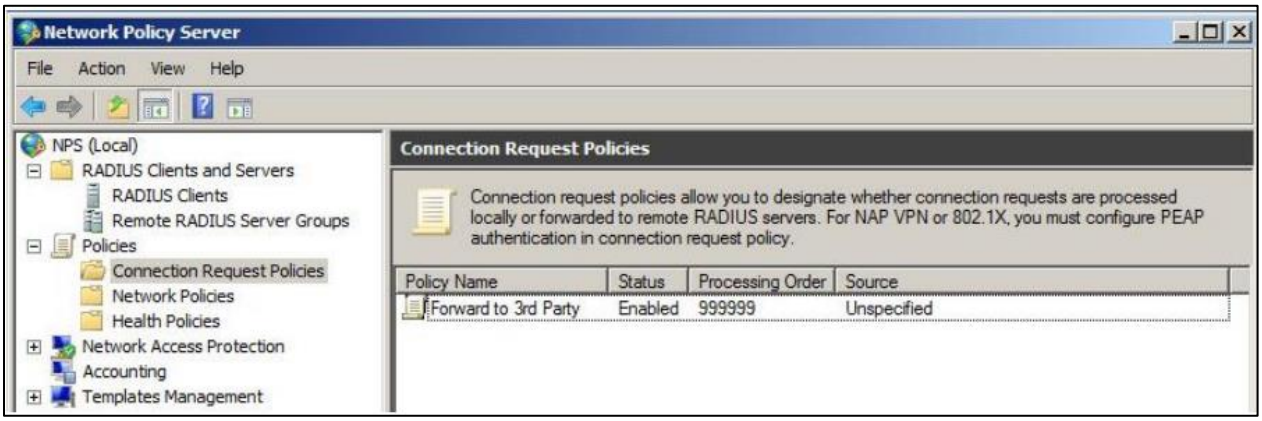
To configure SafeNet Agent for NPS for Remote RADIUS Server Groups:

1. Open the Network Policy Server (NPS) console.
2. In the left pane, double-click **RADIUS Clients and Servers,** right-click **Remote RADIUS Server Groups**, then click **New**.
   a. In the **Group name** box, type a name for the new RADIUS server group, then click **Add**.
   b. In the **Add RADIUS Server** dialog box, under **RADIUS Server**, enter your previous OTP solution as a RADIUS server.
   c. Click **OK** to save.
   d. Ensure that you add this NPS server as a RADIUS client on the previous OTP solution.

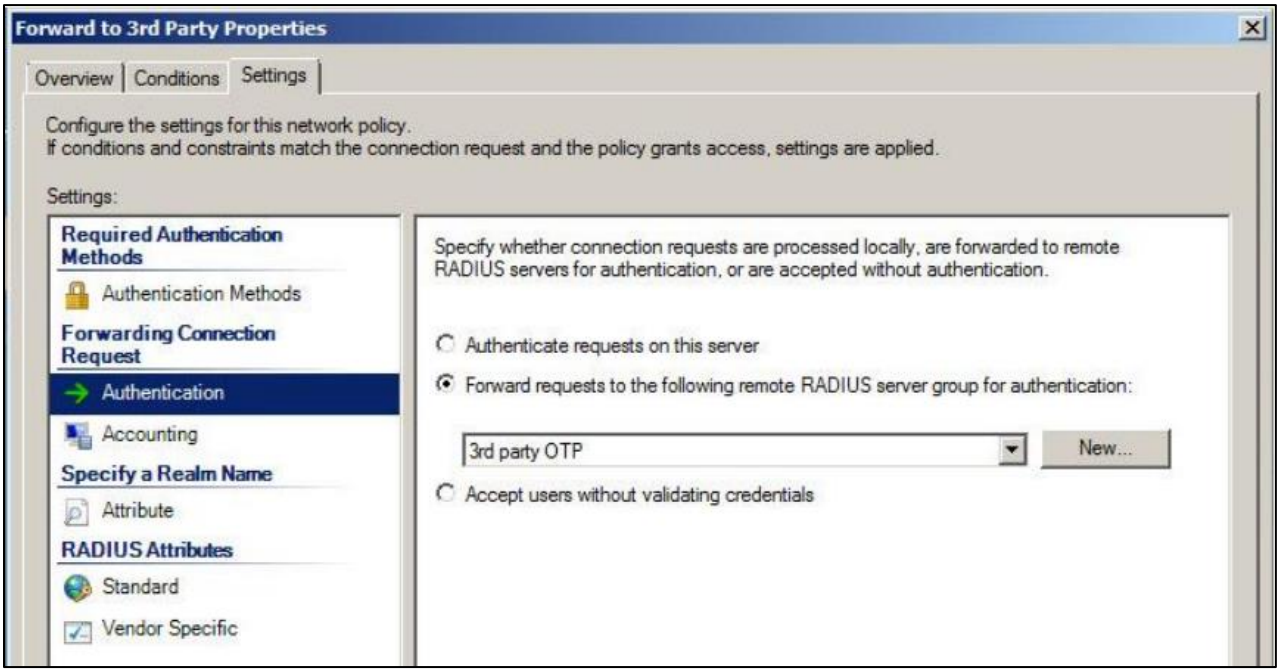


(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

3. In the left pane, under **Policies**, right-click **Connection Request Policies**, then click **New**.
   a. In the **Policy Name** box, type a name for the new policy.
   b. Create a policy that forwards connection requests to the newly created remote RADIUS server group for authentication.
   c. Click **OK** to save.

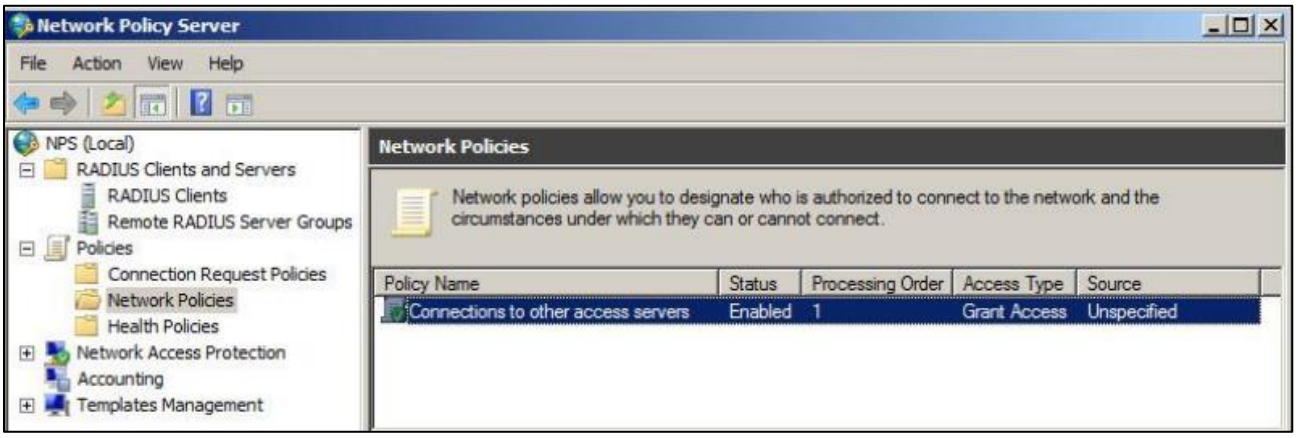


(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

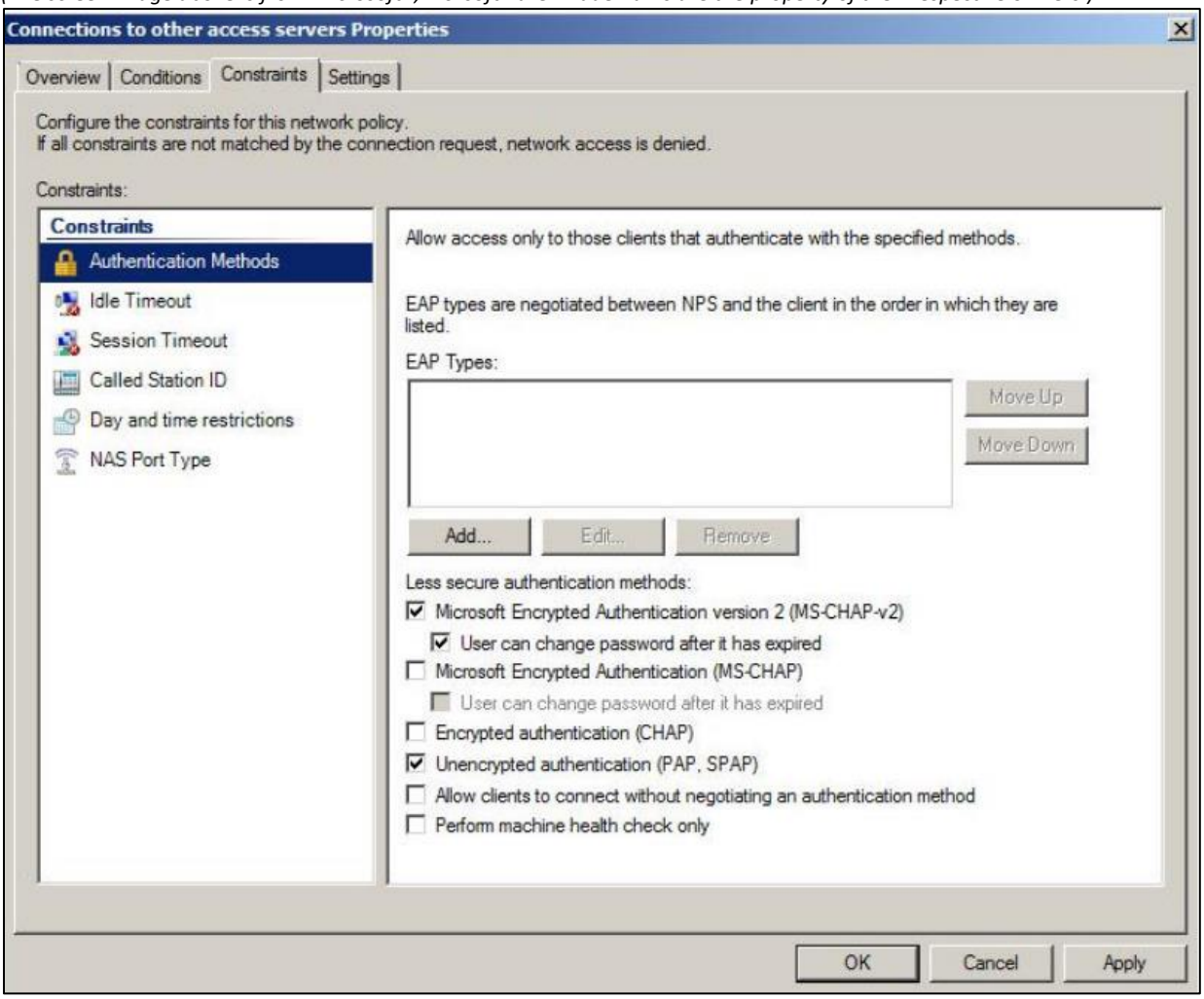


(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

4. In the left pane, under **Policies**, right-click **Network Policies**, then click **New**.
   a. In the **Policy Name** box, type a friendly name for the new policy.
   b. Complete the remaining fields as appropriate.
   c. Click **OK** to save.
   d. Right-click the new policy, then click **Edit**.
   e. Click the **Constraints** tab and select the **Unencrypted authentication (PAP, SPAP)** check box.
   f. Click **OK** to save.



(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)



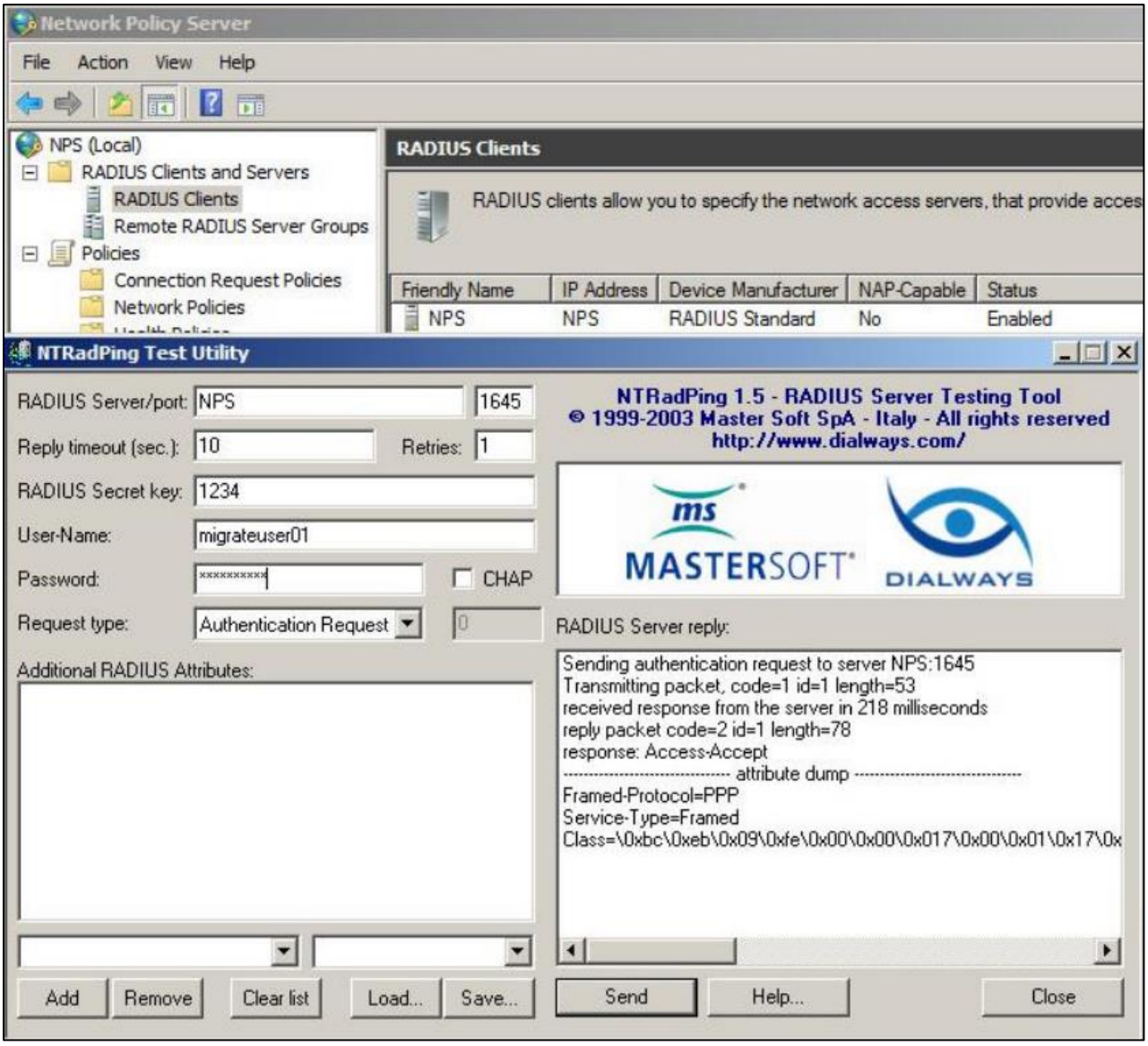
(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

5. On the NPS server, add your local machine and your VPN appliance as RADIUS clients.

> **NOTE:** Ensure that you enable the Migration Mode. To configure Exceptions in Migration Mode, please refer Configuring Exceptions for Migration Mode section.

6. Use a RADIUS client tool, such as NTRadPing, to authenticate against the local NPS.

NPS should forward the request to your previous OTP solution.

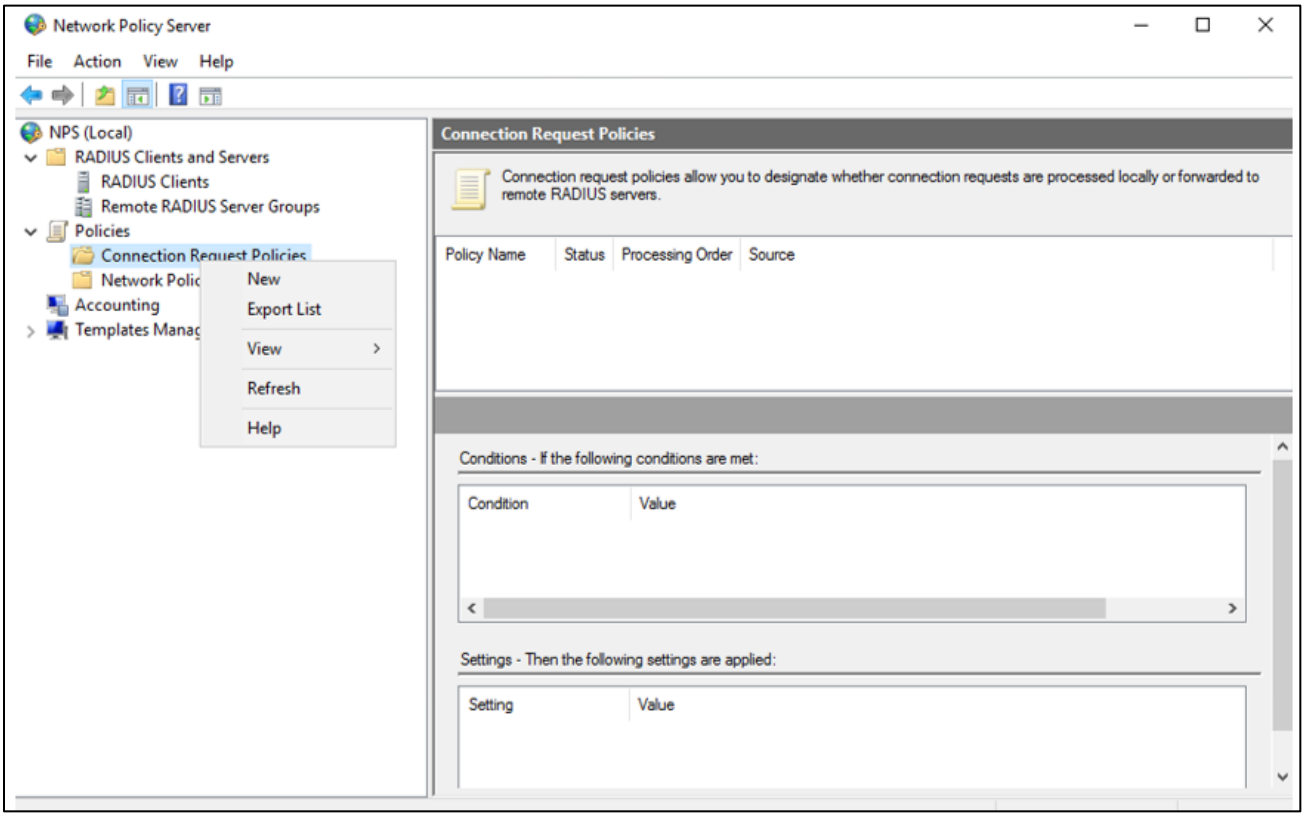


(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

Configuring NPS to use SafeNet Agent

To create a Connection Request Policy:

1. Select **Start > Administrative Tools > Network Policy Server**.

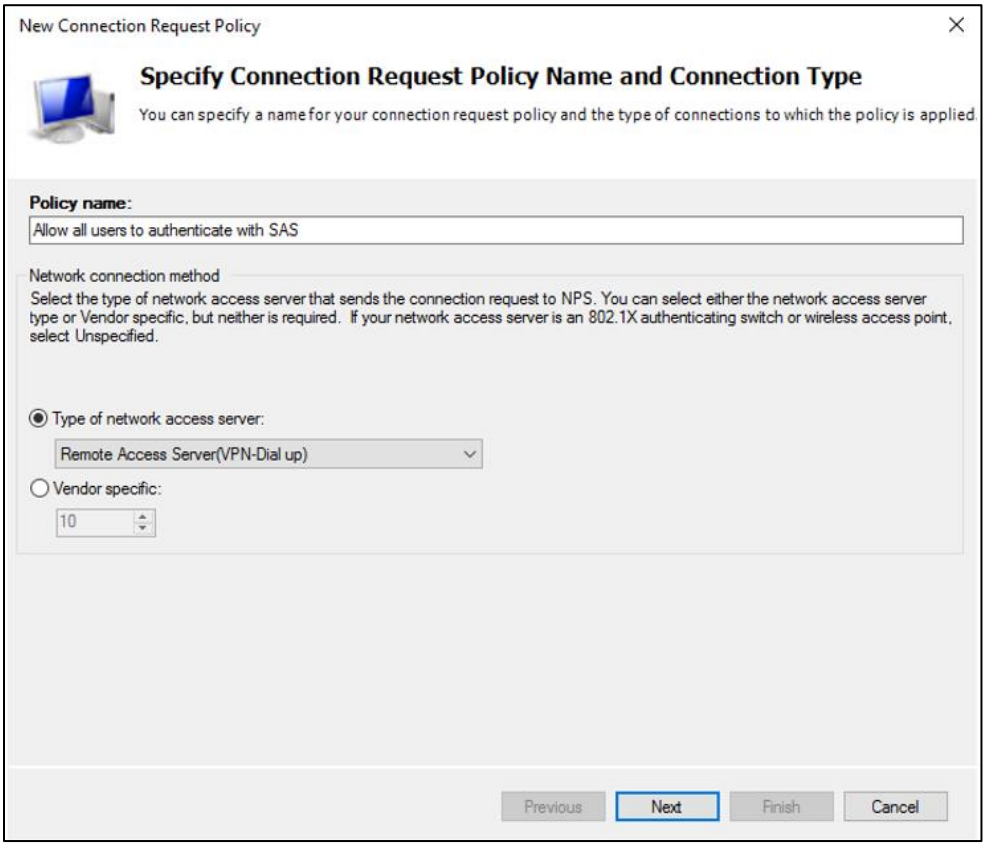


(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

2. In the left pane,
   a. Double-click **Policies**.
   b. Right-click **Connection Request Policies** and select **New**.

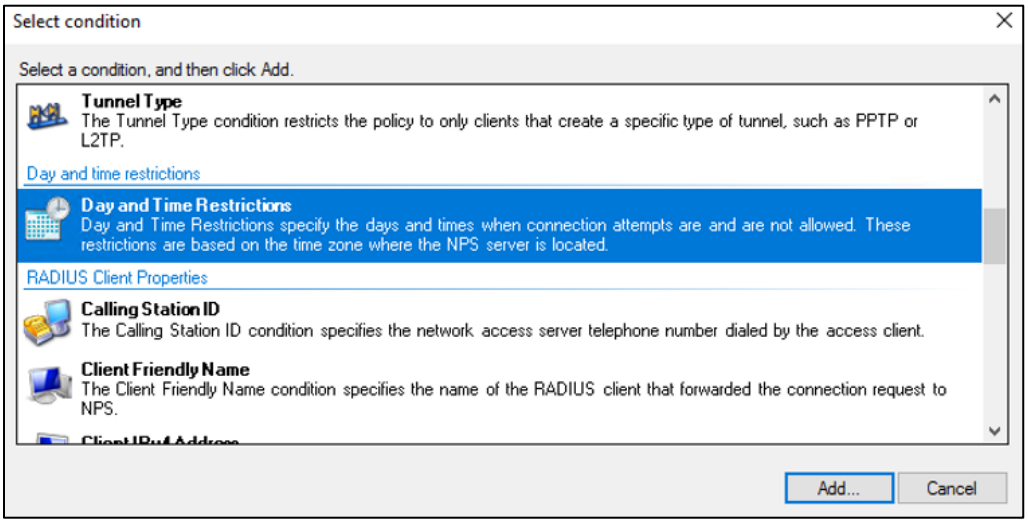
3. On the **New Connection Request Policy** window, complete the following fields and click **Next**:

Policy name	Enter a name for the policy. For example, **Allow all users to authenticate with SAS**.
Type of network access server	Select the required type of network server, from the drop-down list.



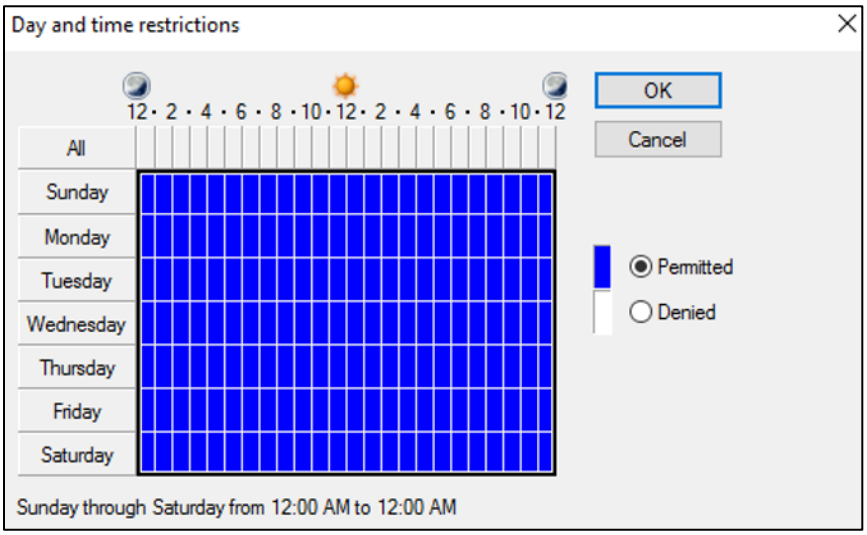
(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

4. On the **Select condition** window, select **Day and Time Restrictions** and click **Add**.



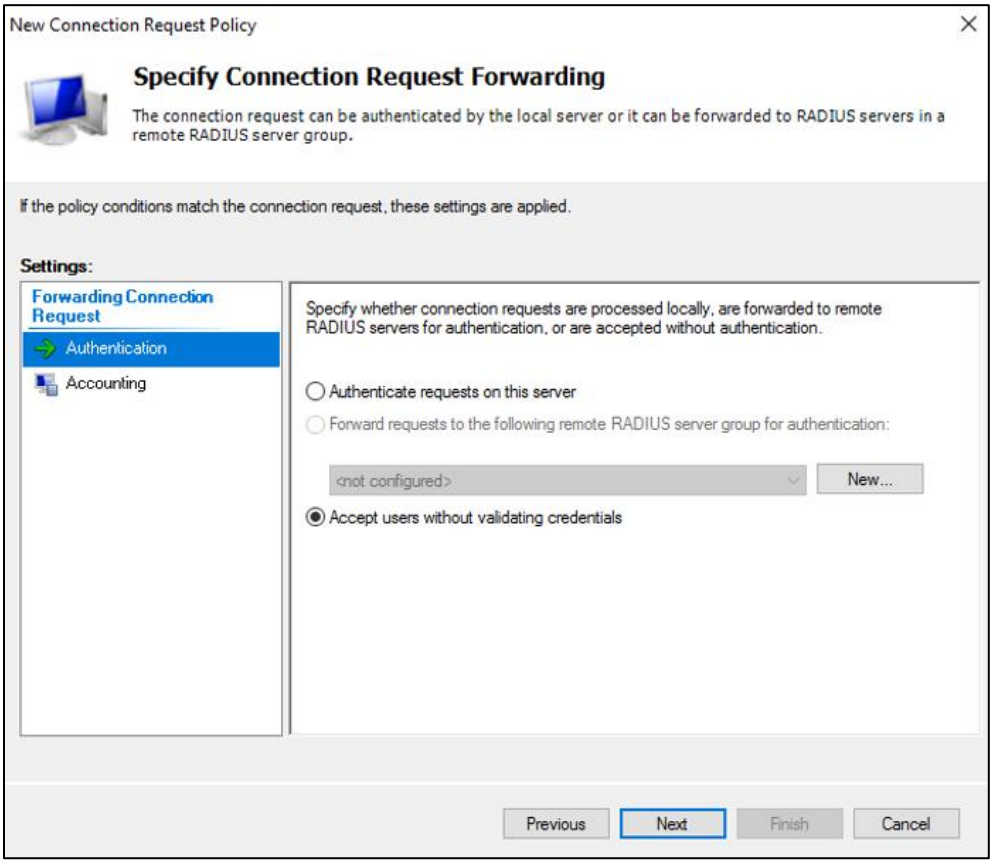
(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

5. On the **Day and time restrictions** window, select **Permitted** and click **OK**.



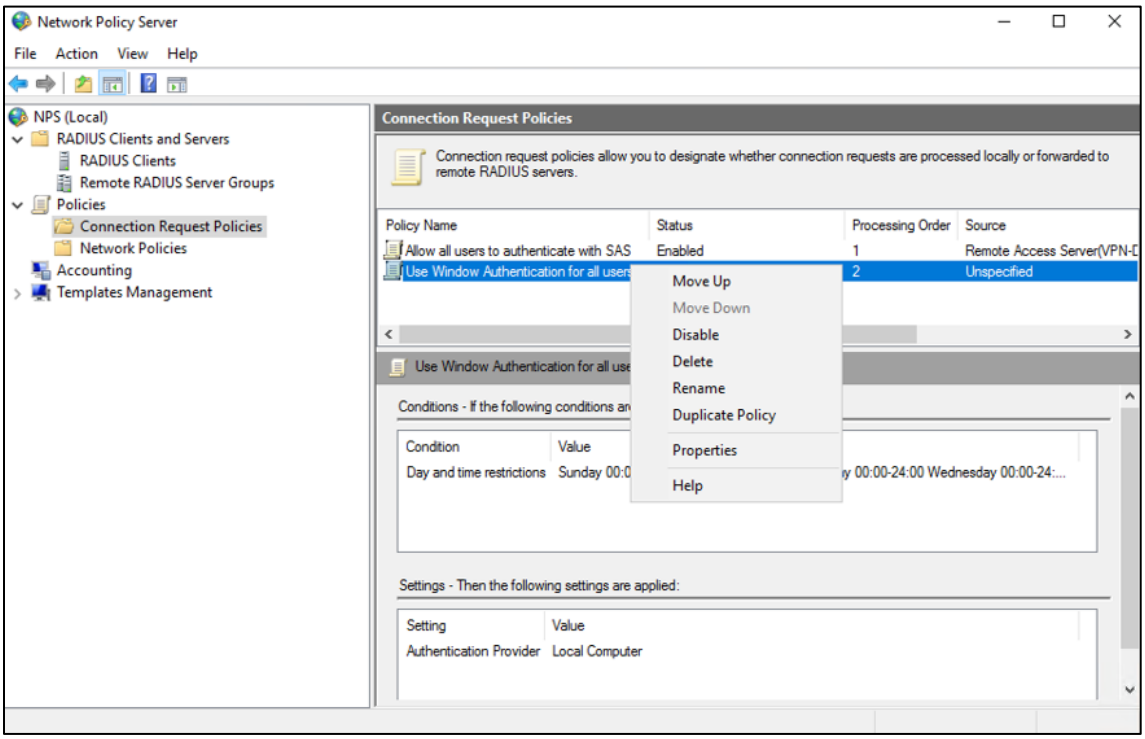
(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

6. On the **Specify Connection Request Forwarding** window, select **Accept users without validating credentials** and click **Next**. This setting will cause authentication requests to be intercepted by the SafeNet NPS Agent, and is required in order to allow the agent to function correctly.



(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

7. Click **Next** and then click **Finish**.
8. On the **Network Policy Server** window:
   a. In the left pane, select **Policies** > **Connection Request Policies**.
   b. In the right pane, right-click **Use Windows Authentication for all users** and select **Disable**.



(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

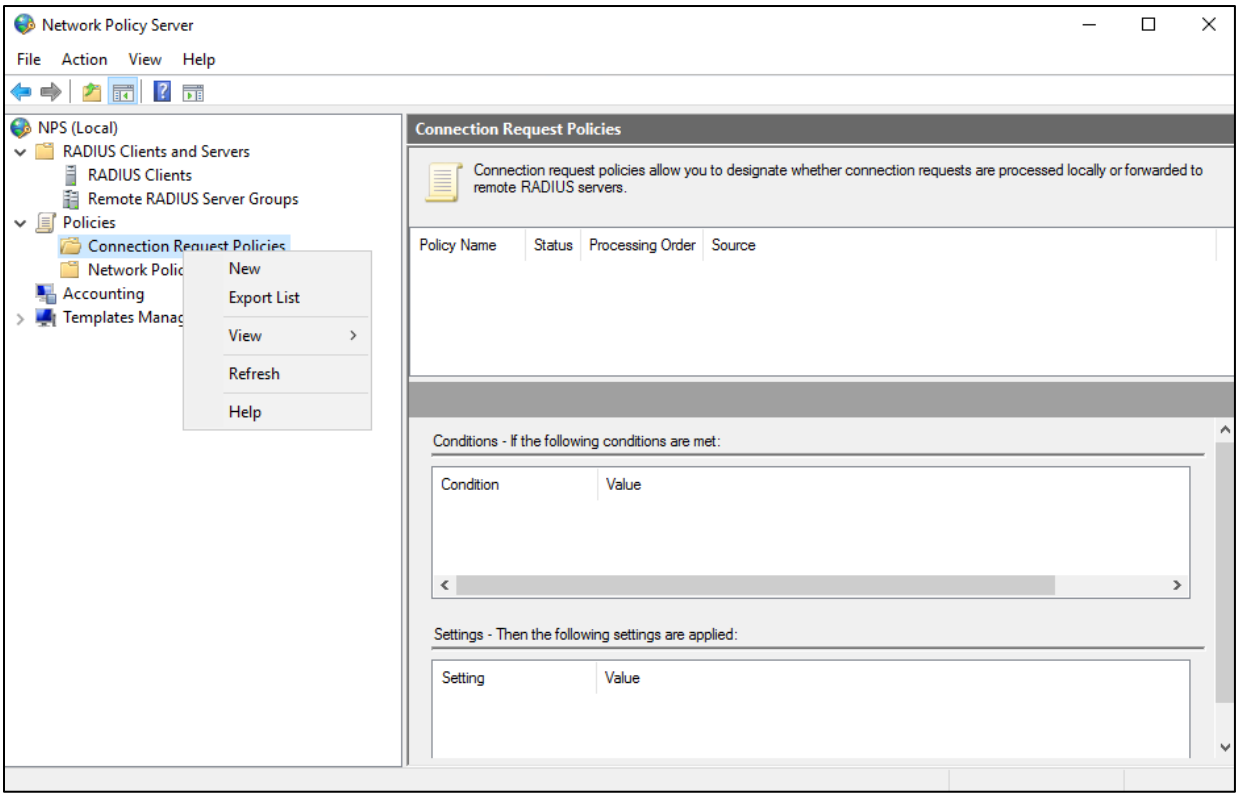
9. Close the window.

Configuring CRP to use Local Authentication

The Network Policy Server can be configured to authenticate the request on the local server.

To create a Connection Request Policy (CRP):

1. Select **Start > Administrative Tools > Network Policy Server**.

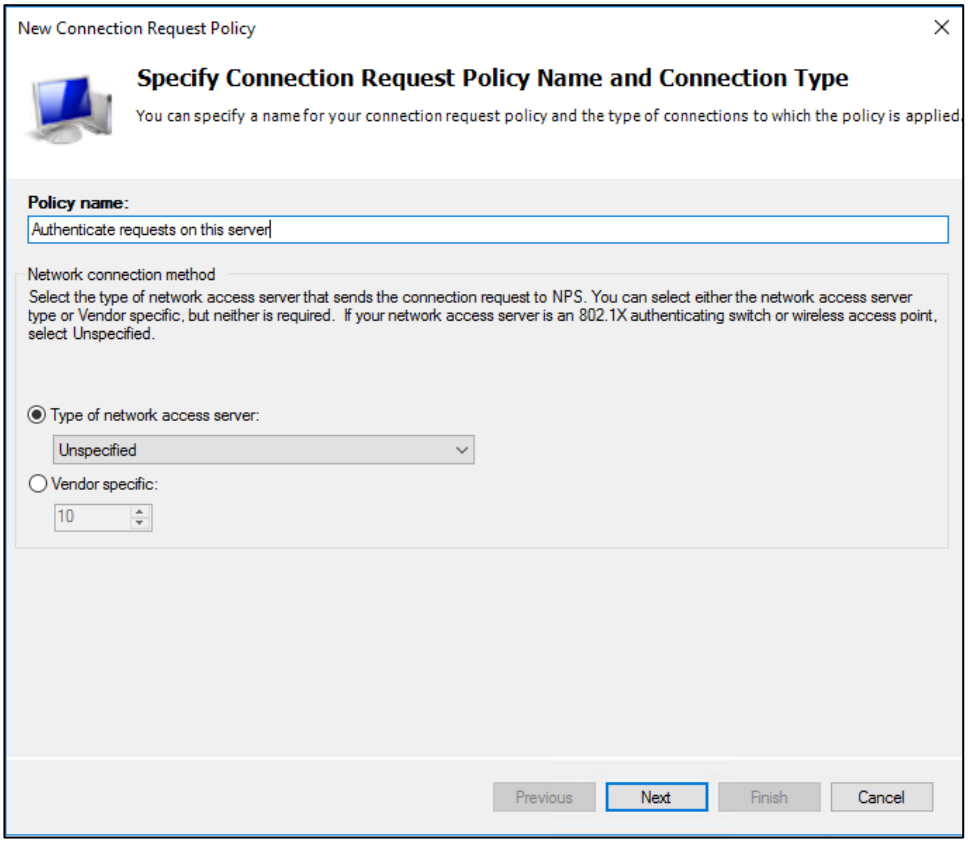


(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

2. In the left pane,
   a. Double-click **Policies**.
   b. Right-click **Connection Request Policies** and select **New**.

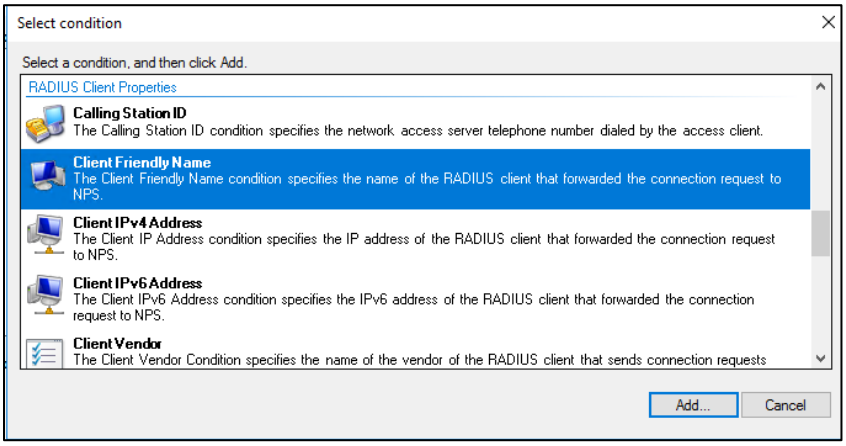
3. On the **New Connection Request Policy** window, complete the following fields and click **Next**:

Policy name	Enter a name for the policy. For example, **Authenticate requests on this server**
Type of network access server	Select *Unspecified* from the drop-down list.



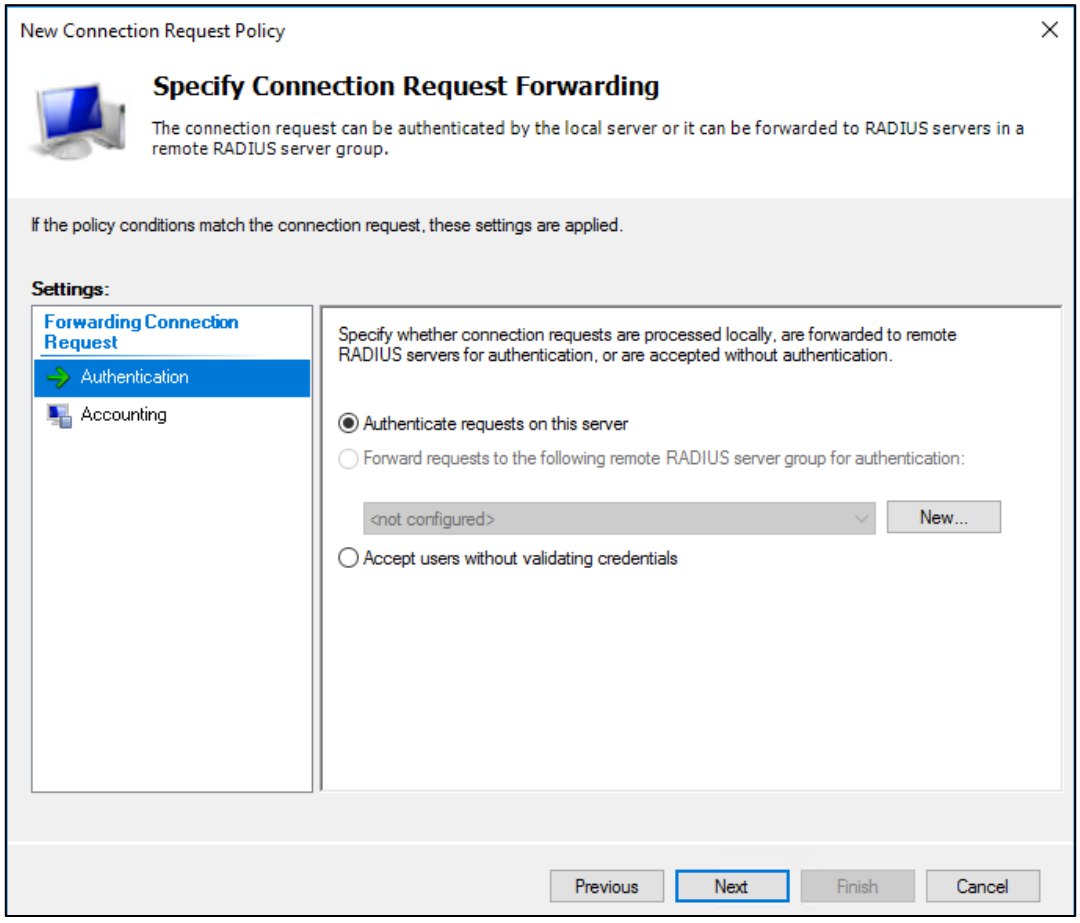
(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

4. On the **Select condition** window, select the conditions to uniquely identify the Connection Request Policy like User Name, Client IPv4 Address, Client Friendly Name, and so on. Click **Add**.



(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

5. On the **Specify Connection Request Forwarding** window, select **Authenticate requests on this server** and click **Next**.



(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

6. Click **Next** and then click **Finish**.

NOTE: To enforce the SafeNet authentication for the above policy, modify the registry key **SendAuthRequestOnThisServertoSAS** at **`HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\AuthRadius`** to **0**.

CHAPTER 2: Installing and Upgrading SafeNet Agent for NPS

Important: Log onto Windows as an administrator and run the installer as an administrator when installing or upgrading the SafeNet Agent for NPS.

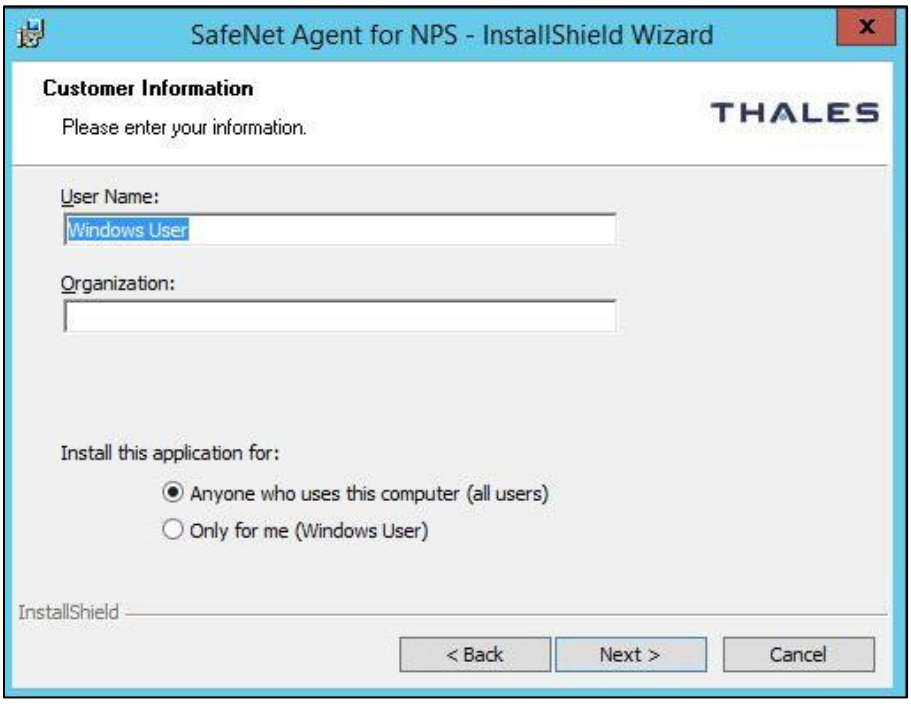
Installing SafeNet Agent for NPS

To install the SafeNet Agent for NPS:

1. Log on to the server on which the SafeNet Agent for NPS is installed.
2. Locate and run the applicable installer:
   SafeNet Agent for NPS (for 64-bit servers)
3. On the **Welcome to the InstallShield Wizard…** window, click **Next**.

4. On the **License Agreement** window, select **I accept the terms of the license agreement** and click **Next.**

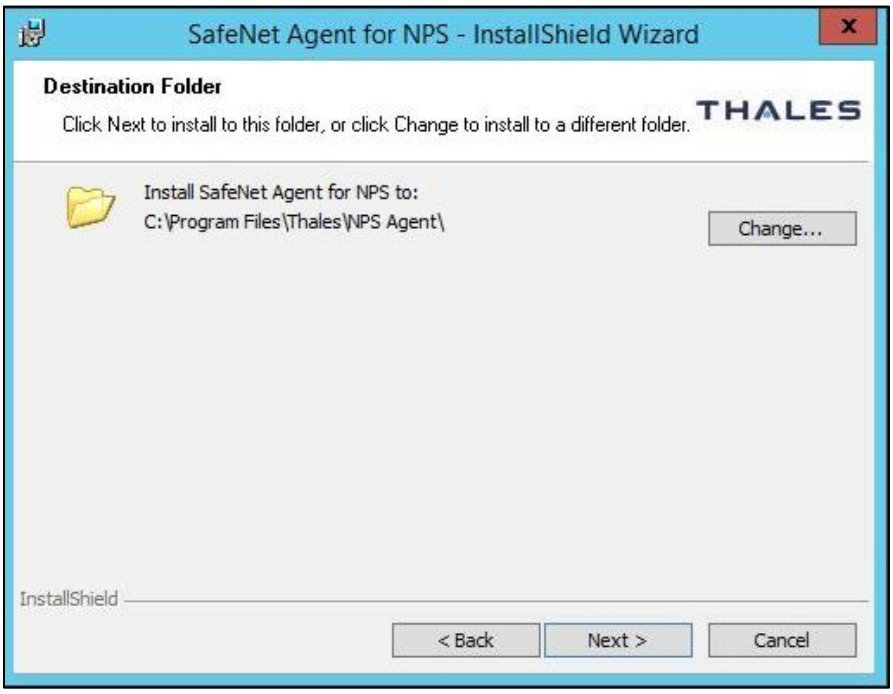
5. On the **Customer Information** window, enter **User Name** and **Organization** (any names can be used) and click **Next**.



6. On the **Destination Folder** window, perform one of the following steps:

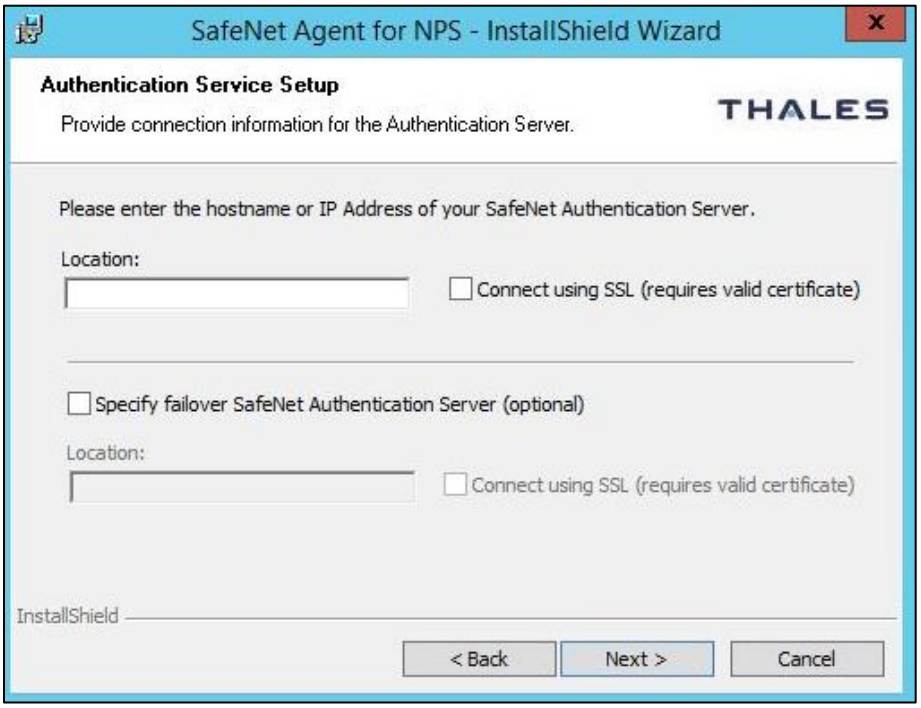
> To change the installation folder, click **Change** and navigate to the required folder, and click **Next**.

> To accept the default installation folder as displayed, click **Next**.

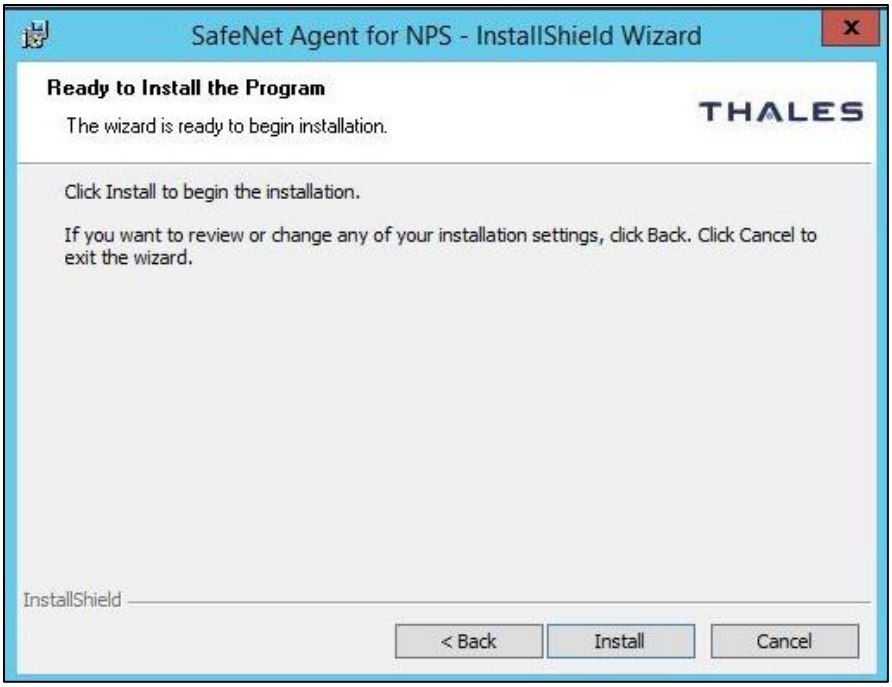


7. On the **Authentication Service Setup** window, complete the following fields and click **Next**:

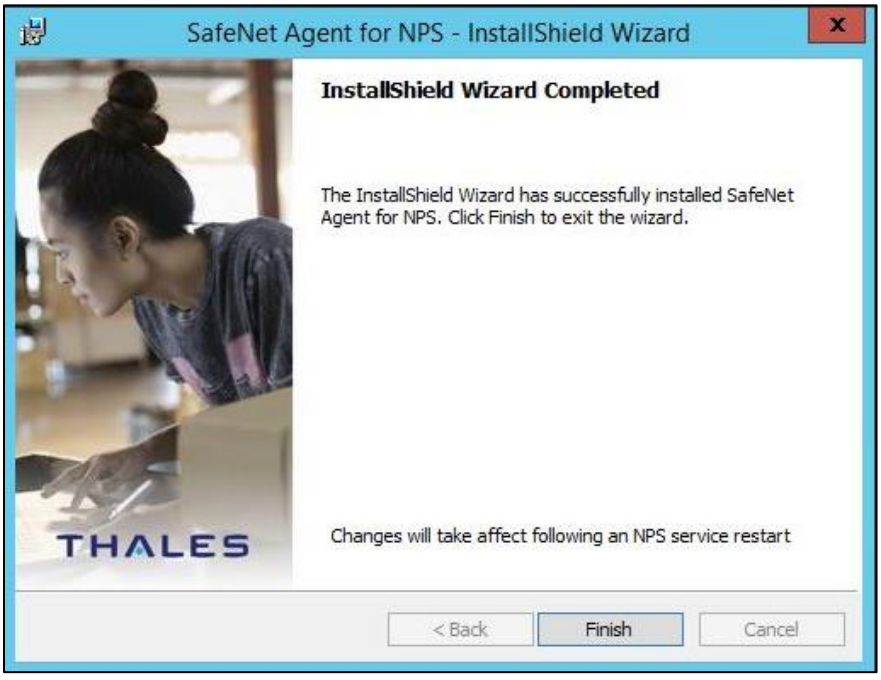
Location	Enter the hostname or IP address of the primary SafeNet server.
Connect using SSL (requires valid certificate)	Select to use the SSL/TLS v1.2. This option requires installation of a valid certificate on the NPS server.
Specify failover SafeNet Authentication Server (optional)	Select if a failover SafeNet server is available.
Location	Add the hostname or IP address of the failover SafeNet server.



8. On the **Ready to Install the Program** window, click **Install**.



9. Once the installation is completed, the **InstallShield Wizard Completed** window is displayed. Click **Finish** to exit the installation wizard.



Upgrading SafeNet Agent for NPS

The SafeNet Agent for NPS **v3.0.1** supports upgrade from **v2.0** onwards.

> **NOTE:** Upgrade is not supported on Windows Server 2019.

Upgrade from versions earlier than 2.0 is not supported.

> **NOTES:**
>
> - Close the **SafeNet Agent Management Console (earlier, SAS - NPS Configuration)** window before the upgrade.
> - Stop the **Network Policy Server** service prior to the upgrade.

To upgrade to SafeNet Agent for NPS 3.0.1 from version 2.0 onwards, run the SafeNet Agent for NPS 3.0.1 installation wizard (**SafeNet Agent for NPS**).

CHAPTER 3: Configuring SafeNet Server for RADIUS Return Attributes

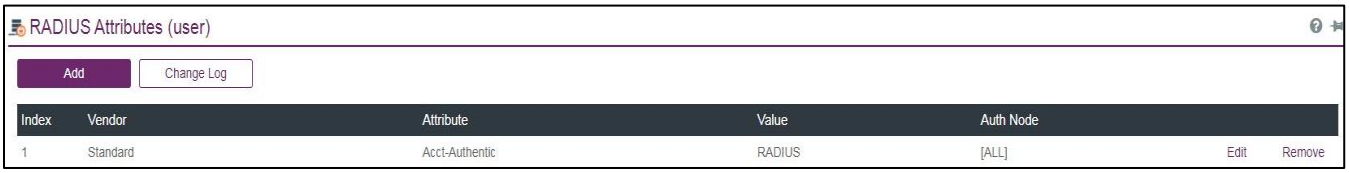
To work with RADIUS Return Attributes, complete the following tasks:

- Add the required SafeNet Server RADIUS Return Attributes (See **Adding SafeNet Server RADIUS Return Attributes**).
- Block authentication without SafeNet Server RADIUS Return Attributes (See **Configuring SafeNet Server**).

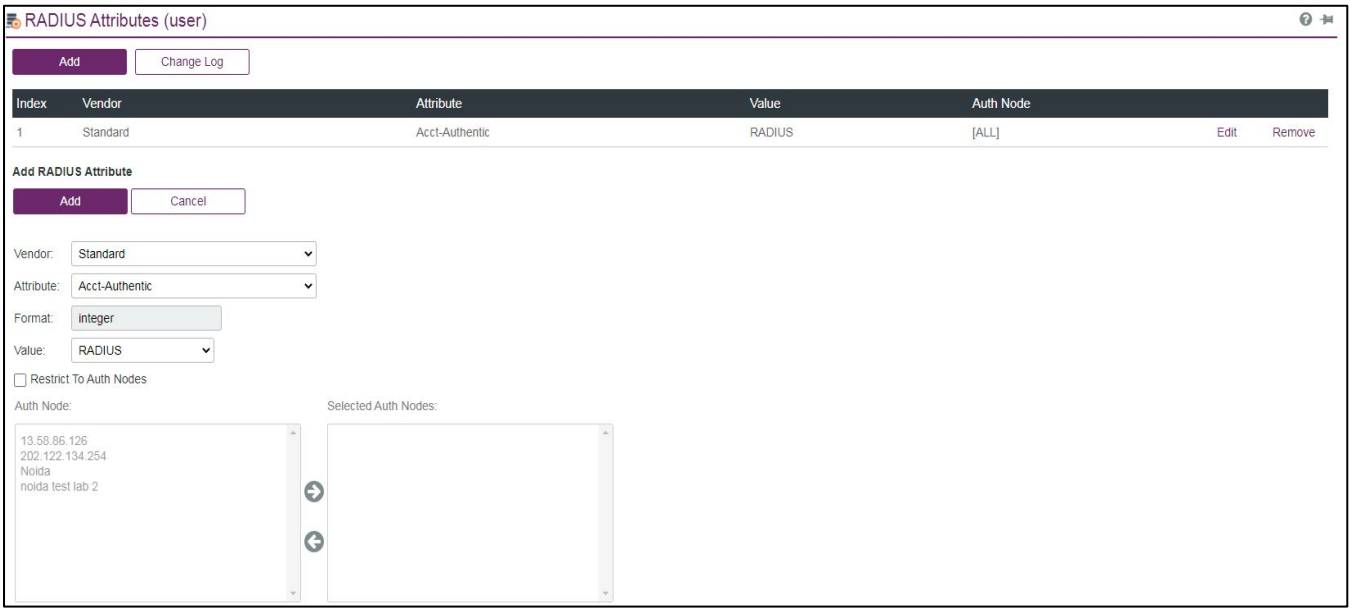
Adding SafeNet Server RADIUS Return Attributes

To add the required SafeNet Server RADIUS Return Attributes, perform the following steps:

1. In **SafeNet Server Management Console**, select **Virtual Servers > Assignment > Radius Attributes (user)**.



2. Click **Add**.



3. Enter the following fields:

Vendor	Select the RADIUS Client provider.
Attribute	Select the required attribute. The range of available attributes varies according to the vendor.
Format	Select appropriate format (For example, integer, sting, date, IP, string).
Value	Select a value for the attribute.

4. To restrict attributes to specific auth nodes, complete the following steps:
   a. Select **Restrict To Auth Nodes**.
   b. In the **Auth Node** box, select required Auth Nodes.
   c. Click the right arrow to move the selected Auth Nodes to the **Selected Auth Nodes** box.

NOTE: If the RADIUS Return Attribute is configured for **[ALL]** auth nodes, define at least one Auth Node in the SafeNet Server environment. If you are setting up with a specific Auth Node, it must be defined first, and then used.

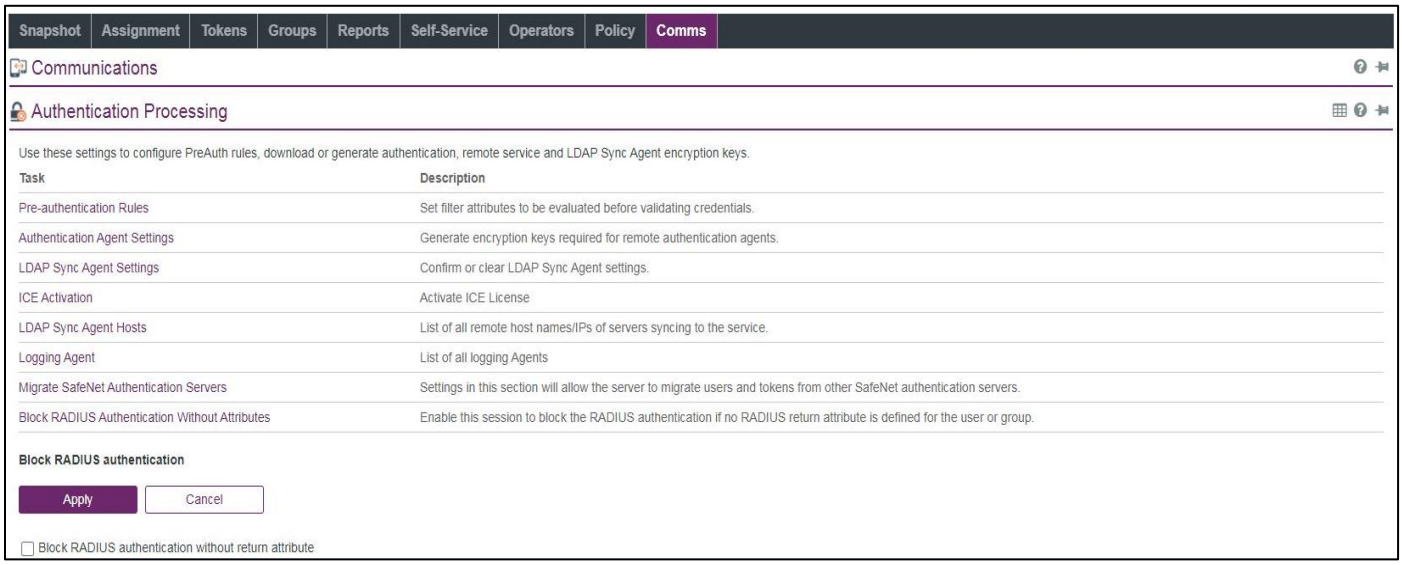
Configuring SafeNet Server

You can configure SafeNet Server to block authentication if RADIUS Return Attributes are not configured in the SafeNet Server.

To block RADIUS authentication without attributes, perform the following steps:

1. In **SafeNet Server Management Console**, navigate to **Virtual Servers > Comms.**
2. To enforce the use of SafeNet Server RADIUS Return Attributes, click **Block RADIUS Authentication Without Attributes** option (from the **Task** list) and click **Apply**.

NOTES:
If **Block RADIUS Authentication without Attributes** is selected, you must also complete the following actions, otherwise the authentication will fail.
>In **SafeNet Server Management Console**, configure **SafeNet Server RADIUS Return Attributes** (see **Adding SafeNet Server RADIUS Return Attributes**).
>In **SafeNet Agent Management Console** (earlier, SAS NPS Configuration Management), **NPS Settings** tab, select **SafeNet Server RADIUS Return Attributes Enabled** (see **Configuring NPS Settings**).


Snapshot
Assignment
Tokens
Groups
Reports
Self-Service
Operators
Policy
Comms
Communications
Authentication Processing
Use these settings to configure PreAuth rules, download or generate authentication, remote service and LDAP Sync Agent encryption keys.
Task
Description
Pre-authentication Rules
Set filter attributes to be evaluated before validating credentials.
Authentication Agent Settings
Generate encryption keys required for remote authentication agents.
LDAP Sync Agent Settings
Confirm or clear LDAP Sync Agent settings.
ICE Activation
Activate ICE License
LDAP Sync Agent Hosts
List of all remote host names/IPs of servers syncing to the service.
Logging Agent
List of all logging Agents
Migrate SafeNet Authentication Servers
Settings in this section will allow the server to migrate users and tokens from other SafeNet authentication servers.
Block RADIUS Authentication Without Attributes
Enable this session to block the RADIUS authentication if no RADIUS return attribute is defined for the user or group.
Block RADIUS authentication
Apply
Cancel
Block RADIUS authentication without return attribute

CHAPTER 4: Transferring Configuration Settings (Export/ Import)

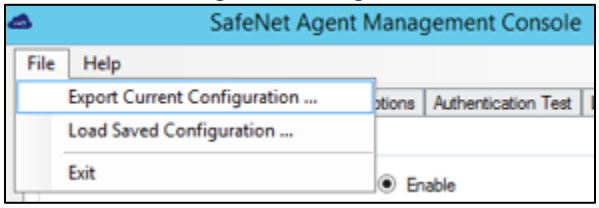
If reinstalling SafeNet Agent for NPS 3.0.1, you can export the configuration from the previous installation and import into the reinstalled application.

You cannot import settings from a version of SafeNet Agent for NPS previous to version 2.0.

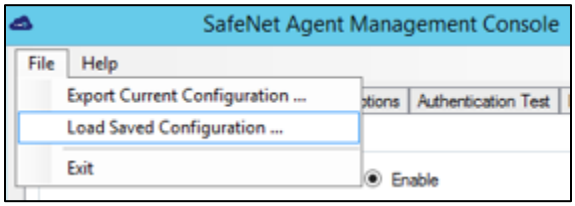
NOTES:
> Always work in **Run as administrator** mode when installing, uninstalling, enabling, or disabling the SafeNet Agent for NPS.
> The Export/ Import procedure can be performed only to and from the folder where the previous version of the SafeNet Agent for NPS was installed.

To reinstall the SafeNet Agent for NPS 3.0.1 and import configuration settings, perform the following steps:

1. In the installed SafeNet Agent for NPS, export the configurations as follows:
   a. In the **SafeNet Agent Management Console** window, select **File > Export Current Configuration**.

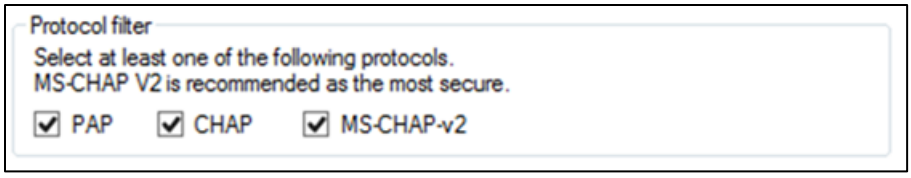


   b. In the **Save As** window, click **Save** to save the configuration file.
2. Uninstall SafeNet Agent for NPS.
3. Manually delete the **NPS** folder (located at **Program Files > SafeNet**).
4. To reinstall SafeNet Agent for NPS, run the installation file, **SafeNet Agent for NPSx64.exe** as an administrator. (See **Installing SafeNet Agent** section)
5. In the newly installed SafeNet Agent for NPS, load the saved settings as follows:
   a. In the **SafeNet Agent Management Console** window, select **File > Load Saved Configuration**.



   b. In the **Open** window, select the saved configuration file (.**bsidconfig**) and click **Open**.

6. Ensure that the selected protocols, in the **NPS Settings** tab, are the same as in the previous installation:



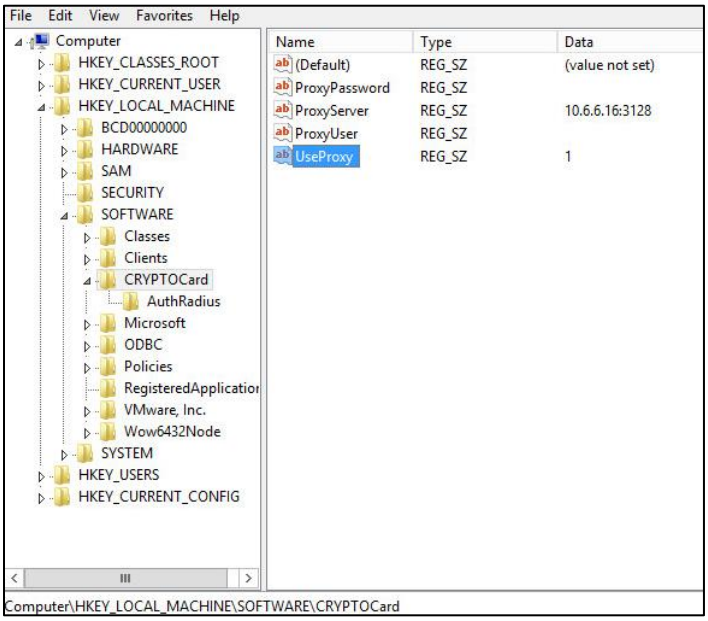
7. Enable **SafeNet Agent for NPS** in the **SafeNet Agent Management Console** window.

NOTES:
After installing **SafeNet Agent for NPS 3.0.1**, the SSL server certificate check is disabled by default.
To change the setting, go to **SafeNet Agent Management Console** > **Communications Tab** > **Authentication Server Settings**, and clear **Disable SSL server certificate check**.

CHAPTER 5: Configuring SafeNet Authentication Service Agent to use Proxy Server

To support the use of a proxy server, create the following new registry keys at **HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard**

Name	Type	Data
ProxyPassword	Reg_SZ	The proxy server password (if required).
ProxyServer	Reg_SZ	The IP address of the proxy server (compulsory).
ProxyUser	Reg_SZ	The proxy server user name (if required).
UseProxy	Reg_SZ	1 – use proxy server 0 – do not use proxy server



NOTE: Restart the NPS service, after adding/editing any registry keys.

CHAPTER 6: Configuring SafeNet Agent for NPS

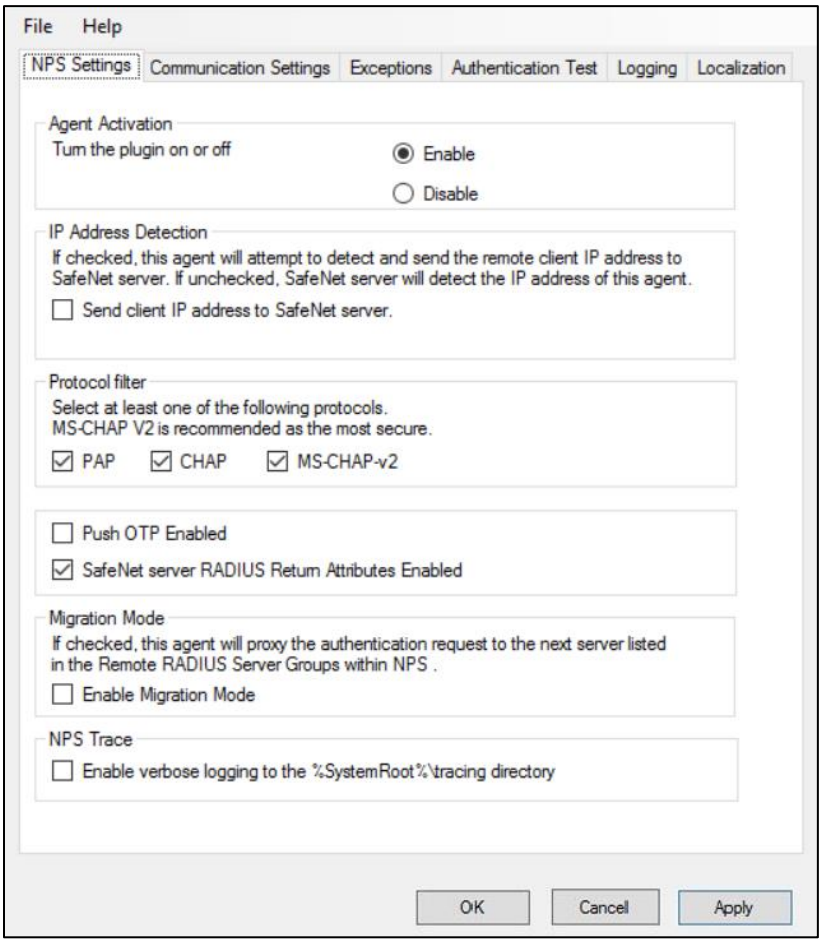
To launch **SafeNet Agent Management Console**: Select **Start > All Programs > SafeNet > NPS Agent Manager**.

> **Important:** Run **SafeNet Agent Management Console** as an administrator when configuring the SafeNet Agent for NPS.

Configuring NPS Settings

To configure NPS settings, perform the following steps:

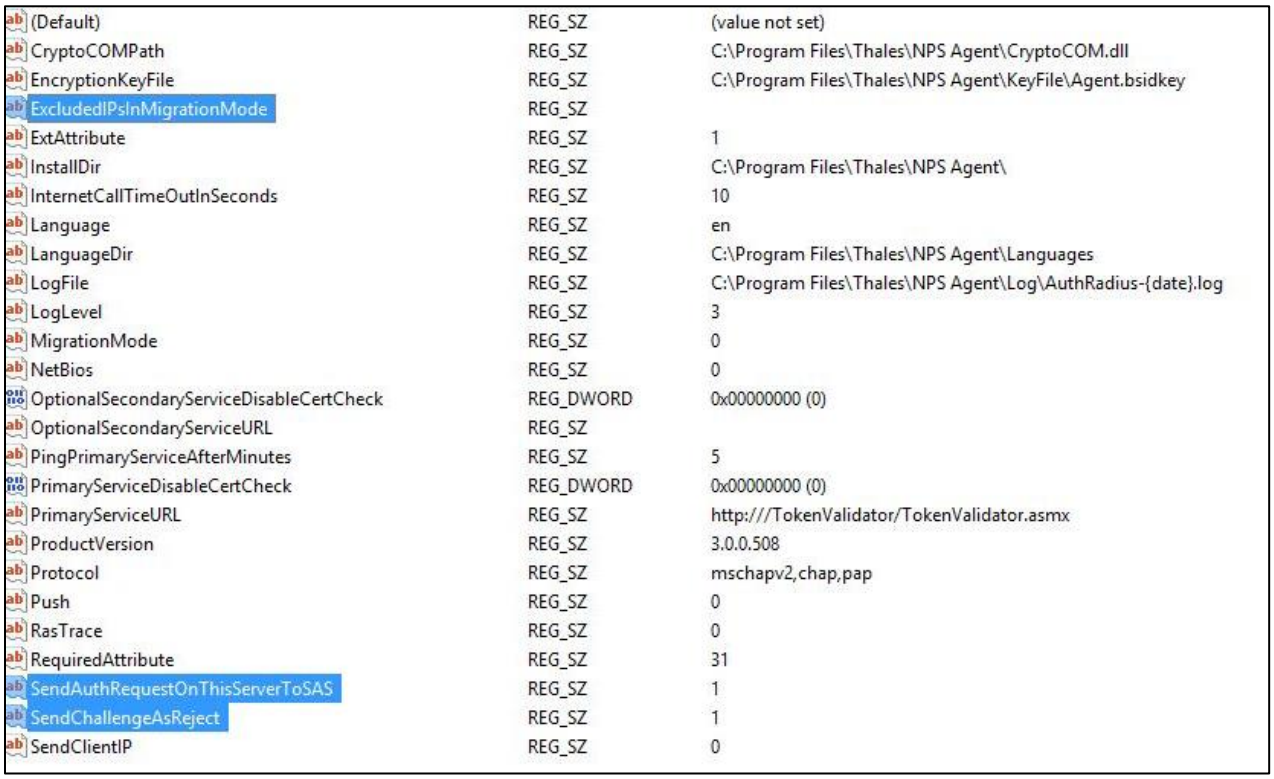
1. Select **NPS Settings** tab.



2. To activate the agent, select **Enable** for **Turn the plugin on or off** option.

3. To activate the feature to detect and send the remote client IP address to SafeNet server:
   a. Select **Send client IP address to SafeNet server**.
   b. Modify the following registry keys at **`HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\AuthRadius`**

Name	Type	Data
RequiredAttribute	Reg_SZ	265
SendClientIP	Reg_SZ	1 – will use the Required Attribute data settings



4. Select at least one of the authentication protocols.
   > PAP
   > CHAP
   > MS-CHAP v2

   NOTE: We recommend using MS-CHAP v2, the most secure option.

5. To enable OTP Push, select **Push OTP Enabled**.

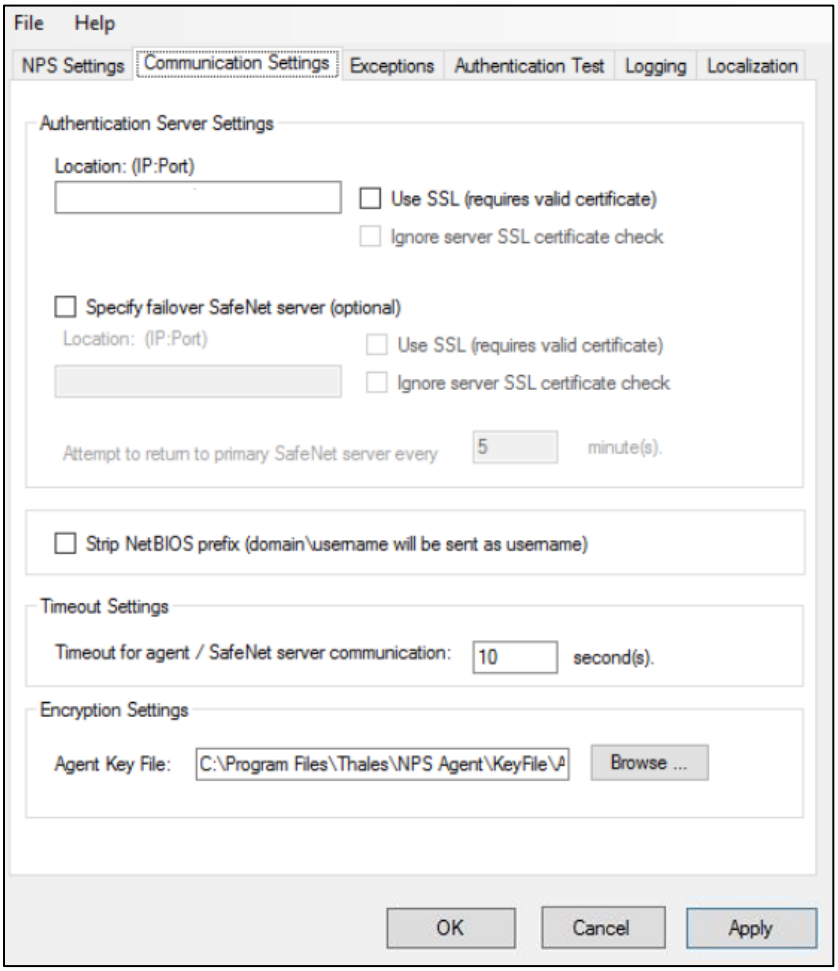
6. To enable SafeNet Server RADIUS return attributes, select **SafeNet server RADIUS Return Attributes Enabled** (selected by default).
7. To allow users to proxy the authentication request to the next server listed in the Remote RADIUS Server Groups within NPS, select **Enable Migration Mode**.
8. To enable detailed logging, select **Enable verbose logging to the %SystemRoot%\ tracing directory**.
9. Click **Apply**.
10. Restart Network Policy Server.

Configuring Communication Settings

NOTE: To set the encryption settings, the **Agent Key File** must be downloaded from the SafeNet Agent Management Console. Ensure that the **Agent Key File** is secured on your file system in a system-protected folder, accessible only to privileged accounts.

To configure communication settings, perform the following steps:

1. Select **Communication Settings** tab.



2. In the **Location (IP:Port)** field, enter the SafeNet server name.

3. Select one of the following options:
   - **Use SSL (requires valid certificate)** – SSL must be used.
   - **Ignore server SSL certificate check** – SSL is not required.

   NOTE: The use of SSL certificates is strongly recommended.

4. If a failover SafeNet server is required, select **Specify failover SafeNet server (optional)** and complete the following steps:
   a. In the **Location (IP:Port)** field, enter the SafeNet server name.
   b. Select one of the following options:
      – **Use SSL (requires valid certificate)** – SSL must be used.
      – **Ignore server SSL certificate check** – SSL is not required.
   c. In the **Attempt to return to primary server every** field, enter the number of minutes required between each attempt to return to the primary server.
5. In the **Strip NetBIOS prefix (domain\username will be sent as username)** field, select if the SafeNet server username is required without the prefix **domain**.

   NOTE: The realm-stripping feature applies to SafeNet server usernames only. Active Directory usernames are not affected.

6. In the **Timeout for agent / SafeNet server communication** field, enter the maximum timeout (in seconds) for each authentication attempt. For example: If a maximum timeout of 10 seconds is entered, and the authentication response takes longer than 10 seconds, the system will timeout.
7. In the **Agent Key File** field, click **Browse** and navigate to the file.

   NOTE:
   - It is strongly recommended to use the default location for the **Agent Key File**, to avoid possible errors. If you need to use a new **Agent Key File**, replace it at the default location.
   - To use the **AES-GCM** key standard, the administrator needs to download a new *Agent.bsidkey* file from SafeNet server, and update the same (in the agent) at **Configuration Management** > **Communications** > **Agent Encryption Key File**. To download the *Agent.bsidkey* file, follow the steps:
     1. Login to your SafeNet server account, and navigate to **COMMS** > **Authentication Processing**.
     2. Under **Task** list, click **Authentication Agent Settings** link and download the *Agent.bsidkey* file.

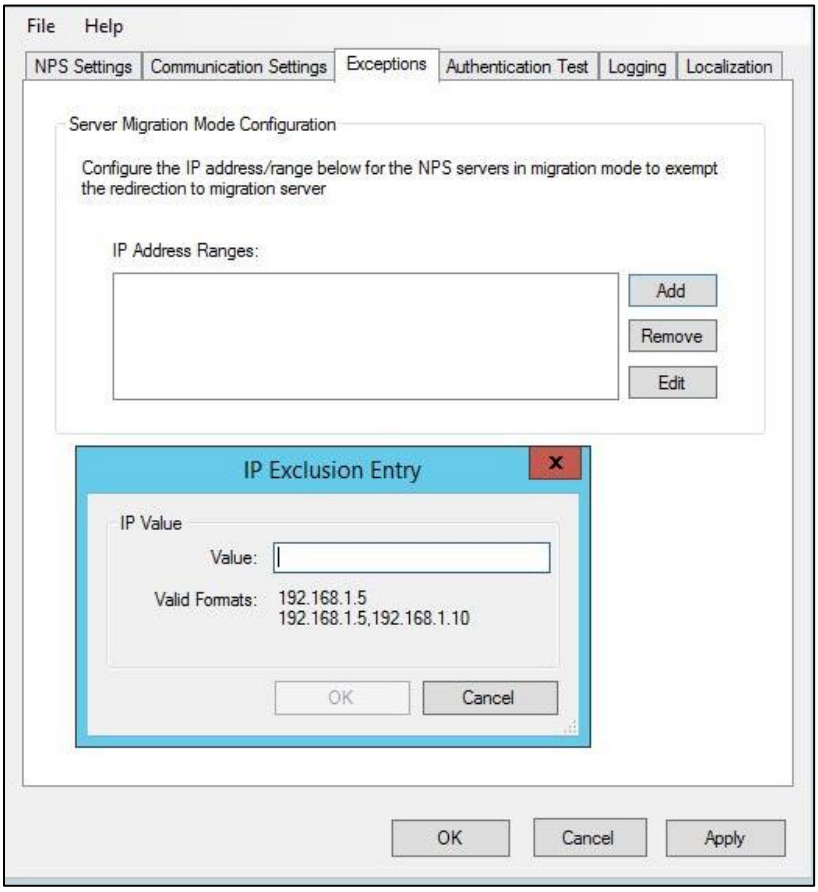
8. Click **Apply**.
9. Restart Network Policy Server.

Configuring Exceptions for Migration Mode

NOTE: Before configuring Exceptions, you must enable the **Migration Mode** in NPS settings tab.

To configure exceptions, perform the following steps:

1. Select **Exceptions** tab.
2. Click **Add** to enter the IP address/range for the NPS servers in migration mode to exempt the redirection to the migration server.



> To remove IP address/range, select an item and click **Remove**.

> To edit IP address/range, select an item and click **Edit**.

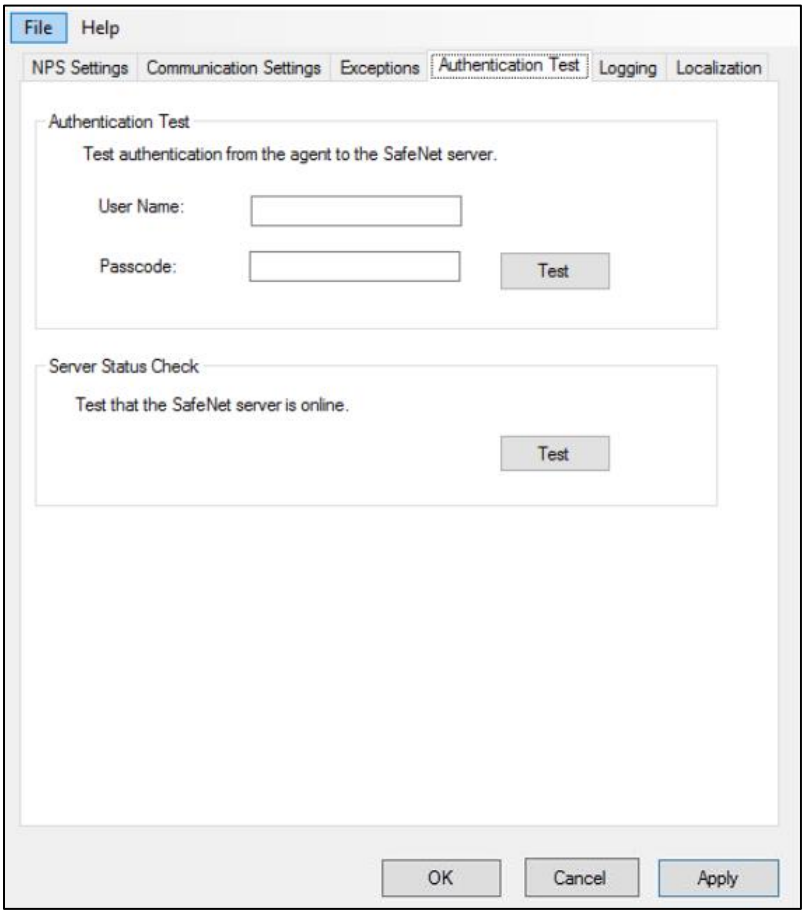
3. Click **Apply**.
4. Restart Network Policy Server.

NOTE: If Safenet Agent for NPS is installed on migration server (with migration mode enabled), then you need to configure IP address of the host server in Exceptions tab of management console in the migration server and vice-versa.

Performing Authentication Test and Server Status Check

To test authentications to the SafeNet server, perform the following steps:

1. Select **Authentication Test** tab.



2. Under **Authentication Test**, enter the **User Name** and **Passcode**.
3. Click **Test**.

   A message is displayed with the result of the test.

To test if the authentication server is online:

1. Select **Authentication Test** tab.
2. Click **Test** under **Server Status Check**.

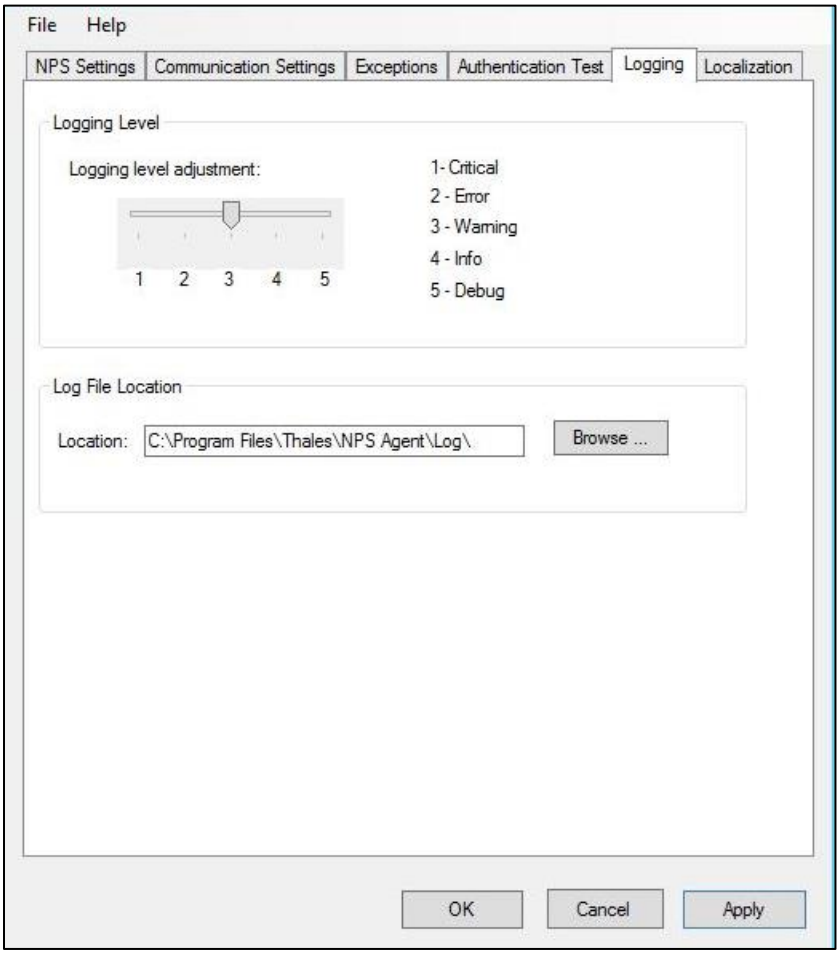
   A message is displayed indicating if the SafeNet sever is online.

> **NOTE:** A known limitation makes this agent falsely report SafeNet server offline when working via a proxy server. This error can be disregarded.

Configuring Logging Level

To set the logging level, perform the following steps:

1. Select **Logging** tab.



2. Drag the pointer on the **Logging level adjustment** scale to the required level, with the following definitions:

> 1 - Critical

> 2 - Error

> 3 - Warning

> 4 - Info

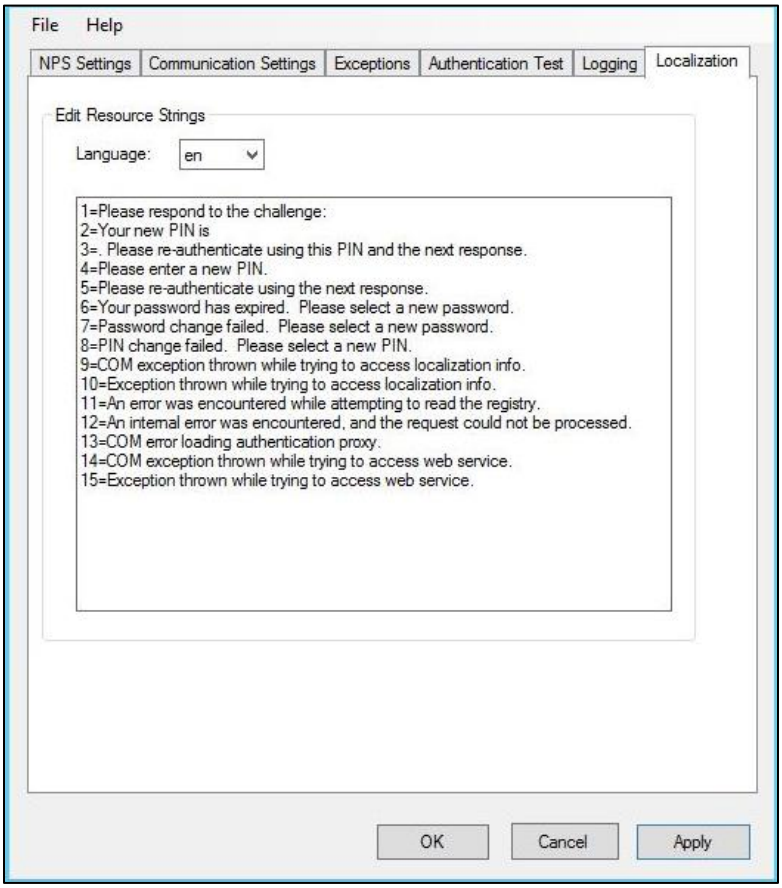
> 5 - Debug (recommended)

3. To enter the log file location in the **Location** field, click **Browse** and navigate to the folder where you want the log file to be stored.
4. Click **Apply**.
5. Restart Network Policy Server.

Configuring Localization Settings

To configure localization settings, perform the following steps:

1. Select **Localization** tab.



2. Select the required language from the **Language** drop-down list.
3. To add or edit text, type directly into the text box and click **Apply**.
4. Restart Network Policy Server.

   The strings are forwarded to the VPN device based on the state of the token during authentication (for example, the token is in New PIN mode).

> **NOTE:** The default location of the resource string file is the **`\languages\en`** folder. Since any upgrade of the agent will overwrite changes made in this directory, to avoid losing those changes, read about customizing SAS in the ***SafeNet Authentication Service Administrator Guide***.

Configuring Push Notification for IP Address

The SafeNet Agent for NPS can be configured to display the IP address of the end-user device in the MobilePASS+ login request notification screen.

To display the end-user IP in MobilePASS+ login request notification screen, create the following new registry keys at **`HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\AuthRadius`**.

Name	Type	Data
SendUserIP	Reg_SZ	1 – Send user IP to end-user device 0 – Do not send user IP to end-user device
RequiredUserIpAttribute	Reg_SZ	8 – Display IP address (Different values will display different RADUIS return attributes)