SMS PASSCODE 2017 CLOUD EDITION

ADMINISTRATOR'S GUIDE

REV. 1.0 (OCTOBER 2017)

TABLE OF CONTENTS

Table	of Contents	2
1 Ir	ntroduction	4
2 N	lotation	4
3 N	lew Features in Version 2017 Cloud Edition	5
4 E	nd-of-life	6
5 F	eature Overview	7
5.1	Authentication Clients	7
5.2	Security	8
5.3	Deployment	9
5.4	Administration	9
6 C	Components	10
7 L	icensing	11
8 S	System Requirements	11
8.1	Remote Desktop Service Protection	14
9 Ir	nfrastructure	16
9.1	Component Communication	17
10 P	Pre-Installation Actions	18
10.1	1 USS Account	18
10.2	2 USS AD Connector	21
10.3	3 Check System Requirements	22
1	0.3.1 Installation of NPS	23
1	0.3.2 Protection of RD Web Access using IIS Website Protection	23
1	0.3.3 Protection of RD Session Hosts using Windows Logon Protection	30
1	0.3.4 Protection of VDI Infrastructures	32
11 U	Jpgrade	33
12 F	irst-time Installation	33
12.1	1 Installation of Software	33
13 A	Add/Remove Components	48
14 P	Post-Installation Actions	49
15 U	JSS Administration Portal	49
15.1	1 Dispatch Polices	50
15.2	2 Provisioning the CensorNet App	52
	5.2.1 System Requirements for the CensorNet App	
16 C	Configuring Authentication Clients	
16.1	1 Configuring Citrix Web Interface Protection	56
16.2	2 Configuring RADIUS Protection	57

16.2.1	Configuring RADIUS Protection on a Windows Server	57
16.2.2	Advanced Configuration of the RADIUS Protection Component	60
16.3 Co	nfiguring AD FS 2.0 Protection	72
16.3.1	Background	73
16.3.2	AD FS 2.0 Infrastructure	74
16.4 Co	nfiguring AD FS 3.0/4.0 Protection	76
16.4.1	Background	76
16.4.2	AD FS 3.0/4.0 Infrastructure	76
16.4.3	Configuring the MFA Adapter for AD FS 3.0	78
16.4.4	Configuring the MFA Adapter for AD FS 4.0	80
16.4.5	Uninstalling the MFA Adapter	82
16.5 Co	nfiguring IIS Website Protection	82
16.5.1	ISAPI Filter	82
16.5.2	ISAPI Filter Configuration File	82
16.5.3	The IsapiAdmin Tool	83
16.5.4	ISAPI Filter Configuration File Syntax	87
16.6 Co	nfiguring Windows Logon Protection	90
16.6.1	Windows Logon User Exclusion Groups	90
16.6.2	Remote Desktop Logon Timeout	91
16.6.3	RDP Listener Exclusion	91
16.6.4	Credential Provider Filtering	94
17 Configu	ration Tool	95
17.1 Co	lecting End-User IP Addresses	96
17.2 Co	mmand Line Arguments	99
18 Trouble	shooting	100
18.1 Co	mponent Communication Problems	100
18.2 RD	Web Protection	101

© 2017 CensorNet A/S. 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 2017 Cloud Edition" installer is used for installing SMS PASSCODE in cloud mode.

This document describes how to install, configure and administer SMS PASSCODE 2017 in *cloud mode*. For an *on-premise* installation, please consult the "SMS PASSCODE 9.0 SP2 Administrator's Guide".

2 NOTATION

Shorthand	Description
AD	Active Directory
AD FS	Active Directory Federation Services
IIS	Internet Information Server: Optional component/role on a Windows Server.
Machine	This is a general term used to denote a server or a workstation
NPS	Network Policy Server: Optional Role on a Windows Server 2008/2012/2016. This Role is the Microsoft implementation of a RADIUS server.
ОТР	One-time passcode
OWA	Microsoft Outlook Web Access
RD	Remote Desktop
RDS	Microsoft Remote Desktop Services
SMS PASSCODE authentication client	One of the SMS PASSCODE components Citrix Web Interface Protection, RADIUS Protection, AD FS Protection, IIS Website Protection or Windows Logon Protection, i.e. one of the components responsible for authentication for a specific type of client.
USS	CensorNet's Unified Security Service. The USS administration portal is available here: https://portal.clouduss.com

3 NEW FEATURES IN VERSION 2017 CLOUD EDITION

SMS PASSCODE 2017 *cloud edition* is the first SMS PASSCODE version supporting an infrastructure making use of cloud services, providing the most convenient installation experience ever.

SMS PASSCODE 2017 contains most of the renowned MFA protections known from previous versions of SMS PASSCODE. Only the MFA protections need to be installed, no need to install any Database service, Administration Interface, Authentication Backend Service or Transmission Service. All such services are replaced with cloud services delivered by CensorNet.

SMS PASSCODE 2017 is the latest member of the series of components that has been integrated in to the CensorNet *Unified Security Service* (USS). This means that as an administrator you can now also use the USS administration portal (https://portal.clouduss.com) for administration of MFA protection, administration of user synchronizations from AD, as well as inspecting MFA log data and charts. For example, you can customize your own MFA dashboard in the USS administration portal, showing different types of charts about the MFA authentications of your users.

For an overview regarding the infrastructure for SMS PASSCODE in *cloud mode*, please see section 9 (page 16).

Note: Whereas SMS PASSCODE 2017 supports *cloud mode* only, the next release of SMS PASSCODE is expected to consist of a unified installer, supporting both *cloud mode* and *on-premise mode*.

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
SMS PASSCODE 1.8	31.07.2013
SMS PASSCODE 2.x	31.07.2013
SMS PASSCODE 3.x	01.01.2015
SMS PASSCODE 4.x	01.07.2015
SMS PASSCODE 5.x	01.01.2016
SMS PASSCODE 6.x	01.01.2017
SMS PASSCODE 7.x	01.01.2018
SMS PASSCODE 8.0	01.01.2019
SMS PASSCODE 8.0 SP1	01.01.2020
SMS PASSCODE 9.0	01.10.2020
SMS PASSCODE 9.0 SP1	01.02.2021
SMS PASSCODE 9.0 SP2	01.09.2021
SMS PASSCODE 2017	01.11.2021

5 FEATURE OVERVIEW

SMS PASSCODE is a versatile multi-factor authentication system with an extensive list of great features. The most important of these features are described in the following subsections.

5.1 Authentication Clients

SMS PASSCODE provides comprehensive protection for a broad range of authentication clients. The following clients are currently supported in *cloud mode*:

✓ Citrix Web Interface

✓ RADIUS clients

Supported are:

- Check Point
- Cisco
- Citrix Access Gateway
- F5
- Juniper
- Palo Alto
- Any other RADIUS client supporting PAP with challenge/response
- Any other RADIUS client supporting MS-CHAP v2¹

✓ Applications protected by AD FS 2.0

Supports protection of any applications that are using form-based authentication and are protected by AD FS 2.0 using SAML 2.0, WS-Federation or WS-Trust. Examples are:

- Microsoft Office 365 Web Clients
- Google Apps
- SalesForce

✓ Applications protected by AD FS 3.0 / 4.0

Supports multi-factor authentication in any of the scenarios supported by the AD FS 3.0 / 4.0 infrastructure, for example:

- ...when accessing claims-based applications within your enterprise
- ...when accessing resources in any federation partner organization
- ...when accessing internally hosted Web sites or services, published via the Web Application Proxy
- ...when accessing resources or services in the cloud, like Microsoft Office 365, Google Apps and SalesForce
- ...when approving new devices during a Workplace Join.

¹ For best user experience, the RADIUS client must support to show the challenge message returned by the SMS PASSCODE protected RADIUS server.

✓ Internet Information Server (IIS) Websites

Supports protection of the following types of IIS websites:

- Outlook Web Access 2007 (SP3) / 2010 / 2013 / 2016
- Remote Desktop Web Access (Windows Server 2008 R2, 2012 R2 and 2016)
- IIS Websites using Basic or Integrated Windows Authentication

✓ Windows Logon

Protection of:

- Remote Desktops (RDP Connections)
- VDI machines
- Windows servers
- Windows workstations

SMS PASSCODE is **fully integrated** into all supported authentication clients. No extra user actions are necessary to trigger the transmission of passcodes – the authentication is very intuitive, which makes user training unnecessary.

5.2 Security

SMS PASSCODE provides improved security from several aspects. From a technical point of view, SMS PASSCODE provides these important security features:

- ✓ Strong authentication security with protection against modern internet threats such as advanced Phishing-attacks, because passcodes are:
 - Session-specific (opposite to hardware-token based solutions!)
 - Randomly created in real-time without the usage of any pre-deterministic algorithm (opposite to hardware-token based solutions as well as many competing message-based solutions)
 - Challenge-based
 - Time-constrained
- ✓ Cryptographically strong random passcodes are generated using FIPS-140 validated crypto modules

✓ Encryption

 Encryption of all traffic between the on-premise authentication clients and the CensorNet USS cloud service.

From a user perspective, SMS PASSCODE provides increased security compared to e.g. traditional hardware-token based solutions due to:

- ✓ High user awareness of stolen or lost cell phone means shorter period before counteractions are taken
- ✓ High user awareness of the necessity to block SIM card of stolen or lost cell phone to prevent misuse, which implies lock down of access using SMS PASSCODE
- ✓ Users can lock their stolen or lost cell phone (SIM card) themselves meaning faster reaction and shorter period of security breach

✓ Users are automatically alerted in case their user credentials have been stolen, since they will start receiving passcode messages not requested by themselves

5.3 Deployment

Installation of SMS PASSCODE is **very simple**, since SMS PASSCODE is an "out-of-the-box" **end-to-end** solution. In *cloud mode*, you simply need to install SMS PASSCODE authentication clients on the servers that need MFA protection. Nothing else is needed, since all administration and transmission services are provided as cloud services.

Unlike traditional hardware-token based solutions, SMS PASSCODE works without distribution of any hardware-tokens. As a result, the **logistic overhead involved is minimal** and **rollout is much faster**. You can get SMS PASSCODE up and running with thousands of users within minutes. Just extract all cell phone numbers from your Active Directory as you import your users to the CensorNet USS portal, using the CensorNet USS AD Connector².

5.4 Administration

The daily administration of SMS PASSCODE is simple due to:

- ✓ No logistic overhead regarding administration and distribution of hardware-tokens.
- ✓ No need to involve IT personnel in the event of a lost cell phone, since users will quickly discover the loss and act on own impulse to block the SIM card.

Additionally, the CensorNet USS AD Connector service allows administration of SMS PASSCODE users in your Active Directory. The following is a list of USS AD Connector service features:

- ✓ Works "out-of-the-box". No schema extension of your AD is needed!
- ✓ Supports encrypted secure communication
- ✓ Supports extraction of users from multiple separate AD Domains
- Customizable extraction of several user attributes, like (mobile) phone numbers and email addresses.

Finally, as an administrator, you can administer the SMS PASSCODE product using the graphical user interface of the CensorNet USS portal, provided as a cloud service. Among others, the portal allows administrators to inspect MFA log data and charts.

² The CensorNet USS AD Connector is available here: http://help.clouduss.com/ad-connector-download

6 COMPONENTS

SMS PASSCODE in *cloud mode* is composed of the following software components:

Component	Description
Citrix Web Interface Protection	Citrix Web Interface integration, providing SMS PASSCODE multifactor authentication for Citrix Web Interface users. It is optionally possible to run the Citrix Web Interface protection side-by-side with hardware-token based two-factor authentication systems, e.g. RSA SecurID® or SafeWord®.
RADIUS Protection	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. RADIUS protection is provided by means of an extension for the Microsoft Network Policy Server (NPS).
AD FS Protection	Integrates with Microsoft Active Directory Federation Services (AD FS), providing SMS PASSCODE multi-factor authentication for applications protected by AD FS 2.0/3.0/4.0.
IIS Website Protection	 Microsoft Internet Information Server (IIS) integration, providing SMS PASSCODE multi-factor authentication for IIS websites. Currently the following types of websites are supported: Microsoft Outlook Web Access 2007, 2010, 2013 and 2016³ IIS websites using Basic or Integrated Windows Authentication³ Microsoft Remote Desktop Web Access (RD Web Access), on Windows Server 2008 R2, Windows Server 2012 R2 and Windows Server 2016. SMS PASSCODE authentication can be enabled or disabled for each specific IIS website – it is even possible to configure different settings for specific URL's and/or specific client IP addresses. IIS Website protection is provided by means of an ISAPI filter.
Windows Logon Protection	Windows Logon integration, providing SMS PASSCODE multi- factor authentication for users logging on Windows machines. This is for example useful for protecting Microsoft Remote Desktop Services environments, or VMware View virtual clients. SMS PASSCODE authentication can be enabled or disabled for each specific RDP Listener. Windows Logon integration is provided by means of a Credential Provider.

³ Please note that when protecting an OWA 2013 or 2016 site, only form-based authentication is supported

The term *SMS PASSCODE Authentication client* is used in the subsequent sections of this documentation to denote one of the components: Citrix Web Interface Protection, RADIUS Protection, AD FS Protection, IIS Website Protection or Windows Logon Protection.

7 LICENSING

Before installing SMS PASSCODE in *cloud mode*, you must sign up for a CensorNet USS account with MFA licenses assigned.

The USS MFA module is licensed per user. You are allowed to install the SMS PASSCODE components as many times as you like, as long as you have acquired an MFA client access license (CAL) for each user logging in using SMS PASSCODE multi-factor authentication.

Component	Number of installations allowed	License requirements
Citrix Web Interface Protection	No limitation.	Each user needs to have an MFA CAL.
RADIUS Protection	No limitation.	Each user needs to have an MFA CAL.
AD FS Protection	No limitation.	Each user needs to have an MFA CAL.
IIS Website Protection	No limitation.	Each user needs to have an MFA CAL.
Windows Logon Protection	No limitation.	Each user needs to have an MFA CAL.

8 SYSTEM REQUIREMENTS

In this section, the system requirements are listed for each SMS PASSCODE software component (cf. section 6).

Please note:

In general, SMS PASSCODE components require the **Microsoft .NET 4.5 Framework**; except when installing SMS PASSCODE AD FS protection on a Windows Server 2008 R2 (AD FS 2.0).

Component	Requirement
Citrix Web Interface Protection	 Supported operating systems: Windows Server 2008 R2 (x64) You must install Citrix Web Interface on the server and publish at least one Web Interface before installing this component. The following Citrix Web Interface versions are supported: Citrix Web Interface 5.3.0 Citrix Web Interface 5.4.0 Citrix Web Interface 5.4.2

Component	Requirement
RADIUS Protection	 Supported operating systems: Windows Server 2008 R2 (x64) Windows Server 2012 (x64) Windows Server 2012 R2 (x64) Windows Server 2016 (x64) Please note: Only Windows Server Editions including the Network Policy Service (NPS) are supported. This means, that for example Windows Server 2008 Web Edition, Windows Server 2012 Hyper-V Edition and Windows Server 2012 Storage Edition are not feasible. Network Policy Service (NPS) must be installed before installing this component. 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 Challenge Response. Among others the following RADIUS clients support Challenge Response: Cisco ASA Cisco ASA Cisco VPN Concentrator 3000 Citrix NetScaler Gateway Palo Alto Check Point FW-1/VPN-1 NG/FP3 F5 BigIP Fortigate SSL VPN Juniper SSL VPN Dell SonicWall SRA, Dell SonicWall NSA VMWare Horizon View WatchGuard Firebox Please contact your SMS PASSCODE reseller or support@smspasscode.com for further information regarding supported RADIUS clients.
AD FS Protection	 Supported operating systems: Windows Server 2008 R2 (x64) Windows Server 2012 (x64) Windows Server 2012 R2 (x64) Windows Server 2016 (x64) Microsoft AD FS 2.0/3.0/4.0 must be installed <u>before</u> installing this component⁴.
IIS Website Protection	 Supported operating systems: Windows Server 2008 R2 (x64) Windows Server 2012 (x64) Windows Server 2012 R2 (x64) Windows Server 2016 (x64)

 $^{^4}$ On Windows Server 2012, please note, that AD FS 2.0 is not supported on Hyper-V, Storage or MultiPoint Editions.

Component	Requirement
Windows Logon Protection	 Supported operating systems: Windows 7 (x86/x64) Windows 8 (x86/x64) Windows 8.1 (x86/x64) Windows 10 (x86/x64) Windows Server 2008 R2 (x64) Windows Server 2012 (x64) Windows Server 2012 R2 (x64) Windows Server 2016 (x64) Remote Desktop is supported.

8.1 Remote Desktop Service Protection

Access to a Remote Desktop Services infrastructure can be protected by SMS PASSCODE multifactor authentication in several ways:

- Protection on the RD Session Hosts: You can decide to install SMS PASSCODE
 Windows Logon Protection on each RD Session Host. This will ensure that multi-factor
 authentication will occur in the Windows Logon session, when a RemoteApp or remote
 desktop is started on an RD Session Host. If you have a VDI infrastructure, you can also
 use this approach, and install SMS PASSCODE Windows Logon Protection on each VDI
 machine.
- Protection on the RD Web Access server: If remote access to your RDS infrastructure is
 provided via an RD Web Access site, then you can decide to install SMS PASSCODE IIS
 Website Protection on the RD Web Access server in order to require users to perform multifactor authentication, before getting access to the RD Web Access site.

The following table summarizes the options available on different operating systems:

Operating System	Protecting RD Session Hosts or VDI machines using SMS PASSCODE Windows Logon Protection	Protecting RD Web Access Site using SMS PASSCODE IIS Website Protection
Windows Server 2008 R2	Yes	Yes
Windows Server 2012	Yes	No
Windows Server 2012 R2	Yes	Yes⁵
Windows Server 2016	Yes	Yes⁵
Windows 7	Yes	
Windows 8	Yes	N/A
Windows 8.1	Yes	IV/A
Windows 10	Yes	

© 2017 CENSORNET A/S. ALL RIGHTS RESERVED.

⁵ RDP Client 8.1 or later required.

The next table summarizes the advantages and disadvantages of the two approaches:

	Protecting RD Session Hosts using SMS PASSCODE Windows Logon Protection	Protecting RD Web Access Site using SMS PASSCODE IIS Website Protection
Advantages	 Independent of the RDP Client version. In addition, works fine with any 3rd party RDP clients. Independent of the RDS infrastructure. The RD Gateway and RD Web Access Site can reside on separate servers. Supports RDP shortcuts for accessing RemoteApps through the RD Gateway. 	 Simpler to administer, if you have many RD Session Hosts, since SMS PASSCODE protection only has to be installed on a single server. Security: Performs multi-factor authentication as early as possible, before the user gets access to the RD Session Host. Users only have to perform multi-factor authentication once, when accessing the RD Web Access Site. Not, when starting each RemoteApp in the RD Web Access Site.
Disadvantages	 If you have many RD Session Hosts, you will need to install SMS PASSCODE Windows Logon Protection on each host. If users access RemoteApps on different RD Session Hosts, they will need to perform multi-factor authentication several times. Security: Important to ensure that the RD Gateway is configured to only grant access to hosts protected by SMS PASSCODE Windows Logon Protection. Otherwise, security could be compromised, since unprotected hosts could be externally accessed without multi-factor authentication. Since all users accessing the RD Session hosts are validated by SMS PASSCODE, this means that all users must have been imported into the USS, including users that only have internal access without multi-factor authentication. Such users must be configured to bypass multi-factor authentication. 	 Requires the RD Gateway and RD Web Access site to reside on the same server. Does not support RDP shortcuts for accessing RemoteApps through the RD Gateway. Not supported on Windows Server 2012 (but supported on Windows Server 2012 R2). 3rd party RDP clients might not work. Specific for Windows Server 2012 R2 and Windows Server 2016: All RDP clients must be on version 8.1 or later (which is supported on Windows 7 SP1 and later). When starting a RemoteApp in the RD Web Access Site, the RDP file must always be opened after download, also in Internet Explorer. The feature "Connect to a remote PC" in the RD Web Access site (Internet Explorer only) will not work.

As you can see from the tables above, you have the following options, when protecting Remote Desktop Services using SMS PASSCODE multi-factor authentication:

- Windows Server 2008 R2 / Windows Server 2012 R2 / Windows Server 2016: When
 using Remote Desktop Services on Windows Server 2008 R2 / 2012 R2 / 2016 you have
 two options to implement SMS PASSCODE authentication:
 - Protecting an RD Web Access site directly on the IIS:
 Install the SMS PASSCODE IIS Website Protection component on the server hosting the RD Web Access Site. It is mandatory, that the RD Web Access site and the RD Gateway reside on the <u>same</u> server. This server must NOT be a domain controller. Form-based authentication and single sign-on (SSO) is supported⁶.
 - Protecting Windows Logon on all RD Session Host servers:
 Install the SMS PASSCODE Windows Logon Protection component on each RD Session Host requiring SMS PASSCODE protection.
- Windows Server 2012: When using Remote Desktop Services on Windows Server 2012 (not R2), please install the SMS PASSCODE Windows Logon Protection component on each RD Session Host server requiring SMS PASSCODE protection.

Please refer to sections 10.3.2 and 10.3.3 for details about setting up RDS Protection.

9 INFRASTRUCTURE

This section gives an overview for the SMS PASSCODE infrastructure, when installed in *cloud mode*.

In cloud mode, the SMS PASSCODE infrastructure consists of:

- SMS PASSCODE MFA authentication clients installed on each on-premise server that needs MFA protection.
- USS AD Connector installed on-premise to synchronize AD users from an AD domain controller to the CensorNet USS cloud service.
- The USS CensorNet cloud service

© 2017 CENSORNET A/S. ALL RIGHTS RESERVED.

⁶ On Windows Server 2008 R2, if you experience any of the problems during single sign-on described in the MS support article http://support.microsoft.com/kb/977507, then please apply the suggested workaround / fix.

LAN DMZ Internet Firewall Multi-factor authentication RADIUS Server RADIUS client MS NPS SMS PASSCODE RADIUS Protection Windows Machine MS AD FS Server (2.0/3.0/4.0) Windows Logon Protection SMS PASSCODE AD FS Protection Multi-factor authentication Web Server (IIS) - e.g. OWA or RDWEB Server **USS Cloud Services** SMS PASSCODE IIS Website Protection **Message Transmission Services** USS Admin Portal **AD Domain Controller** Log Database Citrix Web Interface Server AD sync Citrix Web Interface Protection Push AD Changes USS AD Connector

The diagram below illustrates the *cloud mode* infrastructure:

9.1 Component Communication

All on-premise components, meaning all SMS PASSCODE authentication clients and the USS AD Connector, connect to the USS cloud services using HTTPS. Therefore, it is important that your firewall will allow outgoing HTTPS traffic from any such server, to the URL of the USS cloud services (https://webservice.clouduss.com).

Access to the USS cloud services is granted using valid USS credentials. For SMS PASSCODE authentication clients, such credentials are entered in to the SMS PASSCODE Configuration Tool (cf. section 17). For the USS AD Connector, the credentials are entered in to the USS AD Connector Setup Tool.

The USS AD Connector connects to your domain controller using LDAP or LDAPS, depending on the configuration of such sync in the USS Administration Portal.

10 PRE-INSTALLATION ACTIONS

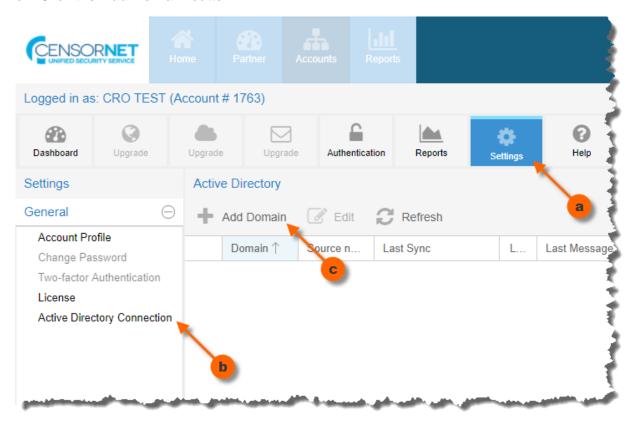
This section describes the actions to perform BEFORE running the SMS PASSCODE installation program. Please read this section carefully.

10.1 USS Account

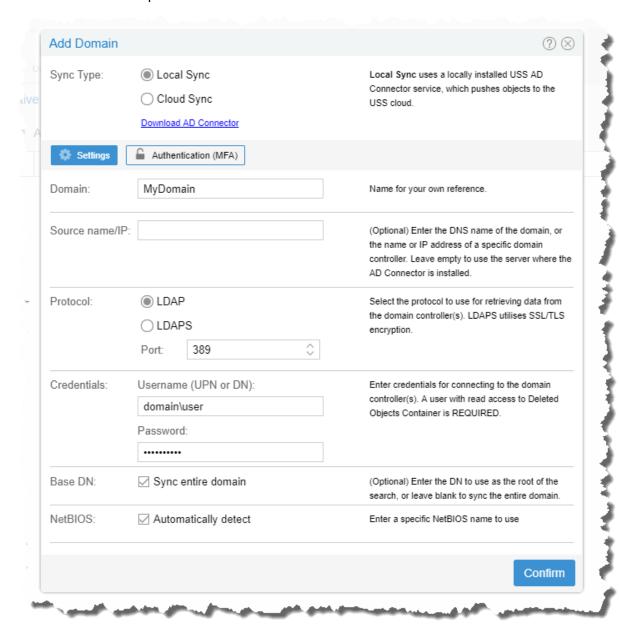
Before installing SMS PASSCODE 2017, you must have signed up for a CensorNet USS account that has MFA licenses assigned, and you must have valid credentials for logging in to the account in the USS portal (on https://portal.clouduss.com). During installation of SMS PASSCODE 2017, you will need to enter such USS credentials to allow the locally installed SMS PASSCODE clients to access the USS cloud service. Consider creating a dedicated USS account, only used for SMS PASSCODE 2017 access to the USS.

Within the USS portal, you need to configure the following, BEFORE installing SMS PASSCODE 2017:

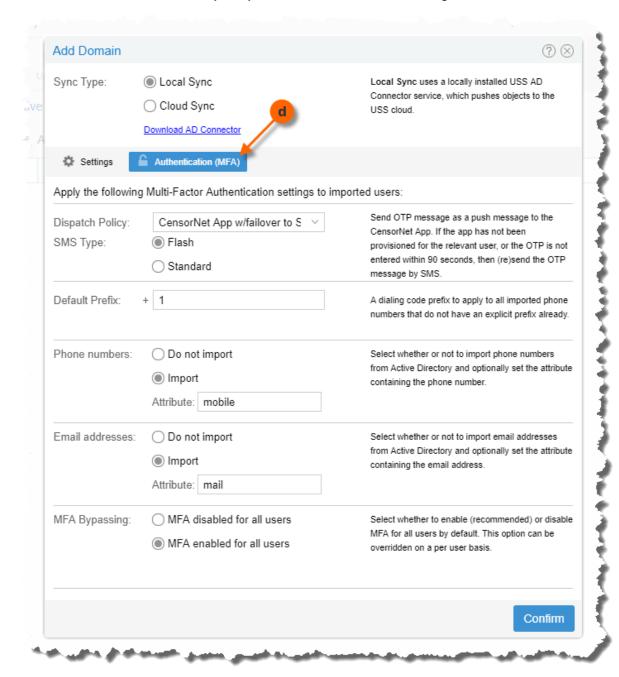
- Ensure all users are imported from your local AD that need to log in to the SMS PASSCODE 2017 protected systems. Within the USS portal, AD synchronization settings for a domain are created using the following procedure:
 - a. Select the **Settings** section.
 - b. Click Active Directory Connection
 - c. Click the Add Domain button.



On the **Add Domain** dialog, enter required information to connect to your local domain controller. For example:



d. Click the **Authentication (MFA)** tab to set MFA related settings:

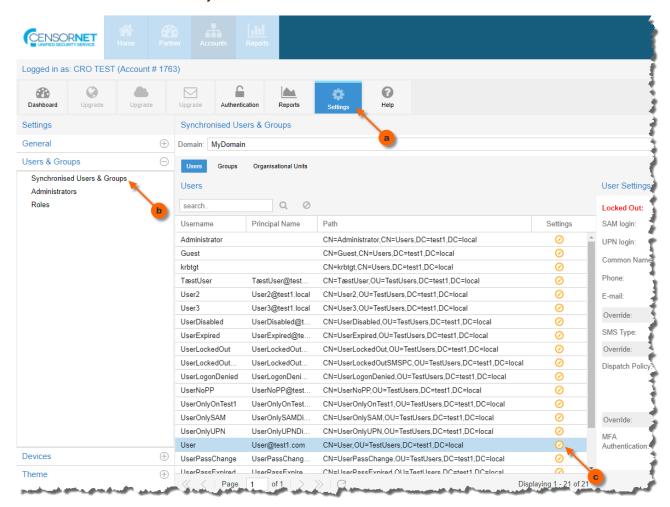


By default, the settings on the **Authentication (MFA)** tab will apply to all imported users from this domain, but can be overridden on each individual user.

For the synchronization of AD users from your local domain to the USS actually to happen, you must install the USS AD Connector. This is described in section 10.2 below.

When users have been synchronized to the USS, you can inspect such users and override individual settings. Proceed as follows, to do so:

- a. Select the **Settings** section.
- b. Click Synchronised Users & Groups
- c. Click on the user that you want to view or edit.



10.2 USS AD Connector

The CensorNet USS AD Connector is a Windows background service that synchronizes relevant AD data for users and groups from your on-premise AD(s) to the USS cloud service.

One USS AD Connector installation can synchronize data for one or multiple ADs to the USS, to either a single USS account or distributed to several USS accounts, depending on how you configure it.

For users to authenticate using SMS PASSCODE in *cloud mode*, it is <u>mandatory</u> to synchronize their AD user accounts to the USS cloud service using the CensorNet USS AD Connector.

Therefore, it is recommended to install and configure the USS AD Connector, before installing SMS PASSCODE.

Installation of the USS AD Connector is described here: http://help.clouduss.com/ad-connector-download

10.3 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 8 (page 11).

Please remember:

Citrix Web Interface Protection

If you are planning to install the **Citrix Web Interface Protection** component, then a supported version of Citrix Web Interface must be installed on the Citrix Web Interface server beforehand and at least one Citrix Web Interface must have been published.

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 10.3.1 (page 23)

AD FS Protection

If you are planning to install the **AD FS Protection** component, then AD FS 2.0, 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 sections 16.3 (page 72) and 16.4 (page 76), regarding AD FS 2.0 and AD FS 3.0/4.0, respectively.

IIS Website Protection

If you are planning to install the **IIS Website Protection** component, please ensure that the applications that are going to be protected are working correctly with standard authentication beforehand. Read section 16.5 (page 82) for more details regarding the **IIS Website Protection** component.

Microsoft Remote Desktop Services Protection

If you are planning to protect Microsoft Remote Desktop Services, please notice that there are several ways to achieve this:

- Windows Server 2008 R2 / Windows Server 2012 R2 / Windows Server 2016:
 Either protect the RD Web Access Site using the SMS PASSCODE IIS Website
 Protection component (cf. section 10.3.2, page 23), or protect each RD Session
 Host using the SMS PASSCODE Windows Logon Protection component (cf. section 10.3.3, page 30).
- Windows Server 2012: Protect each RD Session Host using the SMS PASSCODE Windows Logon Protection component (cf. section 10.3.3, page 30).

10.3.1 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

```
Administrator: Command Prompt

C:\>serverManagerCmd -i NPAS-Policy-Server
..

Start Installation...
[Installation] Succeeded: [Network Policy and Access Services] Network Policy Server.
<100/100>
Success: Installation succeeded.

C:\>
```

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

```
Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator\ add-windowsfeature npas-policy-server
Success Restart Needed Exit Code Feature Result
True No Success (Network Policy and Access Services, Netwo...

PS C:\Users\Administrator\

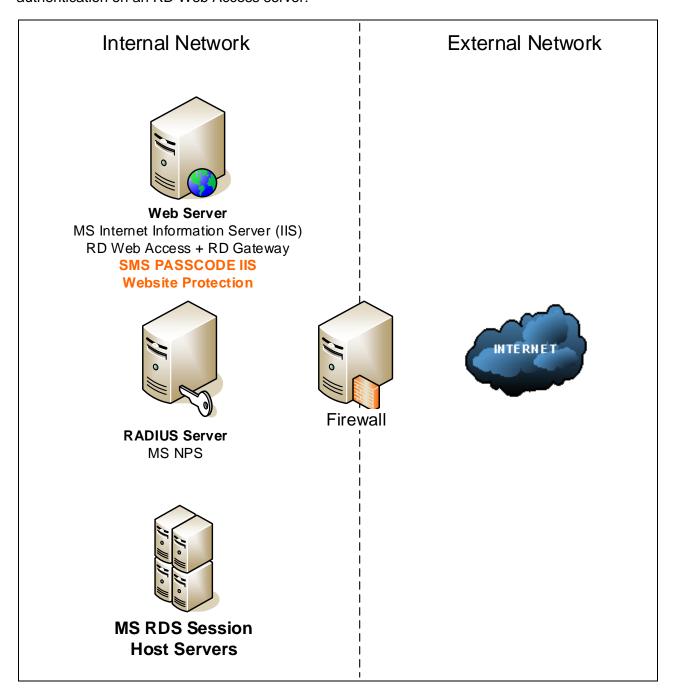
PS C:\Users\Administrator\
```

10.3.2 Protection of RD Web Access using IIS Website Protection

This section describes how to protect the Remote Desktop Web Access Site on a Windows Server 2008 R2, Windows Server 2012 R2 or Windows Server 2016.

Please note that it is mandatory to access the RD Session Host servers through an **RD Gateway** when protecting access to Remote Desktop Services (RDS) using an RD Web Access Site.

The following diagram illustrates the required infrastructure setup for performing SMS PASSCODE authentication on an RD Web Access server:



SMS PASSCODE protected RD Web Access site with multi-factor authentication performed on the Web Server

Please note:

- The SMS PASSCODE RADIUS protection component cannot be installed on the RADIUS server.
- The Web Server and RADIUS server could be consolidated to a single server (installing both NPS and IIS on the same server).
- The SMS PASSCODE **IIS Website Protection** component must be installed on the Web Server (i.e. the RD Web Access server).

- It is mandatory, that the RD Web Access site and RD Gateway site reside on the <u>same</u> server.
- Please note:
 - Single sign-on in the RD Web Access site is supported.
 - Accessing RemoteApps through the RD Web Feed is not supported.
 - If the "Password Change" feature is enabled in the RD Web Access Site, then the "Password change" site is NOT protected by SMS PASSCODE multi-factor authentication. Consequently, users will be able to change their password without a multi-factor authentication (but are always forced to perform MFA before accessing any RemoteApps).
 - Specific for Windows Server 2012 R2 and Windows Server 2016: Only RDP Clients version 8.1 and later are supported. Access via older RDP Clients will be denied access. RDP Client 8.1 is supported on Windows 7 SP1 and later.

IMPORTANT: SMS PASSCODE **RD Web Access protection** will ensure that all users MUST authenticate using the RD Web Access site before any RemoteApps can be accessed through the RD Gateway. In other words, any attempt to access RemoteApps through the RD Gateway, without any prior authentication in the RD Web Access Site, will fail.

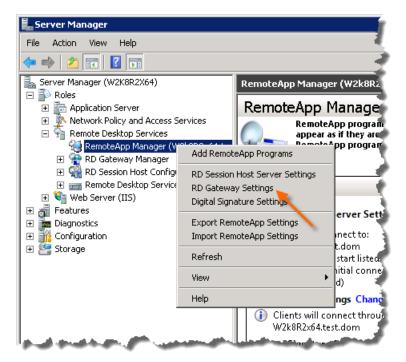
In the subsections below you will find detailed instructions regarding the required setup to protect your RD Web Access Site. In both subsections, the term "Web Server" refers to the corresponding server in the network diagram above (the server with both the RD Web Access Site and RD Gateway installed).

- Windows Server 2008 R2: Section 10.3.2.1 (below).
- Windows Server 2012 R2 / 2016: Section 10.3.2.2 (page 28).

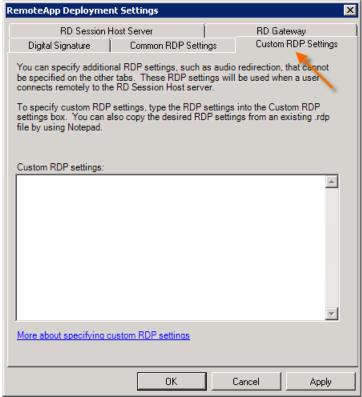
10.3.2.1 Protecting RD Web Access (Windows Server 2008 R2)

To protect the RD Web Access Site using SMS PASSCODE multi-factor authentication on a Windows Server 2008 R2, please follow the instructions below:

- Set up the Web Server if this has not been done yet. I.e. install IIS, RD Web Access Site and RD Gateway on the Web Server. Do NOT install SMS PASSCODE IIS Website Protection on the Web Server yet.
- Test and verify that remote access (from the external network) to RemoteApps through the RD Web Access Site works as expected (using only AD credentials for authentication). If you are planning to use single sign-on (SSO):
 - a. Test and verify that SSO works as expected.
 - b. It is strongly recommended, when using SSO, to update the *renderscripts.js* file on the RD Web Access Site. To do this, on the server hosting the RD Web Access site go to http://support.microsoft.com/kb/977507 and click the "Fix it" button on this page. This will update the *renderscripts.js* file.
- 3. You are now ready to add SMS PASSCODE protection as described in the steps below.
- 4. Perform the following actions on each RD Session Host server: In the Server Manager right-click the **RemoteApp Manager** and select **RD Gateway Settings**.



a. Select the **Custom RDP Settings** tab.



b. Enter the following two lines into the **Custom RDP settings** textbox:

pre-authentication server address:s:https://fqdn/rdroot
require pre-authentication:i:1

...where *fqdn* must be replaced with the fully qualified domain name of the SSL certificate used for publishing the RD Web Access site, and *rdroot* must be replaced with the RD Web Access URL ("RDWeb" by default).

5. Now, install **SMS PASSCODE IIS Website Protection** on the Web Server. During the installation, enable SMS PASSCODE protection of the RD Web Access Site:

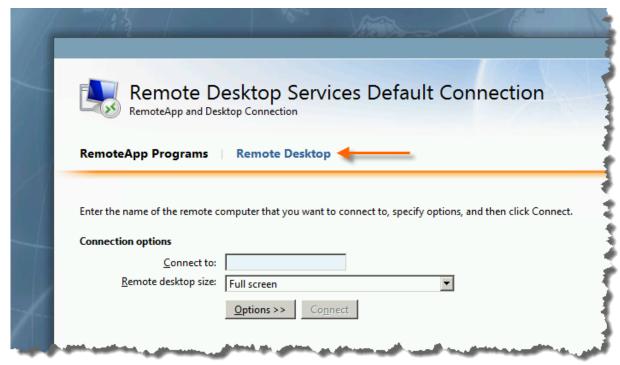


6. Test that SMS PASSCODE authentication works as expected.

This completes the procedure for protecting the RD Web Access Site on a Windows Server 2008 R2, using SMS PASSCODE multi-factor authentication. If you are using the **Remote Desktop** feature in the RD Web Access Site, then please read the following subsection.

10.3.2.1.1 Protection of RD Web Desktops using IIS Website Protection

On a Windows Server 2008 R2, if you have protected the RD Web Access Site using SMS PASSCODE IIS Website Protection as described in the previous section, <u>and</u> you are making use of the RD Web **Remote Desktop** feature (accessing full desktops of internal machines through the RD Gateway)...



...then please note, that you have to complete some additional steps to make access to the

Remote Desktops work with SMS PASSCODE multi-factor authentication. Please follow the procedure below, performing the specified actions on the server hosting the RD Web Access Site:

- 1. Make a backup of the following file: C:\Windows\Web\RDWeb\en-US\desktops.aspx
- 2. Now edit the original desktops.aspx file, and search for the text "authentication level". Replace the line...

```
...with the following two lines...
RDPstr += "require pre-authentication:i:1\n";
```

RDPstr += "pre-authentication server address: s: https://fqdn/rdroot\n";

...where £qdn must be replaced with the fully qualified domain name of the SSL certificate used for publishing the RD Web Access site, and xdroot must be replaced with the RD Web Access URL ("RDWeb" by default).

3. Save the changes to the desktops.aspx file.

RDPstr += "authentication level:i:2\n";

4. Test that Remote Desktops can be accessed through the SMS PASSCODE protected RD Web Access Site.

10.3.2.2 Protecting RD Web Access (Windows Server 2012 R2 and 2016)

To protect the RD Web Access Site using SMS PASSCODE multi-factor authentication on a Windows Server 2012 R2 or Windows Server 2016, please follow the instructions below:

- Set up the Web Server if this has not been done yet. I.e. install IIS, RD Web Access Site and RD Gateway on the Web Server. Do NOT install SMS PASSCODE IIS Website Protection on the Web Server yet.
- Test and verify that remote access (from the external network) to RemoteApps through the RD Web Access Site works as expected (using only AD credentials for authentication). If you are planning to use single sign-on (SSO), then please also test and verify that SSO works as expected.
- 3. Now, install **SMS PASSCODE IIS Website Protection** on the Web Server. During the installation, enable SMS PASSCODE protection of the RD Web Access Site:



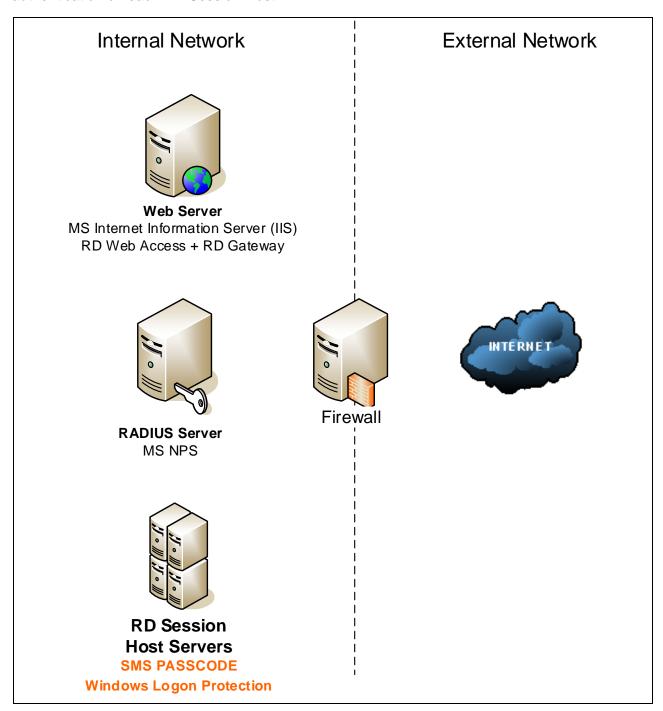
- 4. Test that SMS PASSCODE authentication works as expected.
 - a. On Windows Server 2012 R2, if multi-factor authentication works, when accessing the RD Web Access site, but starting RemoteApps fails with the error message...
 - "This RDP File is corrupted. The remote connection cannot be started"
 - ...then please read section 18.2 (page 101) for solving this issue.
 - b. On Windows Server 2016, if single sign-on (SSO) does not work, meaning the user has to re-authenticate on the RD Session Host, then please read section 18.2 (page 101) for solving this issue.

This completes the procedure for protecting the RD Web Access Site on a Windows Server 2012 R2 / 2016, using SMS PASSCODE multi-factor authentication.

10.3.3 Protection of RD Session Hosts using Windows Logon Protection

On Windows Server 2008 R2, Windows Server 2012 (R2) and Windows Server 2016, the RDS infrastructure can be protected using SMS PASSCODE multi-factor authentication by installing the **SMS PASSCODE Windows Logon Protection** component on <u>each</u> RD Session Host (i.e. every server publishing RemoteApps and remote desktops).

The following diagram illustrates the required infrastructure setup for performing SMS PASSCODE authentication on each RD Session Host:



SMS PASSCODE protected RDS infrastructure with multi-factor authentication performed on the RD Session Host servers

Please note:

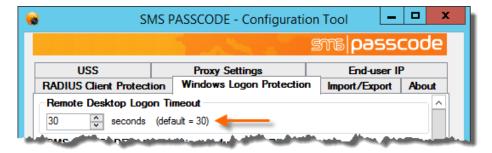
- The SMS PASSCODE RADIUS protection component cannot be installed on the RADIUS server.
- The Web Server and RADIUS server could be consolidated to a single server (installing both NPS and IIS on the same server).
- The SMS PASSCODE Windows Logon Protection component must be installed on each RD Session Host Server.
- SMS PASSCODE multi-factor authentication will even work, if RD Session Hosts are published for direct external access, bypassing the RD Gateway. However, for security reasons, this is not recommended.

Below follow detailed instructions regarding the required setup to protect your RDS infrastructure using the SMS PASSCODE Windows Logon Protection component:

- 1. Set up the RDS infrastructure without installing any SMS PASSCODE components yet.
- 2. Test and verify that remote access (from the external network) to the RDS Server(s) works as expected (using only AD credentials for authentication). Ensure to test all relevant scenarios (relevant browser types, client types, internal/external access).
- 3. Ensure that <u>external</u> access is only allowed to the RD Session Hosts that you are planning to protect using SMS PASSCODE. This is configured in the Network Resources tab in the Resource Authorization Policy.

IMPORTANT: Any RD Session Host <u>without</u> the SMS PASSCODE Windows Logon Protection component installed is accessible without multi-factor authentication. In other words, if any such server is externally accessible, then external access is provided without multi-factor authentication.

- 4. Now install the **SMS PASSCODE Windows Logon Protection** component on <u>each</u> RD Session Host server.
 - a. By default, the Remote Desktop Logon Timeout is set to 30 seconds. In case you expect SMS PASSCODE authentications to last longer in special cases (e.g. because of advanced Dispatch Policies with failover on expired OTPs), then it is recommended to extend the Remote Desktop Logon Timeout accordingly. This can be done in the SMS PASSCODE Configuration Tool on the Windows Logon Protection tab, either when the Configuration Tool pops up during installation of SMS PASSCODE Windows Logon Protection, or alternatively afterwards by starting the Configuration Tool manually.



Please note, that you must restart the RD Session Host before a new value of the **Remote Desktop Logon Timeout** setting takes effect.

5. If you would like to disable SMS PASSCODE multi-factor authentication for clients accessing the RD Session Hosts from the internal network (LAN), you have the following option: Create an additional RDP Listener on the relevant RD Session Host and configure the RD Gateway to use one of the RDP Listeners, and internal access to use the other RDP Listener. Configure SMS PASSCODE to apply multi-factor authentication only for the RDP Listener used by the RD Gateway. Please read section 16.6.3, page 91, for more details how to set up and configure RDP Listener exclusion.

10.3.4 Protection of VDI Infrastructures

If you want to protect access to virtual machines in a VDI infrastructure using SMS PASSCODE multi-factor authentication, you can install SMS PASSCODE Windows Logon Protection on each virtual desktop host.

You can run the SMS PASSCODE Configuration Tool with command line arguments to distribute any necessary SMS PASSCODE settings to all virtual desktop hosts (please read section 17.2, page 99, for more details).

11 UPGRADE

SMS PASSCODE 2017 *cloud edition* is the first version of SMS PASSCODE that supports *cloud mode*. There is no upgrade path from a previous on-premise installation to a *cloud mode* installation. If you want to switch from an on-premise installation to a *cloud mode* installation, you must uninstall the previous version of SMS PASSCODE first, and then perform a new, fresh installation in *cloud mode*.

12 FIRST-TIME INSTALLATION

To install SMS PASSCODE you must complete two steps:

- 1. Install software (section 12.1, page 33).
- 2. Configure SMS PASSCODE (section 14, page 49).

These two steps are described in the specified sections.

12.1 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 6 (page 10), 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 <u>each</u> 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.

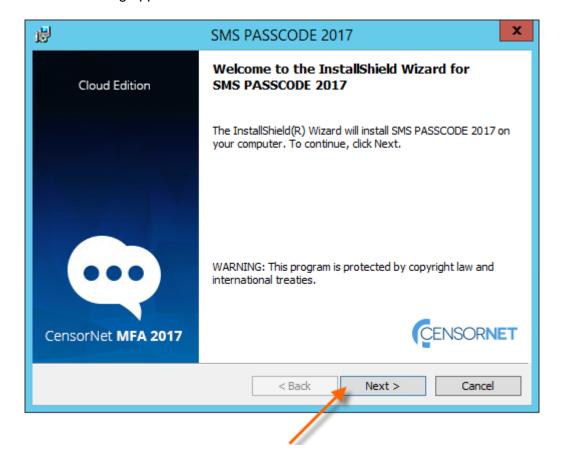
IMPORTANT: The sequence of dialogs is automatically tailored during an installation according to the components selected for installation. The workflow below describes all potential dialogs that may appear during an installation. You may not see all dialogs during your specific installation – skip forward 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 **SmsPasscode-2017-x86.exe** (32-bit) or **SmsPasscode-2017-x64.exe** (64-bit) to a local path on the machine.

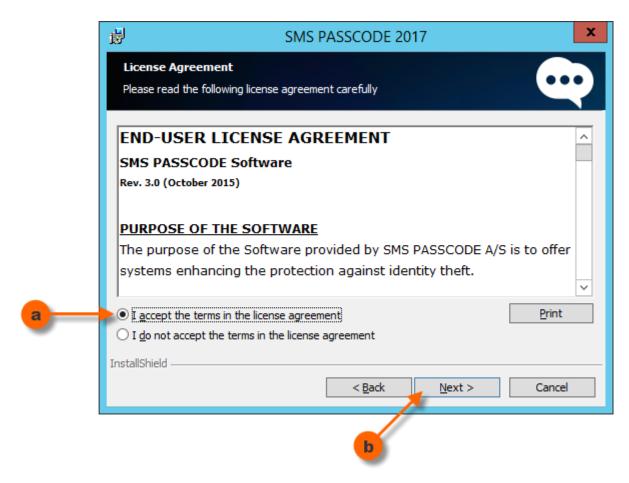
3. Start the installation by double-clicking the setup file:



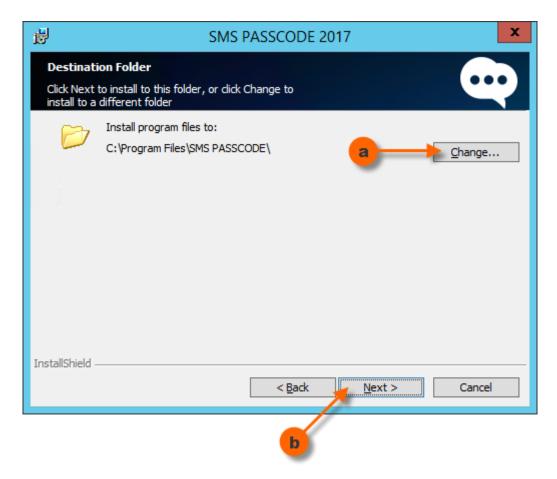
4. A Welcome dialog appears. Click the **Next** button.



- 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 6 (page 10) 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 13)

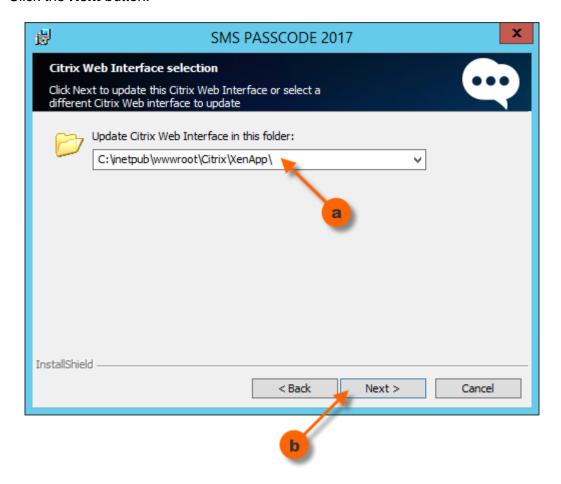
PLEASE NOTE:

If a component is disabled for selection, this is caused by system requirements not being fulfilled for this component (cf. section 8, page 11)

b. Click the Next button.

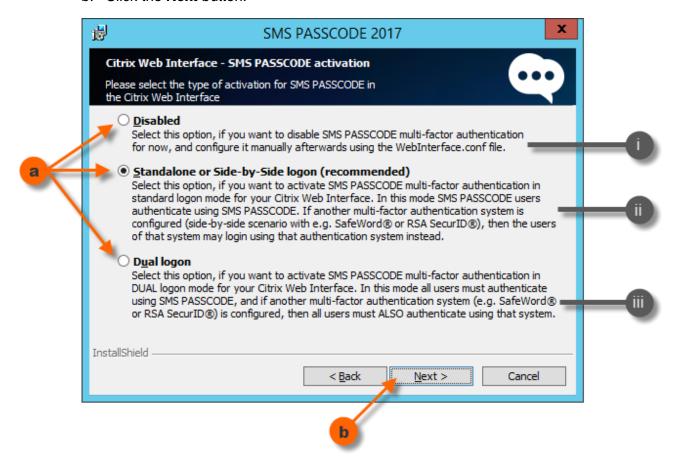


- 8. If a dialog appears, for selecting the Citrix Web Interface to protect using SMS PASSCODE:
 - a. Please select the physical path for the Citrix Web Interface⁷ to be protected by SMS PASSCODE authentication.
 - b. Click the Next button.

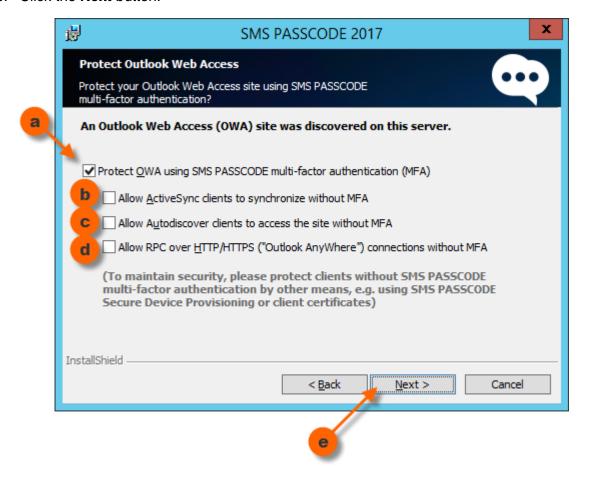


⁷ Currently the installation program only supports activation of SMS PASSCODE protection for a single Citrix Web Interface. If you need to protect several Citrix Web Interfaces on the same server, then this is also possible. Please contact support@smspasscode.com for instructions on how to do this.

- 9. If a dialog appears, for selecting the scenario you would like to use for the protection of the Citrix Web Interface with SMS PASSCODE:
 - a. Select one of the following three scenarios:
 - i. **Disabled**: Select this option to disable SMS PASSCODE authentication for now and enable it manually afterwards (as described in section 16.1).
 - ii. Standalone or Side-by-Side logon: Select this option (recommended) to activate standard SMS PASSCODE authentication. If no other kind of multifactor authentication system is activated, then all users must now authenticate using SMS PASSCODE to log on to the Citrix Web Interface this is called Standalone logon. If another kind of multi-factor authentication system is activated (e.g. RSA SecurID® or SafeWord®), then the users can either authenticate using SMS PASSCODE or the other authentication system this is called Side-by-Side logon.
 - iii. **Dual logon**: Select this option if you need extra high security. If no other kind of multi-factor authentication system is activated, then this option is identical with option (ii). I.e. all users are authenticated using SMS PASSCODE to log on to the Citrix Web Interface this is called *Standalone* logon. However, if another multi-factor authentication system is activated (e.g. RSA SecurID® or SafeWord®), then all users must now authenticate both using SMS PASSCODE and the other authentication system to log on this is called *Dual* logon.
 - b. Click the Next button.

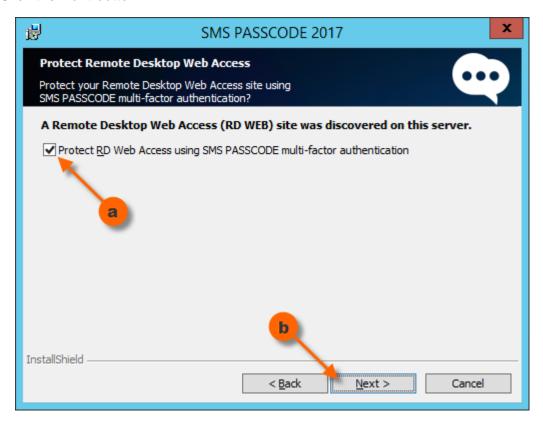


- 10. If a dialog appears, for configuring SMS PASSCODE protection of an OWA site:
 - Select this option if the OWA site on the server should be protected using SMS PASSCODE authentication.
 - b. Select this option to allow ActiveSync clients to synchronize using the OWA site on this server. In this case, SMS PASSCODE authentication will be disabled for ActiveSync requests. Please maintain security by protecting the ActiveSync clients by other means, e.g. using the SMS PASSCODE Secure Device Provisioning component⁸.
 - c. Select this option to allow ActiveSync clients to send AutoDiscover requests to the OWA site. In this case, SMS PASSCODE authentication will be disabled for AutoDiscover requests.
 - d. Select this option to allow RPC over HTTP/HTTPS connections using the OWA site on this server. In this case, SMS PASSCODE authentication will be disabled for RPC over HTTP/HTTPS requests. Please maintain security by protecting these clients by other means.
 - e. Click the Next button.

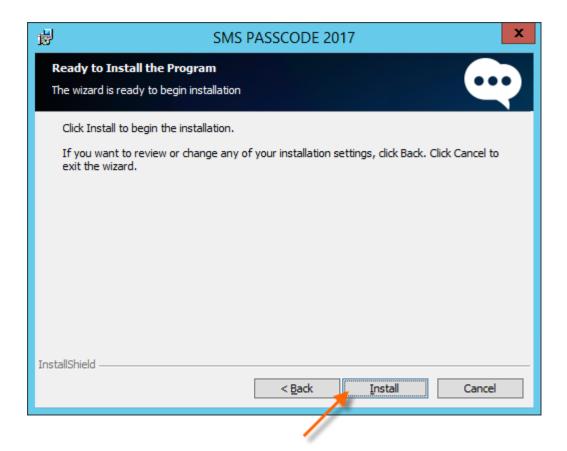


⁸ Please note, that for now the Secure Device Provisioning component is only available in the SMS PASSCODE on-premise solution. It will be available for *cloud mode* in an upcoming version.

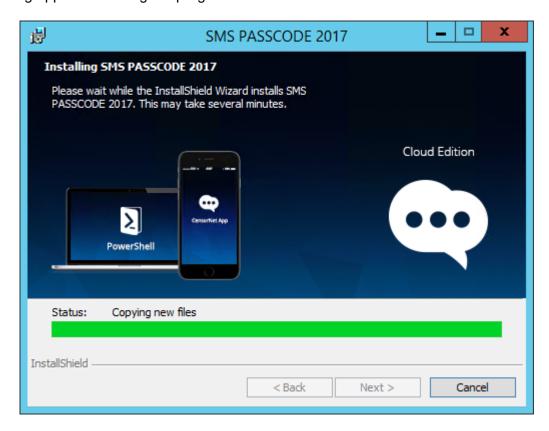
- 11. If a dialog appears, for configuring SMS PASSCODE protection of an RD Web Access site (only supported on Windows Server 2008 R2, 2012 R2 and 2016, cf. section 8.1, page 14):
 - a. Select this option if the RD Web Access site on the server should be protected using SMS PASSCODE authentication.
 - b. Click the Next button.



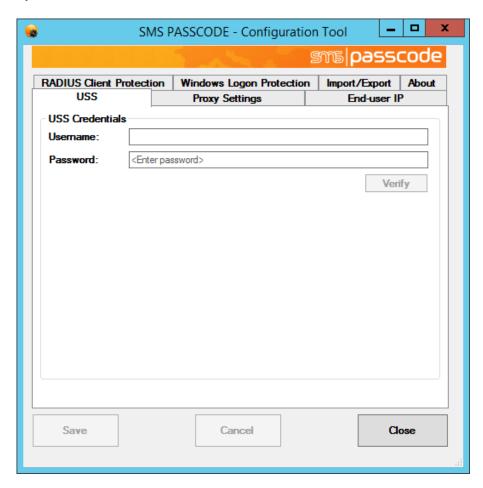
12. You are now ready to perform the installation according to the choices you have made. Click the **Install** button.



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



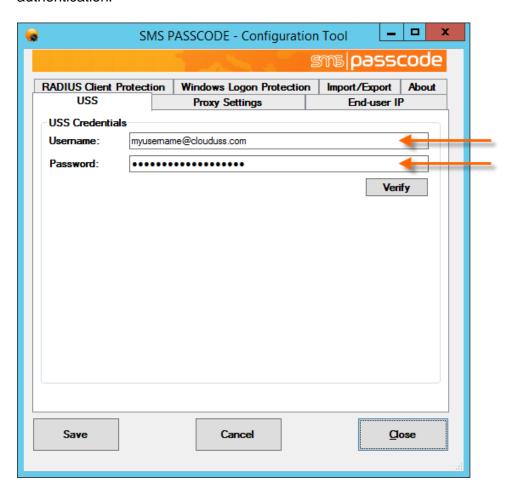
14. At some stage during the installation, the **SMS PASSCODE Configuration Tool** is automatically started:



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 CensorNet USS cloud service and save the settings before the SMS PASSCODE installation is complete. Please follow the instructions below.

a. On the **USS** tab, enter credentials for the USS account to be used for multi-factor authentication:

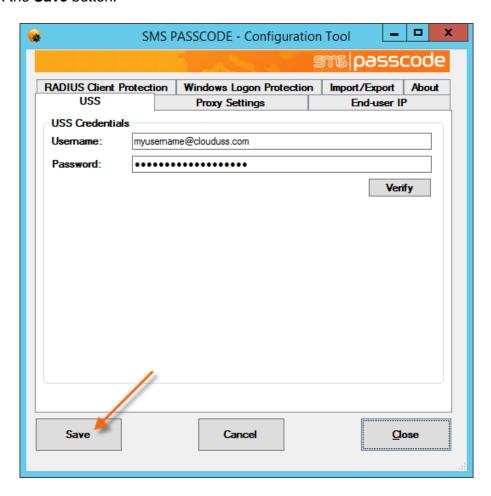


It is recommended to click the **Verify** button to check, that you have entered valid credentials, and that it is possible to connect to the USS cloud service. If connecting to the USS fails, this could be because your network infrastructure requires communication to go via a proxy server. In that case,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

Important: Always remember to specify USS credentials

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

b. Click the Save button.

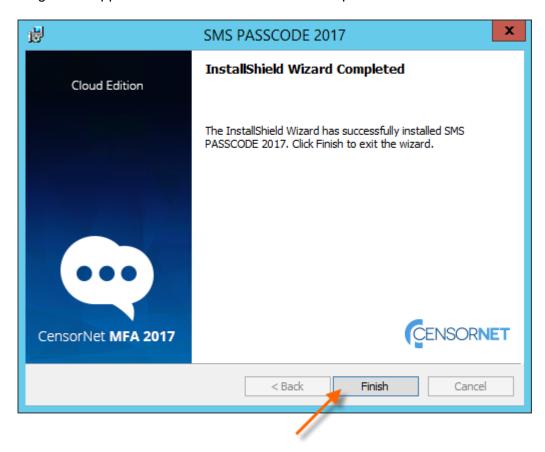


In case a warning message appears regarding error prone entries: Please correct all errors and click the **Save** button again.

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.

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

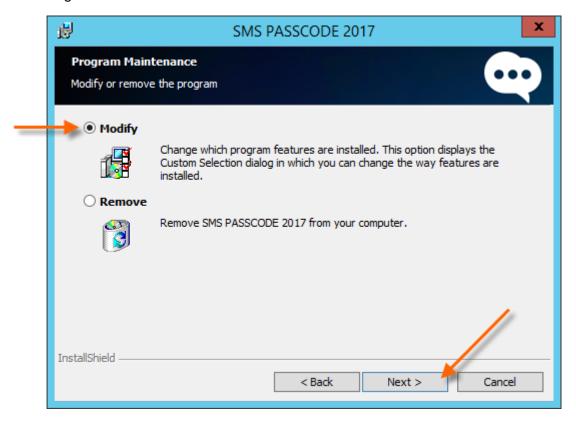


- 16. The installation of SMS PASSCODE is now complete on the current machine. You should now perform any necessary configurations of this machine (cf. section 14).
- 17. If more machines are part of the installation: Please go back to step 1 (page 33) and follow the same instructions for the next machine.

13 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.

14 POST-INSTALLATION ACTIONS

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

- 1) Configuration of the **Citrix Web Interface Protection** component. Please read section 16.1 (page 56).
- 2) Configuration of the **RADIUS Protection** component. Please read section 16.2 (page 57).
- 3) Configuration of the **AD FS Protection** component. Please read section 16.3 (page 72) regarding AD FS 2.0, and section 16.4 (page 76) regarding AD FS 3.0/4.0.
- 4) Configuration of the **IIS Website Protection** component. Please read section 16.5 (page 82).
- 5) Configuration of the **Windows Logon Protection** component. Please read section 16.6 (page 90).

15 USS ADMINISTRATION PORTAL

The USS administration portal allows you to perform administrative tasks related to your SMS PASSCODE protected systems, including:

- Configuration of import of users from your Active Directory
- Configuring settings on the imported users, for example defining the Dispatch Policy. The
 Dispatch Policy allows you to define, whether a user should receive passcode messages by
 SMS, email or using the CensorNet App.
- Viewing reports and charts regarding past login attempts to SMS PASSCODE protected systems.

For more details regarding the USS portal, please go to https://help.clouduss.com/authentication-product-overview.

15.1 Dispatch Polices

In the USS portal, you can define a Dispatch Policy for each user that has been imported from Active Directory (by the CensorNet USS AD Connector).

A Dispatch Policy defines, how passcode messages are sent to each user. The Dispatch Policy is defined on the domain sync settings for a domain, and applies to all users imported from such domain, but can also be overridden on each individual user.

The following Dispatch Policies are currently available:

Dispatch Policy	Description
SMS	Messages will be sent by SMS to the phone number set on the user. If no phone number has been set, then no message will be sent.
Email	Messages will be sent by email to the email address set on the user. If no email address has been set, then no message will be sent.
CensorNet App	Messages will be sent encrypted to the CensorNet App on the device that the user has provisioned using the phone number set on the user. If no phone number has been set, or the user has not provisioned a device with the CensorNet App, then no message will be sent.
SMS w/failover to email	Messages will be sent by SMS to the phone number set on the user. If no phone number has been set, or if the user does not enter the passcode before timeout, then the message will be (re)sent to the email address set on the user.
CensorNet App w/failover to SMS	Messages will be sent encrypted to the CensorNet App on the device that the user has provisioned using the phone number set on the user. If no phone number has been set, then no message will be sent. Otherwise, if the user has not provisioned a device with the CensorNet App, or if the user does not enter the passcode before timeout, then the message will be (re)sent by SMS to the phone number set on the user.
CensorNet App w/failover to email	Messages will be sent encrypted to the CensorNet App on the device that the user has provisioned using the phone number set on the user. If no phone number has been set, or if the user has not provisioned a device with the CensorNet App, or if the user does not enter the passcode before timeout, then the message will be (re)sent by email to the email address set on the user.

Dispatch Policy	Description
Voice call w/failover to SMS	Messages are read aloud for the user using a voice call to the phone number set on the user. If no phone number has been set, then no message is sent. If the user does not enter the passcode before timeout, then the message is resent by SMS to the phone number set on the user.

The CensorNet App is an app for smart phones, that can be used as an alternative way to deliver passcode messages to end-users. It has the following important features:

- It is free of charge.
- The user is automatically notified using push notifications.
- Messages are transmitted end-to-end encrypted, meaning they are encrypted within the CensorNet cloud service, and can only be decrypted by the actual instance of the CensorNet app on the user's smart phone.

Please note, that to send messages to the CensorNet App, you need to go through the following steps:

- 1. Ensure that the relevant users are assigned to a Dispatch Policy that uses the CensorNet App.
- 2. Ensure, that relevant end-users download the CensorNet App from the relevant app store and install it. Whenever a user starts the CensorNet App for the first time, the user will automatically be guided through a provisioning workflow, whereby the user connects the specific instance of the CensorNet App to his phone number in a secure way (using SMS-based multi-factor authentication). This is described in the next section.

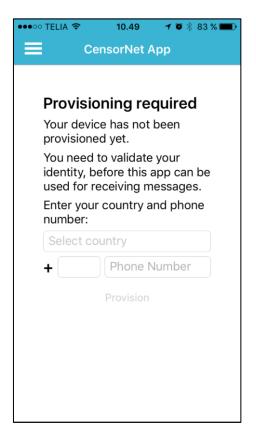
15.2 Provisioning the CensorNet App

The first time a user starts the CensorNet App after having installed it, the user needs to go through a provisioning flow, to assign his phone number to the specific instance of the app. This flow is described below.

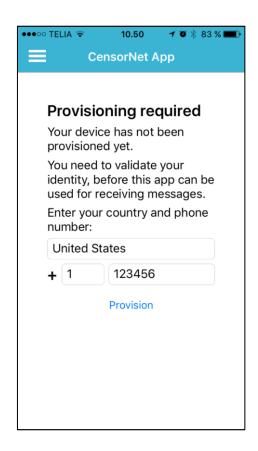
Note: For security reasons, every phone number can only be assigned to a single instance of an installed CensorNet App.

This means that whenever the same phone number is assigned to a new instance of the CensorNet App (on a new device), earlier provisioned devices will stop working immediately.

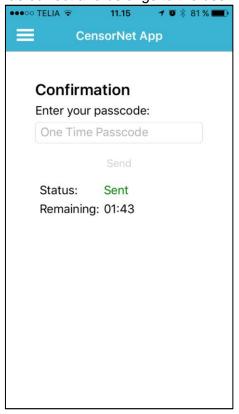
1. The first time the app is started, the following page is shown to the user:



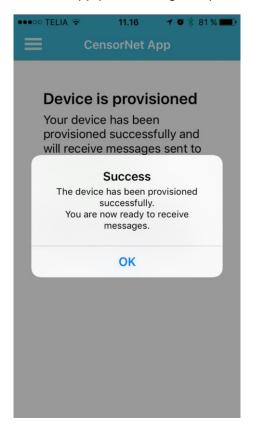
2. The user enters his phone number, including the international prefix. For example:



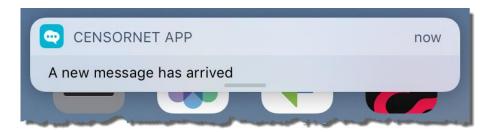
3. When the user clicks the "Provision" link, a one-time passcode (OTP) is send by SMS to the specified phone number. The user must enter the received OTP in order to verify, that the entered phone number was correct and belongs to the user:



4. If the correct OTP is entered, the app provisioning completes successfully:



- 5. The user is now ready to receive encrypted messages using the CensorNet App.
- 6. Whenever the user receives a new message, a push notification will be shown:



The user simply needs to tap the message, and the CensorNet App will automatically open, decrypt the received message and show it to the user.

15.2.1 System Requirements for the CensorNet App

System requirements for the CensorNet App itself:

- Must be installed on a smartphone
- Supported on iOS, version 10.0 or later.
- Supported on Android, version 4.0.3 or later

16 CONFIGURING AUTHENTICATION CLIENTS

16.1 Configuring Citrix Web Interface Protection

If you have installed the optional **Citrix Web Interface Protection** component, you will normally not need to perform any further configuration of this.

Manual configuration of the Citrix Web Interface <u>scenario</u> is only necessary if you decide to change the scenario to a different setting than selected during installation. For example, if the scenario **Disabled** was selected during installation, and you would like to activate SMS PASSCODE authentication for the Citrix Web Interface afterwards.

The procedure for changing the Citrix Web Interface Protection scenario is:

- 1. Open the file **WebInterface.conf** using Notepad. This file is located in the subfolder Conf of the root folder of the Citrix Web Interface. The default path is:
 - <u>Citrix Web Interface 5.x:</u>
 C:\Inetpub\wwwroot\Citrix\XenApp\conf\WebInterface.conf
- 2. Edit the line containing SMSPASSCODE=xxxx. Change it to:
 - SMSPASSCODE=Off
 SMS PASSCODE is disabled.
 - SMSPASSCODE=On
 SMS PASSCODE is enabled (Standalone or Side-By-Side logon).
 - SMSPASSCODE=Both
 SMS PASSCODE is enabled (Standalone or Dual logon).
- 3. Save the WebInterface.conf file.

16.2 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 multifactor 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 16.2.1 below.
 - When step 1 has been completed, all RADIUS clients should work immediately with SMS PASSCODE multi-factor authentication enabled, using the <u>default</u> 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 16.2.2, page 60.

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 16.2.2.1, page 65).

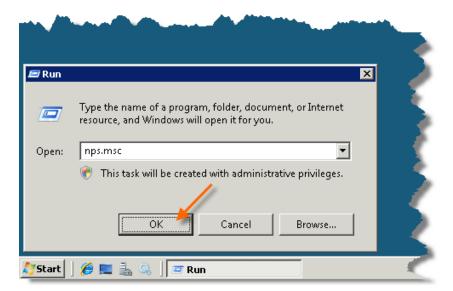
16.2.1 Configuring RADIUS Protection on a Windows Server

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:

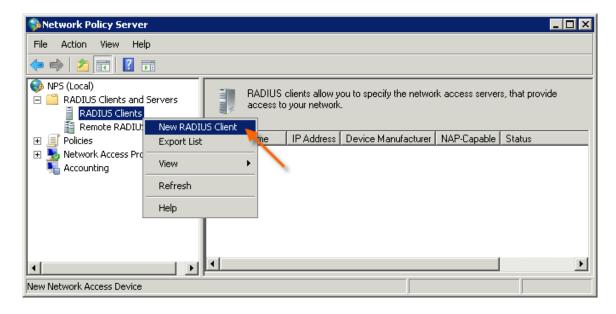
1. Configure all RADIUS clients in the usual way by specifying the **NPS server** as the RADIUS server. If you are in doubt how to perform the configuration, please refer to the configuration guide of the specific RADIUS client in question.

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.

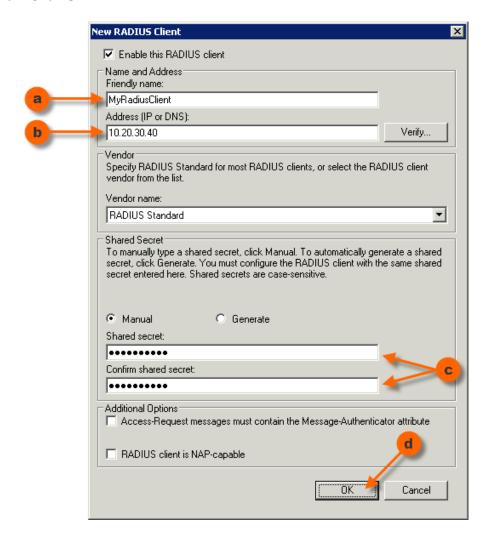
- 2. Start the NPS Management Console:
 - a. Select Run... in the Windows Start menu
 - b. Enter nps.msc
 - c. Click OK

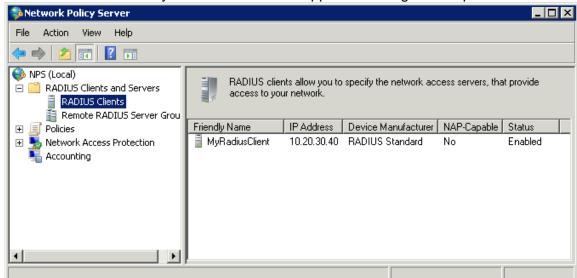


- 3. The NPS Management Console is shown.
- 4. Now you must create all your RADIUS Clients in the NPS Management Console. If these have already been created beforehand, you can skip to step 9.
- 5. To create a RADIUS Client:
 - a. Right-click the RADIUS Clients node.
 - b. Select New RADIUS Client.



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





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

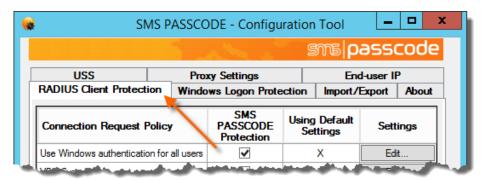
- 8. Repeat steps 5-7 if you need to create more RADIUS Clients.
- This completes the standard configuration of RADIUS authentication using SMS PASSCODE. Please test each RADIUS client to make sure that RADIUS authentication works as expected.

16.2.2 Advanced Configuration of the RADIUS Protection Component

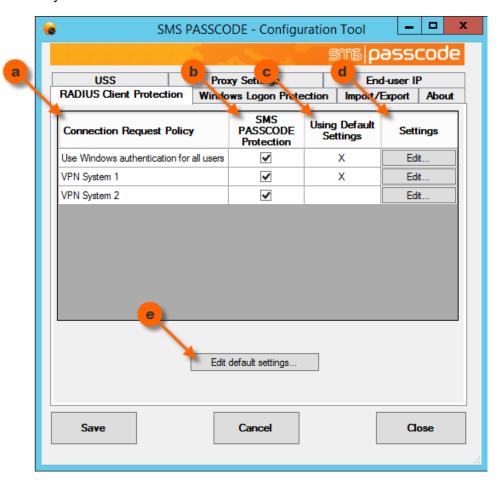
This section describes, how you can maintain advanced settings of the SMS PASSCODE RADIUS Protection component.

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) 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).

NOTE: 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.

Explanation

(b) 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.

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.

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.

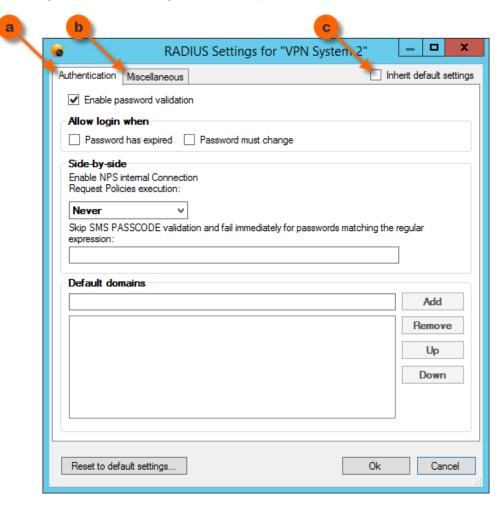
Clear the checkbox in a specific row to disable the SMS PASSCODE RADIUS Protection component for the CRP listed in column (a). All RADIUS authentication requests made through such a CRP will be handled by the NPS default functionality.

(c) When maintaining SMS PASSCODE RADIUS Protection settings, you can maintain default settings, 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.

Column (c) indicates, whether the corresponding CRP of column (a) has been configured to use *default settings* (marked with an "X") or to use specific settings (marked with an empty cell).

- (d) Click the **Edit...** 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 *default settings* again.
- (e) Click the **Edit default settings...** button to edit the *default settings*, i.e. the settings that apply to all CRPs with an "X" in column (c).

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 Authentication: (a) This tab contains settings that affect the authentication behavior of the RADIUS Protection component. Please read section 16.2.2.1 (page 65) for further details. (b) Miscellaneous: 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 16.2.2.2 (page 71) for further details. (c) Inherit default settings 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.

16.2.2.1 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

- 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".
- 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 in the USS. Normally this will mean that a random OTP is generated and sent to the user, and a **Challenge Request** is sent back to the RADIUS client.
- 7. The user receives the passcode and enters it. The RADIUS client forwards the passcode as a **Challenge Response** to the RADIUS server.
- The RADIUS server verifies, whether the passcode received is valid or not, resulting in either an Access Accept or Access Reject packet being sent back to the RADIUS client, respectively.

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

RADIUS Settings for "VPN System 2" Inherit default settings Authentication Miscellaneous Enable password validation Allow login when Password has expired
 Password must change Side-by-side Enable NPS internal Connection Request Policies execution: Skip SMS PASSCODE validation and fail immediately for passwords matching the regular expression: Default domains d Add Remove Up Down

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

The settings have the following purposes:

Reset to default settings.

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).

Ok

Cancel

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. 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 "**S**kip SMS PASSCODE **v**alidation and **f**ail immediately for passwords matching the regular expression" in the Side-by-Side section. "SVF" is an abbreviation for "**S**kip **V**alidation and **F**ail".

The possible options for the NPS IL setting are:

NPS IL setting	Description
Never	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>).
	This means that any authentication and authorization settings of CRPs , and/or any settings of NPs will be ignored. This is the default setting.
Always	Step 5 of the Standard Authentication Flow is changed. Instead of skipping,
, anayo	authentication is now forwarded to the internal NPS logic. I.e. CRP and NP 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.
	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> .

NPS IL setting	Description
On failure only	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 NPS IL setting is set to Never .
	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> .
	In other words, CRP and NP 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.
	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.
	WARNING: When selecting the option On Failure only, never set the CRP to allow access without validating credentials. This would grant access to users without any validation at all.

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 entered⁹. 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 <u>skipped</u> altogether, meaning no user resolve or password validation is performed. Instead, the steps 2-4 are immediately treated as <u>failed</u>. 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.

⁹ 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
 Standard SMS PASSCODE multi- factor authentication must be performed for all users. No need for Network Policy support. 	Set the NPS IL setting to Never.
 Standard SMS PASSCODE multi- factor authentication must be performed for all users. Support for Remote Access Policies is needed. 	 Set the NPS IL setting to Always. Set the CRP authentication setting to Authenticate on this server.
 You have two different RADIUS authentication systems (SMS PASSCODE and another one). Some users will only use one type of authentication, whereas some users might use both types of authentication. 	 Set the NPS IL setting to On Failure Only. Set the CRP authentication setting to forward requests to the other RADIUS system. Optional: If the password for the other authentication system is NOT the user's AD password, and this authentication system is used often by users, which are also 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 SVF setting that will identify the passwords of the other 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.
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.	 Set the NPS IL setting to Always. Set the CRP authentication setting to forward requests to the other RADIUS system. Clear setting (a), "Enable password validation", to skip the initial validation of the password for all requests from the RADIUS client(s) in question.

NOTE:

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

d. **Default domains**

This setting is relevant, if you need to authenticate users from a domain different from the one, of which the NPS server is a member. To achieve this, you must add the domains to the list, from which users are allowed to log in. The list of domains has two purposes:

- 1. <u>Restriction</u>: Users are only allowed to log in from the domains listed. Even if a user logs in with a fully qualified username, the login is denied, if the domain is not found in the domain list.
- 2. <u>Prioritization</u>: If you need to authenticate users from different domains, but do not wish to force the users to enter or select the domain explicitly during authentication, then the SMS PASSCODE system needs to know, in which order to search for a matching domain. The search will occur in the exact order in which the domains are listed.

When the domain list is empty, this is treated as if the list contained two entries, equal to the NETBIOS name and the DNS name of the domain that the NPS server has joined. This will allow users of the local domain to log in using their username only or using their UPN.

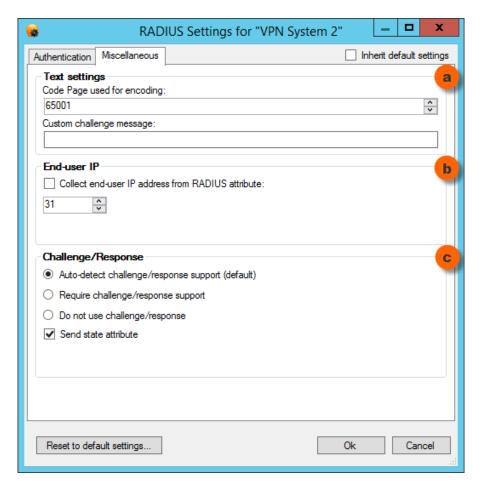
IMPORTANT (Restriction always applies)

Even when users try to log in using a fully qualified user name, access is denied, unless the domain is present in the domain list. You must add both the NETBIOS and DNS domain names to the list, if you want users to be able to log in using both domain formats.

Since you can customize different settings per CRP of the NPS, this allows you to define different domain lists for logins via different CRPs.

16.2.2.2 Miscellaneous RADIUS settings

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



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.

Custom challenge message: By default, SMS PASSCODE RADIUS Protection will send the message "Enter PASSCODE" when the user is requested to enter the SMS PASSCODE during the RADIUS challenge. Using this setting, you can change this message to a different text. This is useful for localization of the message, or in case your RADIUS client will only accept specific text(s) in the RADIUS challenge.

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.

16.3 Configuring AD FS 2.0 Protection

The SMS PASSCODE **AD FS Protection** component adds multi-factor authentication to applications that are accessible via AD FS 2.0, 3.0 and 4.0. This section describes the integration with <u>AD FS 2.0</u>, and describes how to configure SMS PASSCODE **AD FS Protection** for AD FS 2.0. For AD FS 3.0/4.0, please read section 16.4 (page 76).

SMS PASSCODE **AD FS Protection** for <u>AD FS 2.0</u> allows you to apply SMS PASSCODE multifactor authentication to cloud applications that have been configured to validate users by means of form-based authentication through AD FS 2.0.

If you have already, before installing the SMS PASSCODE AD FS Protection component, successfully configured one or more (cloud) applications to use AD FS 2.0 form-based authentication, then you simply need to install the SMS PASSCODE AD FS Protection component on your AD FS 2.0 server(s), and SMS PASSCODE multi-factor authentication will be added to your cloud application(s) without any need of further actions.

On the other hand, if you have not configured your cloud applications to use AD FS 2.0 form-based authentication yet, then it is recommended to do so, <u>before</u> installing the SMS PASSCODE AD FS Protection component, and to ensure that standard authentication works as expected.

16.3.1 Background

It is becoming more and more common that cloud applications, also known as *Service Providers*, do not perform user authentication by themselves, but instead delegate the authentication to a 3rd party authentication service, also known as an *Identity Provider*. To ensure that Service Providers and Identity Providers from different vendors can communicate with each other, different standards have been introduced for exchanging authentication and authorization data. Some of the most important of such standards are:

- SAML 2.0
- WS-Trust
- WS-Federation

Well-known examples of cloud applications using one of these standards are:

- Microsoft Office 365 Web Clients
- Google Apps
- SalesForce

Microsoft has implemented a Windows server role called Active Directory Federation Services (AD FS), which is a concrete example of an *Identity Provider* that supports all three of the standards mentioned above. AD FS 2.0 is useful for companies and organizations already relying on a Microsoft AD infrastructure, because it makes it possible to use the existing AD user accounts for authentication when accessing cloud applications.

<u>Windows Server 2008 R2:</u> AD FS 2.0 is available as a free download from Microsoft. It is supported on Windows Server 2008 R2 (please look up current system requirements as specified by Microsoft).

<u>Windows Server 2012:</u> AD FS 2.0 is a built-in feature in the Windows Server 2012 **Standard** and **Datacenter** editions. You must install the feature using the Server Manager.

16.3.2 AD FS 2.0 Infrastructure

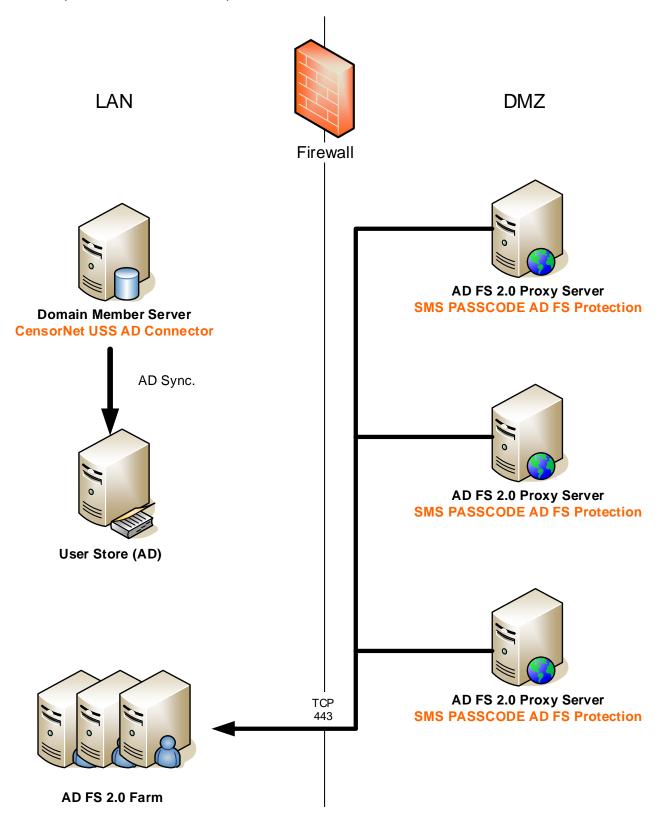
This section describes on which servers you should install the SMS PASSCODE AD FS Protection component.

When deploying AD FS 2.0 you have several options, ranging from a single server configuration to an AD FS 2.0 server farm, possibly even including AD FS 2.0 Proxy servers for remote users.

The typical scenario is:

- AD FS 2.0 Proxy servers are located in your perimeter network (DMZ) and will allow remote
 users to access cloud applications using form-based authentication. You should install the
 SMS PASSCODE AD FS Protection component on any of these proxy servers that
 supports authentication of a cloud application that you would like to protect with SMS
 PASSCODE multi-factor authentication.
- AD FS 2.0 servers on your internal network will be used for easy single sign-on to cloud applications for users already authenticated on your internal network. You will normally NOT install SMS PASSCODE AD FS Protection on these servers, unless you want to enforce multi-factor authentication in this case as well, or because you have no AD FS 2.0 Proxy servers in your infrastructure.

An example of an installation setup is shown below:



Another scenario is to make use of the Microsoft Unified Access Gateway (UAG) and let it act as an AD FS 2.0 Proxy server. In this case, you must not use the SMS PASSCODE AD FS Protection component, but instead configure the UAG to authenticate using a RADIUS server protected by the

SMS PASSCODE RADIUS Protection component (this component is described in section 16.2, page 57).

16.4 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 2.0, 3.0 and 4.0. This section describes the integration with <u>AD FS 3.0</u> and <u>AD FS 4.0</u>, and describes how to configure SMS PASSCODE **AD FS Protection** for AD FS 3.0/4.0. For AD FS 2.0, please read section 16.3 (page 72).

SMS PASSCODE **AD FS Protection** for <u>AD FS 3.0/4.0</u> 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.

16.4.1 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.

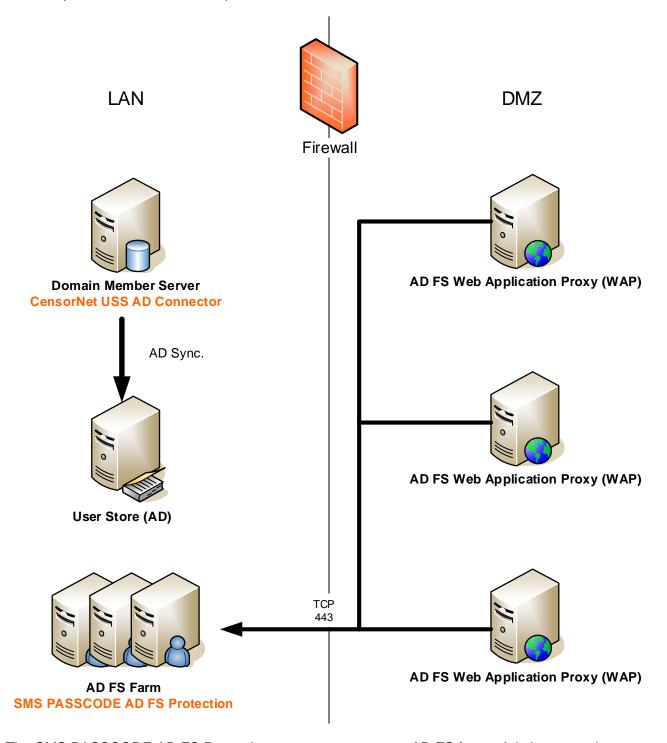
Any such authentication scenarios supported by the AD FS infrastructure can be extended with SMS PASSCODE multi-factor authentication (MFA), by installing SMS PASSCODE AD FS Protection on your AD FS server(s) and enabling MFA for the applications of your choice, in the AD FS management console.

16.4.2 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 <u>AD FS main server(s)</u>, not on the Web Application Proxy servers.

An example of an installation setup is shown below:



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

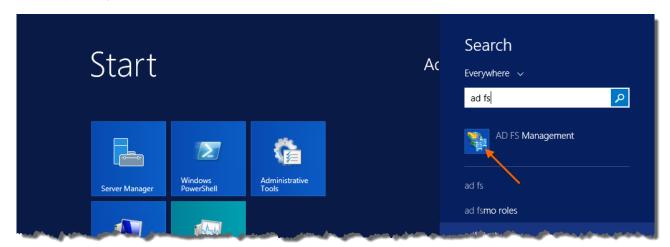
The installation of the AD FS Protection component on each AD FS server will install a so-called SMS PASSCODE AD FS **MFA Adapter** on every such server. You need to configure this MFA Adapter, to activate SMS PASSCODE multi-factor authentication. This is described below in sections 16.4.3 and 16.4.4 for AD FS 3.0 and 4.0, respectively.

16.4.3 Configuring the MFA Adapter for AD FS 3.0

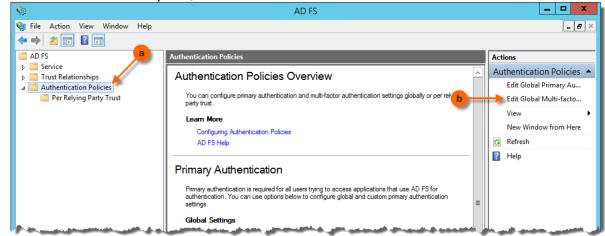
This section applies to <u>Windows Server 2012 R2</u>. It is described below, how you enable the SMS PASSCODE MFA Adapter, after you have installed it on your AD FS server (or on every AD FS server, in case of an AD FS farm).

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...



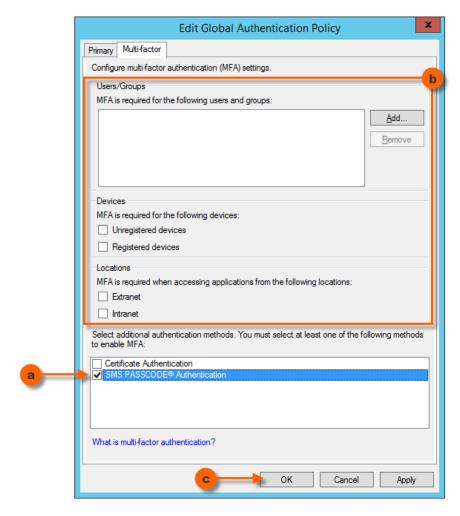
- 3. The dialog Edit Global Authentication Policy opens, with the tab Multi-factor selected.
 - a. In the bottom listbox, select the checkbox **SMS PASSCODE Authentication** in order to enable the SMS PASSCODE MFA Adapter.
 - Additionally, in order for multi-factor authentications to be triggered, you 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 afterwards¹⁰.

¹⁰ 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.

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.

c. Click the **OK** button.



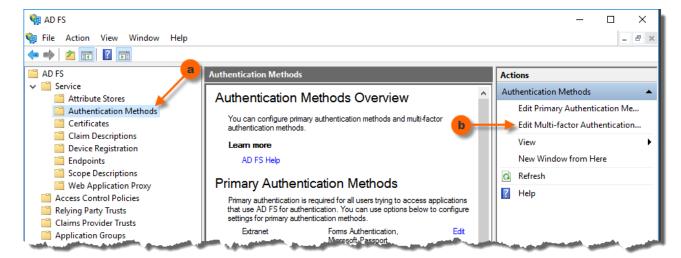
After having enabled and configured the SMS PASSCODE MFA adapter, please make sure to test the authentication behavior of the affected applications, in order to ensure the expected authentication behavior.

16.4.4 Configuring the MFA Adapter for AD FS 4.0

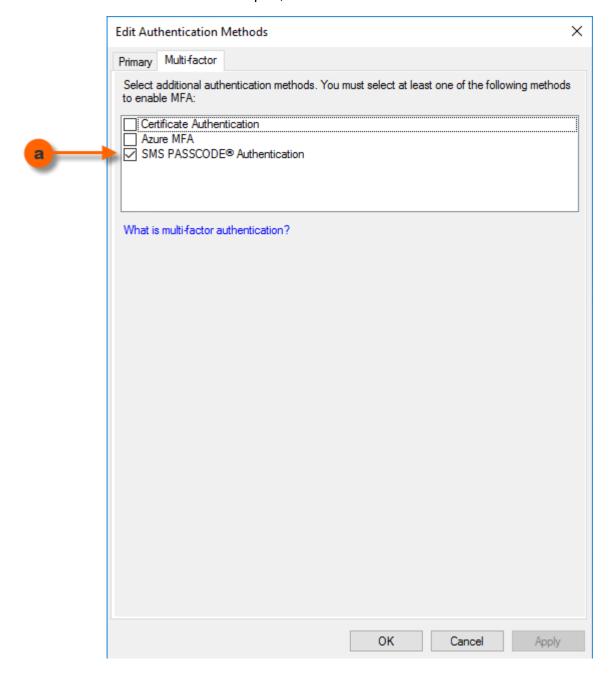
This section applies to <u>Windows Server 2016</u>. It is described below, how you enable the SMS PASSCODE MFA Adapter, after you have installed it on your AD FS server (or on every AD FS server, in case of an AD FS farm).

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.

16.4.5 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.

16.5 Configuring IIS Website Protection

If you have installed the optional **IIS Website Protection** component on a server hosting Microsoft Outlook Web Access (OWA) or Microsoft RD Web Access, you will normally enable protection of the OWA or RD Web Access site during installation and will not have to perform any further configurations afterwards. However, you may decide to perform further configuration of the **IIS Website Protection** component in the following cases:

- a. If a new website is added to the IIS, then, by default, access to this site will be disallowed by the SMS PASSCODE **IIS Website Protection** component. In this case, you have to *refresh* the **IIS Website Protection** configuration file to allow access to this website.
- b. If you wish to protect other websites than OWA or RD Web Access by SMS PASSCODE authentication, then you have to enable this manually. Please note, that the SMS PASSCODE IIS Website Protection component currently only supports protection of OWA sites, RD Web Access sites (Windows 2008 R2, 2012 R2 and 2016 only) and websites using Basic or Integrated Windows Authentication.
- c. If you wish to disable SMS PASSCODE authentication for specific websites, then you can do this manually.
- d. The SMS PASSCODE **IIS Website Protection** component also offers advanced configuration options. For example, it is possible to configure authentication rules depending on the clients' source IP-addresses.

16.5.1 ISAPI Filter

The SMS PASSCODE **IIS Website Protection** component is implemented using an **ISAPI filter**. This ISAPI filter is added to the IIS running on the server and extends the behavior of the IIS.

The default path of the ISAPI filter is:

C:\Program Files\SMS PASSCODE\ISAPI\SMSPasscodeISAPIFilter.dll

16.5.2 ISAPI Filter Configuration File

The behavior of the ISAPI filter is controlled by a XML configuration file. The default path of this configuration file is:

C:\Program Files\SMS PASSCODE\ISAPI\Config.xml

You can control the behavior of the ISAPI filter by making changes to this configuration file. The most common configuration changes are made easiest using the command line tool called **IsapiAdmin**. This tool is by default located here:

```
C:\Program Files\SMS PASSCODE\ISAPI\IsapiAdmin.exe
```

The syntax and usage of the **IsapiAdmin** tool is described in section 16.5.3 below.

Another way to change the configuration file is by making changes to this file manually using a text editor (e.g. Notepad). This allows for more advanced configuration changes. The syntax of the configuration file is described in detail in section 16.5.4.

IMPORTANT:

Whenever changes are made to the ISAPI filter configuration file using the **IsapiAdmin** tool, these changes take effect immediately.

Whenever changes are made to the ISAPI filter configuration file manually, these changes do <u>not</u> take effect until the **SMS PASSCODE ISAPI Service** has been restarted.

16.5.3 The IsapiAdmin Tool

The default path of the command line tool IsapiAdmin is:

```
C:\Program Files\SMS PASSCODE\ISAPI\IsapiAdmin.exe
```

This tool has four main features:

- a. Enable SMS PASSCODE authentication for a specific website on the local IIS.
- b. Disable SMS PASSCODE authentication for a specific website on the local IIS.
- c. Refresh the ISAPI filter configuration file, allowing access to all newly added websites on the local IIS.
- d. List the websites on the local IIS.

The following sub-sections describe the syntax of the **IsapiAdmin** tool.

16.5.3.1 Enable Protection of a Website

To enable SMS PASSCODE authentication for a specific website, use the -protect option in one of the following two ways:

The different arguments of the command are described in the table below.

Argument	Description
-protect	This argument instructs the tool to protect a website.
-name	This argument is used to specify the name of the website to protect. Example: IsapiAdmin -protect -name "Default Web Site"
-siteID	This argument is used to specify the ID of the website to protect. The default website always has ID 1. Example: IsapiAdmin -protect -siteID 1 Use IsapiAdmin -list to get a list of the IDs of the different websites (described in section 16.5.3.4, page 87).
-DirName (optional)	This optional argument is used to specify the name of the virtual directory that is created within the website that is being protected. This virtual directory contains files needed by the ISAPI filter. If the argument is not present, the default name SmsPasscodeLogon is used. Example: IsapiAdmin -protect -name "Default Web Site" -DirName "MyName"
-owa (optional)	This argument is required if the website is an OWA Website using form-based authentication . For websites using Basic or Integrated Windows Authentication, please omit this argument.
-allowActiveSync (optional)	This argument is only allowed together with the <code>-owa</code> argument. It instructs the ISAPI filter to disable SMS PASSCODE authentication for ActiveSync connections.
-allowAutoDiscover (optional)	This argument is only allowed together with the <code>-owa</code> argument. It instructs the ISAPI filter to disable SMS PASSCODE authentication for ActiveSync AutoDiscover requests.
-allowRpcOverHttps (optional)	This argument is only allowed together with the <code>-owa</code> argument. It instructs the ISAPI filter to disable SMS PASSCODE authentication for RPC over HTTP/HTTPS connections.
-rdweb	This argument is required if the website is an RD Web Access site using form-based authentication . For websites using Basic or Integrated Windows Authentication, please omit this argument. Please note that in order to protect an RD Web Access site, additional actions are required (cf. section 10.3.2, page 23).

Examples:

 Enable SMS PASSCODE authentication for an OWA site using form-based authentication, allow ActiveSync, disallow RPC over HTTP/HTTPS connections:

```
IsapiAdmin -protect -name "Default Web Site" -owa -allowActiveSync
```

...or since the Default Web Site always has ID 1, you could also enter:

```
IsapiAdmin -protect -siteID 1 -owa -allowActiveSync
```

 Enable SMS PASSCODE authentication for the SMS PASSCODE Web Administration Interface:

```
IsapiAdmin -protect -name "SMS PASSCODE Admin"
```

• Enable SMS PASSCODE authentication for an OWA site using Basic or Integrated Windows Authentication:

```
IsapiAdmin -protect -name "Default Web Site"
```

16.5.3.2 Disable Protection of a Website

To disable SMS PASSCODE authentication for a specific website, use the -unprotect option in one of the following two ways:

IsapiAdmin -unprotect -name "Web Site Name" - or IsapiAdmin -unprotect -siteID "Web Site ID"

The different arguments of the command are described in the table below.

Argument	Description
-unprotect	This argument instructs the tool to disable protection of a website.
-name	This argument is used to specify the name of the website to unprotect. Example: IsapiAdmin -unprotect -name "Default Web Site"
-siteID	This argument is used to specify the ID of the website to unprotect. The default website always has ID 1. Example: IsapiAdmin -unprotect -siteID 1 Use IsapiAdmin -list to get a list of the IDs of the different websites (described in section 16.5.3.4, page 87).

Examples:

Disable SMS PASSCODE authentication for an OWA site:

```
IsapiAdmin -unprotect -name "Default Web Site"
```

...or since the Default Web Site always has ID 1, you could also enter:

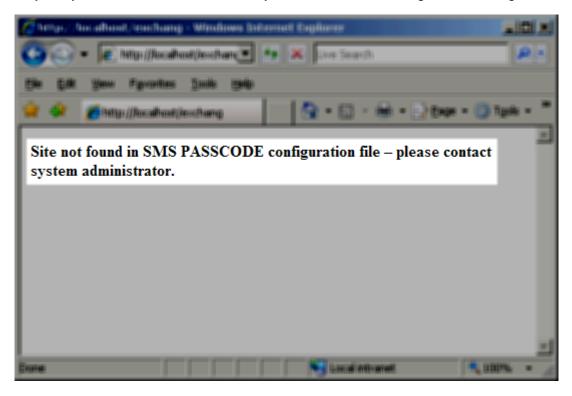
```
IsapiAdmin -unprotect -siteID 1
```

 Disable SMS PASSCODE authentication for the SMS PASSCODE Web Administration Interface:

```
IsapiAdmin -unprotect -name "SMS PASSCODE Admin"
```

16.5.3.3 Refresh the Configuration File

The ISAPI filter configuration file specifies, for each website, whether SMS PASSCODE authentication is enabled or disabled. However, if a new website is added to the local IIS, and this website is not listed in the ISAPI filter Configuration file, then the ISAPI filter will disallow access to this site. If you try to access the website, then you will see the following error message:



To allow access to such a website, you must either enable or disable SMS PASSCODE authentication as described above in section 16.5.3.1 or 16.5.3.2, respectively. Another possibility is to use the "refresh" option using the following syntax:

```
IsapiAdmin -refresh
```

Executing this command will automatically detect all websites present in the local IIS and add all missing websites to the ISAPI filter configuration file. All missing websites are added with SMS PASSCODE authentication disabled.

16.5.3.4 List ID of Websites

The **IsapiAdmin** command line tool also has a feature for showing a list of all websites present in the local IIS. This list displays the name and ID of each site. The syntax for showing the list of websites is:

```
IsapiAdmin -list
```

16.5.4 ISAPI Filter Configuration File Syntax

The configuration of the ISAPI filter is stored in a XML configuration file. The default path of this file is:

```
C:\Program Files\SMS PASSCODE\ISAPI\Config.xml
```

The following subsections describe the anatomy (syntax) of this file in detail.

IMPORTANT:

Whenever changes are made to the ISAPI filter configuration file manually, these changes do <u>not</u> take effect until the **SMS PASSCODE ISAPI Service** has been restarted.

16.5.4.1 <CONFIG> Element

At the top level, the configuration file contains one <CONFIG> element, which again contains one or more <SITE> elements.

```
<CONFIG>
<SITE />
...
<SITE />
</CONFIG>
```

The configuration file must contain a <SITE> element for each website in the local IIS.

16.5.4.2 **<SITE>** Element

Each site element of the configuration file contains the settings for a specific website in the local IIS:

Each SITE element contains the following attributes:

- name: Specifies the name of the website that is configured by this <SITE> element.
- smspasscodedir: Specifies the URL of the virtual directory containing the files that are needed by the SMS PASSCODE ISAPI filter during SMS PASSCODE authentication.
 Recommended value is "/SmsPasscodeLogon/". It is recommended to enable SMS PASSCODE authentication for a website using the IsapiAdmin tool because this tool will

automatically create the required virtual directory and configure it correctly (please read section 16.5.3.1, page 83).

SMS PASSCODE authentication is enabled by default for each website that is named by a SITE element. However, each SITE element may contain one or more <URL> elements that configure authentication behavior of the website.

16.5.4.3 < URL> Element

The <URL> elements within a <SITE> element define the authentication behavior of the website. The syntax is:

Each <URL> element contains the following attributes:

- path: Specifies the URL to which this element applies. Please note, that the configuration
 of this element applies to all sub-URLs as well, unless these are overruled by another,
 more specific <URL> element.
- smspasscode: Boolean attribute defining whether SMS PASSCODE authentication should be enabled (smspasscode="true") or disabled (smspasscode="false") for the specified URL.
- **credentials**: This is an **optional** attribute. It should not be specified for websites or virtual directories that are using Basic or Integrated Windows Authentication.

For OWA sites using **form-based authentication**, **credentials="OWA"** should be specified for the following virtual directories:

- o /exchange
- o /exchweb
- o /owa

For RD Web Access sites using **form-based authentication**, **credentials**="**rdweb**" should be specified for the following virtual directories:

/rdweb

Normally, you will not set the attribute **credentials** manually. Use the tool **IsapiAdmin** with the -owa or -rdweb option to protect an OWA site or RD Web access site, respectively (please read section 16.5.3.1, page 83).

16.5.4.4 <host> Element

Each <URL> element may contain one or more <host> elements. Using a <host> element you can override the configuration of the parent <URL> element depending on the client's source IP address. The syntax is:

```
<host ip="x.x.x.x" smspasscode="true|false" />
```

I.e. each <host> element contains the following attributes:

- **ip**: Specifies the source IP address of the client(s) that this element applies to. Wildcards are allowed, e.g. **ip**="**192.168.***". Also, you may specify **ip**="**localhost**"; in this case the element applies to all requests from the local host, no matter if the requests are coming from IP address 127.0.0.1 or from any other locally assigned IP address.
- smspasscode: Boolean attribute defining whether SMS PASSCODE authentication should be enabled (smspasscode="true") or disabled (smspasscode="false") for the specified client(s).

16.5.4.5 Configuration Examples

This section shows different examples for configuring websites:

• Enable SMS PASSCODE authentication for the default website:

```
<CONFIG>
<SITE name="Default Web Site" smspasscodedir="/SmsPasscodeLogon/" >
<URL path="/" smspasscode="true" />
<URL path="/SmsPasscodeLogon" smspasscode="false" />
</SITE>
</CONFIG>
```

Disable SMS PASSCODE authentication for the default website:

 Enable SMS PASSCODE authentication for the default website, but only for the URL's starting with "/secure":

 Enable SMS PASSCODE authentication for the default website, but not for clients requesting from IP addresses 192.168.*:

• Enable SMS PASSCODE authentication for an OWA site using form-based authentication:

16.6 Configuring Windows Logon Protection

If you have installed the optional SMS PASSCODE **Windows Logon Protection** component, you will normally not have to perform any further configuration of this.

The **Windows Logon Protection** component is implemented by means of a **custom Credential Provider**.

16.6.1 Windows Logon User Exclusion Groups

You may optionally configure users who should be excluded from SMS PASSCODE authentication during Windows Logon. To support this, two local¹¹ user groups have been created on the computer during installation:

- **SMS PASSCODE console exclusion**: All users being member of this group are subject to the following rules:
 - They must authenticate using SMS PASSCODE when they log on to the computer using a Remote Desktop (RDP).
 - They will <u>not</u> authenticate using SMS PASSCODE when they log on locally using the console. I.e. only user name and Windows password is required to log on in this case.
- SMS PASSCODE general exclusion: All users being member of this group will log on to the computer without SMS PASSCODE authentication – whether they log on using Remote Desktop (RDP) or locally using the console.

¹¹ The groups are created as AD groups when the SMS PASSCODE Windows Logon Protection component is installed on a Domain Controller. Still, the groups only have effect on Windows Logon on the local computer.

By default, all users being member of the local Administrators group are automatically added during installation to the **SMS PASSCODE console exclusion** group. This ensures that local administrators will always be able to log on using the local console.

16.6.2 Remote Desktop Logon Timeout

When attempting RDP access to a machine, the connection terminates within 30 seconds by default, if the Remote Desktop Logon has not completed within this time limit. This might be a problem when you are using SMS PASSCODE Windows Logon Protection, and you in some cases expect completion of SMS PASSCODE multi-factor authentications to take longer than 30 seconds; for example in case of using advanced Dispatch Policies, where a second OTP is sent to the user, in case the first one expires. To extend the Remote Desktop Logon Timeout, select the **Windows Logon Protection** tab in the SMS PASSCODE Configuration tool, and select an appropriate timeout value in the top of the tab:



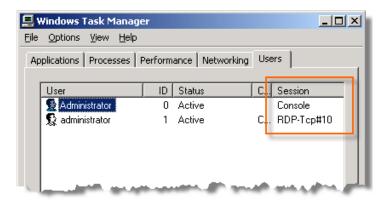
IMPORTANT

Whenever you change the **Remote Desktop Logon Timeout** setting, the new value does not take effect until the computer has been restarted.

16.6.3 RDP Listener Exclusion

Whenever you log on to a Windows session on a Windows machine, your session is established through a specific *WinStation*. The most common WinStations are **Console** and **Rdp-Tcp**. The **Console** WinStation is used when logging on using the local console, whereas the **Rdp-Tcp** WinStation is used when logging on using an RDP connection (tcp port 3389 by default). The **Rdp-Tcp** Winstation is also called an **RDP Listener**.

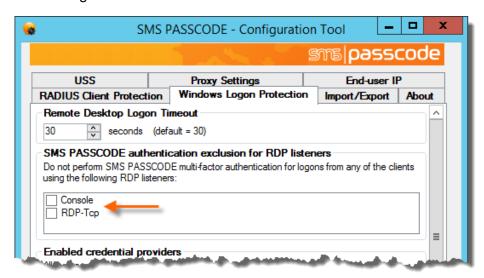
You can see which **WinStation** has been used to establish each session on a machine by inspecting the **Users tab** in the **Task Manager**. Each session will be named using the name of the corresponding **WinStation**.



By default, when SMS PASSCODE **Windows Logon Protection** has been installed on a computer, all Windows sessions will be protected using SMS PASSCODE authentication, unless SMS PASSCODE authentication is skipped due to the rules of exclusion groups (cf. section 16.6.1, page 90).

However, it is also possible to disable SMS PASSCODE **Windows Logon Protection** for individual WinStations. For example, you can disable **Windows Logon Protection** for the Console WinStation to disable SMS PASSCODE authentication for all local console logons, independent of group exclusion membership; or you can disable **Windows Logon Protection** for individual RDP Listeners, in case you have created some custom RDP Listeners by yourself.

WinStations / RDP Listeners exclusion is configured on the **Windows Logon Protection** tab of the SMS PASSCODE Configuration Tool:



16.6.3.1 Creating a custom RDP Listener

You can create new custom RDP Listeners on a Windows machine. Why would you like to do this? For example, it might be useful in the following scenario: A machine is accessible through RDP, but you only want users to be authenticated by SMS PASSCODE **Windows Logon Protection** when users are logging on from the external network. When logging on from the internal LAN, users should be allowed to log on using standard Windows authentication. This can be achieved using the following setup:

- On the target machine: Create a new RDP Listener and assign a non-standard RDP port to this listener, e.g. port 4000.
- Configure your firewall to allow access on port 4000 from the external network.
- Configure your firewall to use Network-Address-Translation (NAT) regarding all RDP requests on port 4000 from the external network. NAT should be configured to transfer all RDP requests from port 3389 to port 4000. This means that all external RDP requests will connect to the target machine using the new custom RDP Listener.
- Exclude the standard RDP Listener from SMS PASSCODE Windows Logon Protection.

Using such a setup, all users on the internal LAN can make a standard RDP connection (using TCP port 3389) to the standard RDP Listener on the target machine and will be allowed to log in using standard Windows authentication, because the standard RDP Listener has been excluded from SMS PASSCODE **Windows Logon Protection**. All external requests will hit the target machine using the custom RDP Listener (on TCP port 4000), i.e. these users are required to perform SMS PASSCODE authentication to establish a Windows session on the target machine.

The scenario above is also possible without configuring NAT in the firewall. However, in this case, the external users will manually have to change the TCP port of the RDP connection to the TCP port of the custom RDP Listener.

To create a custom RDP Listener, please follow this procedure:

- 1. Make a backup of your registry.
- 2. Open the registry using regedit.exe.
- 3. Locate the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp Right-click the key and export it to a file.

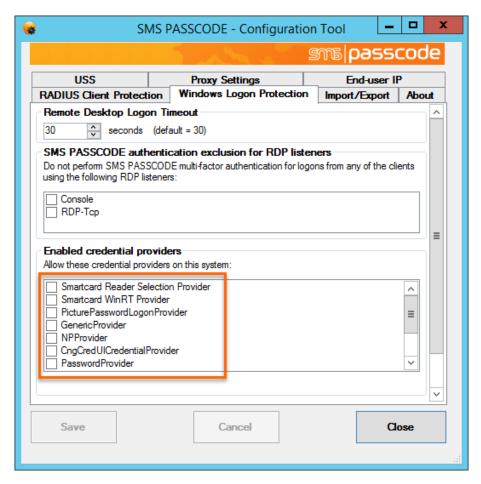
- 4. Open the exported file. Change the name of the key "RDP-Tcp" to a new name of own choice. This will be the name of the custom RDP Listener. Additionally, change any other required settings, e.g. **PortNumber**. Save the file.
- 5. Import the modified file into the registry. The registry will now contain a new key with the name of the custom RDP Listener. This new key is located below the key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations

16.6.4 Credential Provider Filtering

As mentioned previously, the SMS PASSCODE Windows Logon Protection component is implemented by means of a **custom Credential Provider**. Please notice, that the SMS PASSCODE installation will automatically disable all other installed credential providers¹² by default, restricting users to log on only using SMS PASSCODE authentication.

If you wish to allow users to log on using other installed Credential Providers, you can enable these Credential providers on the **Windows Logon Protection** tab of the SMS PASSCODE Configuration Tool:

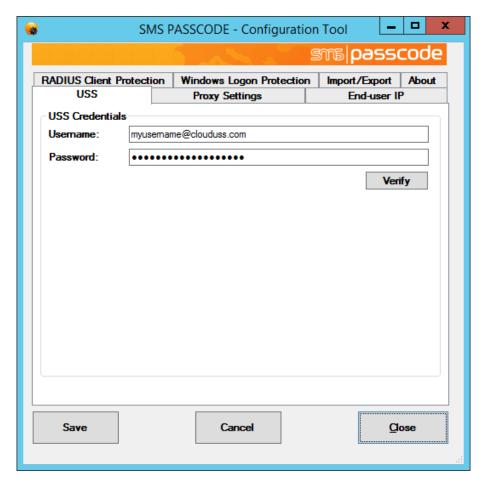


¹² Actually the SMS PASSCODE installation might leave some specific 3rd party credential providers enabled that are known to co-exist with SMS PASSCODE without disabling or conflicting with SMS PASSCODE authentication during the Windows Logon. The VMware Credential Provider installed on VMware View 4.0 clients is an example of this.

17 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 actual number of tabs shown depends on the current configuration and the components that have been installed. The different tabs have the following purposes:

Tab	Explanation
USS	This tab allows you to enter credentials of an USS account for accessing the USS cloud service. Only users existing within that USS account will be able to log in using SMS PASSCODE multi-factor authentication. Click the Verify button on this tab to verify the connection to the USS cloud service, and verify the validity of the credentials entered.
Proxy Settings	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.
End-user IP	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.

Tab	Explanation
Windows Logon Protection	This tab appears only when SMS PASSCODE Windows Logon Protection has been installed on the local machine. The tab allows configuring different settings related to the Windows Logon Protection component. Please read section 16.6 (page 90) for more details.
RADIUS Client Protection	This tab appears only when SMS PASSCODE RADIUS Protection has been installed on the local server. The tab allows configuring different settings related to the RADIUS Protection component. Please read section 16.2.2 (page 60) for more details.
Import/Export	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. When exporting settings, you will be prompted to enter a password that is used for protecting (encrypting) confidential data in the text file. This password will be requested, when you try to import the settings file. Please note, that it is possible to import and export settings from the command line (e.g. from a batch file or login script). This is useful, if you would like to mass-import SMS PASSCODE settings to many machines, e.g. when protecting virtual machines like VMware View clients with SMS PASSCODE Windows Logon Protection, and you need to apply the same settings to all such clients. The syntax for importing and exporting settings is described in section 17.2 (page 99).

17.1 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, IIS Website Protection and Windows Logon 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 unknown end-user IP.
Network connection	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. 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.

End-user IP source option

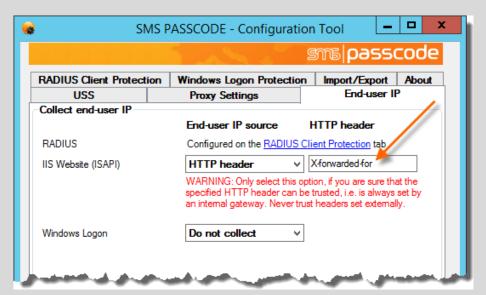
Explanation

HTTP Header

This option is only available for services hosted by a Microsoft Internet Information Server (IIS), meaning:

- SMS PASSCODE Citrix Web Interface Protection
- SMS PASSCODE IIS Website Protection
- SMS PASSCODE AD FS Protection

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 **X-forwarded-for**¹³ is suggested, but you can enter any other name into the textbox, that appears:



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. Examples of such reverse proxies are Citrix Secure Gateway/Citrix Access Gateway Standard¹⁴, Bluecoat and NetScaler.

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.

WARNING!

Take great care, when using this option. Only use this option, when you have ensured that the specified HTTP header is **always** 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.

¹³ In case of AD FS, X-MS-Forwarded-Client-IP is suggested, since this is the default HTTP header used by the Microsoft Web Application Proxy.

¹⁴ HTTP header **X-forwarded-For** is hard-coded and enabled by default

17.2 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:"filename"	This argument instructs the configuration tool to export all current settings to the file with the name filename . Please remember to use quotes if the filename contains spaces.
-import:"filename"	This argument instructs the configuration tool to import settings from the file with the name filename . 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 <u>without actually saving</u> 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
```

18 TROUBLESHOOTING

This section describes some common errors and the corresponding solutions:

- Component communication problems: Section 18.1 (below)
- RD Web Protection does not work: Section 18.2 (page 101)

18.1 Component Communication Problems

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

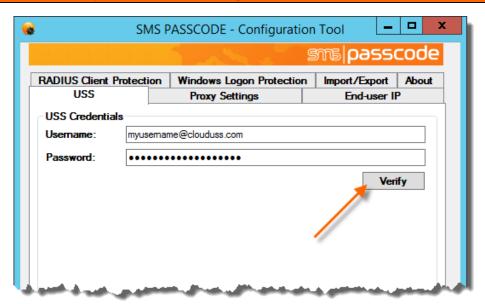
- The USS credentials entered on the USS tab in the SMS PASSCODE Configuration Tool are invalid. Maybe the password is incorrect, or the user account has been deleted?
- Communication to the cloud service is blocked by a firewall.
- Communication needs to go through a local web proxy, but this has not 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 CensorNet USS cloud service:

Diagnosing component communication

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



18.2 RD Web Protection

If signing of RDP files is enabled on your RD Web Access server, you might experience issues with your SMS PASSCODE protected RD Web site. The symptoms are:

 Windows Server 2012 R2: Starting RemoteApps from the RD Web site fails with the error message...

"This RDP File is corrupted. The remote connection cannot be started."

 Windows Server 2016: When starting RemoteApps, users need to re-authenticate on the RD Session Host (single sign-on not working).

If above applies to your installation, you need to re-configure your RD session collection. This is accomplished by executing the following PowerShell commands on the RD Web Access server:

Import-Module RemoteDesktop

 $\label{lem:configuration} \textbf{Get-RDS} ession \textbf{Collection} - \textbf{CustomRdpProperty "gatewaycredentials} source: i: 5"$

Hereafter, users should be able to start RemoteApps from the RD Web Access site.

If you later on need to revert the re-configuration of the RD session collection, this is accomplished by executing the following PowerShell commands on the RD Web Access server:

Import-Module RemoteDesktop

 $Get-RDS ession Collection \mid Set-RDS ession Collection Configuration - Custom Rdp Property \verb|"`n"|$

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 CensorNet A/S prior to disclosing information from this document.