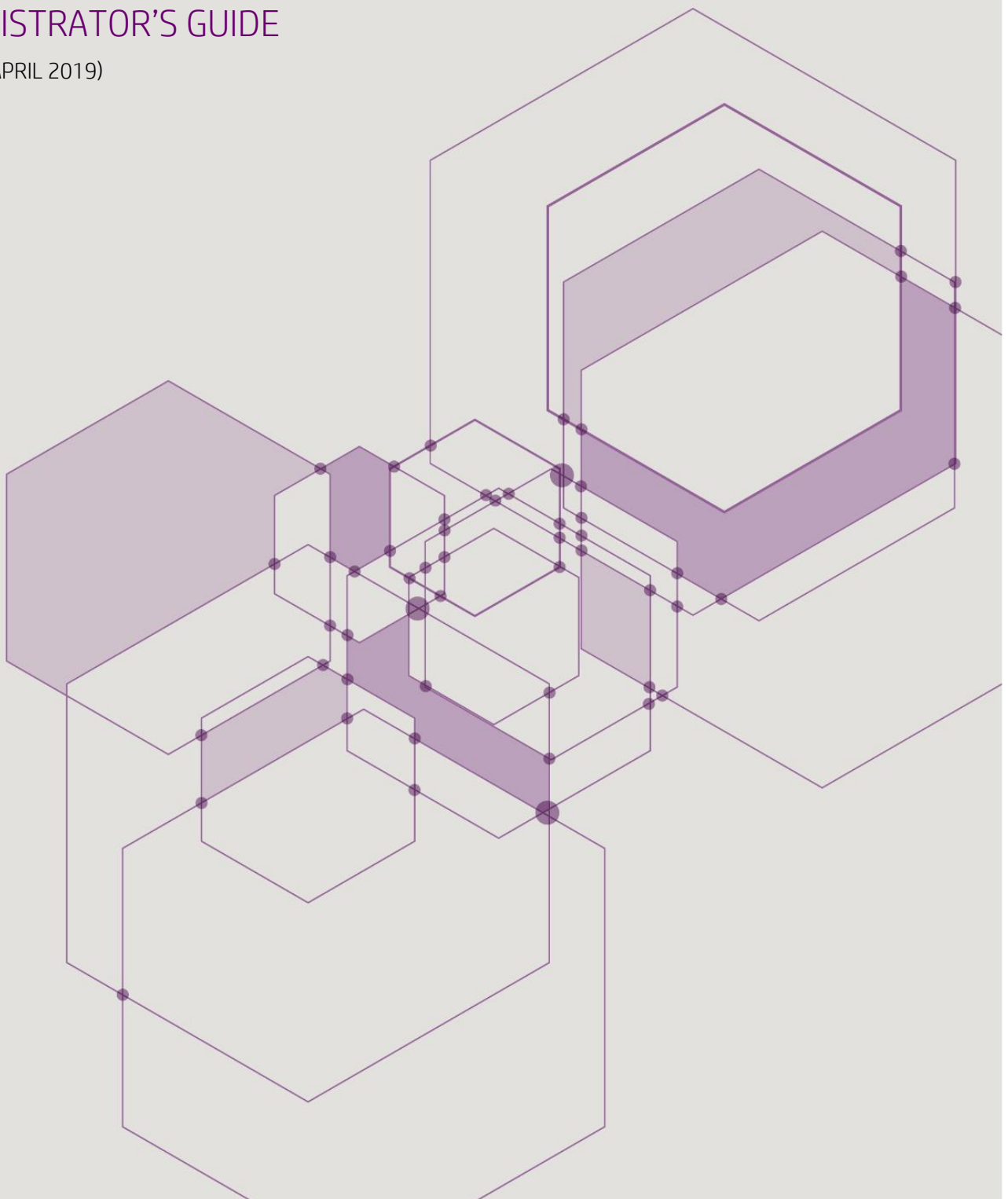


# SMS PASSCODE **Cloud Service Connector**

## ADMINISTRATOR'S GUIDE

REV. 1.0 (APRIL 2019)



# TABLE OF CONTENTS

Table of Contents.....	2
1 Introduction.....	3
2 Notation .....	3
3 New Features in Cloud Service Connector .....	4
4 End-of-life .....	4
5 Components .....	5
6 System Requirements.....	6
7 Pre-Installation Actions .....	7
7.1 Check System Requirements.....	7
7.1.1 Installation of NPS.....	7
8 Upgrade.....	8
9 First-time Installation.....	8
9.1 Installation of Software.....	8
10 Add/Remove Components.....	19
11 Post-Installation Actions.....	20
12 Configuring Authentication Clients .....	21
12.1 Configuring RADIUS Protection .....	21
12.1.1 Configuring RADIUS Protection on a Windows Server .....	22
12.1.2 Advanced Configuration of the RADIUS Protection Component .....	25
12.2 Configuring AD FS 3.0/4.0 Protection .....	37
12.2.1 Background .....	38
12.2.2 AD FS 3.0/4.0 Infrastructure .....	38
12.2.3 Configuring the MFA Adapter for AD FS 3.0.....	38
12.2.4 Configuring the MFA Adapter for AD FS 4.0.....	40
12.2.5 Uninstalling the MFA Adapter .....	43
13 Configuration Tool.....	43
13.1 Collecting End-User IP Addresses .....	44
13.2 Command Line Arguments .....	46
14 Troubleshooting .....	48
14.1 Component Communication Problems.....	48

© 2019 Entrust Datacard. Trademarks are the property of their respective owners.

## 1 INTRODUCTION

SMS PASSCODE is a versatile multi-factor authentication (MFA) system with an extensive list of great features. SMS PASSCODE can be installed in *on-premise mode*, with the complete infrastructure installed on-premise, or in *cloud mode*, with only SMS PASSCODE authentication clients (“agents”) installed on the on-premise servers that need MFA protection.

The “SMS PASSCODE Cloud Service Connector” installer is used for installing SMS PASSCODE in *cloud mode*.

This document describes how to install, configure and administer SMS PASSCODE Cloud Service Connector. For an *on-premise* installation, please consult the “SMS PASSCODE 2018 Administrator’s Guide”.

## 2 NOTATION

Shorthand	Description
<b>AD</b>	Active Directory
<b>AD FS</b>	Active Directory Federation Services
<b>IIS</b>	Internet Information Server: Optional component/role on a Windows Server.
<b>Machine</b>	This is a general term used to denote a server or a workstation
<b>NPS</b>	Network Policy Server: Optional Role on a Windows Server 2008/2012/2016. This Role is the Microsoft implementation of a RADIUS server.
<b>OTP</b>	One-time passcode
<b>OWA</b>	Microsoft Outlook Web Access
<b>RD</b>	Remote Desktop
<b>RDS</b>	Microsoft Remote Desktop Services
<b>SMS PASSCODE authentication client</b>	One of the SMS PASSCODE components <b>Citrix Web Interface Protection, RADIUS Protection, AD FS Protection, IIS Website Protection or Windows Logon Protection</b> , i.e. one of the components responsible for authentication for a specific type of client.

### 3 NEW FEATURES IN CLOUD SERVICE CONNECTOR

*SMS PASSCODE Cloud Service Connector* is the first SMS PASSCODE version that makes it possible to connect SMS PASSCODE MFA protections directly with the IntelliTrust™ cloud service provided by Entrust Datacard.

The IntelliTrust™ service includes an admin portal that is hosted in the cloud. It supports a series of authenticators, including:

- Push authentication using the Entrust Mobile Soft Token app
- Push authentication using the Entrust Mobile Smart Credentials app
- One-time passcode sent by SMS
- One-time passcode sent by email
- One-time passcode via tokens
- Temporary access code

### 4 END-OF-LIFE

This section summarizes end-of-life (EOL) for the different SMS PASSCODE versions. After the EOL date, support and hotfixes will not be provided anymore for the version in question.

Version	EOL
<b>SMS PASSCODE 8.0 and older</b>	Already end of life
<b>SMS PASSCODE 8.0 SP1</b>	January 1, 2020
<b>SMS PASSCODE 9.0</b>	October 1, 2020
<b>SMS PASSCODE 9.0 SP1</b>	February 1, 2021
<b>SMS PASSCODE 9.0 SP2</b>	September 1, 2021
<b>SMS PASSCODE 2017</b>	November 1, 2021
<b>SMS PASSCODE 2018</b>	September 1, 2022
<b>SMS PASSCODE Cloud Service Connector</b>	March 1, 2023

## 5 COMPONENTS

SMS PASSCODE *Cloud Service Connector* is composed of the following software components:

Component	Description
<b>RADIUS Protection</b>	<p>Integrates with RADIUS systems providing SMS PASSCODE multi-factor authentication for RADIUS clients. It is optionally possible to run this integration side-by-side with other RADIUS authentication systems, e.g. hardware-token based two-factor authentication systems.</p> <p>RADIUS protection is provided by means of an extension for the Microsoft Network Policy Server (NPS).</p>
<b>AD FS Protection</b>	<p>Integrates with Microsoft Active Directory Federation Services (AD FS), providing SMS PASSCODE multi-factor authentication for applications protected by AD FS 3.0/4.0.</p>

The term ***SMS PASSCODE Authentication client*** is used in the subsequent sections of this documentation to denote one of the components: **RADIUS Protection** or **AD FS Protection**.

## 6 SYSTEM REQUIREMENTS

In this section, the system requirements are listed for each SMS PASSCODE software component (cf. section 5).

**Please note:**

In general, SMS PASSCODE components require the **Microsoft .NET 4.5 Framework**.

Component	Requirement
<b>RADIUS Protection</b>	<ul style="list-style-type: none"> <li>Supported operating systems: <ul style="list-style-type: none"> <li>Windows Server 2008 R2 (x64)</li> <li>Windows Server 2012 (x64)</li> <li>Windows Server 2012 R2 (x64)</li> <li>Windows Server 2016 (x64)</li> </ul> </li> </ul> <p><b>Please note:</b> Only Windows Server Editions including the Network Policy Service (NPS) are supported. This means, that for example <i>Windows Server 2008 Web Edition</i>, <i>Windows Server 2012 Hyper-V Edition</i> and <i>Windows Server 2012 Storage Edition</i> are not feasible.</p> <ul style="list-style-type: none"> <li>Network Policy Service (NPS) must be installed <u>before</u> installing this component.</li> <li>Supported RADIUS clients: All RADIUS clients that support the PAP or MS-CHAP v2 authentication protocol. The best user experience is achieved using RADIUS clients that support PAP with <b>Challenge Response</b>. Among others the following RADIUS clients support <b>Challenge Response</b>: <ul style="list-style-type: none"> <li>Cisco ASA</li> <li>Cisco VPN Concentrator 3000</li> <li>Citrix NetScaler Gateway</li> <li>Palo Alto</li> <li>Check Point FW-1/VPN-1 NG/FP3</li> <li>F5 BigIP</li> <li>Fortigate SSL VPN</li> <li>Juniper SSL VPN</li> <li>Dell SonicWall SRA, Dell SonicWall NSA</li> <li>VMWare Horizon View</li> <li>WatchGuard Firebox</li> </ul> </li> </ul> <p>Please contact your SMS PASSCODE reseller or <a href="mailto:support@smsspasscode.com">support@smsspasscode.com</a> for further information regarding supported RADIUS clients.</p>
<b>AD FS Protection</b>	<ul style="list-style-type: none"> <li>Supported operating systems: <ul style="list-style-type: none"> <li>Windows Server 2012 R2 (x64)</li> <li>Windows Server 2016 (x64)</li> </ul> </li> <li>Microsoft AD FS 3.0/4.0 must be installed <u>before</u> installing this component.</li> </ul>

## 7 PRE-INSTALLATION ACTIONS

### 7.1 Check System Requirements

Before running an SMS PASSCODE installation, please make sure that all system requirements are fulfilled for the components that you are planning to install. System requirements are listed in section 6 (page 6).

Please remember:

- **RADIUS Protection**

If you are planning to install the **RADIUS Protection** component, then the *Network Policy Server* (NPS) role must be added to the relevant server beforehand. Installation of NPS is described in section 7.1.1 (page 7)

- **AD FS Protection**

If you are planning to install the **AD FS Protection** component, then AD FS 3.0 or 4.0 must be installed on the relevant server beforehand. It is also recommended to configure any (cloud) applications beforehand and ensure that standard AD FS authentication works without SMS PASSCODE. For more details, please read section 12.2 (page 37).

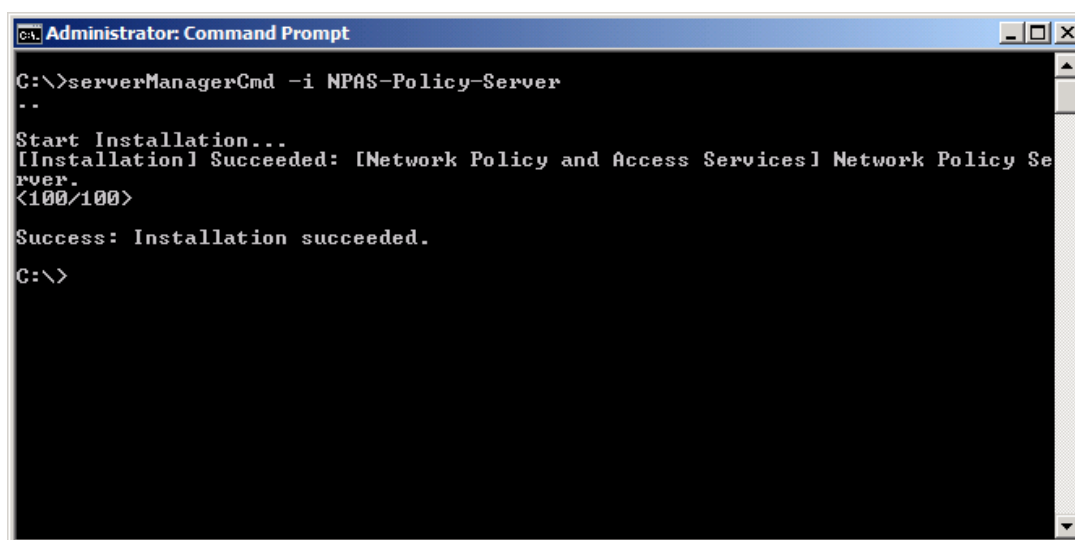
#### 7.1.1 Installation of NPS

This section describes how to install the Microsoft Network Policy Server (NPS) role on a Windows Server. You only need to install NPS if you are planning to install the SMS PASSCODE **RADIUS Protection** component on this server.

##### Windows Server 2008 R2

To install NPS on a Windows Server 2008 R2, please use the Server Manager or run the following command in a command prompt:

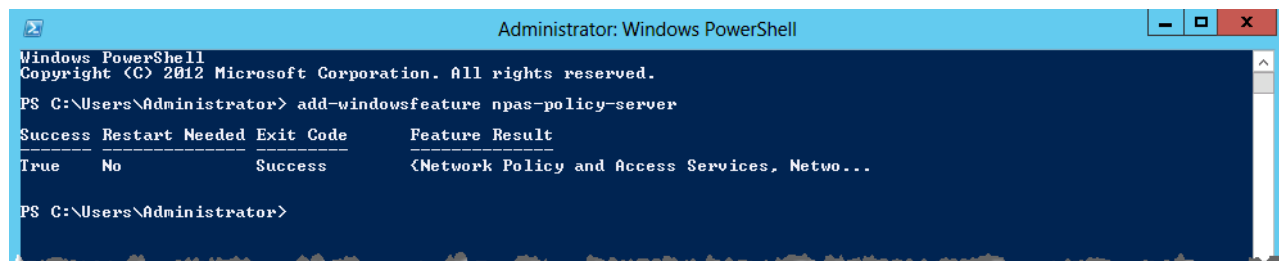
```
ServerManagerCmd -i NPAS-Policy-Server
```



## Windows Server 2012 (R2) / 2016

To install NPS on a Windows Server 2012 (R2) or 2016, please use the Server Manager or run the following command in a PowerShell console:

```
add-windowsfeature npas-policy-server
```



## 8 UPGRADE

SMS PASSCODE *Cloud Service Connector* supports only upgrades of SMS PASSCODE RADIUS Protection and SMS PASSCODE AD FS Protection 3.0/4.0, from the SMS PASSCODE 2017 Cloud Edition.

There is no upgrade path from a previous on-premise installation to a *Cloud Service Connector* installation. If you want to switch from an on-premise installation to a *Cloud Service Connector* installation, you must uninstall the previous version of SMS PASSCODE first, and then perform a new, fresh installation of *Cloud Service Connector*.

## 9 FIRST-TIME INSTALLATION

To install SMS PASSCODE *Cloud Service Connector* you must complete two steps:

1. Install software (section 9.1, page 8).
2. Configure SMS PASSCODE (section 11, page 20).

These two steps are described in the specified sections.

### 9.1 Installation of Software

This section describes the procedure for installing the SMS PASSCODE software.

#### IMPORTANT

You must have administrator rights to install any SMS PASSCODE components.

#### IMPORTANT

Close all other applications while installing SMS PASSCODE.

As explained in section 5 (page 5), SMS PASSCODE is composed of several software **components**. You can install each component by itself or together with other SMS PASSCODE

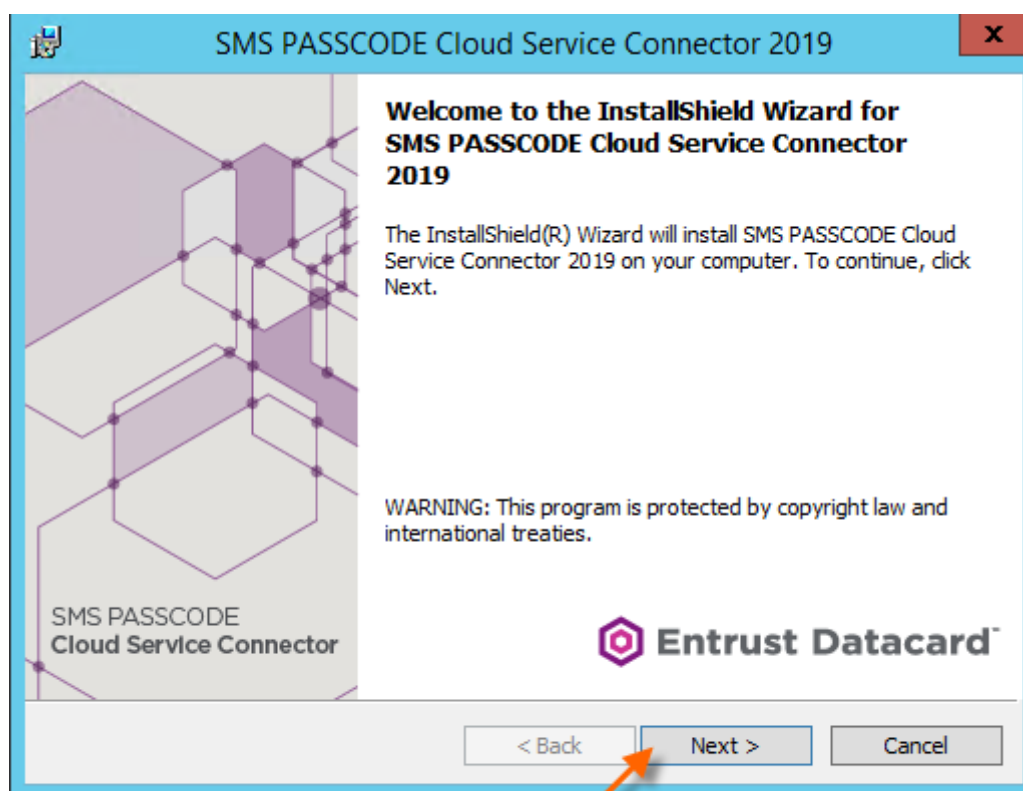


components on a machine. You have complete control of how to distribute the components on several machines.

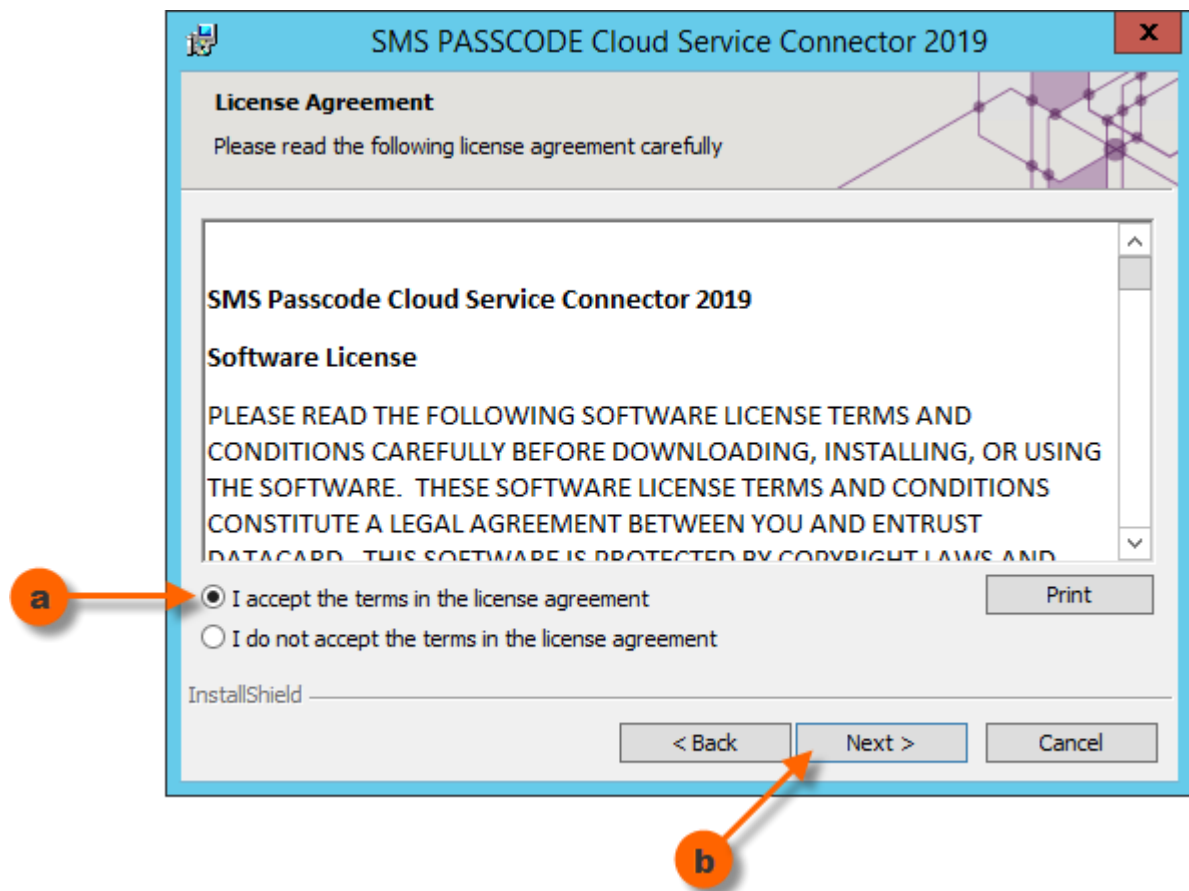
The procedure for an SMS PASSCODE installation is to run the installation package on each involved machine and select the components to be installed on this machine. The actions for installing components on each machine are listed below. Please repeat these actions on each machine being part of the SMS PASSCODE installation.

**IMPORTANT:** The sequence of dialogs is automatically tailored during an installation according to the components selected for installation. The workflow below describes all potential dialogs that may appear during an installation. You may not see all dialogs during your specific installation – skip forward in the workflow in case a dialog is not shown.

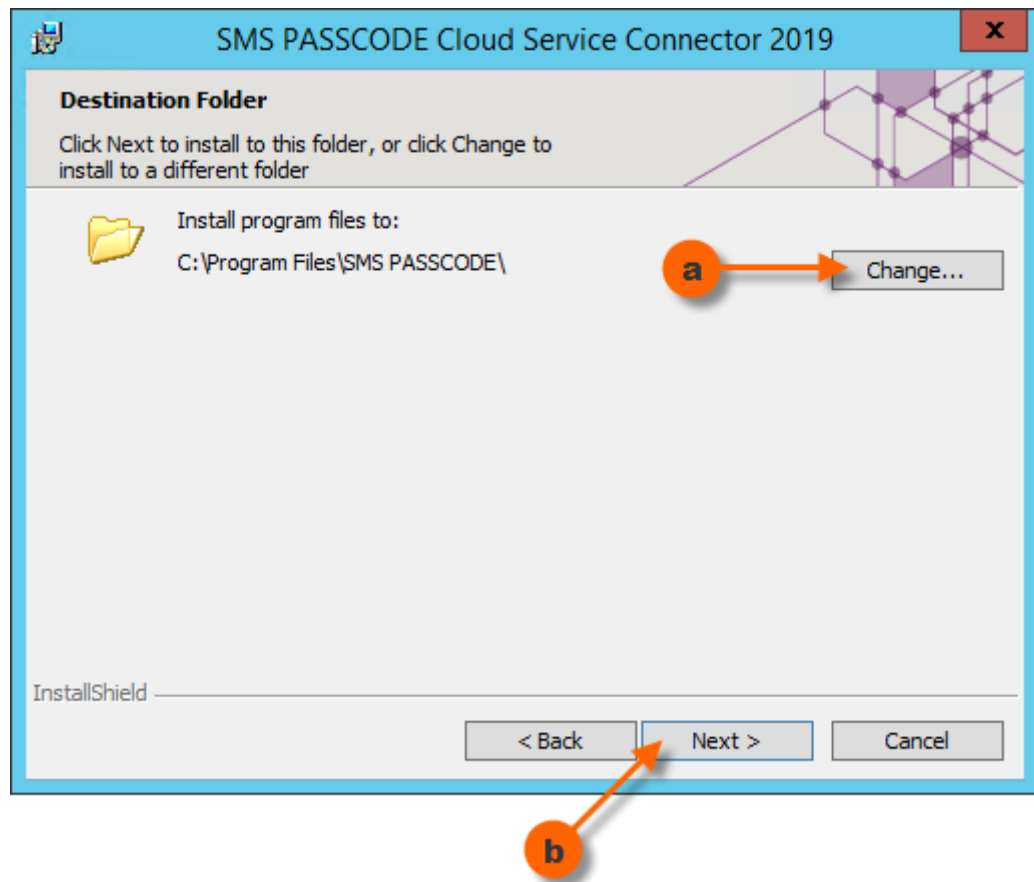
1. Log on to the machine using a user account with local administrator rights.
2. Copy **SmsPasscodeCloudServiceConnector-2019.exe** to a local path on the machine.
3. Start the installation by double-clicking the setup file.
4. A Welcome dialog appears. Click the **Next** button.



5. An End-User License Agreement (EULA) appears. Please read the agreement carefully. If you accept the EULA:
  - a. Click on **I accept the terms in the license agreement**.
  - b. Click the **Next** button.



6. A dialog appears, for selecting the installation folder:
  - a. It is recommended to use the proposed default installation folder. In case you want to change the path anyhow: Click the **Change** button and select a new path.
  - b. Click the **Next** button.



7. A dialog for selecting **Authentication Clients** appears.
  - a. Select the components that you would like to install on this machine. Please read section 5 (page 5) for more details on each component. You may click the question mark buttons in the dialog window to get more information.  
Please note: The selection of Authentication Clients is NOT permanent. In case you would like to add or remove Authentication Clients you can always run the installation again afterwards (cf. section 10)

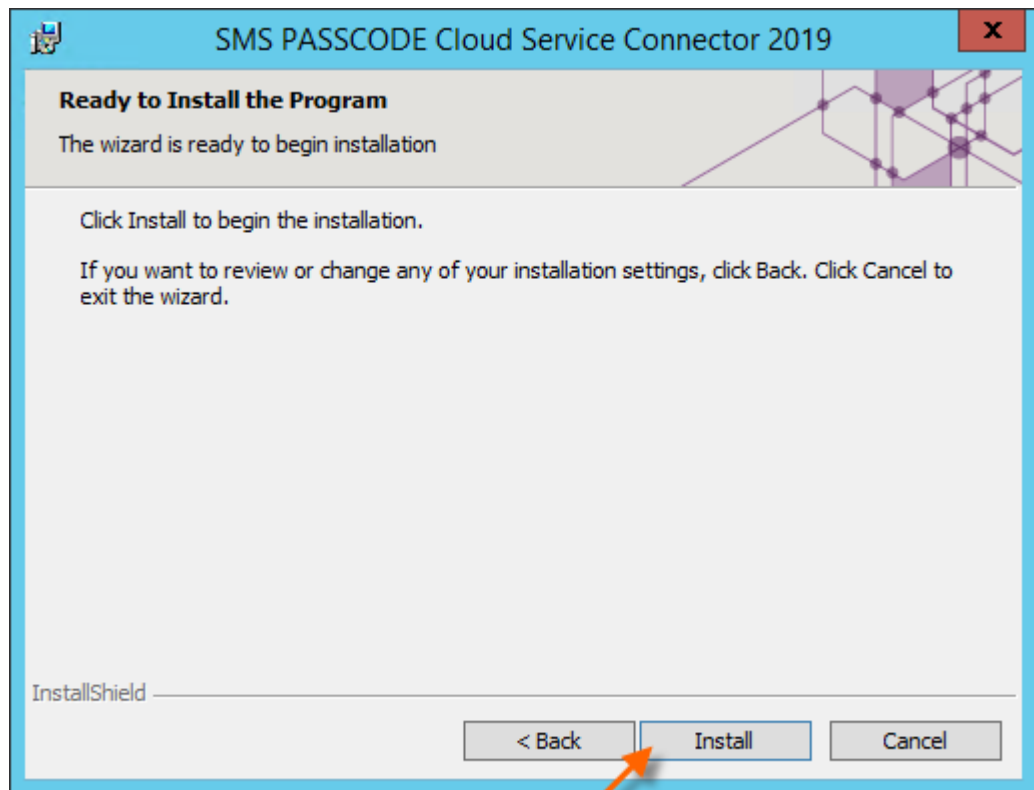
**PLEASE NOTE:**

If a component is disabled for selection, this is caused by system requirements not being fulfilled for this component (cf. section 6, page 6)

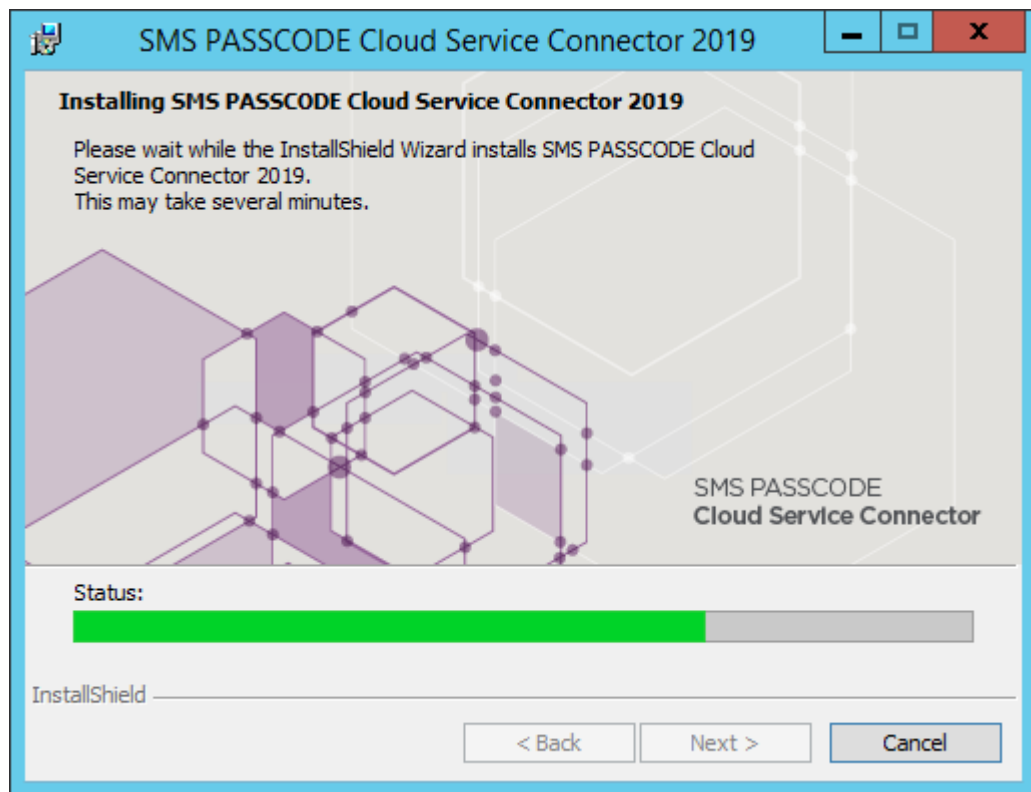
- b. Click the **Next** button.



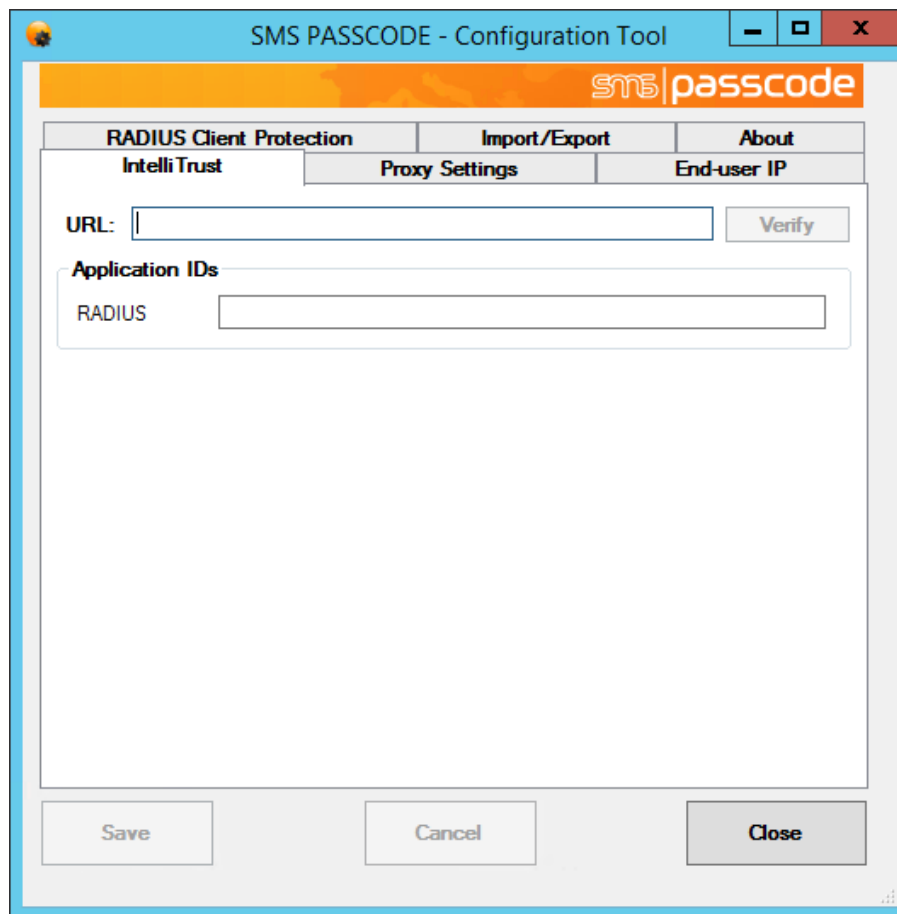
8. You are now ready to perform the installation according to the choices you have made. Click the **Install** button.



9. A dialog appears showing the progress of the installation...



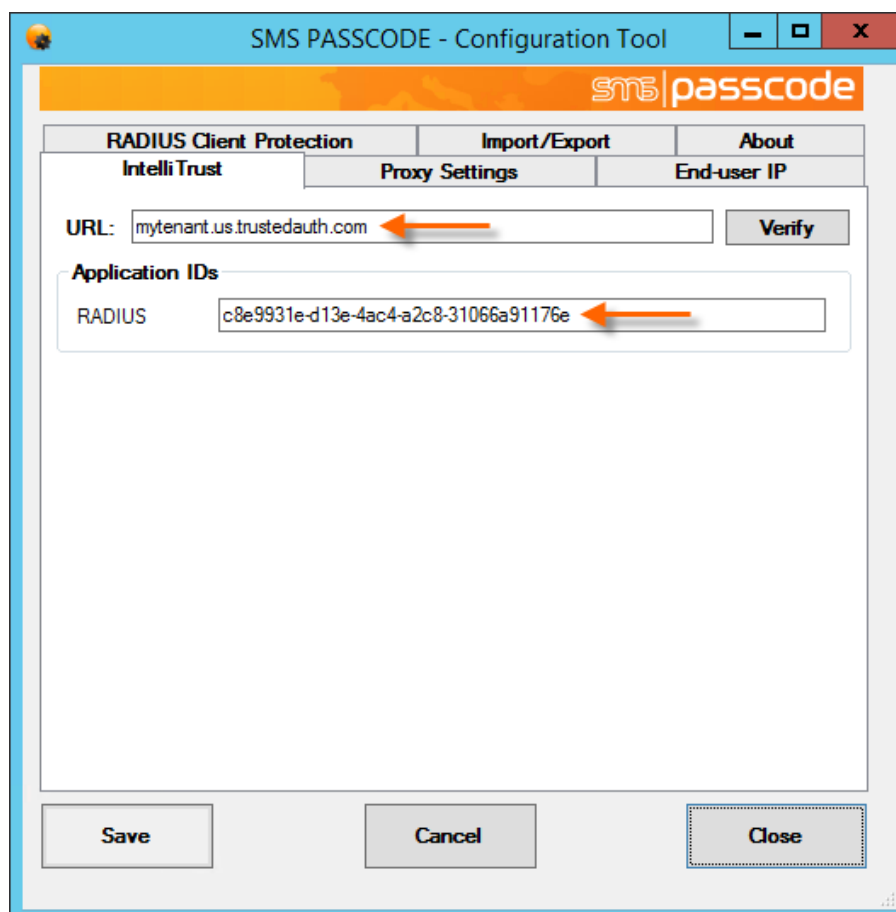
10. At some stage during the installation, the **SMS PASSCODE Configuration Tool** is automatically started:



This tool is used for configuring the SMS PASSCODE components installed on the current machine. You may not see all the tabs shown in the picture above because the user interface of the **SMS PASSCODE Configuration Tool** is automatically adapted according to the components installed.

You must now configure a connection to the IntelliTrust™ cloud service and save the settings before the SMS PASSCODE installation is complete. Please follow the instructions below.

- a. On the **IntelliTrust** tab, enter the URL for your IntelliTrust tenant, and an application ID for each SMS PASSCODE protection installed. Example:



The screenshot shows the 'SMS PASSCODE - Configuration Tool' window. The 'IntelliTrust' tab is selected. The 'URL' field contains 'mytenant.us.trustedauth.com' and the 'Application IDs' field contains 'c8e9931e-d13e-4ac4-a2c8-31066a91176e'. A 'Verify' button is next to the URL field. At the bottom are 'Save', 'Cancel', and 'Close' buttons.

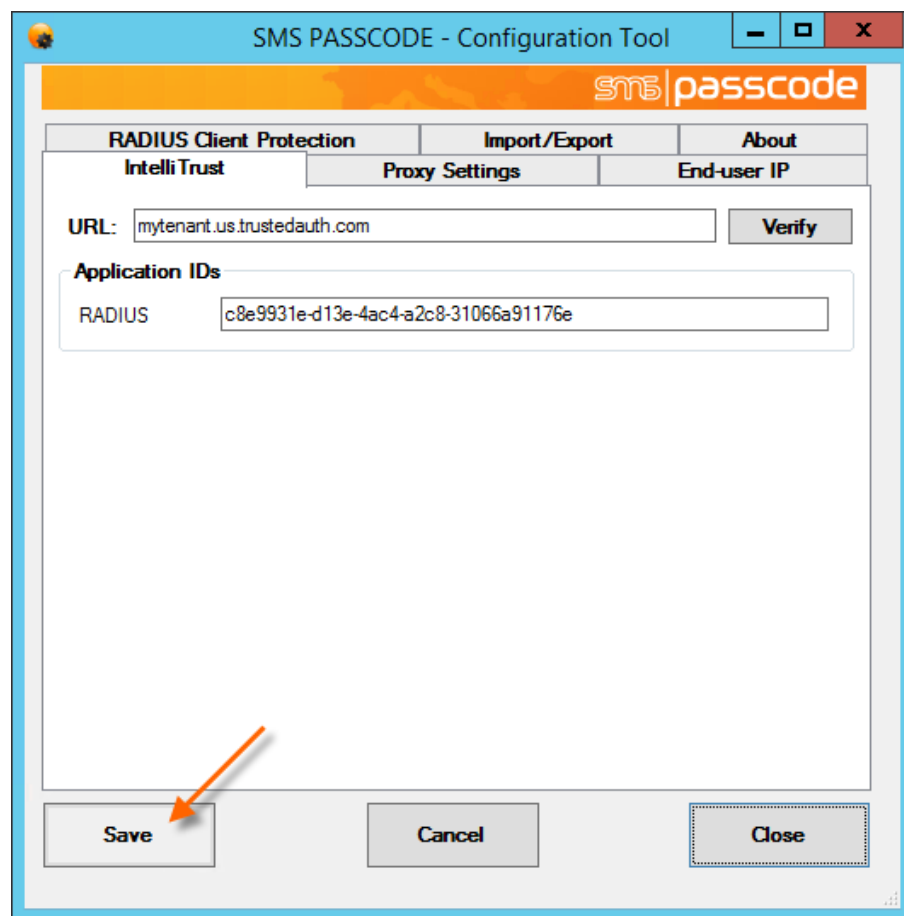
It is recommended to click the **Verify** button to check, that you have entered a valid tenant URL, and that it is possible to connect to the IntelliTrust cloud service. If connecting to IntelliTrust fails, this could be because your network infrastructure requires communication to go via a proxy server. In that case, configure proxy settings on the **Proxy Settings** tab, then retry the **Verify** button.

**Important: Always remember to specify IntelliTrust connection data**

Entry of valid IntelliTrust connection data is mandatory. Without such valid data, the authentication client will not be able to connect correctly to the IntelliTrust cloud service, causing authentication attempts to fail.



- b. Click the **Save** button.

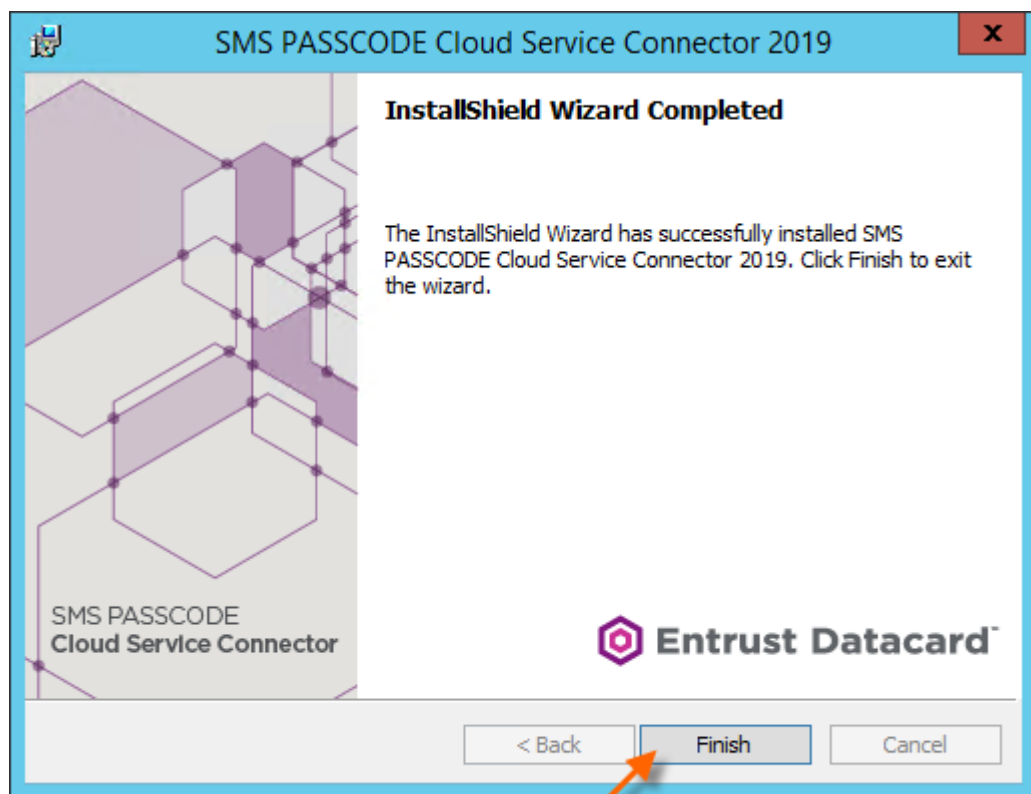


In case a warning message appears regarding error prone entries:  
Please correct all errors and click the **Save** button again.

- c. Click the **Close** button. The installation will now continue.

**Please note:** If you have entered incorrect data in the SMS PASSCODE Configuration Tool by accident or if you wish to change some settings later on, then you can always run the **SMS PASSCODE Configuration Tool** again manually. A shortcut to this tool is created in the Windows Start menu.

11. The dialog below appears when the installation has completed. Click the **Finish** button.

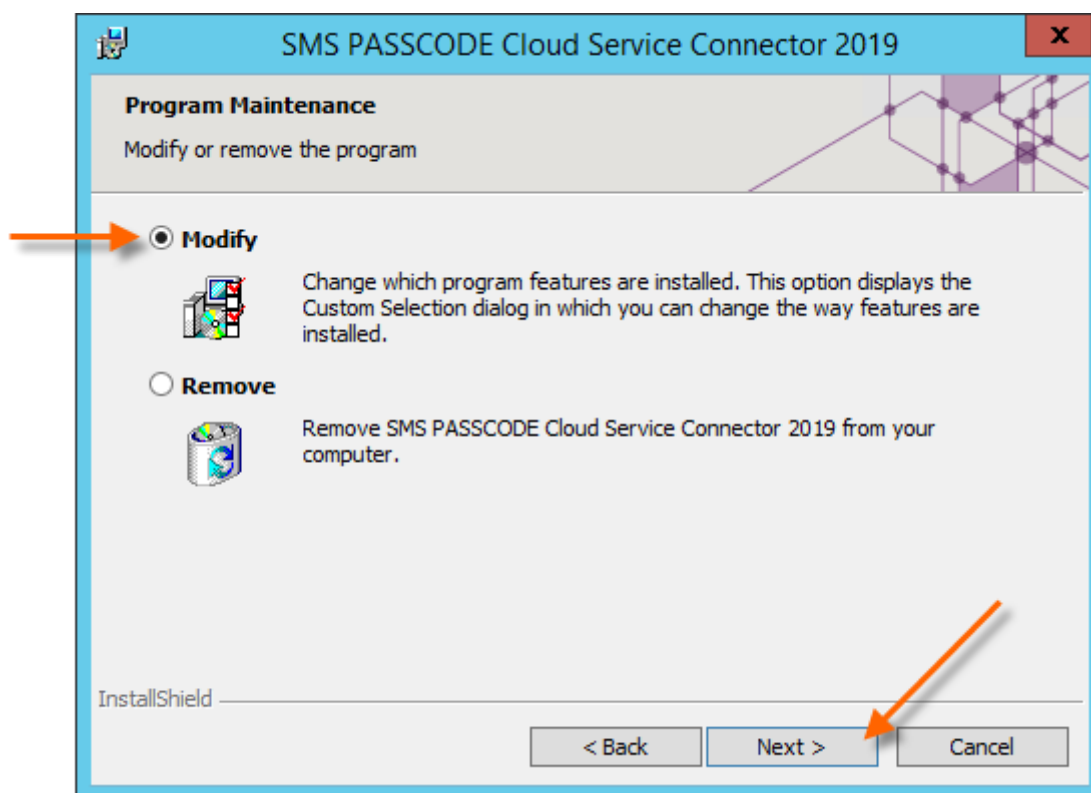


12. The installation of SMS PASSCODE is now complete on the current machine. You should now perform any necessary configurations of this machine (cf. section 11).
13. If more machines are part of the installation: Please go back to step 1 (page 9) and follow the same instructions for the next machine.

## 10 ADD/REMOVE COMPONENTS

If you wish to add or remove some components from the SMS PASSCODE installation, you can always run the SMS PASSCODE installation again – as often as you like. In this way, you can add or remove *SMS PASSCODE Authentication Clients*.

To add/remove *SMS PASSCODE Authentication Clients*, simply run the SMS PASSCODE installation program again – just as you would do during a first-time installation. You will notice that a different dialog is shown in this case:



Please select **Modify** in this dialog and click the **Next** button. After this, follow the same procedure as you did during first-time installation.

## 11 POST-INSTALLATION ACTIONS

After having completed the SMS PASSCODE installation, you may perform additional configuration of the different authentication clients:

- 1) Configuration of the **RADIUS Protection** component.  
Please read section 12.1 (page 21).
- 2) Configuration of the **AD FS Protection** component.  
Please read section 12.2 (page 37) regarding AD FS 3.0/4.0.

## 12 CONFIGURING AUTHENTICATION CLIENTS

### 12.1 Configuring RADIUS Protection

This section describes the configuration steps you must perform if you have installed the optional SMS PASSCODE **RADIUS Protection** component, in order to achieve SMS PASSCODE multi-factor authentication for your RADIUS clients.

The SMS PASSCODE RADIUS Protection component is implemented as an extension to the Microsoft Network Policy Server (NPS), which is an optional role of the Windows Server operating system. Below, **NPS server** designates the server where the SMS PASSCODE RADIUS Protection component is installed.

The required configuration steps are:

1. You must ensure that your RADIUS clients have been created and configured within the NPS server. This is described in section 12.1.1 below.

When step 1 has been completed, all RADIUS clients should work immediately with SMS PASSCODE multi-factor authentication enabled, using the default settings of the SMS PASSCODE RADIUS Protection component.

2. Optionally, you might want to configure advanced settings for some of your RADIUS clients. For example allow users to log in, when their password has expired, or enable collection of end-users' IP addresses. In these cases, the SMS PASSCODE Configuration Tool allows you to configure such settings. Either, you can maintain the same settings across all your RADIUS clients, or you can even decide to maintain such settings per Connection Request Policy (CRP) of the NPS server. Since CRPs can identify RADIUS connections on many different conditions, this provides a lot of flexibility. For example, you can configure different settings per RADIUS client, per user or per RADIUS client vendor.

Configuring RADIUS settings in the SMS PASSCODE Configuration tool is described in section 12.1.2, page 25.

#### IMPORTANT:

By default, authentication and authorization settings of CRPs and settings of Network Policies (NP) are ignored during SMS PASSCODE authentication. However, you can enable internal NPS logic to apply CRP/NP settings (cf. section 12.1.2.1, page 30).

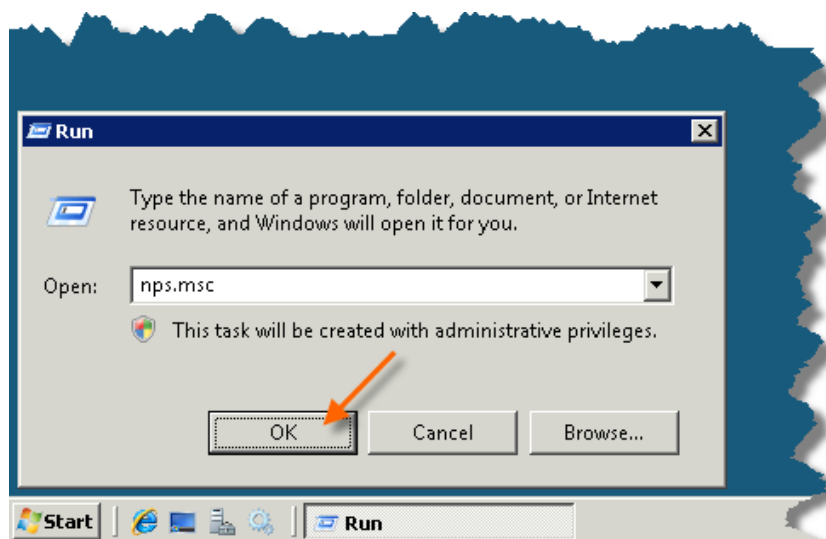
### 12.1.1 Configuring RADIUS Protection on a Windows Server

This section describes how to set up the connection between your RADIUS clients and the NPS server (if not already done beforehand). After this, SMS PASSCODE multi-factor authentication should work out-of-the-box, for the configured RADIUS clients, using default settings for the SMS PASSCODE RADIUS Protection component. Please follow the procedure below:

1. Configure all RADIUS clients in the usual way by specifying the **NPS server** as the RADIUS server. If you are in doubt how to perform the configuration, please refer to the configuration guide of the specific RADIUS client in question.

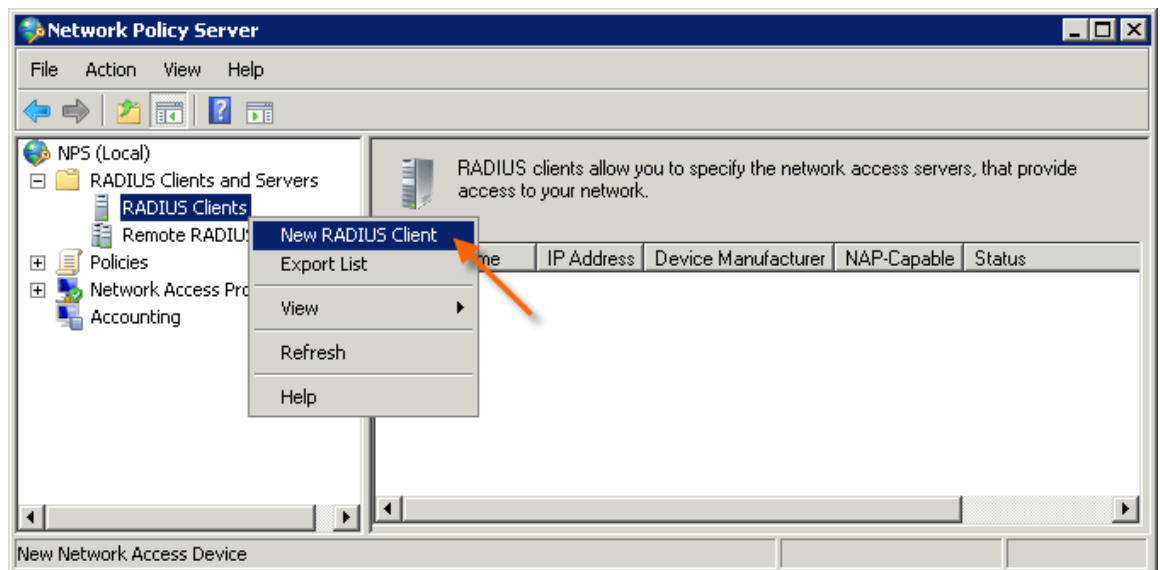
**Important:** The user experience is best for RADIUS clients supporting *Challenge Response*. If *Challenge Response* support is configurable on the RADIUS client, please enable it.

2. Start the NPS Management Console:
  - a. Select **Run...** in the Windows Start menu
  - b. Enter `nps.msc`
  - c. Click **OK**



3. The NPS Management Console is shown.
4. Now you must create all your RADIUS Clients in the NPS Management Console. If these have already been created beforehand, you can skip to step 9.

5. To create a RADIUS Client:
  - a. Right-click the **RADIUS Clients** node.
  - b. Select **New RADIUS Client**.



6. The **New RADIUS Client** dialog appears.
- Enter a “friendly name” of the RADIUS Client.
  - Enter the IP address of the RADIUS Client.
  - Enter and confirm the **Shared Secret**. It must match the shared secret configured on the RADIUS Client.
  - Click **OK**.

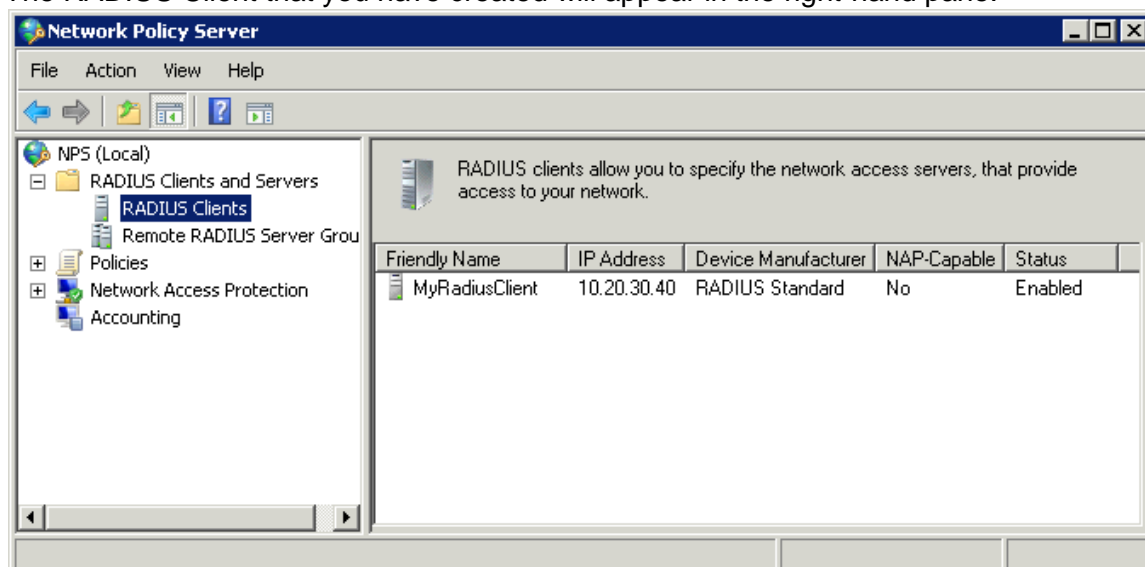
The screenshot shows the 'New RADIUS Client' dialog box. It has a title bar with a close button. The dialog is divided into several sections:

- Enable this RADIUS client:** A checked checkbox.
- Name and Address:** A section with two text boxes. The first is labeled 'Friendly name:' and contains 'MyRadiusClient'. The second is labeled 'Address (IP or DNS):' and contains '10.20.30.40'. There is a 'Verify...' button to the right of the address box.
- Vendor:** A section with a dropdown menu labeled 'Vendor name:' showing 'RADIUS Standard'.
- Shared Secret:** A section with a text area containing instructions: 'To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.' Below this are two radio buttons: 'Manual' (selected) and 'Generate'. There are two text boxes for the shared secret, both filled with dots. Arrows labeled 'c' point to these two boxes.
- Additional Options:** A section with two checkboxes: 'Access-Request messages must contain the Message-Authenticator attribute' and 'RADIUS client is NAP-capable'. An arrow labeled 'd' points to the 'OK' button.

At the bottom right are 'OK' and 'Cancel' buttons.



7. The RADIUS Client that you have created will appear in the right-hand pane:



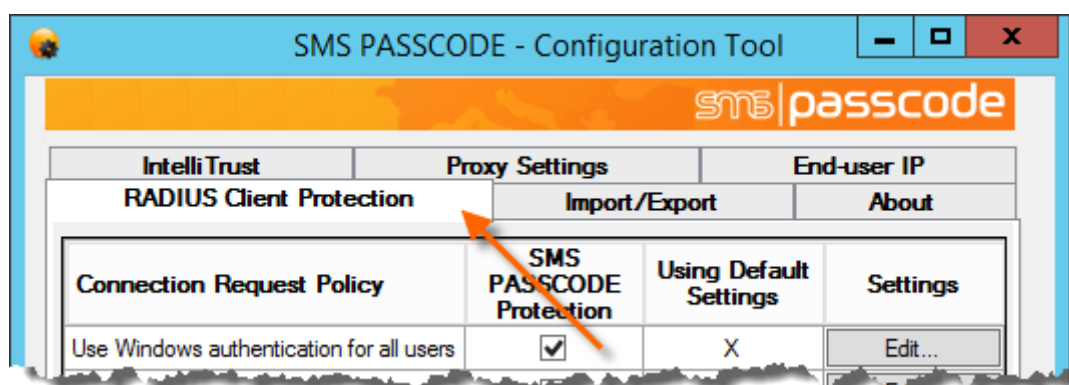
8. Repeat steps 5-7 if you need to create more RADIUS Clients.
9. This completes the standard configuration of RADIUS authentication using SMS PASSCODE. Please test each RADIUS client to make sure that RADIUS authentication works as expected.

### 12.1.2 Advanced Configuration of the RADIUS Protection Component

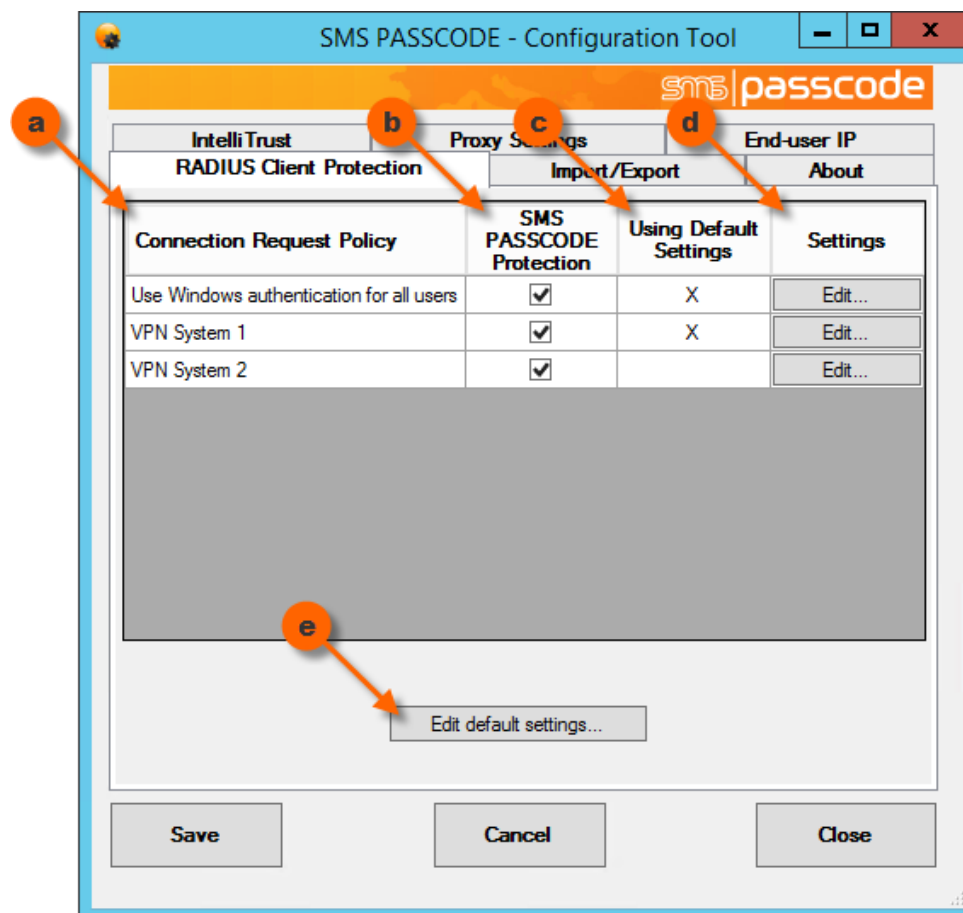
This section describes, how you can maintain advanced settings of the SMS PASSCODE RADIUS Protection component.

To maintain such settings, you need to start the SMS PASSCODE Configuration Tool, which is available via the Windows Start Menu.

After opening the SMS PASSCODE Configuration Tool from the Windows Start Menu you will see several tabs. Select the **RADIUS Client Protection** tab to configure the advanced RADIUS settings:



On the **RADIUS Client Protection** tab, you will see a table of the Connection Request Policies (CRPs) that currently exist in the NPS:

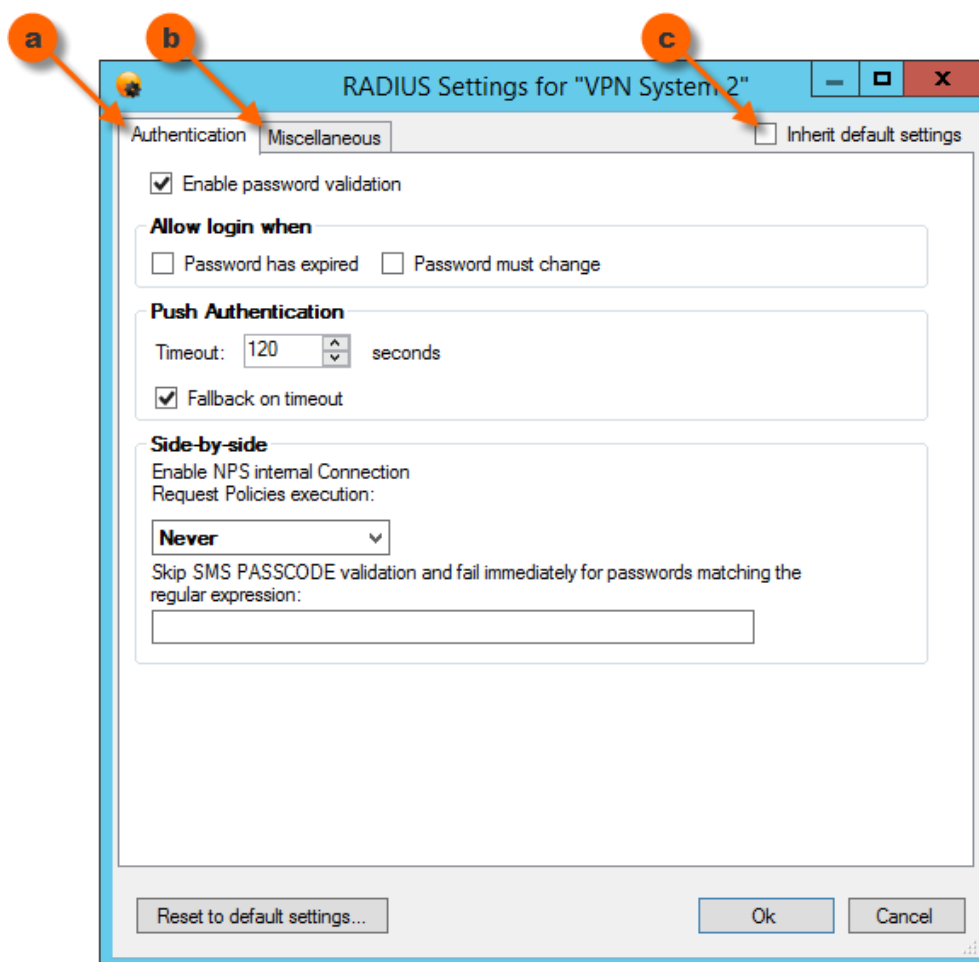


The columns of the table are explained below:

	Explanation
(a)	<p>Column (a) lists the names of all the CRPs that currently exist in the NPS. Whenever you create or delete CRPs in NPS, such changes are automatically reflected in the Configuration Tool (when you restart it).</p> <p><b>NOTE:</b> It is NOT recommended to rename CRPs in NPS. A renamed CRP will be treated as a new CRP in the SMS PASSCODE Configuration Tool, meaning any previous CRP-specific SMS PASSCODE settings will be lost.</p>

	Explanation
(b)	<p>Column (b) specifies, whether the SMS PASSCODE RADIUS Protection component is enabled for the corresponding CRP in column (a). A selected or cleared checkbox indicates that the SMS PASSCODE RADIUS Protection component is enabled or disabled, respectively.</p> <p>The SMS PASSCODE RADIUS Protection component is enabled by default for all CRPs. This also applies to new CRPs, if you create such later on.</p> <p>Select the checkbox in a specific row to enable SMS PASSCODE RADIUS Protection for the CRP listed in column (a). All RADIUS authentication requests made through such a CRP are handled by the SMS PASSCODE NPS extension, allowing for SMS PASSCODE multi-factor authentication.</p> <p>Clear the checkbox in a specific row to disable the SMS PASSCODE RADIUS Protection component for the CRP listed in column (a). All RADIUS authentication requests made through such a CRP will be handled by the NPS default functionality.</p>
(c)	<p>When maintaining SMS PASSCODE RADIUS Protection settings, you can maintain <i>default settings</i>, which will apply to all CRPs by default. However, it is possible to apply specific settings to selected CRPs, if this is needed, for example in order to handle different requirements for different RADIUS clients.</p> <p>Column (c) indicates, whether the corresponding CRP of column (a) has been configured to use <i>default settings</i> (marked with an "X") or to use specific settings (marked with an empty cell).</p>
(d)	<p>Click the <b>Edit...</b> button in column (d) to edit the SMS PASSCODE RADIUS settings for a specific CRP. This allows you to define CRP-specific settings for the CRP listed in column (a), or to revert the CRP back to <i>default settings</i> again.</p>
(e)	<p>Click the <b>Edit default settings...</b> button to edit the <i>default settings</i>, i.e. the settings that apply to all CRPs with an "X" in column (c).</p>

When clicking the edit buttons (d) or (e), a new window will open, which allows you to configure the CRP-specific settings or default settings, respectively:



As shown, the window contains the following controls at the top of the window:

	Explanation
(a)	<u>Authentication:</u> This tab contains settings that affect the authentication behavior of the RADIUS Protection component. Please read section 12.1.2.1 (page 30) for further details.
(b)	<u>Miscellaneous:</u> This tab contains miscellaneous settings of the RADIUS Protection component regarding text encoding, end-user IP address collection, challenge/response behavior and more. Please read section 12.1.2.2 (page 36) for further details.
(c)	<u>Inherit default settings</u> This checkbox is only visible, when editing CRP-specific settings. Clear the checkbox to override the default settings and set CRP-specific settings. Select the checkbox in order to inherit the default settings, meaning any changes to the default settings will also apply to the CRP in question.

**IMPORTANT:**

Whenever you change any of the RADIUS Client Protection settings, you must restart the **Network Policy Server** service, before the changes take effect. The SMS PASSCODE Configuration Tool will automatically suggest performing this action for you when the changed settings are saved.

### 12.1.2.1 RADIUS Authentication Settings

The **Authentication** tab contains several settings that allow modification of the *standard authentication flow* of the SMS PASSCODE RADIUS Protection component. The *standard authentication flow*, defining the flow with all settings set to their default values, is defined as follows:

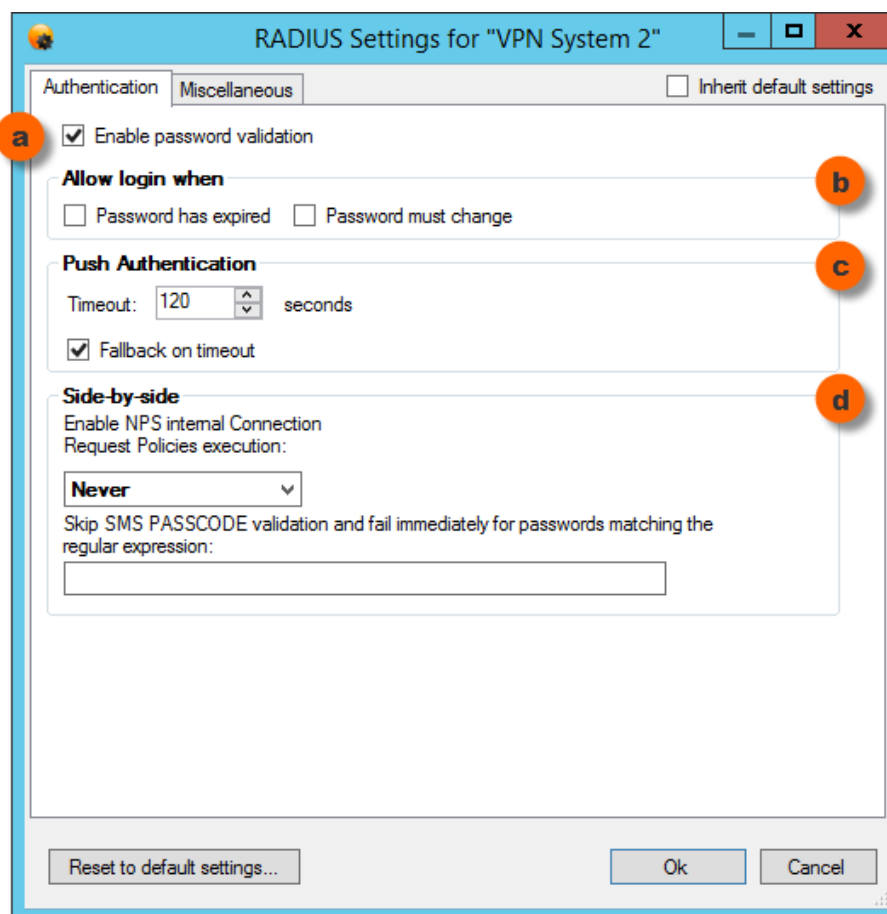
#### SMS PASSCODE RADIUS Protection component

#### Standard Authentication Flow

1. An **Access Request** packet containing a username and a password is received from a RADIUS client.
2. The NPS extension resolves the user, i.e. checks whether the user has been imported in to the USS. If the user cannot be determined (uniquely), then access is denied.
3. The NPS extension checks, whether the user is allowed to log in, for example that the user has not been locked out. If the user is not allowed to log in, then access is denied.
4. The password is verified using Windows Authentication. In this case, access is denied, if any of the following conditions are true:
  - a. The user password is incorrect.
  - b. The user is locked out or denied access.
  - c. The user password has expired.
  - d. The user password has been flagged "Must change at next logon".
5. Internal NPS logic is skipped.  
(I.e. all authentication and authorization settings of the active Connection Request Policy and all settings of the Network Policy are ignored)
6. Now multi-factor authentication is performed according to the user's settings. If a challenge-based authenticator is used, like a random OTP, then a **Challenge Request** is sent back to the RADIUS client. If push authentication is used, the RADIUS request will be hanging, until the user approves the push authentication.
7. In case a challenge-based authenticator is used, the user enters a response, for example an OTP received by SMS or email. The RADIUS client forwards the entered response as a **Challenge Response** to the RADIUS server.
8. In case a challenge-based authenticator is used, the RADIUS server now verifies, whether the response received is valid or not, resulting in either an **Access Accept** or **Access Reject** packet being sent back to the RADIUS client, respectively. If push authentication is used, the RADIUS server returns an **Access Accept** or **Access Reject** packet, depending on whether the user accepted or rejected the authentication request.

It is described below how you can modify the individual steps of the *Standard Authentication Flow*.

The **Authentication** tab contains the following settings:



The settings have the following purposes:

**a. Enable password validation**

This setting defines whether password validation must occur at all. By default, it is enabled. Clear the checkbox to skip step 4 of the *Standard Authentication Flow*. In this case, no password validation will be performed, unless internal NPS logic is enabled (cf. item d below).

**WARNING:**

Use this setting with great caution. It is only recommended to skip password validation for RADIUS clients that will check the user password by themselves, before the RADIUS request is sent to the RADIUS server, or if internal NPS logic is enabled (setting d) and set to validate the password. If this is not observed, users can log in without the need to enter any valid password.

**b. Allow login when**

This setting controls the behavior of steps 4c and 4d of the *Standard Authentication Flow*. By default, the SMS PASSCODE RADIUS Protection component will reject an authentication attempt from a user using an expired password or using a password that has been flagged “must be changed at next logon”. However, you can change this behavior. This might make sense when a user is requesting remote access using a VPN connection. In this case, it might be acceptable to give the user network access and in this way allow the user to renew/change the password.

**Password has expired:** Select this setting to allow successful authentication with a password

that has expired.

**Password must change:** Select this setting to allow successful authentication with a password that has been flagged “must change at next logon”.

**c. Push Authentication**

In case push authentication is used, the RADIUS server will let the network call from the RADIUS client hang, until the end-user has either approved or rejected the authentication request inside the Entrust Mobile app. However, as the RADIUS client will not wait forever on a network reply, the RADIUS server will eventually have to time out and send a reply, if the end-user does not take action in time. The **Timeout** setting defines, for how long the RADIUS server must wait for a user accept/reject action, before timing out. It is important to adjust this timeout setting according to the timeout setting of the RADIUS client. The RADIUS server timeout should be at least 1 second less than the RADIUS client timeout. It is recommended to configure your RADIUS client to have a timeout of at least 45 seconds, if possible – in order to allow your end-users to have enough time to accept/reject push authentication requests.

On timeout, if the **Fallback on timeout** setting is enabled, and if the authentication settings of the user have been configured to allow an alternative, challenge-based authenticator, then the RADIUS server will return a Challenge-Response packet to the RADIUS client, thereby allowing the user to enter a response for the alternative authentication mechanism. On the other hand, if **Fallback on timeout** is NOT enabled, or if the authentication settings of the user have been configured to NOT allow an alternative, challenge-based authenticator, then the RADIUS server will return an **Access Reject** packet on timeout.

**d. Side-by-side**

This section contains settings that define how the SMS PASSCODE RADIUS Protection component will interact with the internal NPS logic. This is an advanced topic, and changing these settings is typically only required, if you need to set up a side-by-side scenario, where users can log in either using SMS PASSCODE or another RADIUS authentication system. However, changing the settings can also be required in other cases, where the internal NPS logic is required, e.g. if you would like to make use of the functionality provided by NPS through **Connection Request Policies** or **Network Policies**.

The following abbreviations are used below:

- **CRP:** Connection Request Policy
- **NP:** Network Policy
- **NPS IL setting:** The setting called “Enable NPS internal Connection Request Policies execution” in the Side-by-Side section. “IL” is an abbreviation for “Internal Logic”.
- **SVF setting:** The setting called “Skip SMS PASSCODE validation and fail immediately for passwords matching the regular expression” in the Side-by-Side section. “SVF” is an abbreviation for “Skip Validation and Fail”.



The possible options for the **NPS IL setting** are:

NPS IL setting	Description
<b>Never</b>	<p>The SMS PASSCODE RADIUS component takes full control of the authentication and performs a standard SMS PASSCODE multi-factor authentication. All internal NPS logic is skipped (as described in step 5 of the <i>Standard Authentication Flow</i>).</p> <p>This means that any authentication and authorization settings of <b>CRPs</b>, and/or any settings of <b>NPs</b> will be ignored.</p> <p>This is the default setting.</p>
<b>Always</b>	<p>Step 5 of the <i>Standard Authentication Flow</i> is changed. Instead of skipping, authentication is now forwarded to the internal NPS logic. I.e. <b>CRP</b> and <b>NP</b> settings will be applied. This means, that if the CRP is set to perform an authentication or is set to forward authentication to another RADIUS server, then this will be executed.</p> <p>Access is denied, if any CRP/NP logic denies access, e.g. because authentication according to the CRP fails, or because access is not allowed according to the NP. Otherwise, authentication will continue at step 6 of the <i>Standard Authentication Flow</i>.</p>
<b>On failure only</b>	<p>First steps 1-4 of the <i>Standard Authentication Flow</i> are executed normally. If the user has not been denied access so far, then the <i>Standard Authentication Flow</i> continues as defined by default. I.e. the same behavior is achieved, as when the <b>NPS IL setting</b> is set to <b>Never</b>.</p> <p>However, if the user is denied access during any of the steps 2-4, then the internal NPS logic will be executed, and the remaining part of the <i>Standard Authentication Flow</i> will be <u>skipped</u>.</p> <p>In other words, <b>CRP</b> and <b>NP</b> settings will be applied. Access is denied, if any CRP/NP logic denies access, e.g. because authentication according to the CRP fails, or because access is not allowed according to the NP.</p> <p>On the other hand, if the user is allowed to log in according to the CRP/NP settings, then the user is granted access <u>immediately</u>, i.e. no multi-factor authentication by SMS PASSCODE occurs in this case.</p> <div> <p><b>WARNING:</b></p> <p>When selecting the option <b>On Failure only</b>, <u>never</u> set the CRP to allow access without validating credentials. This would grant access to users without any validation at all.</p> </div>

The authentication behavior can be modified additionally using the **SVF setting**:

- i. Empty (default):  
This setting has no effect.
- ii. Non-empty (password filtering):  
If you enter a regular expression into this field, SMS PASSCODE will check, on each authentication attempt, whether the regular expression matches the password

entered<sup>1</sup>. If it does not match, then the authentication continues normally. On the other hand, if there is a match, then steps 2-4 of the *Standard Authentication Flow* are skipped altogether, meaning no user resolve or password validation is performed. Instead, the steps 2-4 are immediately treated as failed. As a result, the following behavior is achieved with a matching password:

**NPS IL setting** set to **Never**: The user is denied access.

**NPS IL setting** set to **Always**: The user is denied access.

**NPS IL setting** set to **On Failure Only**: The internal NPS logic will be applied, CRP and NP settings are applied, and no multi-factor authentication is performed by SMS PASSCODE.

---

<sup>1</sup> This is only supported, when the RADIUS client uses the PAP protocol. MS-CHAP v2 is not supported, since the password is not available in clear text for comparison in this case.

Below, a number of use case scenarios are listed, and it is described how to set settings accordingly:

Use case	Required settings
<ul style="list-style-type: none"> <li>Standard SMS PASSCODE multi-factor authentication must be performed for all users.</li> <li>No need for Network Policy support.</li> </ul>	<ul style="list-style-type: none"> <li>Set the <b>NPS IL setting</b> to <b>Never</b>.</li> </ul>
<ul style="list-style-type: none"> <li>Standard SMS PASSCODE multi-factor authentication must be performed for all users.</li> <li>Support for Remote Access Policies is needed.</li> </ul>	<ul style="list-style-type: none"> <li>Set the <b>NPS IL setting</b> to <b>Always</b>.</li> <li>Set the CRP authentication setting to <b>Authenticate on this server</b>.</li> </ul>
<ul style="list-style-type: none"> <li>You have two different RADIUS authentication systems (SMS PASSCODE and another one).</li> <li>Some users will only use one type of authentication, whereas some users might use both types of authentication.</li> </ul>	<ul style="list-style-type: none"> <li>Set the <b>NPS IL setting</b> to <b>On Failure Only</b>.</li> <li>Set the CRP authentication setting to forward requests to the other RADIUS system.</li> <li>Optional: If the password for the <u>other</u> authentication system is NOT the user's AD password, and this authentication system is used often by users, which are <u>also</u> created in the USS, then it can be a problem that AD password validation is attempted often with a wrong password. It could lead to a lockout of AD user accounts. To avoid this, you should enter a regular expression into the <b>SVF setting</b> that will identify the passwords of the <u>other</u> authentication system. On the other hand, if the users using the other authentication system are NOT created in the USS, then there is no problem, since SMS PASSCODE will not perform any AD password validations for such users.</li> </ul>
<ul style="list-style-type: none"> <li>Standard SMS PASSCODE multi-factor authentication must be performed for all users, except the users' passwords should not be validated by AD, but by another RADIUS authentication system.</li> </ul>	<ul style="list-style-type: none"> <li>Set the <b>NPS IL setting</b> to <b>Always</b>.</li> <li>Set the CRP authentication setting to forward requests to the other RADIUS system.</li> <li>Clear setting (a), "Enable password validation", to skip the initial validation of the password for all requests from the RADIUS client(s) in question.</li> </ul>

**NOTE:**

The **SVF setting** only works when the RADIUS client is using the PAP protocol. MS-CHAP v2 is NOT supported.

### 12.1.2.2 Miscellaneous RADIUS settings

The remaining SMS PASSCODE RADIUS Protection settings are collected on the **Miscellaneous** tab:

RADIUS Settings for "VPN System 2"

Authentication Miscellaneous ☐ Inherit default settings

**Text settings**

Code Page used for encoding:  
65001

**End-user IP**

☐ Collect end-user IP address from RADIUS attribute:  
31

**Challenge/Response**

☒ Auto-detect challenge/response support (default)  
☐ Require challenge/response support  
☐ Do not use challenge/response  
☒ Send state attribute

Reset to default settings... Ok Cancel

The settings have the following purposes:

**a. Text settings**

**Code Page used for encoding:** This setting specifies the Windows Code Page used for encoding input texts, i.e. usernames, passwords and passcodes. If the RADIUS client uses a specific code page, please ensure to enter the same code page here. For example, many Cisco VPN clients use code page 1252. If the code page of the RADIUS client and RADIUS server do not match, you might experience authentication problems for users using special characters in their username or password.

**b. End-user IP**

This setting allows you to configure, whether SMS PASSCODE RADIUS Protection must collect the end-user's IP address from a specific attribute of the RADIUS Access Request packet. This can be useful for authentication monitoring. To enable this, select the checkbox **Collect end-user IP address from RADIUS attribute**, and then enter the number of the RADIUS attribute that contains the end-user IP.

### c. **Challenge/Response**

SMS PASSCODE RADIUS Protection supports both RADIUS clients that support or do not support challenge/response. By default, when the first request is received from a RADIUS client after the NPS has started, the SMS PASSCODE NPS extension will auto-detect whether the RADIUS client supports challenge/response or not. If the client does not support challenge/response, then SMS PASSCODE authentication is performed in two steps: first validating the user password in a first RADIUS authentication and then validating the SMS PASSCODE in a second RADIUS authentication. This means a non-session-specific multi-factor authentication is performed; opposite to a challenge/response multi-factor authentication, which will always be session-specific.

If you do not wish to allow the auto-detection mechanism described above, you can customize the behavior, by selecting the appropriate setting:

**Auto-detect challenge/response support:**

This is the default behavior, as described above.

**Require challenge/response support:**

Auto-detection is disabled. Only RADIUS clients supporting challenge/response will be able to authenticate successfully.

**Do not use challenge/response:**

Auto-detection is disabled. Challenge/response is never used. Instead, all authentications are performed in two steps, using non-session-specific multi-factor authentication.

According to the RADIUS RFC, all RADIUS challenge packets should contain a state attribute (which is a session identifier). However, some RADIUS clients seem not to support this state attribute correctly. In case you experience this, you can clear the **Send state attribute** setting, which will force SMS PASSCODE Protection not to insert the state attribute. Clearing the setting is NOT recommended unless it is required.

Since you can customize different settings per CRP of the NPS, this allows you to define different settings for different CRPs – for example collecting end-user IP addresses from different RADIUS attributes for different RADIUS clients.

## 12.2 Configuring AD FS 3.0/4.0 Protection

The SMS PASSCODE **AD FS Protection** component adds multi-factor authentication to applications that are accessible via AD FS 3.0 and 4.0. This section describes the integration with [AD FS 3.0](#) and [AD FS 4.0](#), and describes how to configure SMS PASSCODE **AD FS Protection** for AD FS 3.0/4.0.

SMS PASSCODE **AD FS Protection** for [AD FS 3.0/4.0](#) allows you to apply SMS PASSCODE multi-factor authentication to all authentication scenarios supported by the AD FS 3.0/4.0 infrastructure, spanning from access to cloud applications and published internal web sites, to provisioning of devices during *workplace joins*.

If you have already, before installing the SMS PASSCODE AD FS Protection component, successfully configured your AD FS infrastructure, then you simply need to install the SMS

PASSCODE AD FS Protection component on your AD FS server(s) and enable the SMS PASSCODE multi-factor authentication adapter in the AD FS management console afterwards. The procedure for this is described below.

### 12.2.1 Background

AD FS 3.0/4.0 is an optional Windows Server role in Windows Server 2012 R2 and Windows Server 2016, respectively. It provides an infrastructure that allows identity validation during access to different types of services, using the AD identities of your organization. Examples of “services” are:

- Cloud applications, like Microsoft Office 365, Google Apps and Salesforce.
- Internally hosted websites, published through the Microsoft Web Application Proxy. For example, you can publish an internally hosted Outlook Web Access site.
- *Workplace joins*, allowing people within your organization to approve devices (smartphones and tablets) to let them access data within your organization.

Any such authentication scenarios supported by the AD FS infrastructure can be extended with SMS PASSCODE multi-factor authentication (MFA), by installing SMS PASSCODE AD FS Protection on your AD FS server(s) and enabling MFA for the applications of your choice, in the AD FS management console.

### 12.2.2 AD FS 3.0/4.0 Infrastructure

This section describes on which servers you should install the SMS PASSCODE AD FS Protection component.

When deploying AD FS 3.0/4.0, there are two important server roles: The AD FS main server(s), responsible for performing the actual authentications, and the Web Application Proxy server(s), used for publishing HTTP/HTTPS based applications for external access, as well as functioning as AD FS Proxies. In such a configuration, you will need to install SMS PASSCODE AD FS Protection on the AD FS main server(s), not on the Web Application Proxy servers.

The SMS PASSCODE AD FS Protection component supports AD FS farms. It is important in a farm configuration that SMS PASSCODE AD FS Protection is installed on every AD FS server in the farm.

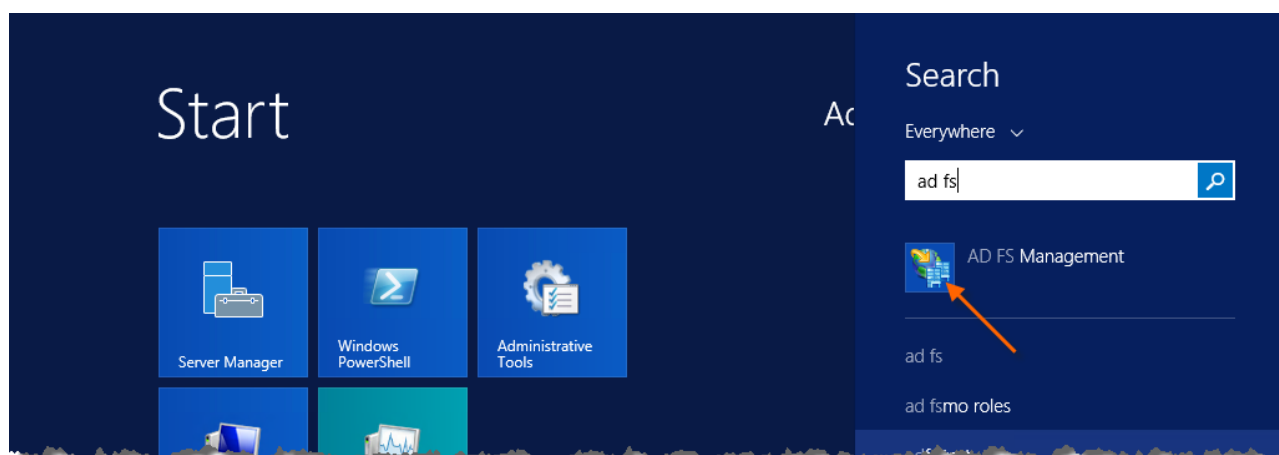
The installation of the AD FS Protection component on each AD FS server will install a so-called SMS PASSCODE AD FS **MFA Adapter** on every such server. You need to configure this MFA Adapter, to activate SMS PASSCODE multi-factor authentication. This is described below in sections 12.2.3 and 12.2.4 for AD FS 3.0 and 4.0, respectively.

### 12.2.3 Configuring the MFA Adapter for AD FS 3.0

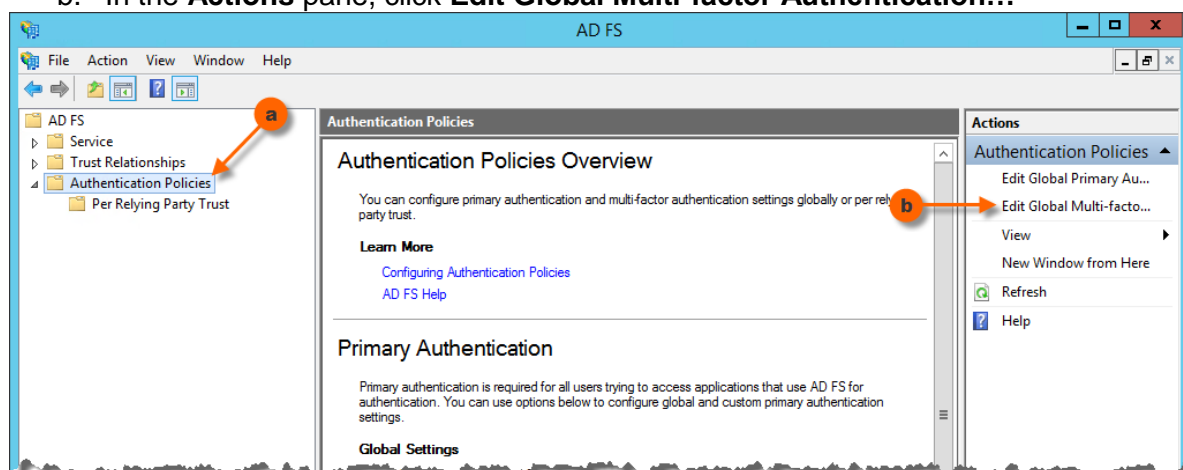
This section applies to Windows Server 2012 R2. It is described below, how you enable the SMS PASSCODE MFA Adapter, after you have installed it on your AD FS server (or on every AD FS server, in case of an AD FS farm).

In order to enable the MFA Adapter, please follow the procedure below:

1. Open the AD FS Management console (`Microsoft.IdentityServer.msc`) on your primary AD FS server:



2. In the AD FS Management console:
  - a. Select the **Authentication Policies** node in the tree to the left.
  - b. In the **Actions** pane, click **Edit Global Multi-factor Authentication...**



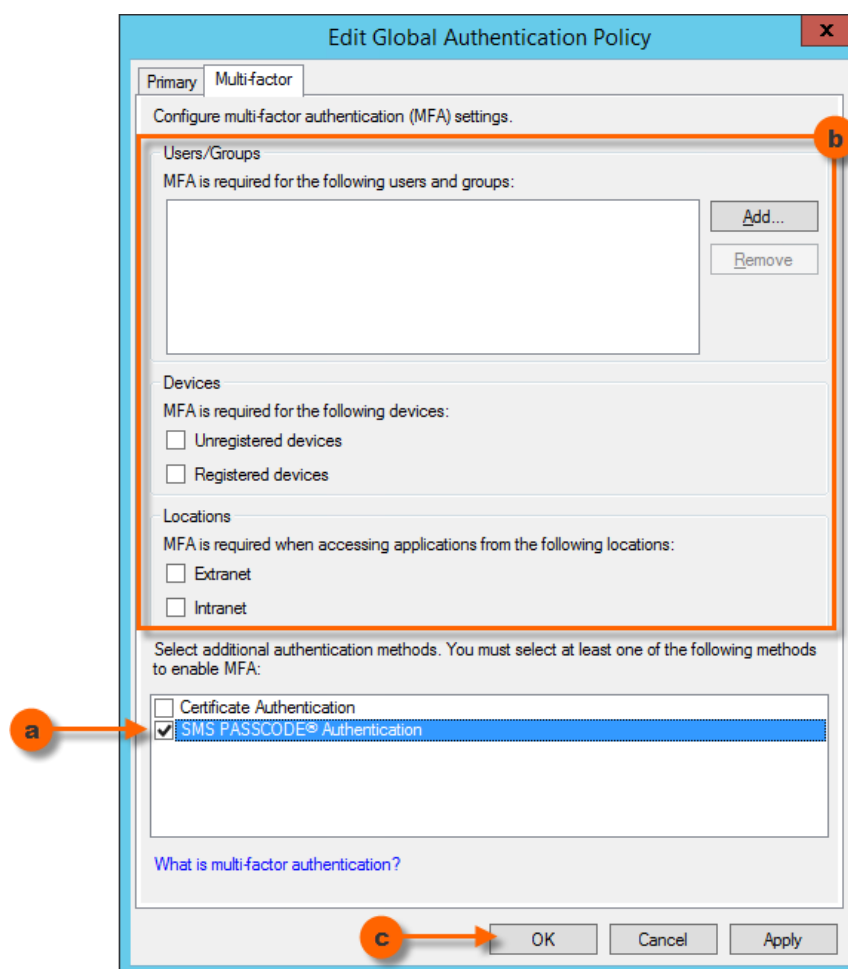
3. The dialog **Edit Global Authentication Policy** opens, with the tab **Multi-factor** selected.
  - a. In the bottom listbox, select the checkbox **SMS PASSCODE Authentication** in order to enable the SMS PASSCODE MFA Adapter.
  - b. Additionally, in order for multi-factor authentications to be triggered, you need to specify the conditions for multi-factor authentication to occur. Either you can specify conditions directly here, on the **Global Authentication Policy**, which will affect all applications ("Relying Parties") – or you may leave the conditions empty here, if you prefer to set individual MFA conditions per application afterwards<sup>2</sup>.

As can be seen, MFA can be activated for specific users/user groups, and/or specific devices (unregistered vs. registered), and/or requests from specific locations (extranet vs. intranet).

For example, you can add the user groups here, from which you are importing SMS PASSCODE users. This will ensure, that all SMS PASSCODE users must perform multi-factor authentication. Alternatively, just select the **Extranet** checkbox in order to ensure, that external requests from any user are multi-factor authenticated.

<sup>2</sup> MFA conditions can be set on a Relying Party Trust, by selecting the specific Relying Party Trust in the AD FS management console, and then click **Edit Custom Multi-factor Authentication...** in the **Actions** pane.

- c. Click the **OK** button.



After having enabled and configured the SMS PASSCODE MFA adapter, please make sure to test the authentication behavior of the affected applications, in order to ensure the expected authentication behavior.

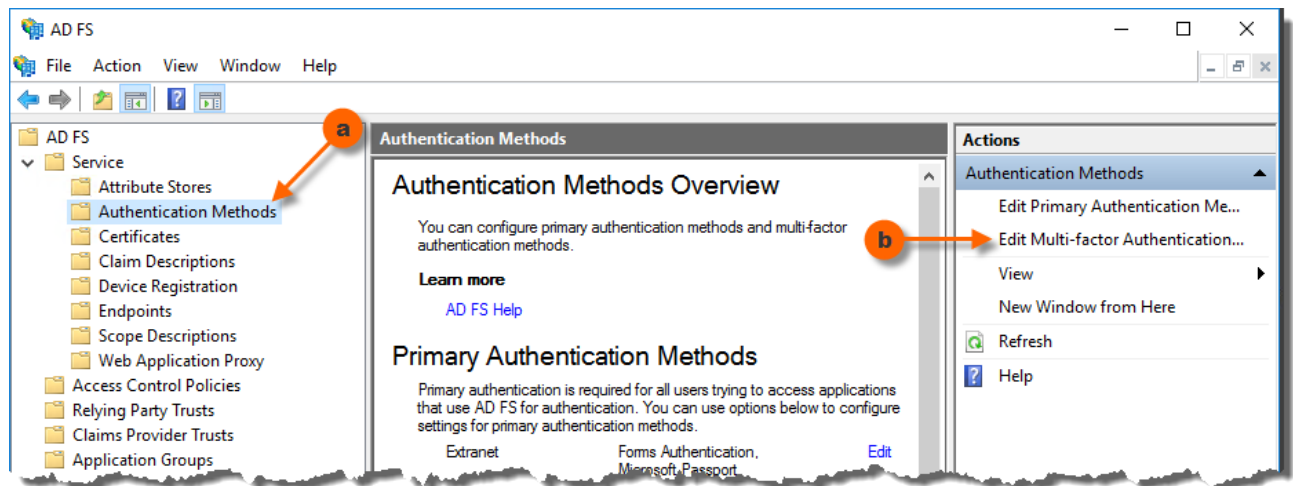
#### 12.2.4 Configuring the MFA Adapter for AD FS 4.0

This section applies to Windows Server 2016. It is described below, how you enable the SMS PASSCODE MFA Adapter, after you have installed it on your AD FS server (or on every AD FS server, in case of an AD FS farm).

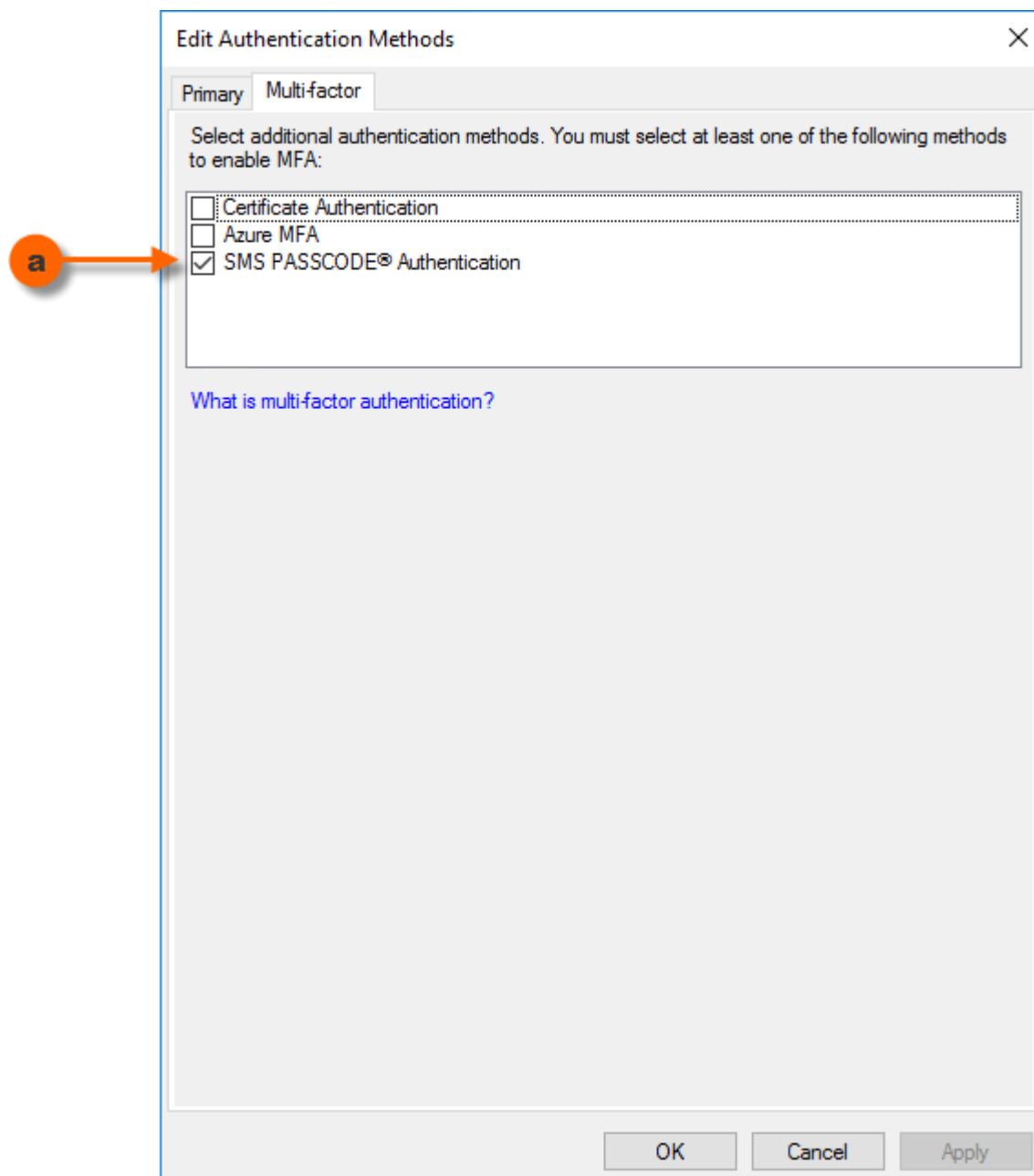
In order to enable the MFA Adapter, please follow the procedure below:

1. Open the AD FS Management console (`Microsoft.IdentityServer.msc`) on your primary AD FS server.
2. In the AD FS Management console:
  - a. Select the **Authentication Methods** node in the tree to the left.
  - b. In the **Actions** pane, click **Edit Multi-factor Authentication Methods...**





3. The dialog **Edit Authentication Methods** opens, with the tab **Multi-factor** selected.
  - a. In the listbox, select the checkbox **SMS PASSCODE Authentication** to enable the SMS PASSCODE MFA Adapter, then click the **OK** button.



4. Additionally, in order for multi-factor authentications to be triggered, you need to specify the conditions for multi-factor authentication (MFA) to occur. This is done by assigning an Access Control Policy that requires MFA to the **Relying Party Trusts**, where you want MFA to occur.

After having enabled the SMS PASSCODE MFA adapter, please make sure to test the authentication behavior of the affected applications, in order to ensure the expected authentication behavior.

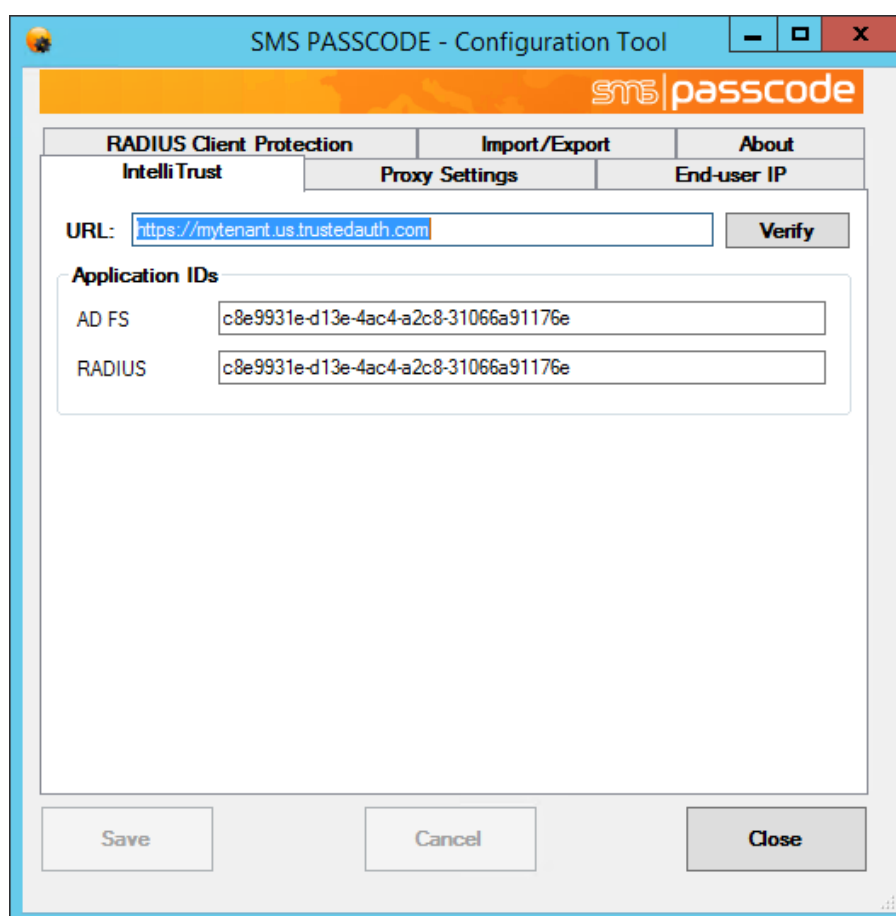
### 12.2.5 Uninstalling the MFA Adapter

In case you uninstall the SMS PASSCODE AD FS Protection component from an AD FS 3.0/4.0 server, please note that this will remove the MFA Adapter only. It will not remove any conditions that you have defined in the AD FS management console, regarding when multi-factor authentication must occur. Consequently, logins might fail after uninstalling the SMS PASSCODE MFA Adapter, unless you manually remove all such conditions for multi-factor authentication.

## 13 CONFIGURATION TOOL

The SMS PASSCODE **Configuration Tool** is used to configure machine specific SMS PASSCODE settings. It is located in the Windows Start Menu.

When you start this tool, you will see several tabs:



The different tabs have the following purposes:

Tab	Explanation
IntelliTrust	This tab allows you to enter connection data for the IntelliTrust™ cloud service. Only users existing within the specified tenant will be able to log in using SMS PASSCODE multi-factor authentication. Click the <b>Verify</b> button on this tab to verify the connection to the IntelliTrust service, and verify the validity of the tenant entered.

Tab	Explanation
<b>Proxy Settings</b>	This tab allows you to enable the usage of a web proxy, meaning that every SMS PASSCODE protection on the local machine will access the USS cloud service via such proxy.
<b>End-user IP</b>	This tab allows you optionally to enable collection of end-user IP addresses for logging purposes. Collection of end-user IP addresses is disabled by default.
<b>RADIUS Client Protection</b>	This tab appears only when SMS PASSCODE <b>RADIUS Protection</b> has been installed on the local server. The tab allows configuring different settings related to the <b>RADIUS Protection</b> component. Please read section 12.1.2 (page 25) for more details.
<b>Import/Export</b>	This tab allows importing and exporting all settings configured in the SMS PASSCODE Configuration Tool. You can either export all settings to a text file or import settings from a text file. This might be useful for backup purposes or for transferring settings from one machine to another one. Please note, that it is possible to import and export settings from the command line (e.g. from a batch file or login script).

## 13.1 Collecting End-User IP Addresses

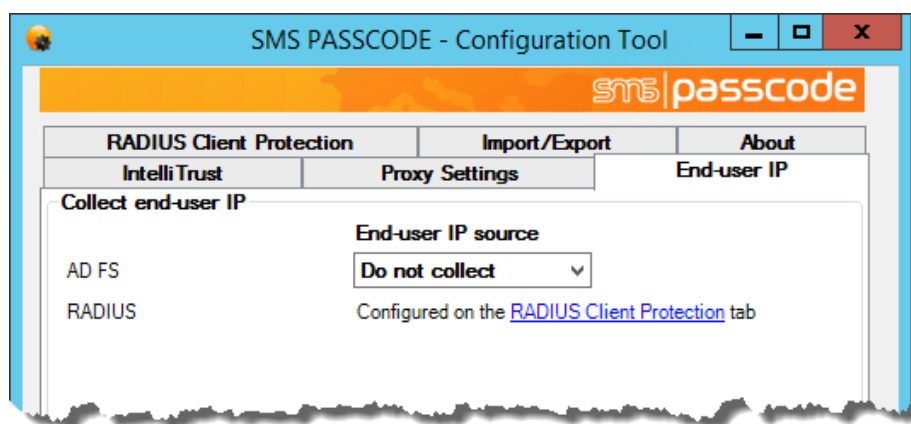
The tab **End-user IP** of the SMS PASSCODE **Configuration Tool** allows you to configure, whether any locally installed SMS PASSCODE authentication clients should collect end-user IP addresses during authentication attempts for logging purposes. When enabled, you will also be able to see which countries are logging in from in the USS reports, determined using geo-IP lookups.

By default, collection of end-user IP addresses is disabled for all clients.

Enabling collection of end-user IP addresses can be done independently for each authentication client installed locally.

**WARNING:** Enabling collection of end-user IP addresses should only be done by network experts having a deep understanding whether the IP addresses are collected correctly in a trustworthy manner.

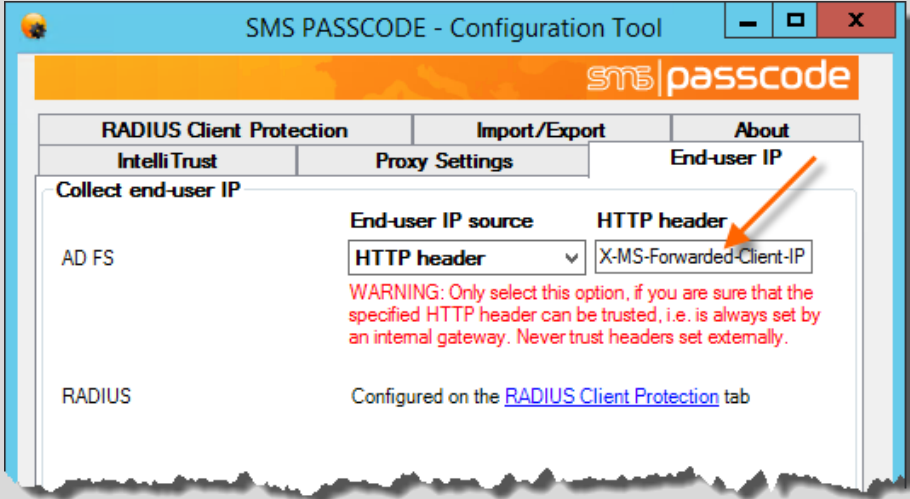
The **End-user IP** tab shows a list of the clients available for configuration. For example, if SMS PASSCODE RADIUS Protection and AD FS Protection are installed locally, the tab will look like this:



**Note:** As can be seen from the screenshot above, end-user IP collection for SMS PASSCODE RADIUS Protection is not configured on the **End-user IP** tab, but on the **RADIUS Client Protection** tab. This is due to the fact, that end-user IP collection can be configured differently per Connection Request Policy of the RADIUS server.

The drop-down boxes are used to select the **End-user IP source** independently per client. The possible options for selection are:

End-user IP source option	Explanation
Do not collect	This is the default option. In this case, the client will NOT collect any end-user IP addresses. Instead, all authentication attempts will have an <b>unknown</b> end-user IP.
Network connection	<p>This option configures the client to report the end-user IP address according to the IP address of the source socket of the network connection. This is the recommended option, but only in case your network infrastructure is configured in such a way that the client recognizes the real end-user IP address.</p> <p>When selecting this option, it is recommended to perform some initial tests from different internal and external IP sources to ensure, that the correct IP addresses are reported.</p>

End-user IP source option	Explanation
<b>HTTP Header</b>	<p>In this case, you may configure the authentication client to collect the end-user IP address from an HTTP header of your own choice. By default, the header <b>X-MS-Forwarded-Client-IP</b><sup>3</sup> is suggested, but you can enter any other name into the textbox, that appears:</p>  <p>This option should be used, when the authentication client is located behind a reverse proxy that hides the real end-user IP address, but at the same time stores the original end-user IP address into an HTTP header.</p> <p>When selecting this option, it is recommended to perform some initial tests from different internal and external IP sources to ensure, that the correct IP addresses are reported.</p> <div style="background-color: red; color: white; padding: 10px; border: 1px solid black;"> <p><b>WARNING!</b> Take great care, when using this option. Only use this option, when you have ensured that the specified HTTP header is <b>always</b> set by an internal network device under your control, e.g. a reverse proxy. If this is not ensured, a hacker might set the specified HTTP header value, thereby faking an incorrect end-user IP address.</p> </div>

## 13.2 Command Line Arguments

The SMS PASSCODE **Configuration Tool** can be started from a command line. The executable is named **Config.exe**. It is located in the SMS PASSCODE installation folder, which by default is:

```
C:\Program Files\SMS PASSCODE
```

When starting the **Configuration Tool** from a command line, you may specify some optional arguments.

To export all current settings, use the following syntax:

```
Config.exe -export:"filename" [-password:"password"] [-quiet]
```

To import settings from a file, use this syntax:

```
Config.exe -import:"filename" [-password:"password"] [-quiet]
```

The command line arguments are described in the table below:

Argument	Description
-export:" <b>filename</b> "	This argument instructs the configuration tool to export all current settings to the file with the name <b>filename</b> . Please remember to use quotes if the filename contains spaces.
-import:" <b>filename</b> "	This argument instructs the configuration tool to import settings from the file with the name <b>filename</b> . Please remember to use quotes if the filename contains spaces.
-password	This optional argument specifies the password for encrypting and decrypting confidential data during export and import, respectively. The password must contain at least 5 characters. This argument is only required if the exported/imported settings contain credentials.
-quiet	This argument instructs the configuration tool to perform the requested action quietly, i.e. without any user interaction. Please note, that this includes a quiet restart of affected services as well, if required.

Examples:

- Open the Configuration Tool and export all current settings to a file named **mySettings.xml**. Encrypt using the password **12345**:

```
Config.exe -export:"mySettings.xml" -password:"12345"
```

- Export all current settings to a file named **mySettings.xml**. Encrypt using the password **12345**. Perform the action quietly, i.e. do not open the Configuration Tool:

```
Config.exe -export:"mySettings.xml" -password:"12345" -quiet
```

- Open the Configuration Tool and import settings from a file named **mySettings.xml**. Decrypt using the password **12345**:

```
Config.exe -import:"mySettings.xml" -password:"12345"
```

Please note, that this will import the settings to the Configuration Tool user interface without actually saving them. I.e. you will have the chance to inspect all the imported settings before clicking the **Save** button and applying the settings.

- Import settings from a file named **mySettings.xml**. Decrypt using the password **12345**. Perform the action quietly, i.e. do not open the Configuration Tool, but instead apply all imported settings right away:

```
Config.exe -import:"mySettings.xml" -password:"12345" -quiet
```

## 14 TROUBLESHOOTING

This section describes some common errors and the corresponding solutions:

- **Component communication problems:**  
Section 14.1 (below)

### 14.1 Component Communication Problems

In case your locally installed SMS PASSCODE authentication client cannot communicate with the IntelliTrust cloud service, this can have several reasons. The typical reasons are:

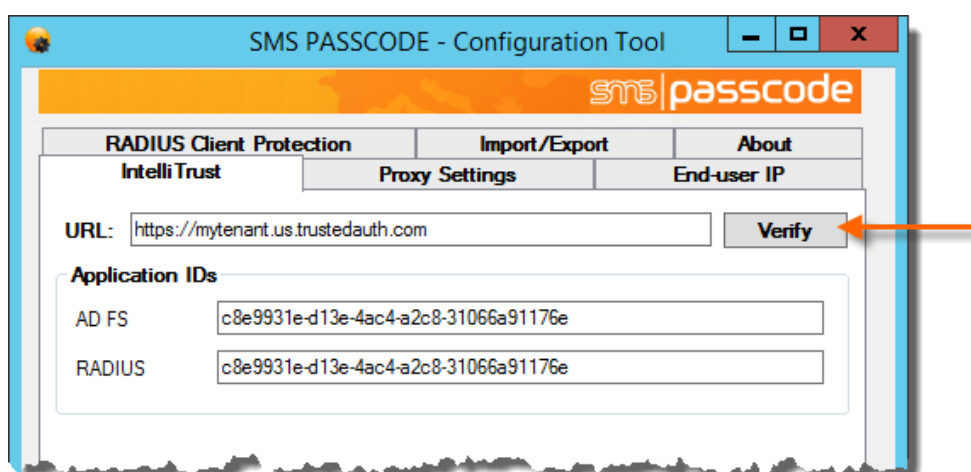
- The connection data on the **IntelliTrust** tab in the SMS PASSCODE Configuration Tool are invalid. Maybe the tenant URL is incorrect, or the application of a specified application ID has been deleted?
- Communication to the cloud service is blocked by a firewall.
- Communication needs to go through a local web proxy, but this has not been configured on the **Proxy Settings** tab in the SMS PASSCODE Configuration Tool.

To diagnose such issues, please proceed as follows:

- Inspect the **SMS PASSCODE Security** event log using the Windows Event Log Viewer. Look for error entries regarding connection issues.
- Use the SMS PASSCODE Configuration Tool for verifying the connection to the IntelliTrust cloud service:

#### Diagnosing component communication

If you wish to check whether the communication to the IntelliTrust cloud service works correctly, you can test the communication using the SMS PASSCODE **Configuration Tool**. The **IntelliTrust** tab contains a **Verify** button for performing such test.





Confidential information

Please note that the information above is intended for SMS PASSCODE customers and partners only with the purpose of implementing and maintaining SMS PASSCODE. Any other use needs to be authorized by Entrust Datacard prior to disclosing information from this document.