SafeNet Authentication Service

Configuration Guide

SAS Agent for Microsoft NPS 1.21

SafeNet. THE DATA PROTECTION COMPANY

Document Information

Product Version	1.21
Document Part Number	007-012390-002, Rev C
Release Date	5 February 2015

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Third-Party Software Acknowledgement

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

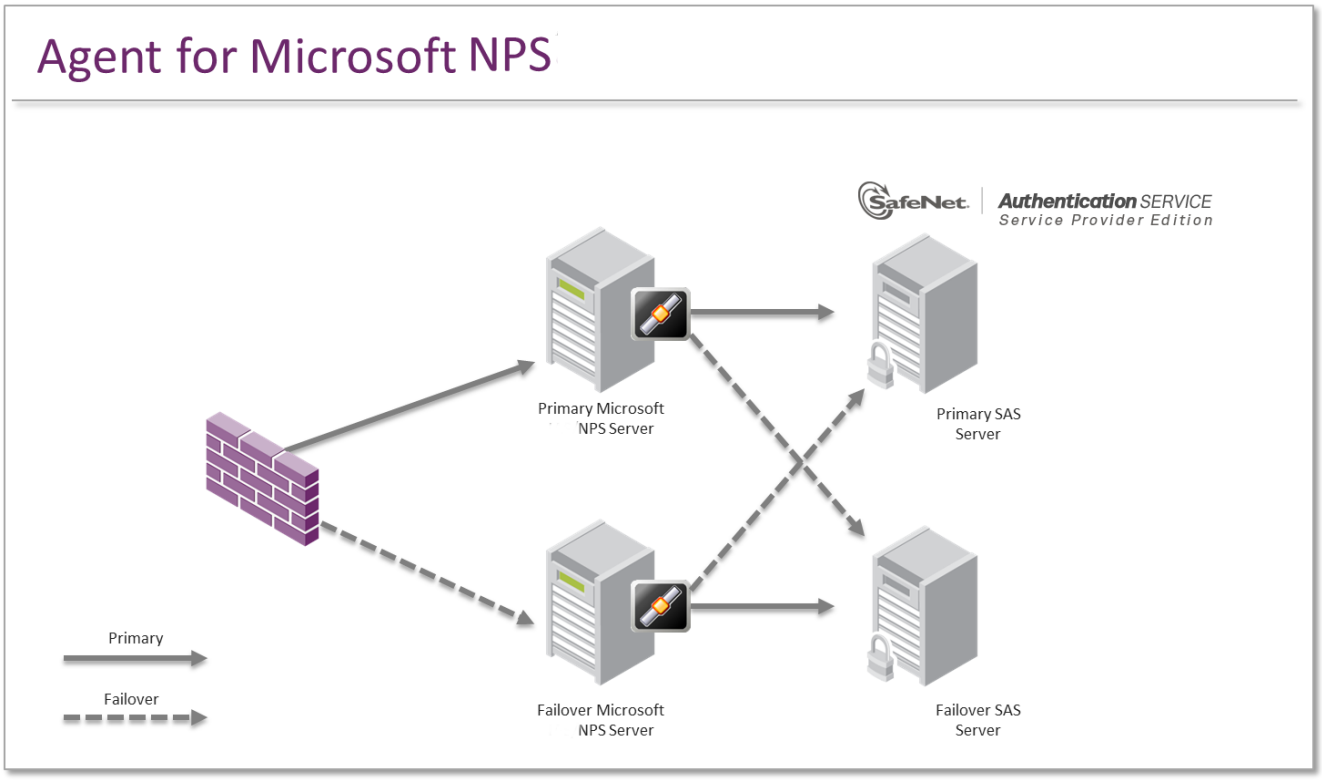
Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Overview

SAS uses the NPS RADIUS components of Windows Server.

To enable SAS to accept RADIUS authentication requests, do the following:

- Install the Windows NPS component.
- Install the SAS Agent on the machine hosting NPS.



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

> **NOTE:** The SAS Microsoft NPS Agent must be installed on same server as 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.

System Requirements

Prerequisites

- Microsoft .Net Framework 3.5 must be installed on the same computer as SAS Agent for Microsoft NPS

Operating Systems

SAS Microsoft NPS Agent is supported on the following Windows operating systems:

- Windows Server 2008 (32-bit)
- Windows Server 2008 R2 (64-bit)
- Windows Server 2012 R2 (64-bit)

Authentication Management Platforms

- SafeNet Authentication Service Cloud
- SafeNet Authentication Service PCE/SPE 3.2.1/3.3.2

Tokens

Hardware Tokens

- SafeNet eToken PASS (time based)
- SafeNet eToken PASS (event based)
- SafeNet eToken 3300
- SafeNet eToken 3400
- SafeNet KT-4
- SafeNet KT-5
- SafeNet RB-1
- SafeNet GOLD

Software Tokens

- SafeNet MP-1
- SafeNet MobilePASS
- SafeNet SMS Authentication

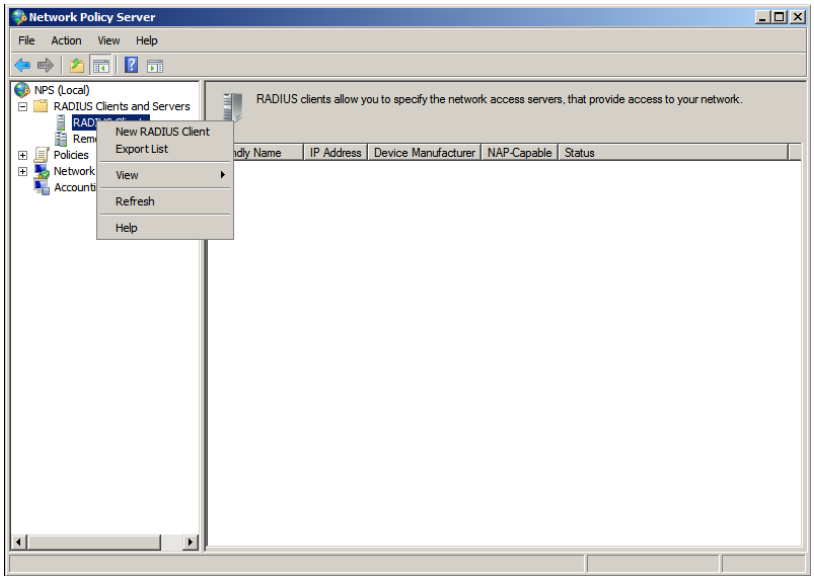
Configuring Microsoft NPS for RADIUS Clients

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

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

To configure Microsoft NPS for RADIUS clients:

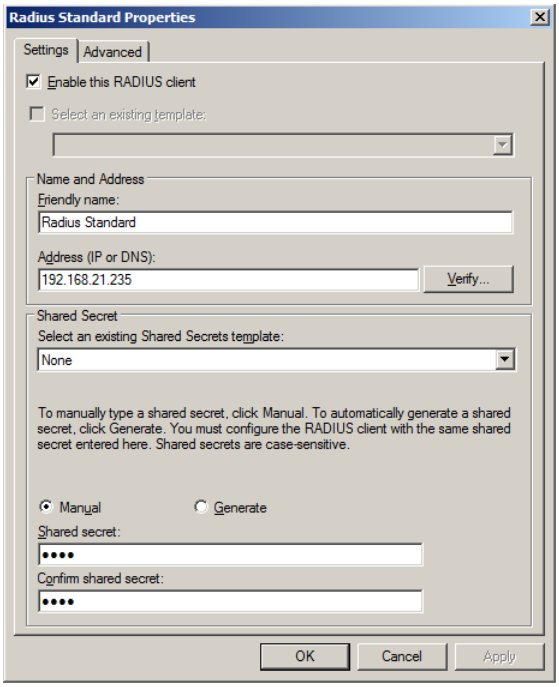
1. Select **Start> Administrative Tools> Network Policy Server.**
2. In the left pane:
   a. Double-click **Select RADIUS Clients and Servers**.
   b. Right-click **RADIUS Client** and then select **New RADIUS Client**.



(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**).
IP Address	Enter the IP address of the remote client.
Vendor name	Add the hostname or IP address of the failover SafeNet Authentication Service server.
Vendor name	Select **RADIUS Standard**.
Shared secret	Select **Manual** and then enter the shared secret value.
Confirm share secret	Re-enter the shared secret value to confirm it.



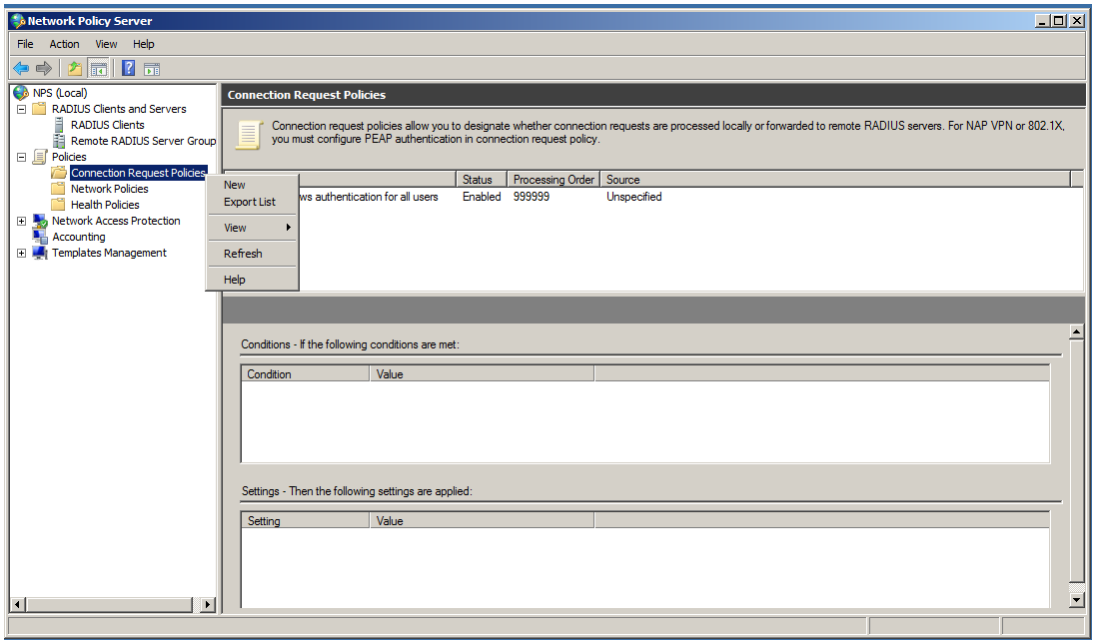
(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

4. Click **OK**.
5. You must restart the Network Policy Server for these changes to take effect.

Configuring Microsoft NPS to Use the SAS Agent

To create a Connection Request Policy:

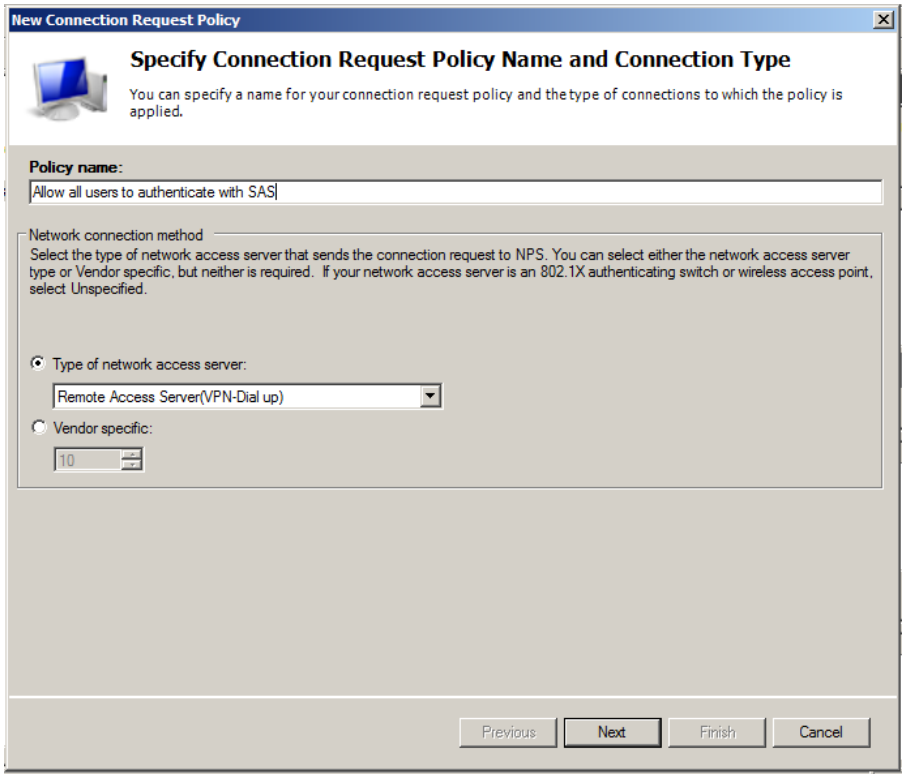
1. Select **Start> Administrative Tools> Network Policy Server**.



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

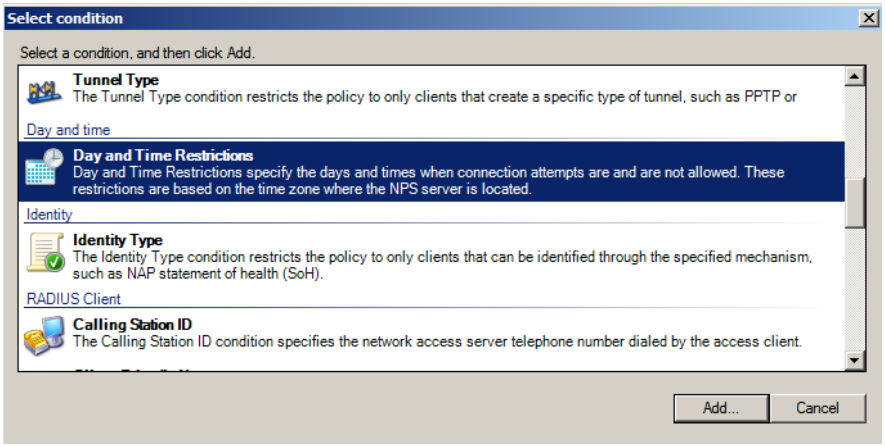
2. In the left pane,
   a. Double-click **Policies**.
   b. Right-click **Connection Request Policies** and then select **New**.
3. On the **New Connection Request Policy** window, complete the following fields and then click **Next**:

Policy name	Enter a name for the policy. For example, **Allow all users to authenticate with SAS**
Type of network access server	Select and form the drop-down list choose the required type of network server.
Specify failover SafeNet Authentication Service Server	Select **Remote Access Server (VPN-Dial up)**.



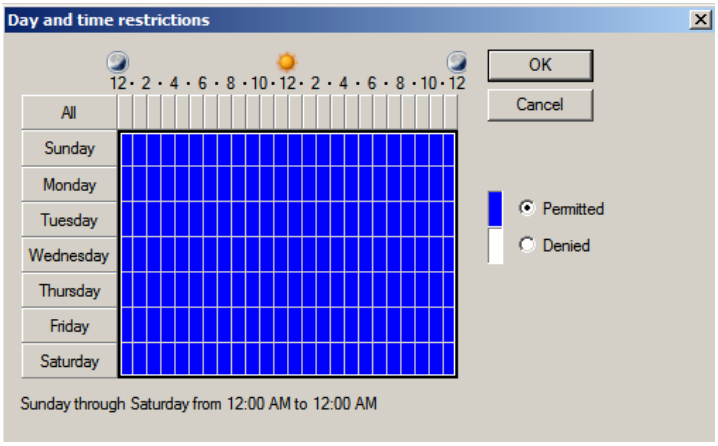
(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

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



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

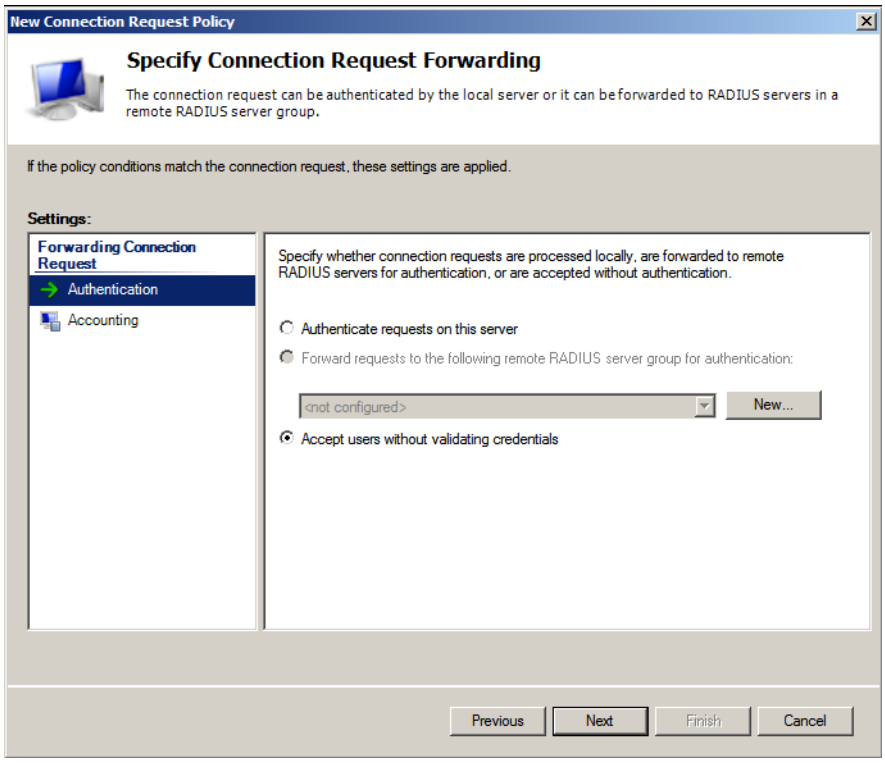
5. On the **Day and time restrictions** window, select **Permitted** and then click **OK**.



(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 then click **Next**.

   This setting will cause authentication requests to be intercepted by the SAS Microsoft NPS Agent, and is required in order to allow the agent to function correctly.



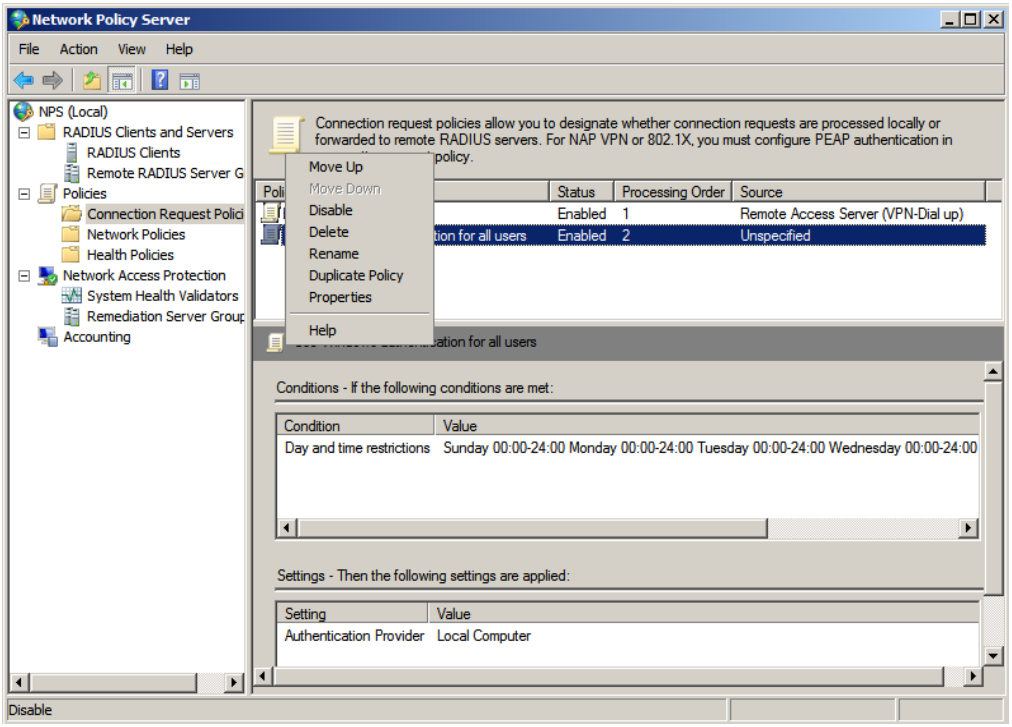
(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

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

8. On the **Network Policy Server** window:

   a. In the left pane, click **Connection Request Policies**.

   b. In the right pane, right-click on **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.

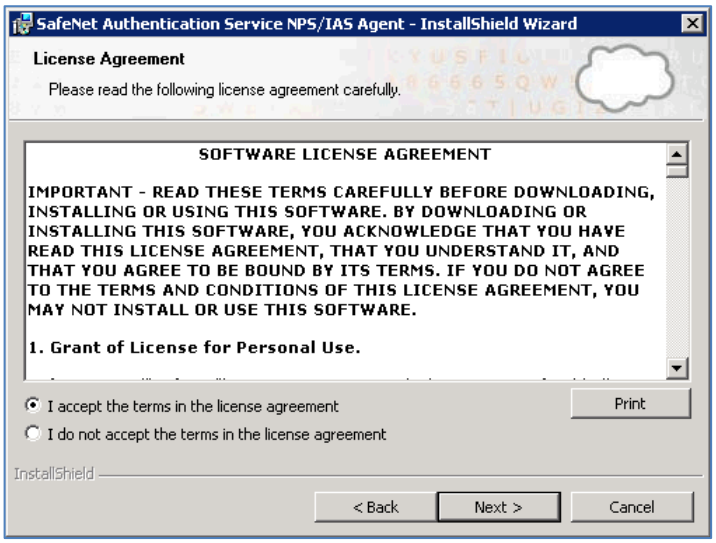
Installing SAS Agent for Microsoft NPS

Important: Log onto Windows as an administrator and run the installer as an administrator when installing the SAS Agent for Microsoft NPS.

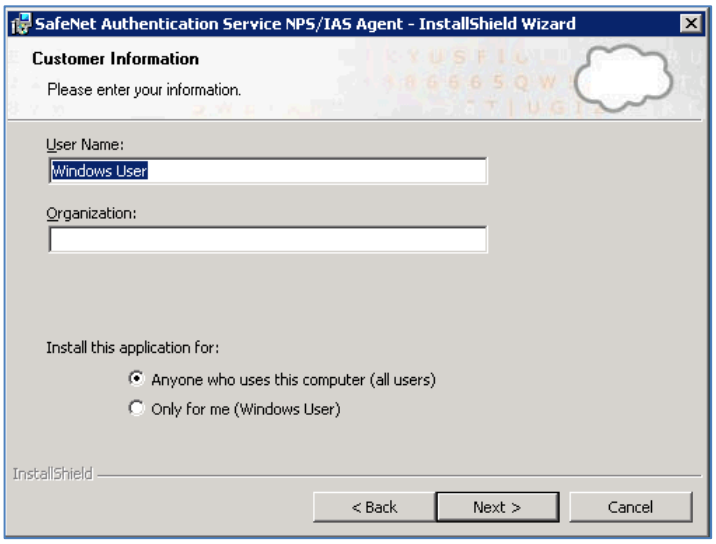
To install the SAS Agent for Microsoft NPS:

1. Log on to the server on which Microsoft NPS is installed.
2. Locate and run the applicable SAS installer:
   - **SafeNet Network Policy Server Agent x32** (for 32-bit servers)
   - **SafeNet Network Policy Server Agent x64** (for 64-bit servers)
3. On the **Welcome to the InstallShield Wizard** window click **Next**.

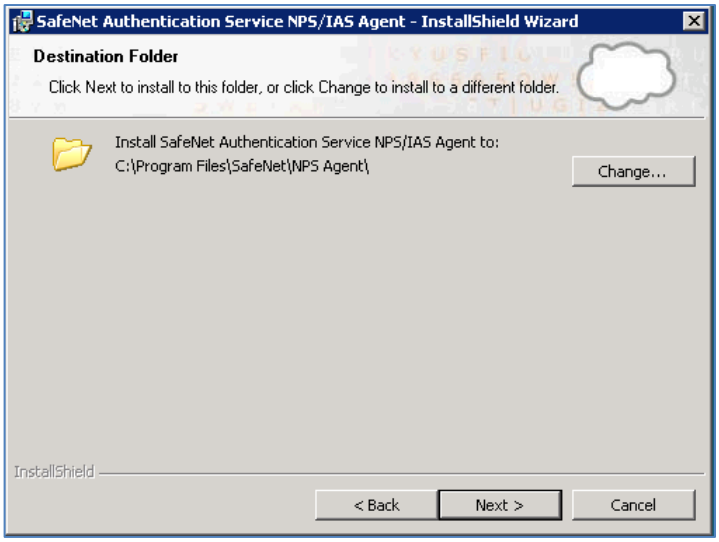
4. On the **License Agreement** window, select **I accept the terms of the license agreement** and then click **Next.**



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

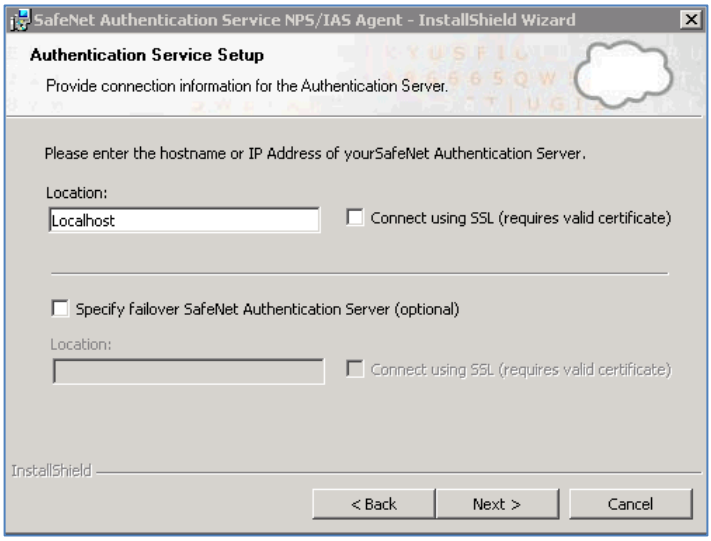


6. On the **Destination Folder** window, do one of the following:
   - To change the installation folder click **Change**, navigate to the required folder, and then click **Next**.
   - To accept the default installation folder as displayed, click **Next**.

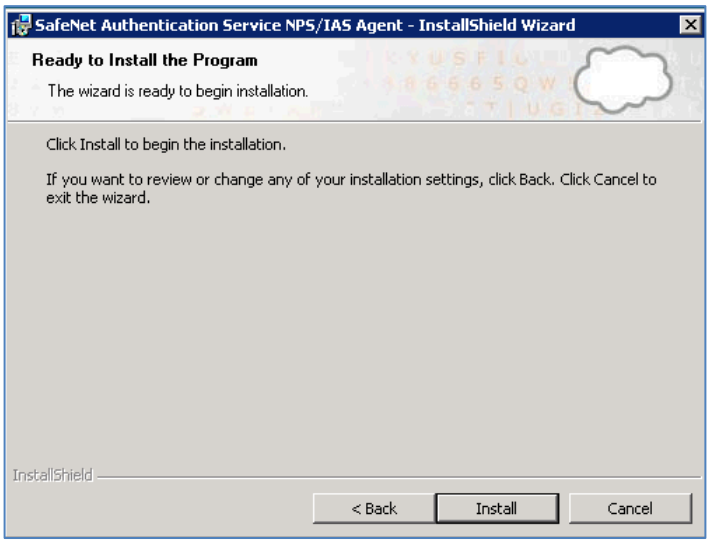


7. On the **Authentication Service Setup** window, complete the following fields and then click **Next**:

Location	Enter the hostname or IP address of the primary SafeNet Authentication Service server.
Connect using SSL	Select to use SSL. This option requires installation of a valid certificate on the NPS server.
Specify failover SafeNet Authentication Service Server	Select if a failover SAS server is available.
Location	Add the hostname or IP address of the failover SafeNet Authentication Service server.

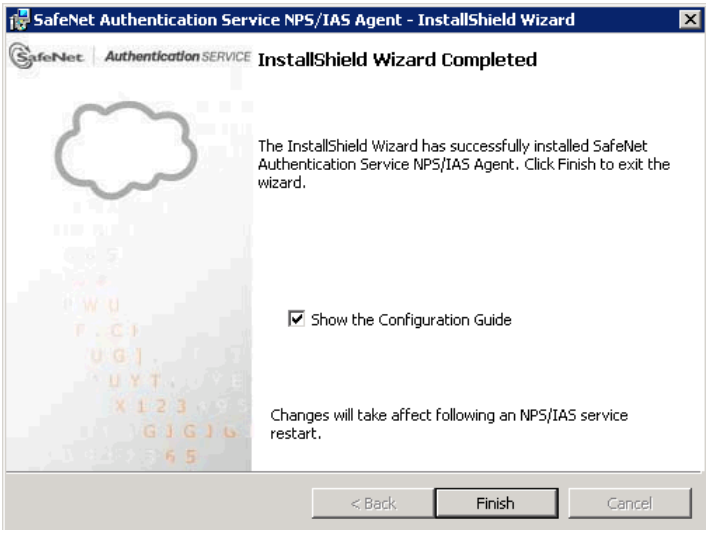


8. On then **Ready to Install the Program** window, click **Install**.



The installation proceeds.

9. On the **InstallShield Wizard Completed** window, select **Show the Configuration Guide** to display configuration instructions, and then click **Finish** to exit the installation wizard.



Configuring SAS Agent for Microsoft NPS

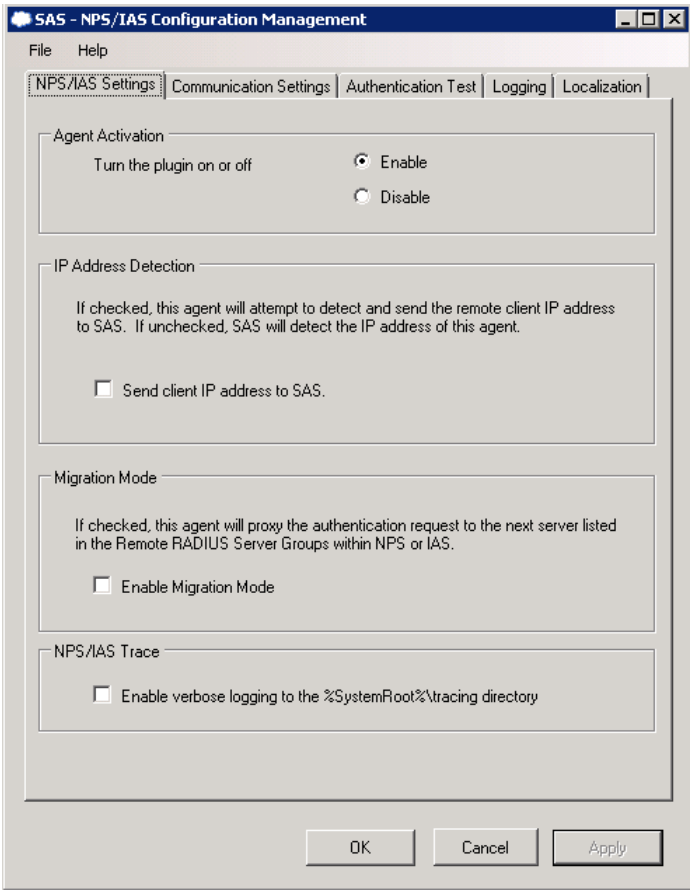
To launch SAS-NPS/IAS Configuration Management, select **Start > All Programs > SafeNet > NPS IAS Agent Configuration.**

> **Important:** Run SAS-NPS/IAS Configuration Management as an administrator when configuring the SAS Agent for Microsoft NPS.

Configuring NPS Settings

To configure the NPS settings:

1. Select the **NPS/IAS Settings** tab.



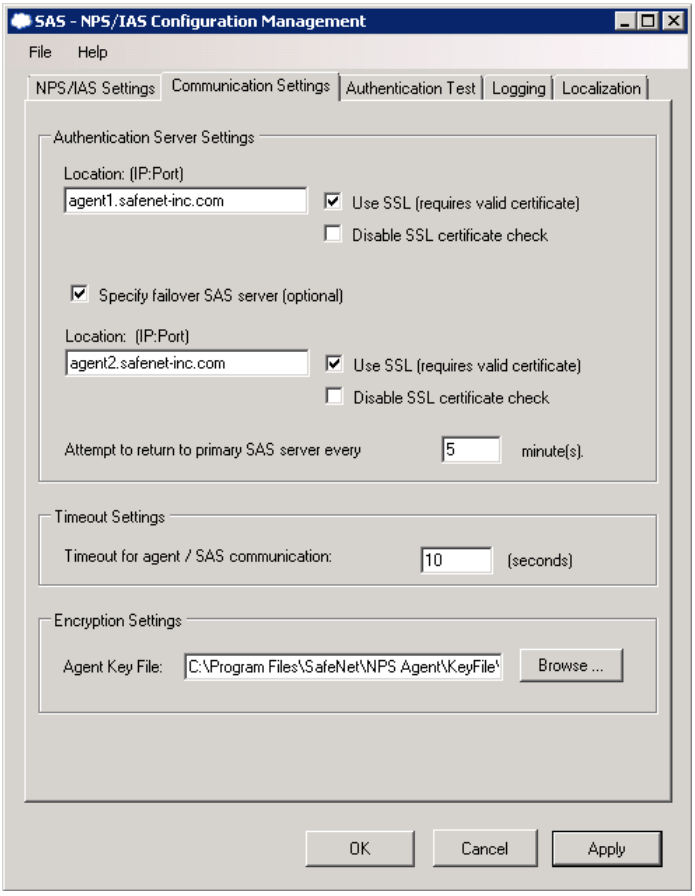
2. To activate the agent, select **Enable** for **Turn the plugin on or off**.
3. To activate the feature to detect and send the remote client IP address to SAS, select **Send IP address to SAS**.
4. To allow users to proxy the authentication request to the next server listed in the Remote RADIUS Server Groups within NPS, select **Enable Migration Mode.**
5. To enable verbose logging, select **Enable verbose logging to the %SystemRoot%\ tracing directory**.
6. Click **Apply**.

Configuring Communication Settings

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

To configure the communication settings:

1. Select the **Communication Settings** tab.



2. In the **Location** field, enter the SAS server name.
3. Select one of the following:
   - **Use SSL (requires valid certificate)** – SSL must be used.
   - **Disable SSL certificate check** – SSL is not required.
4. If a failover SAS server is required, select **Specify failover SAS server (optional)** and then do the following:
   a. In the **Location** field, enter the SAS Server name.
   b. Select one of the following:
      - **Use SSL (requires valid certificate)** – SSL must be used.
      - **Disable SSL certificate check** – SSL is not required.

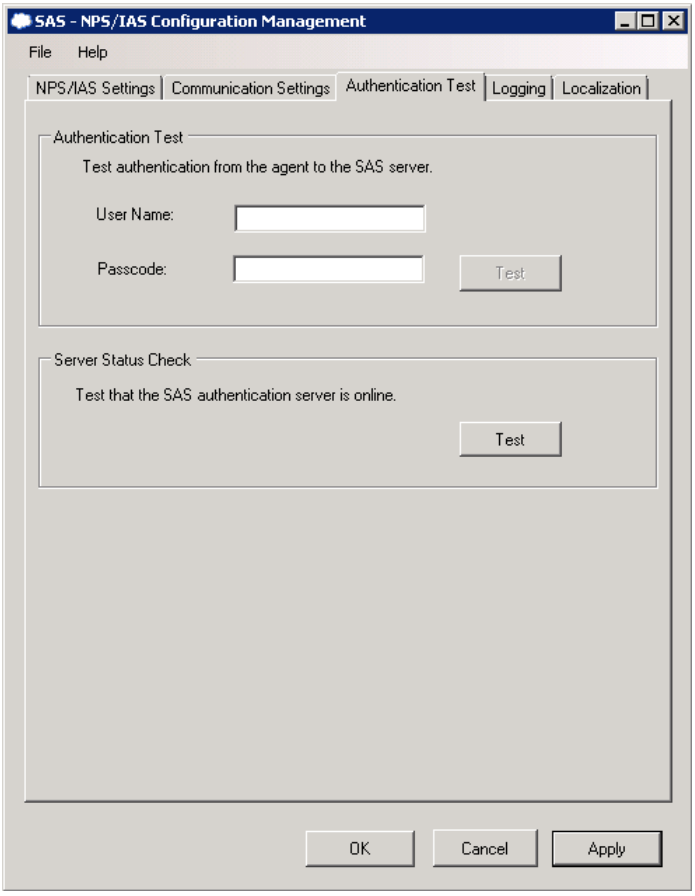
c. **In the Attempt to return to primary server every** field, enter the number of minutes required between each attempt to return to primary server.

5. In the **Timeout for agent / SAS communication** field, enter the maximum timeout in seconds for each authentication attempt.
6. In the **Agent Key File** field click **Browse** and navigate to the file.
7. Click **Apply**.

Performing an Authentication Test

To check that the authentication server is online:

1. Select the **Authentication Test** tab.

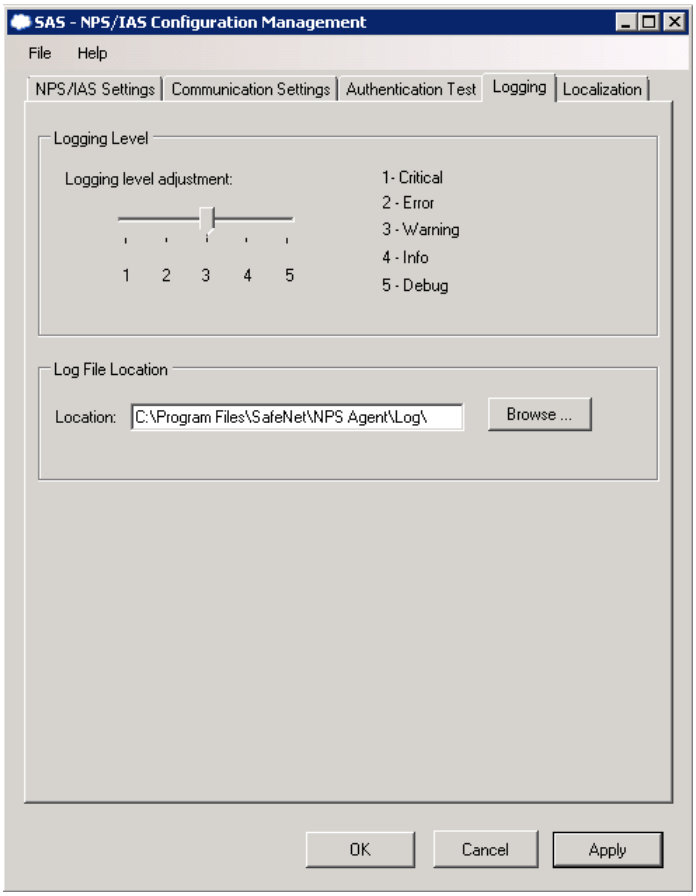


2. Enter the **User Name** and **Passcode**.
3. Click **Test**.
4. Click **Apply**.

Configuring the Logging Level

To set the logging level:

1. Select the **Logging** tab.

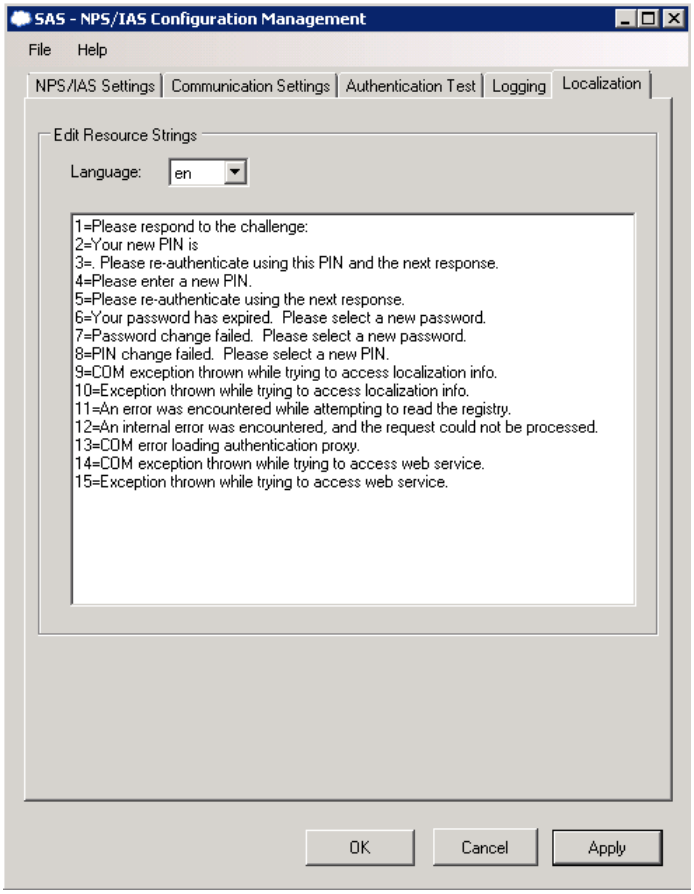


2. Drag the pointer on the **Logging level adjustment** scale to the required level, as follows:
   - 1-Critical
   - 2-Error
   - 3-Warning
   - 4-Info
   - 5-Debug (recommended)
3. To enter the log file location in the **Location** field, click **Browse** and navigate to the folder where the log file is stored.

Configuring Localization Settings

To configure localization settings:

1. Select the **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 then click **Apply**.

   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.*

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet 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 SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when phone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	