

SMS PASSCODE 2020 SP1

ADMINISTRATOR'S GUIDE

REV. 1.1 DECEMBER 2019



TABLE OF CONTENTS

Table of Contents.....	2
1 Introduction.....	9
2 Notation	9
3 Introducing IntelliTrust™	11
4 New Features in Version 2020 SP1	12
4.1 Support for IntelliTrust™ Cloud Service	12
4.2 SMS PASSCODE IIS Website Protection Improvements	12
5 New Features in Version 2020	13
5.1 Support for IntelliTrust™ Cloud Service	13
5.2 Flexible Support for Cloud and On-premise Infrastructures.....	13
5.3 Risk-based Authentication and Push Authentication	14
5.4 Frictionless Hybrid Setup	15
5.5 Support for Windows Server 2019	15
5.6 Improved Web Administration Interface	15
5.7 Deprecated Features	15
6 End-of-life	16
7 Feature Overview.....	17
7.1 Authentication Clients	17
7.2 Security.....	18
7.3 Password Reset Module	19
7.4 Deployment	20
7.5 Administration.....	21
7.6 Enterprise Environment Support	22
7.7 Pluggable Transmission Infrastructure.....	23
8 Components	24
9 Licensing	27
9.1 Authentication Behavior: Authentication Clients	29
9.2 Authentication Behavior: Password Reset	30
9.3 Hardware – Modems.....	30
10 System Requirements.....	31
10.1 Requirements for Location and Behavior Aware Authentication	35
10.2 Remote Desktop Service Protection	36
10.3 Installing the Self-service Website on a Non-DB Server.....	39
11 Infrastructure.....	43
11.1 Component Communication.....	44
11.2 Cloud Setup.....	46

11.3	On-premise Single Server Installation.....	47
11.4	RADIUS Clients	48
11.5	Enterprise Setup	50
11.6	Total Distribution.....	52
12	Pre-Installation Actions	53
12.1	Check SIM Cards.....	53
12.2	Check System Requirements.....	54
12.2.1	Installation of NPS.....	55
12.2.2	Protection of RD Web Access using IIS Website Protection	55
12.2.3	Protection of RD Session Hosts using Windows Logon Protection	62
12.2.4	Protection of VDI Infrastructures.....	64
13	Upgrade.....	65
13.1	Upgrade Considerations	65
13.1.1	Email and Dispatch Plugins Always Allowed for Dispatching	65
13.1.2	Default Dispatch Connector.....	66
13.1.3	New Behavior for Dispatch Policies	66
13.1.4	Secure Device Provisioning.....	66
13.1.5	IIS Website Protection	66
14	First-time Installation.....	67
14.1	Installation of Hardware	67
14.2	Installation of Software.....	67
14.3	Unattended Installation and Uninstallation	93
15	Add/Remove Components	94
16	Post-Installation Actions.....	95
16.1	Overview: Location and Behavior Aware Authentication	96
16.2	Overview: IntelliTrust™ Integration	99
17	Web Administration Interface	100
17.1	Starting the Web Administration Interface	101
17.2	Overview of Policy Types.....	104
17.2.1	Static Relationship between Policy Types	105
17.2.2	Runtime Relationship between Policy Types	107
17.3	General Settings	108
17.3.1	Miscellaneous Settings.....	109
17.3.2	Authentication Settings.....	110
17.3.3	Authentication Monitoring	114
17.3.4	IntelliTrust Settings.....	119
17.4	License Information	122

17.4.1	Applying a License Key	123
17.4.2	License Limits.....	124
17.4.3	License Management	125
17.5	User Integration Policies	126
17.5.1	Enable User Store Integration	128
17.5.2	Simple Setup (AD).....	128
17.5.3	Advanced Setup	129
17.5.4	Settings of a User Integration Policy	131
17.6	User Group Policies	156
17.6.1	Settings of a User Group Policy.....	159
17.7	Passcode Policies.....	184
17.7.1	Settings of a Passcode Policy	186
17.8	Authentication Policies.....	193
17.8.1	Authentication Rule Sequence	195
17.8.2	Settings of an Authentication Policy.....	196
17.8.3	Authentication Policy Examples.....	217
17.9	Token Policies	221
17.9.1	Creating a new Token Policy	223
17.9.2	Settings of a Token Policy in Manual Entry Mode	225
17.9.3	Settings of a Token Policy in Token Seed File Import Mode	229
17.10	Users.....	234
17.10.1	Settings of a User	236
17.10.2	User IP History	247
17.10.3	User Login History	249
17.10.4	Adding and Deleting Users via User Store Integration	250
17.10.5	User Data Filtering.....	251
17.10.6	IntelliTrust User Sync Status	252
17.11	Importing Users	253
17.11.1	Importing and Synchronizing Users from other Data Sources.....	253
17.12	Transmitter Hosts	255
17.12.1	Maintaining Authorized Transmitter Hosts	255
17.12.2	Assigning Dispatchers to a Transmitter	257
17.13	Authentication Backend Service Hosts	258
17.13.1	Maintaining Authorized Authentication Backend Service Hosts	259
17.14	Modems	261
17.14.1	Settings of a Modem.....	262
17.14.2	Removing Modems.....	262

17.15	Email Connectors	263
17.15.1	Settings of an Email Connector	264
17.16	Dispatch Connectors	265
17.16.1	Settings of a Dispatch Connector	267
17.16.2	The Default Dispatch Connector.....	268
17.17	Modem Groups	269
17.17.1	Maintaining a Modem Group	270
17.18	Dispatch Policies	271
17.18.1	Dispatch Policy Rule Sequence.....	272
17.18.2	Settings of a Dispatch Policy	273
17.18.3	Dispatch Policy Examples	286
17.19	Authentication Monitoring	296
17.19.1	Column Filtering	299
17.19.2	Row Filtering	302
17.19.3	Exporting Data.....	303
17.19.4	Switching Data Source	304
17.19.5	Geo-mapping.....	305
17.20	Modem Monitoring.....	307
18	PowerShell Support	308
18.1	Cmdlet Overview	309
18.2	Permissions	311
18.3	Getting Started.....	312
18.4	Examples.....	312
19	Database Audit	313
20	Role-based Administrator Permissions	315
20.1	Defining Role-based Permissions	315
20.2	Role-based Permissions in the Web Administration Interface	317
21	Pluggable Transmission Infrastructure	318
21.1	SMS PASSCODE Cloud Service	320
21.1.1	Provisioning the SMS PASSCODE Mobile App	321
21.1.2	System Requirements for the SMS PASSCODE Mobile App	324
22	Self-service Website	325
22.1	Examples of Usage.....	326
22.2	Self-service Notifications.....	326
22.3	Data Updates.....	327
22.4	Security Concerns	327
22.5	Authentication.....	328

22.5.1	Configuring Authentication Delegation.....	330
22.6	Localization.....	334
23	Password Reset Module	335
23.1	Licensing	336
23.2	Best-Practice Setup of Password Reset.....	337
23.3	Workflow for Performing a Password Reset.....	337
23.3.1	Strict Flow	338
23.3.2	Other Login Flows	343
23.4	Password Reset Infrastructure.....	345
23.5	Security Concerns	348
23.5.1	Publishing the Password Reset Website	348
23.5.2	Protecting the Password Reset Website with SSL/TLS	348
23.5.3	Encryption of the Network Communication with the AD Controller.....	348
23.5.4	Protecting the Password Reset Module against Attacks	348
23.6	Configuring the Password Reset Website.....	349
23.6.1	Configure Communication with the Password Reset Backend Service.....	349
23.6.2	Protect the Password Reset Website using SSL/TLS	350
23.7	Configuring the Password Reset Backend Service	350
23.7.1	Setting Up a Dedicated User Account for Password Reset.....	351
23.7.2	Configure Settings of the Password Reset Backend Service	357
23.8	Password Reset Event Log.....	362
23.9	Localization.....	363
24	Secure Device Provisioning	363
24.1	Background	363
24.2	Deploying Secure Device Provisioning	364
24.2.1	Configuring Microsoft Exchange Server.....	368
24.3	Event Logging.....	374
24.4	Localization.....	375
25	Configuring Authentication Clients	376
25.1	Configuring Citrix Web Interface Protection	376
25.2	Configuring RADIUS Protection	377
25.2.1	Configuring RADIUS Protection on a Windows Server	377
25.2.2	Advanced Configuration of the RADIUS Protection Component	380
25.3	Configuring AD FS Protection	400
25.3.1	Background	400
25.3.2	AD FS Infrastructure.....	400
25.3.3	Configuring the MFA Adapter for AD FS 2012 R2	402

25.3.4	Configuring the MFA Adapter for AD FS 2016/2019	404
25.3.5	Uninstalling the MFA Adapter	406
25.4	Configuring IIS Website Protection	407
25.4.1	Native HTTP Module	407
25.4.2	IIS Website Protection Configuration File	407
25.4.3	The IISAdministration PowerShell Module	408
25.4.4	IIS Website Protection Configuration File Syntax.....	412
25.5	Configuring Windows Logon Protection	415
25.5.1	Windows Logon User Exclusion Groups	415
25.5.2	Remote Desktop Logon Timeout	415
25.5.3	RDP Listener Exclusion	416
25.5.4	Credential Provider Filtering	419
25.5.5	Users' Cached Credentials	420
26	Configuration Tool.....	420
26.1	DB Encryption.....	423
26.2	Collecting End-User IP Addresses	424
26.3	Command Line Arguments	428
27	Backup and Recovery	430
27.1	Backup of Database Files	430
27.2	Backup of Configuration Tool Settings	431
27.3	Backup of Authentication Monitoring Archive	431
27.4	Backup of Self-service Notification Templates	431
28	Troubleshooting	432
28.1	SMS Transmission Problems	433
28.2	Error Message "Unknown user" during Authentication	435
28.3	User Store Integration does not Work as Expected.....	436
28.4	Component Communication Problems.....	437
28.5	Self-service Website	439
28.6	Password Reset Website	440
28.6.1	Fatal Error when Accessing the Password Reset Website.....	440
28.6.2	Access Denied when Accessing the Password Reset Website.....	440
28.7	Secure Device Provisioning	440
28.7.1	Fatal Error when Accessing the Secure Device Provisioning Website	440
28.7.2	No Quarantine Emails Received.....	440
28.8	Token Authentication	440
28.9	RD Web Protection	441

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

1 INTRODUCTION

This document describes how to install, configure, and administer SMS PASSCODE version 2020 Service Pack 1 (SP 1).

2 NOTATION

Term	Description
ActiveSync	Technology developed by Microsoft, used for synchronizing personal Outlook data to handheld devices.
ABS	SMS PASSCODE Authentication Backend Service
AD	Active Directory
AD FS	Active Directory Federation Services
CAS	Client Access Server role of a Microsoft Exchange Server installation
Cloud Setup	A special type of SMS PASSCODE installation, containing only SMS PASSCODE Authentication Clients, which communicate directly with the IntelliTrust™ cloud service. No SMS PASSCODE backend services are used in this type of setup.
DBS	SMS PASSCODE Database Service
DP	Dispatch Policy
Hybrid Setup	A special type of SMS PASSCODE installation, where the SMS PASSCODE backend is configured to communicate with the IntelliTrust™ cloud service.
IIS	Internet Information Server: Optional component/role on a Windows Server.
IntelliTrust™	A multi-factor authentication cloud service offered by Entrust Datacard. For more documentation on IntelliTrust, please refer to: entrust.us.trustedauth.com/documentation/help/admin/index.htm
Machine	This is a general term used to denote a server or a workstation
memoPasscodes™	memoPasscodes™ refers to an SMS PASSCODE innovation making codes easier to read and memorize during authentication
NPS	Network Policy Server: Optional Role on a Windows Server. This Role is the Microsoft implementation of a RADIUS server.
On-premises Setup	A traditional SMS PASSCODE installation, with all components installed on-premises. No usage of the IntelliTrust™ cloud service in this case.
OTP	One-time passcode
OWA	Microsoft Outlook Web Access

Term	Description
RD	Remote Desktop
RDS	Microsoft Remote Desktop Services
PRBS	SMS PASSCODE Password Reset Backend Service
PRWS	SMS PASSCODE Password Reset Website
SMS PASSCODE authentication client	One of the SMS PASSCODE components Citrix Web Interface Protection, RADIUS Protection, AD FS Protection, IIS Website Protection, Windows Logon Protection or Secure Device Provisioning , i.e. one of the components responsible for authentication for a specific type of client.
SMS PASSCODE core component	One of the SMS PASSCODE components Database Service, Web Administration Interface, Self-service Website, Transmitter Service, Authentication Backend Service or PowerShell Support .
SDP	SMS PASSCODE Secure Device Provisioning
SSWS	SMS PASSCODE Self-service Website
TMG	Threat Management Gateway. A Microsoft security gateway server (the successor of the Microsoft ISA Server)
TS	SMS PASSCODE Transmitter Service
UGP	User Group Policy
UIP	User Integration Policy
WAI	SMS PASSCODE Web Administration Interface

3 INTRODUCING INTELLITRUST™

When Entrust Datacard (EDC) acquired SMS PASSCODE back in 2018, one of the main goals was to integrate the best of EDC's existing authentication offerings with the SMS PASSCODE product, to get the best of both worlds. We are proud to release SMS PASSCODE 2020 as the first version that provides such an integration, and thereby allows all SMS PASSCODE customers to optionally leverage the features of EDC's **IntelliTrust™ cloud service**.

IntelliTrust™ is a cloud service offered by EDC, which allows to perform multi-factor authentication using the following features:

- Utilizes a **risk-based authentication engine** that takes contextual information into account during each authentication attempt, and dynamically adapts the login experience according to customizable risk criteria.
- End-users that have installed the *Entrust IdentityGuard Mobile* or *Entrust IdentityGuard Mobile Smart Credential* app on their smartphone can validate their identity during authentication attempts, either using a soft token OTP, or using **Push Authentication**. Push authentication allows end-users to approve their identity, simply by the click of a button within the app.
- **Machine authentication** allows IntelliTrust™ to remember machines that have successfully been used for authentication in the past, and thereby reduce the risk during re-occurring authentication attempts from the same machine. For example, this can be used to only request multi-factor authentication from a machine once a day, and allow simple authentication attempts with username and password only, during the remaining authentication attempts on the same day from the same machine.

SMS PASSCODE 2020 is the first SMS PASSCODE version to integrate with the IntelliTrust™ cloud service. In this version, SMS PASSCODE RADIUS Protection and SMS PASSCODE AD FS Protection have been integrated with the IntelliTrust™ cloud service.

SMS PASSCODE 2020 SP1 release brings a broader support for IntelliTrust™ cloud service among supported authentication clients. In this version, in addition to existing integrations, SMS PASSCODE IIS Website Protection and SMS PASSCODE Windows Logon Protection have been integrated with the IntelliTrust™ cloud service.

Upcoming versions of SMS PASSCODE will integrate even deeper with IntelliTrust™, and thereby provide more IntelliTrust™ authentication features.

The new SMS PASSCODE / IntelliTrust™ integration is optional. If you see value in the options provided by IntelliTrust™, you simply enable the IntelliTrust™ integration within SMS PASSCODE, after installation. We have put great effort to make the integration as simple as possible; among others, all SMS PASSCODE users will automatically be synchronized to the IntelliTrust™ cloud service. On the other hand, if you're happy with the authentication mechanisms provided by SMS PASSCODE in earlier versions, you can just leave the IntelliTrust™ integration disabled (default setting), and continue to use SMS PASSCODE in the same way as previously.

4 NEW FEATURES IN VERSION 2020 SP1

4.1 Support for IntelliTrust™ Cloud Service

Entrust Datacard offers a modern, versatile multi-factor authentication cloud service, called **IntelliTrust™**. SMS PASSCODE 2020 SP1 is the next version of SMS PASSCODE that optionally allows to integrate with IntelliTrust™. Such integration allows SMS PASSCODE to offer many new features via the IntelliTrust™ cloud service, as described in the sections below.

This service pack release brings IntelliTrust™ integration support for the following authentication clients:

- SMS PASSCODE IIS Website Protection
- SMS PASSCODE Windows Logon Protection
- SMS PASSCODE AD FS Protection (Already supported by SMS PASSCODE 2020)
- SMS PASSCODE RADIUS Protection (Already supported by SMS PASSCODE 2020)

IMPORTANT: The IntelliTrust™ integration with **SMS PASSCODE Windows Logon protection** is only supported for the operation systems newer than Windows 7 / Windows Server 2008 R2

The following IntelliTrust™ authentication mechanisms are supported by SMS PASSCODE IIS Website Protection and Windows Logon Protection:

- OTP authentication using soft- and hardware tokens.
- Push authentication, using either the Entrust IdentityGuard Mobile or Entrust IdentityGuard Mobile Smart Credential app.
- OTP authentication, with OTP messages delivered by SMS¹ or email.
- Temporary access code.

In addition, SMS PASSCODE IIS Website Protection supports:

- Machine authentication

For more information on the IntelliTrust™ cloud service, please read:

- entrust.us.trustedauth.com/documentation/help/admin/index.htm

4.2 SMS PASSCODE IIS Website Protection Improvements

IIS Web Site Protection has been renovated and extended with IntelliTrust integration support. The new IIS Web Site protection does not use Internet Server Application Programming Interface (ISAPI) any more to protect IIS web sites, including Microsoft Outlook Web App (OWA) and Microsoft Remote Desktop Web Access (RdWeb). Instead, modern and native to IIS version 7.x and higher, HTTP Modules are used for the purpose.

In addition, the following features have been added:

- User facing login page has been localized to 17 languages

¹ Restrictions apply to SMS delivery. Please read section 5.2 for details.

- PowerShell Administration Support (Please see section 25.4.3 for details)

5 NEW FEATURES IN VERSION 2020

This section summarizes the most important new features introduced in SMS PASSCODE 2020.

5.1 Support for IntelliTrust™ Cloud Service

Entrust Datacard offers a modern, versatile multi-factor authentication cloud service, called **IntelliTrust™**. SMS PASSCODE 2020 is the first version of SMS PASSCODE that optionally allows to integrate with IntelliTrust™. Such integration allows SMS PASSCODE to offer many new features via the IntelliTrust™ cloud service, as described in the sections below.

IMPORTANT: The IntelliTrust™ integration is currently supported for **SMS PASSCODE RADIUS Protection** and **SMS PASSCODE AD FS Protection**. Other SMS PASSCODE protections do not support IntelliTrust™ features yet, but are expected to do so in upcoming SMS PASSCODE releases.

The following IntelliTrust™ authentication mechanisms are supported by SMS PASSCODE RADIUS Protection and SMS PASSCODE AD FS Protection:

- OTP authentication using soft- and hardware tokens.
- Push authentication, using either the *Entrust IdentityGuard Mobile* or *Entrust IdentityGuard Mobile Smart Credential* app.
- OTP authentication, with OTP messages delivered by SMS² or email.
- Temporary access code.

In addition, SMS PASSCODE AD FS Protection supports:

- Machine authentication

For more information on the IntelliTrust™ cloud service, please read:

- entrust.us.trustedauth.com/documentation/help/admin/index.htm

5.2 Flexible Support for Cloud and On-premise Infrastructures

In today's IT departments, we are seeing a big move towards cloud setups, but at the same time we are also seeing companies that prefer to stay with their on-premise installations. At Entrust Datacard, we provide you the flexibility to decide, how much of your multi-factor authentication infrastructure you want to move to the cloud, and how much to keep on-premise. We support a broad range of possible setups:

- **Cloud Setup:** Installation with a very small on-premise footprint. In this case, you only install SMS PASSCODE 2020 authentication clients on-premise, to protect your on-premise systems. You then configure the clients to communicate directly with the IntelliTrust™ cloud service. There is no need for any on-premise installation of SMS PASSCODE 2020 core components in this case.

² Restrictions apply to SMS delivery. Please read section 4.2 for details.

- **Hybrid Setup:** Full SMS PASSCODE 2020 on-premise installation. In this case, you perform a traditional on-premise installation of SMS PASSCODE, including authentication clients and core components. You then configure the backend to communicate with the IntelliTrust™ cloud service to extend the backend with advanced cloud service features. This gives you the best of both worlds.
- **On-premise Setup:** Traditional SMS PASSCODE installation. In this case, you perform a traditional on-premise installation of SMS PASSCODE, including authentication clients and core components. But no configuration of access to cloud services is performed in this case. This allows to have “everything behind the firewall”, including local modems for message transmissions.

Important information regarding IntelliTrust™ licensing:

IMPORTANT: IntelliTrust™ licensing

In case of a **Hybrid Setup**, the usage of the IntelliTrust™ cloud service is included in your SMS PASSCODE license. It means that you can create and connect to an IntelliTrust™ tenant free of charge, as long as you have a perpetual SMS PASSCODE license with valid Software Assurance, or if you have a valid SMS PASSCODE subscription license.

In case of a **Cloud Setup**, you do not need an SMS PASSCODE license. In this case you are allowed to use the SMS PASSCODE Authentication Clients free of charge, as long as they are part of a **Cloud Setup** that connects to an IntelliTrust™ tenant, for which you must have a valid license.

In case of a **Hybrid Setup**, the IntelliTrust™ option of delivering OTP messages by SMS is only supported for SMS PASSCODE licensees on an SMS PASSCODE subscription agreement (and trial licenses). If you're not on a subscription license, but would like to take advantage of a flat price model for SMS delivery, please contact your SMS PASSCODE reseller to hear about the options of converting your existing license to a subscription agreement.

The **Cloud Setup** and **Hybrid Setup** options are new to SMS PASSCODE 2020, and provide access to advanced IntelliTrust™ authentication features (described below).

5.3 Risk-based Authentication and Push Authentication

When utilizing the new **Cloud Setup** or **Hybrid Setup**, SMS PASSCODE 2020 integrates with the IntelliTrust™ cloud service and is thereby extended with many new features, among others:

- **A risk-based authentication engine**, allowing you to configure different authentication behavior depending on contextual risk-based factors during each authentication attempt. Among others, **machine authentication** allows recognition of machines previously used for successful authentication.
- **Push authentication** using any of the existing, renowned mobile apps from Entrust Datacard: *Entrust IdentityGuard Mobile* or *Entrust IdentityGuard Mobile Smart Credential*. Push Authentication allows your end-users to approve authentications from such apps, simply by tapping an “approve button”, without entering any one-time passcode.

5.4 Frictionless Hybrid Setup

In case you decide to go for the new **Hybrid Setup**, a lot has been done to minimize the hassle to extend the on-premise experience to the cloud. This includes:

- Automatic creation of a cloud tenant in IntelliTrust™.
- Automatic synchronization of on-premise user data to IntelliTrust™.

For more details on configuring a Hybrid Setup, see section 17.3.4, page 119.

5.5 Support for Windows Server 2019

SMS PASSCODE 2020 has full support for Windows Server 2019.

5.6 Improved Web Administration Interface

Two pages of the SMS PASSCODE Web Administration Interface have been improved with a new *Quick Filter*, for easy, more flexible data filtering:

- The user overview page (section 17.10.5, page 251).
- The authentication monitor page (section 17.19.2, page 302).

5.7 Deprecated Features

The following, previous SMS PASSCODE features, are no longer supported in SMS PASSCODE 2020 SP1:

- SMS PASSCODE IIS Website Protection for Exchange 2007

The following, previous SMS PASSCODE features, are no longer supported in SMS PASSCODE 2020:

- SMS PASSCODE TMG Website Protection
- SMS PASSCODE AD FS Protection for AD FS 2.0.
Important: AD FS protection is still supported for AD FS 2012 R2, AD FS 2016 and AD FS 2019. Only AD FS versions prior to AD FS 2012 R2 are no longer supported.

6 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 8.0 and older	Already end of life
SMS PASSCODE 8.0 SP1	January 1, 2020
SMS PASSCODE 9.0	October 1, 2020
SMS PASSCODE 9.0 SP1	February 1, 2021
SMS PASSCODE 9.0 SP2	September 1, 2021
SMS PASSCODE 2018	September 1, 2022
SMS PASSCODE 2020	October 1, 2023
SMS PASSCODE 2020 SP1	December 1, 2023

7 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.

7.1 Authentication Clients

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

- ✓ **Citrix Web Interface**
- ✓ **RADIUS clients**
Supported are:
 - Check Point
 - Cisco
 - Citrix Application Delivery Controller (ADC)
(Formerly NetScaler ADC)
 - F5
 - Juniper
 - Palo Alto
 - Any other RADIUS client supporting PAP with challenge/response
 - Any other RADIUS client supporting MS-CHAP v2³
 - Any other RADIUS client when IntelliTrust™ mobile push application is used
- ✓ **Applications protected by AD FS**
Supports multi-factor authentication in any of the scenarios supported by the AD FS 2012 R2, AD FS 2016 and AD FS 2019 infrastructures, 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.
- ✓ **Internet Information Server (IIS) Websites**
Supports protection of the following types of IIS websites:
 - Outlook Web Access 2010 / 2013 / 2016 / 2019
 - Remote Desktop Web Access (Windows Server 2008 R2 / 2012 R2 / 2016 / 2019)
 - IIS Websites using Basic, Integrated Windows Authentication and ASP.Net Form Based Authentication
- ✓ **Windows Logon**
Protection of:
 - Remote Desktops (RDP Connections)

³ For best user experience, the RADIUS client must support to show the challenge message returned by the SMS PASSCODE protected RADIUS server.

- VDI machines
 - Windows servers
 - Windows workstations
- ✓ **Secure Device Provisioning** (for ActiveSync Devices)
Protection for secure provisioning of ActiveSync devices accessing the following versions of Exchange server:
- Exchange Server 2010
 - Exchange Server 2013
 - Exchange Server 2016
 - Exchange Server 2019
 - Exchange Online

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

7.2 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 token-based solutions!)
 - Randomly created in **real-time** without the usage of any pre-deterministic algorithm (opposite to token-based solutions as well as many competing message-based solutions)
 - Challenge-based
 - Time-constrained
- ✓ **Patented location and behavior aware authentication** for even stronger security, making it possible to prohibit access or alert users in case of advanced attacks like some cases of man-in-the-middle attacks
- ✓ **Cryptographically strong random passcodes** are generated using FIPS-140 validated crypto modules
- ✓ **Configurable passcode length, complexity, and lifetime**
- ✓ **Strong encryption**
 - Built-in 256-bit AES encryption of all network communication
 - Optional 256-bit AES encryption of the database files
- ✓ **Brute-force attack protection**
 - Automatic lockout of users on consecutive incorrect password entries
 - Automatic lockout of users on consecutive incorrect passcode entries
- ✓ **Denial-of-service attack protection**

✓ **Lockout Notification**

- Optional feature, immediately notifying a user in the event of a user lockout, thereby giving the user the chance to take immediate counteractions, in case the event is unexpected.

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
- ✓ Users are alerted by irregularities in the contextual message information, in case *location and behavior aware authentication* has been enabled

7.3 Password Reset Module

Many IT helpdesks struggle with the burden of helping end users with password related issues. There are several reasons, why this happens. Some examples are:

- End users are requested to change their password frequently. It sometimes happens during this process that users forget the new password, they chose.
- When end users forget their password, they often try to guess it, attempting logins with different password entries. This usually results in user accounts becoming locked out.
- When end users are requested to change their password before it expires, they do not always perceive prior warnings about this, potentially resulting in blocked access to IT systems.

In many cases, users will not be able to get access to relevant IT systems and continue work, before the IT helpdesk has been able to resolve the problem.

The SMS PASSCODE Password Reset Module was introduced to lessen the burden on IT helpdesks related to password issues, while at the same time making it quicker and simpler for end users to reset their password, when needed. As a result, users can regain access to required IT systems and continue work immediately.

Important characteristics of the SMS PASSCODE Password Reset module are:

- ✓ Convenient:
The SMS PASSCODE Password Reset Module provides a website, where users can reset their own Active Directory password. It is very intuitive to use. Several authentication flows are supported to let users reset their password, for example using their user ID and the personal passcode that was entered (during activation) in the SMS PASSCODE Self-service Website, followed by a one-time passcode (OTP).
- ✓ Hassle-free real-time notifications:
An important part of a password reset system is to ensure that a user is aware of the possibility of resetting his / her password, when needed. The SMS PASSCODE Password Reset Module ensures this in a hassle-free way, without the need to install additional software on PCs or smartphones, by smart usage of automated real-time **notifications**.

Several types of notifications exist in SMS PASSCODE, each of which can be enabled or disabled as required. The idea is that a user will automatically receive a notification that reminds him about the possibility to reset his password, whenever it seems relevant. The following types of notifications are available:

- ✓ SMS PASSCODE logout notification
 - Notifies a user, whenever he is locked out from the SMS PASSCODE system, e.g. due to several log in attempts with a wrong password
- ✓ AD logout notification
 - Notifies a user, whenever he is locked out from AD
- ✓ Password pre-expiration notification
 - Notifies a user, whenever his AD password will expire soon (e.g. within the next 3 days)
- ✓ Password expiration notification
 - Notifies a user, whenever his AD password has just expired

The content of each notification type is customizable. By default, each message contains the URL of the SMS PASSCODE Password Reset Website. This is a user-friendly, effective way to remind the user about the possibility to reset his password by himself; and additionally, to inform where and how to do it.

Note: If a user succeeds resetting his password, the SMS PASSCODE Password Reset module will automatically unlock the user, if he was locked out, whereby the user regains access to all relevant systems.

7.4 Deployment

Installation of SMS PASSCODE is **very simple**, since SMS PASSCODE is an “out-of-the-box” **end-to-end** solution.

The **component architecture** of SMS PASSCODE offers **maximum flexibility** of installation, allowing distribution of SMS PASSCODE components according to your specific needs. Starting from version 2020, you can even decide, how much of your infrastructure you want to reside on-

premise and in the cloud, respectively. You can choose between a **Cloud Setup**, a **Hybrid Setup** and a traditional **On-premise Setup** (cf. section 5.2).

7.5 Administration

The daily administration of SMS PASSCODE is simple due to:

- ✓ **No logistic overhead** regarding administration and distribution of 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.
- ✓ **Smart policy-driven administration** making it easy to maintain settings on a system wide level, user group level or individual user level.
- ✓ **No need to involve IT personnel** when end-users must enter or change personal data like (mobile) phone numbers. The IT personnel can optionally allow end-users to maintain such data themselves using the SMS PASSCODE Self-service Website.
- ✓ **No need to involve IT personnel** when users have forgotten their AD password. The IT personnel can optionally allow end-users to reset their own AD password in a secure manner using the SMS PASSCODE Password Reset Module.
- ✓ **No need to involve IT personnel** when users need to access their email using a new ActiveSync device. The IT personnel can optionally allow end-users to approve new ActiveSync devices themselves, in a secure manner, using the SMS PASSCODE Secure Device Provisioning component.

Additionally, SMS PASSCODE includes an excellent **User Store Integration** feature that allows administration of SMS PASSCODE users in your Active Directory or another type of LDAP directory. The following is a list of User Store Integration features:

- ✓ Works “out-of-the-box”. **No schema extension** of your AD is needed!
- ✓ Supports both **LDAP** and **Global Catalog** lookups.
- ✓ Supports **encrypted secure communication** (for both LDAP and Global Catalog lookups)
- ✓ Supports extraction of users from **multiple separate AD Domains / LDAP directories**
- ✓ Supports **nested groups** including groups from **child domains** and **trusted domains**.
- ✓ Customizable **extraction of several user attributes**, like (mobile) phone numbers, email addresses and token IDs. Even searching through a prioritized list of LDAP attributes is possible.

Finally, as an administrator, you have the flexibility of administering the SMS PASSCODE product using a graphical user interface (section 17, page 100), or using PowerShell script (section 18, page 308).

7.6 Enterprise Environment Support

Failover and scalability are very important in enterprise environments. SMS PASSCODE provides failover and scalability **on all levels thus** providing unmatched support for enterprise environments:

- ✓ Database level:
Each Authentication Backend service **caches all data locally** – meaning independence of backend database and high scalability. I.e. system operation is maintained even in case the backend database is down.
- ✓ Transmitter level:
An **Authentication Backend Service** provides intelligent distribution of all incoming requests to many Transmitter Services, thereby providing full failover and load balancing between all such Transmitter Services. I.e. system operation is maintained even in case a Transmitter Service is down. An unlimited number of Transmitter Services are supported.
- ✓ Modem level:
Each transmitter supports a **modem pool** containing up to 32 modems, thereby providing full failover and load balancing between all modems in a pool. I.e. system operation is maintained even in the event of a modem being down. If SIM cards from different carriers are used, then you can even obtain failover on the telco operator level.
- ✓ Authentication client level:
Each authentication client may forward incoming requests to several Authentication Backend Services. I.e. system operation is maintained even in case some of the Authentication Backend Services are down. An unlimited number of Authentication Backend Services are supported.
- ✓ Authentication type level:
Global diversities of message transmission infrastructures can be a challenge for global enterprises. SMS PASSCODE addresses this issue by providing support for **several message transmission mechanisms and authentication mechanisms**. Users with specific needs can be set to receive one-time-passcode messages by email, voice calls or any other transmission mechanism provided by a dispatch plugin module; or be allowed to authenticate using hardware tokens, software tokens or time-constrained personal passcodes.

Additionally, using **Dispatch Policies** it is possible to control the load balancing of passcode messages and notifications across all modems and other transmission mechanisms at a granular level. Since Dispatch Policies are very flexible, the number of possibilities is enormous. Some examples of the usage are:

- **Prefix load balancing:** Group modems according to the country where they are located. Preferable send SMS messages from modems having the same phone number prefix as the receiver. Additionally, users with specific mobile number prefixes can be set to receive passcodes by alternative dispatching mechanisms, i.e. by email, voice call or external

message transmission providers.

- **Telco operator failover:** Group modems according to their operator. Preferable send SMS messages using a selected operator but use another one for failover (e.g. automatically send another passcode using a second operator if the first passcode could not be sent or was not entered within a specified time limit).
- **Receiver failover:** Allocate both a primary and a secondary phone number to some users. Automatically send another passcode to the secondary phone if the first passcode could not be sent or was not entered within a specified time limit.
- **Adaptive dispatching:** Dynamically switch Dispatch Policy depending on a user's specific authentication context, for example depending on the country a user is logging in from, or the type of client the user is trying to access. For example, this allows automatic switching between modems and dispatch plugin modules, depending on the actual authentication context.

Dispatch Policies are very **flexible**. The flexibility spans from having a single dispatch policy to be used in all cases, to having different Dispatch Policies for any combination of user group, message type and authentication context.

This clearly demonstrates that SMS PASSCODE has been designed and built with even the most demanding enterprise environments in mind.

7.7 Pluggable Transmission Infrastructure

The SMS PASSCODE system provides an advanced transmission infrastructure for sending different types of messages to users. For example, **passcode messages** containing one-time passcodes, or **notifications**, informing users about important events, such as user lockouts or password expirations. For sending such messages, the SMS PASSCODE transmission infrastructure supports many transmission mechanisms. Transmission can occur by SMS, using modems that are directly connected to the SMS PASSCODE Transmitter services, or by email, using SMTP servers.

Additionally, the SMS PASSCODE transmission infrastructure optionally allows transmission using **dispatch plugin modules**, thereby extending the system to transmit messages using any dispatch mechanism that is accessible using a server-based API. For example, transmitting messages using 3rd party web services, or using a direct connection to a short message service center (SMSC). Out-of-the-box, SMS PASSCODE comes with a lot of plugin modules pre-installed, which allows you easily to connect to a long list of external message providers.


One of the pre-installed plugin modules of special interest is the **SMS PASSCODE Cloud Service** plugin. This plugin allows you to send messages as push notifications to end users' smart phones, free of charge, using the SMS PASSCODE Mobile app (see section 21.1, page 320). If you are on a subscription license, the SMS PASSCODE Cloud Service plugin additionally allows you to send messages via SMS or voice calls using a flat-rate cost model, via the SMS PASSCODE Cloud Service.

Finally, the pluggable infrastructure allows you to extend the system with your own transmission mechanisms, should you have very specific message transmission requirements.

Please read section 21 (page 318) for more details.

8 COMPONENTS

SMS PASSCODE is composed of the following software components:

SMS PASSCODE		
Core Components	Authentication Clients	Add-on modules ⁴
<ul style="list-style-type: none"> Database Service Web Administration Interface Transmitter Service Authentication Backend Service Self-service Website PowerShell Support 	<ul style="list-style-type: none"> Citrix Web Interface Protection RADIUS Protection* AD FS Protection* IIS Website Protection* Windows Logon Protection* Secure Device Provisioning (for ActiveSync devices) 	 Password Reset Module

* Supports authentication via the IntelliTrust™ cloud service

Component	Description
Database Service	Database for storing SMS PASSCODE user and configuration data.
Web Administration Interface	Website for maintaining SMS PASSCODE user data and configuration data.
Transmitter Service	Service responsible for the actual dispatching of messages, either using locally attached modems, SMTP servers, or using external message transmission providers (using dispatch plugin modules).
Authentication Backend Service	Service responsible for authentication session management and message handling in general; including passcode generation, passcode verification and load balancing and failover between all Transmitter services, when sending messages.
Self-service Website	Website that allows end-users to maintain some of their personal SMS PASSCODE account settings themselves.
PowerShell Support	A PowerShell module that allows administrators to maintain SMS PASSCODE user data and configuration data using PowerShell cmdlets. Convenient for automation and integration.
Citrix Web Interface Protection	<p>Citrix Web Interface integration, providing SMS PASSCODE multi-factor 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®.</p> <p>Both AD and NDS authentication is supported.</p>

⁴ Please note that separate CALs are required to gain access to add-on modules

Component	Description
RADIUS Protection	<p>Integrates with RADIUS systems providing SMS PASSCODE multi-factor authentication for RADIUS clients. It is optionally possible to run this integration side-by-side with other RADIUS authentication systems, e.g. hardware-token based two-factor authentication systems.</p> <p>This component optionally supports IntelliTrust™ cloud service integration, thereby providing support for IntelliTrust™ authentication mechanisms.</p> <p>RADIUS protection is provided by means of an extension for the Microsoft Network Policy Server (NPS).</p>
AD FS Protection	<p>Integrates with Microsoft Active Directory Federation Services (AD FS), providing SMS PASSCODE multi-factor authentication for applications protected by AD FS 2012 R2, AD FS 2016 and AD FS 2019.</p> <p>This component optionally supports IntelliTrust™ cloud service integration, thereby providing support for IntelliTrust™ authentication mechanisms, incl. machine authentication.</p>
IIS Website Protection	<p>Microsoft Internet Information Server (IIS) integration, providing SMS PASSCODE multi-factor authentication for IIS websites. Currently the following types of websites are supported:</p> <ul style="list-style-type: none"> • Microsoft Outlook Web Access 2010, 2013, 2016 and 2019⁵ • IIS websites using Basic, Integrated Windows Authentication or ASP.Net form Authentication • Microsoft Remote Desktop Web Access (RD Web Access), on Windows Server 2008 R2 / 2012 R2 / 2016 / 2019. <p>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.</p> <p>IIS Website protection is provided by means of a native HTTP module.</p>
Windows Logon Protection	<p>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.</p> <p>SMS PASSCODE authentication can be enabled or disabled for each specific RDP Listener.</p> <p>Windows Logon integration is provided by means of a Credential Provider.</p>

⁵ Please note that when protecting an OWA 2013, 2016 or 2019 site, only form-based authentication is supported

Component	Description
Secure Device Provisioning (for ActiveSync devices)	<p>Integrates SMS PASSCODE with Microsoft Exchange Server's built-in functionality for provisioning of ActiveSync Devices, thereby providing secure, multi-factor authentication based approval of such devices.</p> <p>See system requirements (section 10) for an overview about which versions of Exchange Server are supported.</p> <p>The integration is provided by means of two components:</p> <ul style="list-style-type: none"> • The SMS PASSCODE Secure Device Provisioning website, to which users will be redirected for performing secure approval of ActiveSync devices. • The SMS PASSCODE Secure Device Provisioning backend service, which connects to the Exchange Server to look up and change status of ActiveSync devices.
Password Reset Module <ul style="list-style-type: none"> • Password Reset Website • Password Reset Backend Service 	<p>Add-on module providing a website where SMS PASSCODE users that have forgotten their AD password can reset their password in a secure way.</p> <p>The module consists of two components, which can be installed on separate servers: The SMS PASSCODE Password Reset Website and the SMS PASSCODE Password Reset Backend Service.</p> <p>The Password Reset Website provides the user interface of the Password Reset module. It acts as a proxy for the actual Password Reset logic, which is performed by the Password Reset Backend Service.</p>

The term ***SMS PASSCODE core component*** is used in the subsequent sections of this documentation to denote one of the components: **Database Service (DBS)**, **Web Administration Interface (WAI)**, **Transmitter Service (TS)**, **Authentication Backend Service (ABS)**, **Self-service Website (SSWS)** or **PowerShell Support**.

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**, **Windows Logon Protection** or **Secure Device Provisioning**

Please note the following regarding the different installation options:

- **Cloud Setup:** Currently, the **RADIUS Protection**, **AD FS Protection**, **IIS Website Protection** and **Windows Logon Protection** components are supported in a **Cloud Setup**.
- **Hybrid Setup:** All **SMS PASSCODE core components** are required during this type of setup, except the optional Self-service Website. Additionally, you may install any number of **SMS PASSCODE Authentication Clients**. Please note, that currently the **RADIUS Protection**, **AD FS Protection**, **IIS Website Protection** and **Windows Logon Protection** components support authentication using the IntelliTrust™ cloud service. Remaining SMS PASSCODE Authentication clients will still work in a Hybrid Setup, using traditional SMS PASSCODE authentication.
- **On-premise Setup:** All **SMS PASSCODE core components** are required during this type of setup, except the optional Self-service Website. Additionally, you may install any number of **SMS PASSCODE Authentication Clients**. All such authentication clients are supported in this setup.

9 LICENSING

NOTE: Licensing, as described in this section (and sub sections), only applies to SMS PASSCODE installations in the **On-premise** or **Hybrid Setup**. For a **Cloud Setup**, no SMS PASSCODE backend is present and IntelliTrust™ licensing applies. Please read the SMS PASSCODE End-user License Agreement (EULA) for IntelliTrust™ licensing restrictions that apply depending on the type of SMS PASSCODE license agreement that you have.

This section describes how SMS PASSCODE licensing relates to the SMS PASSCODE components described in the previous section.

When acquiring SMS PASSCODE software, you must take different kinds of licenses into account:

- **Client Access Licenses (CALs)**
Each CAL provides a single end-user the right to access specific types of clients.
- **Dispatch Licenses**
Each dispatch license allows one of the followings:
 - Attach a single hardware modem to the SMS PASSCODE infrastructure.
 - Create a single **Email Connector** in the SMS PASSCODE database to send messages via a specific SMTP server.
 - Create a single **Dispatch Connector** in the SMS PASSCODE database to send messages via a specific **Dispatch Plugin Module**, for example sending messages by SMS or voice call using a 3rd party web service.

Default Dispatch Connector

The SMS PASSCODE system will automatically create a *Default Dispatch Connector*, which is free of charge, meaning it will not occupy a Dispatch License. This Default Dispatch Connector is used to connect to the SMS PASSCODE Cloud Service, which is used for sending messages to the SMS PASSCODE Mobile app and is used by customers on a subscription license to send SMS/Voice call messages.

Please note that you may install every SMS PASSCODE component as many times as you like within your infrastructure, without acquiring extra licenses for this; the one exception being the SMS PASSCODE Database component, which is only allowed to be installed once⁶.

The following types of CALs exist:

- **MFA Standard CAL**
Each such CAL provides a single user the right to access any number of systems protected by SMS PASSCODE Authentication Clients within a single SMS PASSCODE installation.
- **Password Reset CAL**
Each such CAL provides a single user the right to access any number of SMS PASSCODE Password Reset Websites within a single SMS PASSCODE installation.

CALs are allocated to users via *User Group Policies* (cf. section 17.6.1.4, page 181). To get an overview about the total number of allocated licenses, go to the **License** page of the Web Administration Interface (cf. section 17.4, page 122).

The table below summarizes the licensing requirements:

Component	Number of installations allowed	License requirements
Database Service	The Database Service is allowed to be installed once within a single SMS PASSCODE infrastructure.	-
Web Administration Interface	No limitation.	-
Transmitter Service	No limitation.	A dispatch license per modem, email connector and dispatch connector ⁷ .
Authentication Backend Service	No limitation.	-
Self-service Website	No limitation.	-
Citrix Web Interface Protection	No limitation.	Each user needs to have an MFA Standard CAL allocated.
RADIUS Protection	No limitation.	Each user needs to have an MFA Standard CAL allocated.
AD FS Protection	No limitation.	Each user needs to have an MFA Standard CAL allocated.

⁶ If you are on an "Open License Agreement", then you can install the Database service multiple times with the same license code, but you will be billed for the CALs allocated within each such installation. However, for billing purposes it is recommended to request separate license codes per installation, as it makes it easier to understand the CAL usage per installation.

⁷ Only one dispatch license is needed per email/dispatch connector, even if the connector is assigned to several Transmitter Services.

Component	Number of installations allowed	License requirements
IIS Website Protection	No limitation.	Each user needs to have an MFA Standard CAL allocated.
Windows Logon Protection	No limitation.	Each user needs to have an MFA Standard CAL allocated.
Secure Device Provisioning (for ActiveSync devices)	No limitation.	Each user needs to have an MFA Standard CAL allocated.
Password Reset Website	No limitation.	Each user needs to have a Password Reset CAL allocated.
Password Reset Backend Service	No limitation.	-

NOTE: Under specific circumstances, a user might be allowed to log in to an *SMS PASSCODE Authentication client* without an SMS PASSCODE Standard MFA CAL allocated, when bypassing multi-factor authentication. Please read section 9.1 below for details.

9.1 Authentication Behavior: Authentication Clients

The table below summarizes authentication behavior for SMS PASSCODE protected authentication clients. Please note that the behavior can be affected by the Authentication Policy assigned to the user (cf. section 17.8), and by the fact, whether Proof-of-Concept (PoC) mode has been enabled (cf. section 17.3.1):

User Exists in the SMS PASSCODE Database	MFA Standard CAL allocated to the user	Default behavior (PoC mode disabled)	PoC mode enabled
Yes	Yes	If the user attempts to log in to an SMS PASSCODE protected authentication client, authentication occurs according to the user's Authentication Policy. This typically means that multi-factor authentication occurs, unless explicitly defined otherwise by the Authentication Policy.	No change, i.e. default behavior as described in the column to the left.
Yes	No	If the user attempts to log in to an SMS PASSCODE protected authentication client, access is denied unless the user's Authentication Policy is set to <u>bypass</u> multi-factor authentication.	The user can log in to any SMS PASSCODE protected authentication client, <u>bypassing</u> multi-factor authentication (i.e. the user's Authentication Policy is not applied)
No	-	The user is not allowed to log in to any SMS PASSCODE protected authentication client.	No change, i.e. default behavior as described in the column to the left.

9.2 Authentication Behavior: Password Reset

The table below summarizes authentication behavior for the SMS PASSCODE Password Reset Website. Please note that the behavior can be affected by the Authentication Policy assigned to the user (cf. section 17.8), whereas Proof-of-Concept (PoC) mode (cf. section 17.3.1) has no impact in this case:

User Exists in the SMS PASSCODE Database	Password Reset CAL allocated to the user	Default behavior (PoC mode disabled)	PoC mode enabled
Yes	Yes	If the user attempts to log in to the SMS PASSCODE Password Reset Website, authentication occurs according to the user's Authentication Policy. This typically means that multi-factor authentication occurs, unless explicitly defined otherwise by the Authentication Policy.	No change, i.e. default behavior as described in the column to the left.
Yes	No	The user has no access to the SMS PASSCODE Password Reset Website.	No change, i.e. default behavior as described in the column to the left.
No	-	The user has no access to the SMS PASSCODE Password Reset Website.	No change, i.e. default behavior as described in the column to the left.

9.3 Hardware – Modems

When acquiring an SMS PASSCODE license, you may optionally acquire one or more physical modems as well. The usage of modems is not mandatory, because SMS PASSCODE can be operated with or without modem hardware, according to your preferences. Local modems have the advantage of giving you maximum control of the transmission environment.

Please consult your SMS PASSCODE reseller to get advice regarding supported hardware for message transmission.

You need a Dispatch License for each modem that you attach to your SMS PASSCODE infrastructure.

IMPORTANT: When acquiring GSM modems, you must also acquire a SIM card for each GSM modem yourself. SIM cards protected by a PIN code are supported.

10 SYSTEM REQUIREMENTS

In this section, the system requirements are listed for each SMS PASSCODE software component (cf. section 8).

Please note:

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

Component	Requirement
Database Service	<ul style="list-style-type: none"> Supported operating systems: <ul style="list-style-type: none"> Windows Server 2008 R2 (x64) Windows Server 2012 (x64) Windows Server 2012 R2 (x64) Windows Server 2016 (x64) Windows Server 2019 (x64) <p>If you are planning to import users from Active Directory using the User Store Integration feature, it is recommended to install this component on a domain member server or a domain controller.</p> <p>Note: It is mandatory to install the PowerShell Support component on the same server as the Database Service.</p>
Web Administration Interface	<ul style="list-style-type: none"> Supported operating systems: <ul style="list-style-type: none"> Windows Server 2008 R2 (x64) - SP1 required Windows Server 2012 (x64) Windows Server 2012 R2 (x64) Windows Server 2016 (x64) Windows Server 2019 (x64) Microsoft Internet Information Services (IIS) required – automatically installed, if not present. Must be installed on the same server as the Database Service component.
Transmitter Service	<ul style="list-style-type: none"> Supported operating systems: <ul style="list-style-type: none"> Windows Server 2008 R2 (x64) Windows Server 2012 (x64) Windows Server 2012 R2 (x64) Windows Server 2016 (x64) Windows Server 2019 (x64) If you are planning to use local modems: An unused serial port⁸ (COM port) for each modem

⁸ If the server does not have a free serial port, you may use a serial port server instead. When using this solution, you map a virtual serial port on the computer to a serial port on a device, which is connected to the network. SMS PASSCODE has been tested with serial port servers ("Terminal Servers") from Moxa (http://www.moxa.com/product/Serial_Device_Servers.htm). It is recommended to use secure serial port servers, which encrypt the network communication (e.g. Moxa Nport 6000 series). It is also advantageous to use serial port servers in case you need to connect a lot of modems to the same computer, since serial port servers with many serial ports are available.

IMPORTANT: In case of using any Moxa device, please ensure that the installed drivers are supported for the Windows operating system in use.

Component	Requirement
Authentication Backend Service	<ul style="list-style-type: none"> Supported operating systems: <ul style="list-style-type: none"> Windows Server 2008 R2 (x64) Windows Server 2012 (x64) Windows Server 2012 R2 (x64) Windows Server 2016 (x64) Windows Server 2019 (x64)
Self-service Website	<ul style="list-style-type: none"> Supported operating systems: <ul style="list-style-type: none"> Windows Server 2008 R2 (x64) Windows Server 2012 (x64) Windows Server 2012 R2 (x64) Windows Server 2016 (x64) Windows Server 2019 (x64) Microsoft Internet Information Services (IIS) required – automatically installed, if not present. <p>It is recommended to install this component on the same server as the Database Service component. However, it is possible to install this component on a separate server (cf. section 10.3, page 39).</p>
PowerShell Support	<ul style="list-style-type: none"> Supported operating systems: <ul style="list-style-type: none"> 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) Windows Server 2019 (x64) PowerShell version 4.0 or later is required. Please ensure that PowerShell script execution is NOT restricted by a Group Policy. It must be allowed to change the script execution policy of a process to “RemoteSigned” or “Unrestricted”.
Citrix Web Interface Protection	<ul style="list-style-type: none"> Supported operating systems: <ul style="list-style-type: none"> Windows Server 2008 R2 (x64) You must install Citrix Web Interface on the server and publish at least one Web Interface <u>before</u> installing this component. <p>The following Citrix Web Interface versions are supported:</p> <ul style="list-style-type: none"> Citrix Web Interface 5.3.0 Citrix Web Interface 5.4.0 Citrix Web Interface 5.4.2 <ul style="list-style-type: none"> AD and NDS authentication are supported.

Component	Requirement
RADIUS Protection	<ul style="list-style-type: none"> Supported operating systems: <ul style="list-style-type: none"> Windows Server 2008 R2 (x64) Windows Server 2012 (x64) Windows Server 2012 R2 (x64) Windows Server 2016 (x64) Windows Server 2019 (x64) <p>Please note: Only Windows Server Editions including the Network Policy Service (NPS) are supported. This means, that for example <i>Windows Server 2008 Web Edition</i>, <i>Windows Server 2012 Hyper-V Edition</i> and <i>Windows Server 2012 Storage Edition</i> are not feasible.</p> <ul style="list-style-type: none"> Network Policy Service (NPS) must be installed <u>before</u> 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: <ul style="list-style-type: none"> 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 <p>For further information regarding supported RADIUS clients, please contact your SMS PASSCODE reseller. You can also contact support@entrustdatacard.com if you have a support agreement or direct support (Direct support is included in subscription license).</p> <ul style="list-style-type: none"> This component optionally supports IntelliTrust™ cloud service integration, thereby providing support for IntelliTrust™ authentication mechanisms.
AD FS Protection	<ul style="list-style-type: none"> Supported operating systems: <ul style="list-style-type: none"> Windows Server 2012 R2 (x64) Windows Server 2016 (x64) Windows Server 2019 (x64) The AD FS server role must be installed <u>before</u> installing this component. This component optionally supports IntelliTrust™ cloud service integration, thereby providing support for IntelliTrust™ authentication mechanisms, incl. machine authentication.

Component	Requirement
IIS Website Protection	<ul style="list-style-type: none"> Supported operating systems: <ul style="list-style-type: none"> Windows Server 2008 R2 (x64) Windows Server 2012 (x64) Windows Server 2012 R2 (x64) Windows Server 2016 (x64) Windows Server 2019 (x64)
Windows Logon Protection	<ul style="list-style-type: none"> Supported operating systems: <ul style="list-style-type: none"> 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) Windows Server 2019 (x64) Remote Desktop is supported.
Secure Device Provisioning (for ActiveSync devices)	<ul style="list-style-type: none"> The following versions of Microsoft Exchange Server are supported: <ul style="list-style-type: none"> Exchange Server 2010 Exchange Server 2013 Exchange Server 2016 Exchange Server 2019 Exchange Online <p>Note: It is not required to install the component on an Exchange Server, as the component can make a remote connection to the relevant Exchange Server, including Exchange Online.</p> <ul style="list-style-type: none"> Microsoft Internet Information Services (IIS) required – automatically installed, if not present. A certificate is required to protect communication with the Secure Device Provisioning Website using SSL/TLS.
Password Reset Website	<ul style="list-style-type: none"> Supported operating systems: <ul style="list-style-type: none"> Windows Server 2008 R2 (x64) Windows Server 2012 (x64) Windows Server 2012 R2 (x64) Windows Server 2016 (x64) Windows Server 2019 (x64) Microsoft Internet Information Services (IIS) required – automatically installed, if not present. A certificate is required to protect communication with the Password Reset Website using SSL/TLS.

Component	Requirement
Password Reset Backend Service	<ul style="list-style-type: none"> Supported operating systems: <ul style="list-style-type: none"> Windows Server 2008 R2 (x64) Windows Server 2012 (x64) Windows Server 2012 R2 (x64) Windows Server 2016 (x64) Windows Server 2019 (x64) It is recommended to install a certificate on relevant domain controller(s) to encrypt the communication between the Password Reset Backend Service and the domain controller(s) using SSL/TLS.

10.1 Requirements for Location and Behavior Aware Authentication

*Location and behavior aware authentication*⁹ is the overall term for making use of Passcode Policies, Authentication Policies and User IP Histories to achieve a more advanced and secure authentication experience. The pre-requisite for this to work is that the SMS PASSCODE system must be able to collect the correct end-user IP address, from which an authentication attempt originates.

The table below lists the pre-requisites for this with respect to the different types of authentication clients supported by SMS PASSCODE:

Authentication Client	Pre-requisite for collection of end-user IP addresses
Citrix Web Interface Protection IIS Website Protection AD FS Protection Secure Device Provisioning (for ActiveSync devices) Password Reset Module	<p>The pre-requisites for all web-based authentication clients are the same. These clients are running on an Internet Information Server (IIS) that reports the end-user IP address of the web client to the SMS PASSCODE system.</p> <p>A problem might be that the IIS in question is located behind a reverse-proxy (e.g. Citrix Secure Gateway, Citrix Access Gateway, TMG or Web Application Proxy) or other type of network device (e.g. network load balancer), that hides the real end-user IP address from the IIS. If this is the case, you have two options for regaining access to the real end-user IP address:</p> <ul style="list-style-type: none"> Re-configure the network device to report the real end-user IP address to the IIS. Configure the network device to report the real end-user IP address as an HTTP header value. SMS PASSCODE can then be configured to retrieve end-user IP addresses from this specific HTTP header (cf. section 26.2, page 424).
RADIUS Protection	<p>End-user IP addresses are collected from a configurable attribute of the RADIUS packets received from the RADIUS client. I.e. end-user IP addresses can only be collected successfully, in case the RADIUS client supports reporting of end-user IP addresses.</p>

⁹ Please read section 16.1 (page 94) for more details about *location and behavior aware authentication*.

Authentication Client	Pre-requisite for collection of end-user IP addresses
Windows Logon Protection	<p>When accessing the SMS PASSCODE protected machine using RDP, the correct end-user IP address of the RDP client is collected.</p> <p>However, please note that when an RD Gateway is involved, the RD Gateway will act as the RDP client, i.e. the IP address of the RD Gateway will then be reported.</p> <p>If you still would like to get the correct end-user IP address in this case, consider providing external access only through an RD website protected by SMS PASSCODE multi-factor authentication. Collection of end-user IP addresses can then be enabled on the RD website instead.</p>

Important: Collection of end-user IP addresses is disabled by default

By default, collection of end-user IP addresses is disabled for all authentication clients installed. You must use the SMS PASSCODE Configuration Tool to enable collection of end-user IP addresses – and this must be done explicitly for every authentication client where this is wanted. Please read section 26.2 (page 424) for more details.

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.

10.2 Remote Desktop Service Protection

Access to a Remote Desktop Services infrastructure can be protected by SMS PASSCODE multi-factor 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 to require users to perform multi-factor 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	Yes ¹⁰
Windows Server 2016	Yes	Yes ¹⁰
Windows Server 2019	Yes	Yes ¹⁰
Windows 7	Yes	N/A
Windows 8	Yes	
Windows 8.1	Yes	
Windows 10	Yes	

¹⁰ 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	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 be present in the SMS PASSCODE database, including users that only have internal access without multi-factor authentication. Such users must be configured to bypass multi-factor authentication in the SMS PASSCODE system, using Authentication Policies. 	<ul style="list-style-type: none"> 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 / 2016 / 2019: <ul style="list-style-type: none"> 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 / 2012 R2 / 2016 / 2019:** When using Remote Desktop Services on Windows Server 2008 R2 / 2012 R2 / 2016 / 2019 you have two options to implement SMS PASSCODE authentication:
 1. 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 same server. This server must NOT be a domain controller. Form-based authentication and single sign-on (SSO) is supported¹¹.
 2. 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 12.2.2 and 12.2.3 for details about setting up RDS Protection.

10.3 Installing the Self-service Website on a Non-DB Server

As mentioned in the system requirements table in section 10 it is recommended to install the SMS PASSCODE Self-service Website (if installed) on the same server as the SMS PASSCODE Database Service (called the *DBS host* below). However, it is possible to install the website on a separate server. This section describes the required steps.

By default, the SMS PASSCODE Self-service Website runs under the identity "localsystem", which is the reason why it can only access the SMS PASSCODE Database, when it is installed on the same server. To install the website on a separate server, you need to create a dedicated domain user and configure the website to run under such dedicated user identity and grant the dedicated user identity access to the SMS PASSCODE Database. The required steps are described below:

1. Install the SMS PASSCODE Self-service Website on a separate server (cf. section 14.2, page 67). This server is called the *website server* below.
2. Create a new domain user that is dedicated for being used for remote access to the *DBS host*. The user must be a member of the same domain as the *website server*.

¹¹ 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.

3. Log on to the *DBS host*.
 - a. Is the *DBS host* member of the same domain as the *website server*?
 - i. DBS host domain = website server domain:
The user created in step 2 is called the **DB connection user** below.
 - ii. DBS host domain \neq website server domain:
Create a local user on the DBS host, having the same username and password as the user created in step 2 above. This local user is called the **DB connection user** below.

- b. On the *DBS host*, locate the **secret.dat** file. The default location is:

C:\Program Files\SMS PASSCODE\secret.dat

Assign read permissions to this folder for the **DB connection user**.

- c. On the *DBS host*, locate the folder containing the DB files. The default location is:

C:\Program Files\SMS PASSCODE\Database

Assign read and write permissions to this folder for the **DB connection user**.

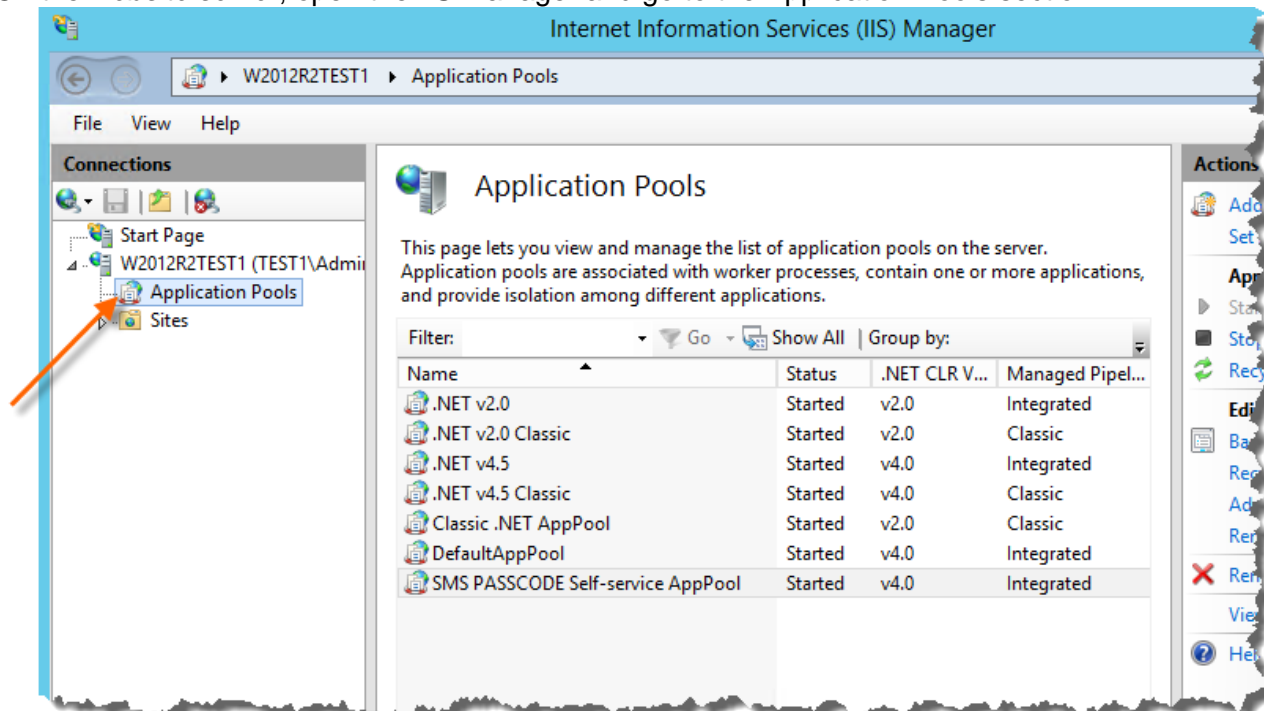
Restart the SMS PASSCODE Database Service. Now the dedicated user (from step 2) will have read and write access to the SMS PASSCODE database from any other server.

4. On the *website server*, locate the **secret.dat** file in the SMS PASSCODE installation folder. The default location is:

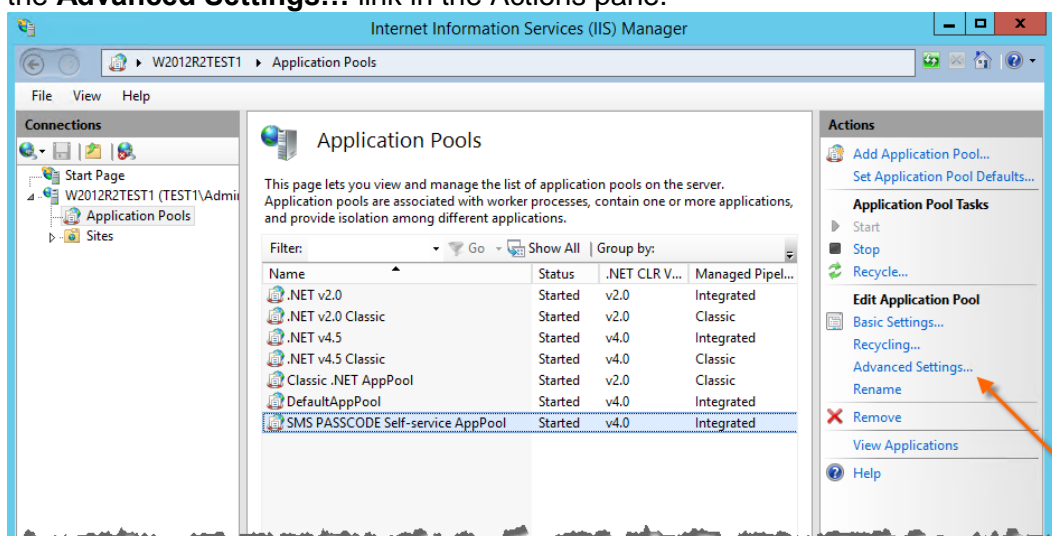
C:\Program Files\SMS PASSCODE\secret.dat

Assign read permissions to this file for the dedicated user created in step 2.

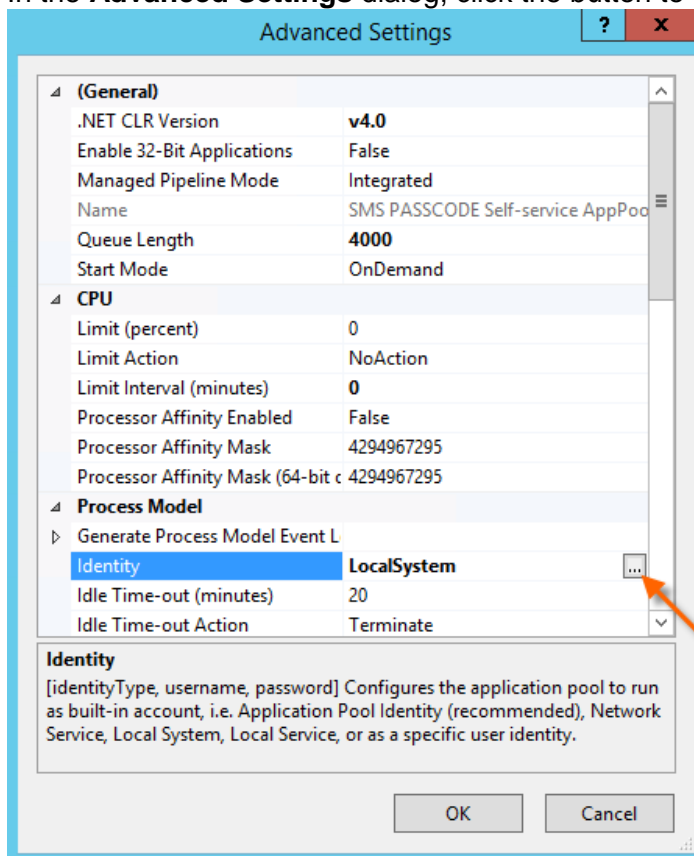
5. On the *website server*, open the IIS manager and go to the Application Pools section:



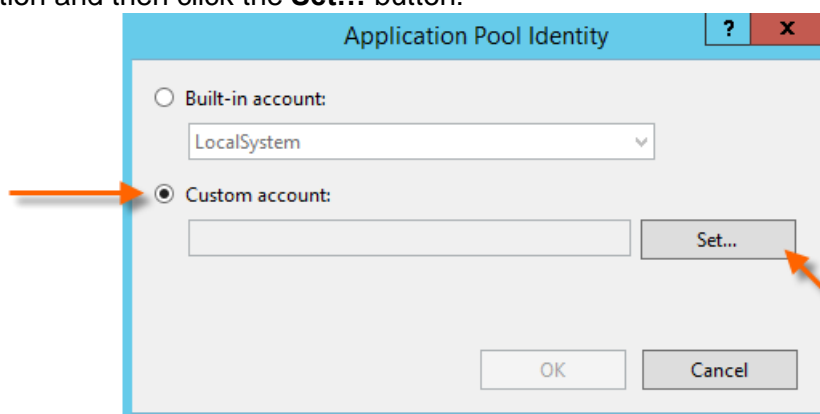
- a. Select the Application Pool **SMS PASSCODE Self-service AppPool**, and then click the **Advanced Settings...** link in the Actions pane.



- b. In the **Advanced Settings** dialog, click the button to the right of the **Identity** setting:



- c. In the **Application Pool Identity** dialog that appears, select the **Custom account** option and then click the **Set...** button:



- d. In the **Set Credentials** dialog that appears, enter the user name and password of the user created in step 2. Then click the **OK** button.
- e. Click the **OK** button in the **Application Pool Identity** dialog.
- f. Click the **OK** button in the **Advanced Settings** dialog.

6. This completes the setup. Start the website and check that everything works as expected.

Note: If you want to use the SMS PASSCODE Configuration Tool to test the connection to the *DBS host*, then you need to take additional actions:

- a. On the *website server*, add the user that was created in step 2 to the local Administrators user group (otherwise, the user is not allowed to start the SMS PASSCODE Configuration Tool).
- b. On the *website server*, start the SMS PASSCODE Configuration Tool using the user account that was created in step 2.
- c. In the SMS PASSCODE Configuration Tool, go to the **Database** tab and test the connection to the *DBS host*.

11 INFRASTRUCTURE

SMS PASSCODE is composed of various software components (cf. section 8) which can communicate with each other across the network. This provides great flexibility regarding the distribution of the components on different servers, which allows for optimization of the SMS PASSCODE deployment according to your specific server infrastructure.

Since you can distribute the SMS PASSCODE components in almost any way you like, there are a huge number of possible installation scenarios. The possibilities span from a simple **Cloud Setup**, to **Hybrid/On-Premise Setups**, that can be very simple with all components installed on the same server, to advanced “total distribution” setups, where all components are distributed onto different machines. Many other scenarios exist between these extremes – you can install some components together on a machine while other components are installed individually on other machines.

The purpose of this section is to show selected network diagrams that illustrate different “sample” SMS PASSCODE installation scenarios.

Please note that if you do not need the flexibility of distributing components to multiple servers but would rather prefer a very simple installation on a single server, you have the option of just installing all required components on a single server.

User Store Integration

When using **User Store Integration** to import users from an Active Directory, it is recommended to install the **Database Service** component on a server that is a member of the domain (installing on a domain controller is also allowed, but not necessary). I.e. when planning for an installation with some components being installed in a DMZ you will typically locate the **Database Service** on the LAN side of the firewall.

11.1 Component Communication

Distributed SMS PASSCODE components communicate via the network. Communication takes place using the TCP/IP protocol – all network messages between SMS PASSCODE components are encrypted using strong 256-bit AES encryption. SMS PASSCODE uses several TCP ports as described below:

Component	Incoming	Outgoing
Database Service	Listens by default on the two TCP ports 9090 and 9091	<ul style="list-style-type: none"> Communicates with all Transmitter Services (TCP port 8989) Communicates with all Authentication Backend Services (TCP port 8988) Communicates with one or more Domain Controllers / LDAP Directories, in case User Store Integration has been enabled (using LDAP or Global Catalog, possibly using SSL) Hybrid Setup: Communicates with the IntelliTrust™ cloud service (https://itcsadminservice.azurewebsites.net) on port 443 (SSL).
Web Administration Interface	Listens by default on TCP port 2000	<ul style="list-style-type: none"> Communicates with the Database Service (TCP port 9091) Communicates with Transmitter Services (TCP port 8989), when using the Modem Monitoring page
Transmitter Service	Listens by default on TCP port 8989	<ul style="list-style-type: none"> Communicates with the Database Service (TCP port 9090) Might communicate with external web services, when Dispatch Connectors are used, typically on port 443. E.g. port 443 (SSL) is used when utilizing the SMS PASSCODE Mobile app.
Authentication Backend Service	Listens by default on TCP port 8988	<ul style="list-style-type: none"> Communicates with the Database Service (TCP port 9090) Communicates with other Authentication Backend Services (TCP port 8988) Communicates with all Transmitter Services (TCP port 8989) Hybrid Setup: Communicates with the IntelliTrust™ cloud service (tenant specific URL) on port 443 (SSL).
Self-service Website	Listens by default on TCP port 3000	<ul style="list-style-type: none"> Communicates with the Database Service (TCP port 9091) Communicates with one or more Domain Controllers, in case User Store Integration has been enabled (using LDAP or LDAPS)

Component	Incoming	Outgoing
SMS PASSCODE Authentication clients	-	<ul style="list-style-type: none"> • On-premise or Hybrid Setup: Communicates with a list of Authentication Backend Services (TCP port 8988). • Cloud Setup¹²: Communicates with the IntelliTrust™ cloud service on port 443 (SSL).
Password Reset Website	Listens by default on TCP port 5000, but should be reconfigured to use SSL (port 443)	<ul style="list-style-type: none"> • Communicates with the Password Reset Backend Service (TCP port 8888)
Password Reset Backend Service	Listens by default on TCP port 8888	<ul style="list-style-type: none"> • Communicates with one or more Domain Controllers (using LDAP or LDAPS) • Communicates with a list of Authentication Backend Services (TCP port 8988)
Secure Device Provisioning	The website listens by default on TCP port 6000, but should be reconfigured to use SSL (port 443)	<ul style="list-style-type: none"> • The backend service communicates with a list of Authentication Backend Services (TCP port 8988), and with an Exchange Server on TCP port 80 or 443, depending on whether http or https is configured, respectively.

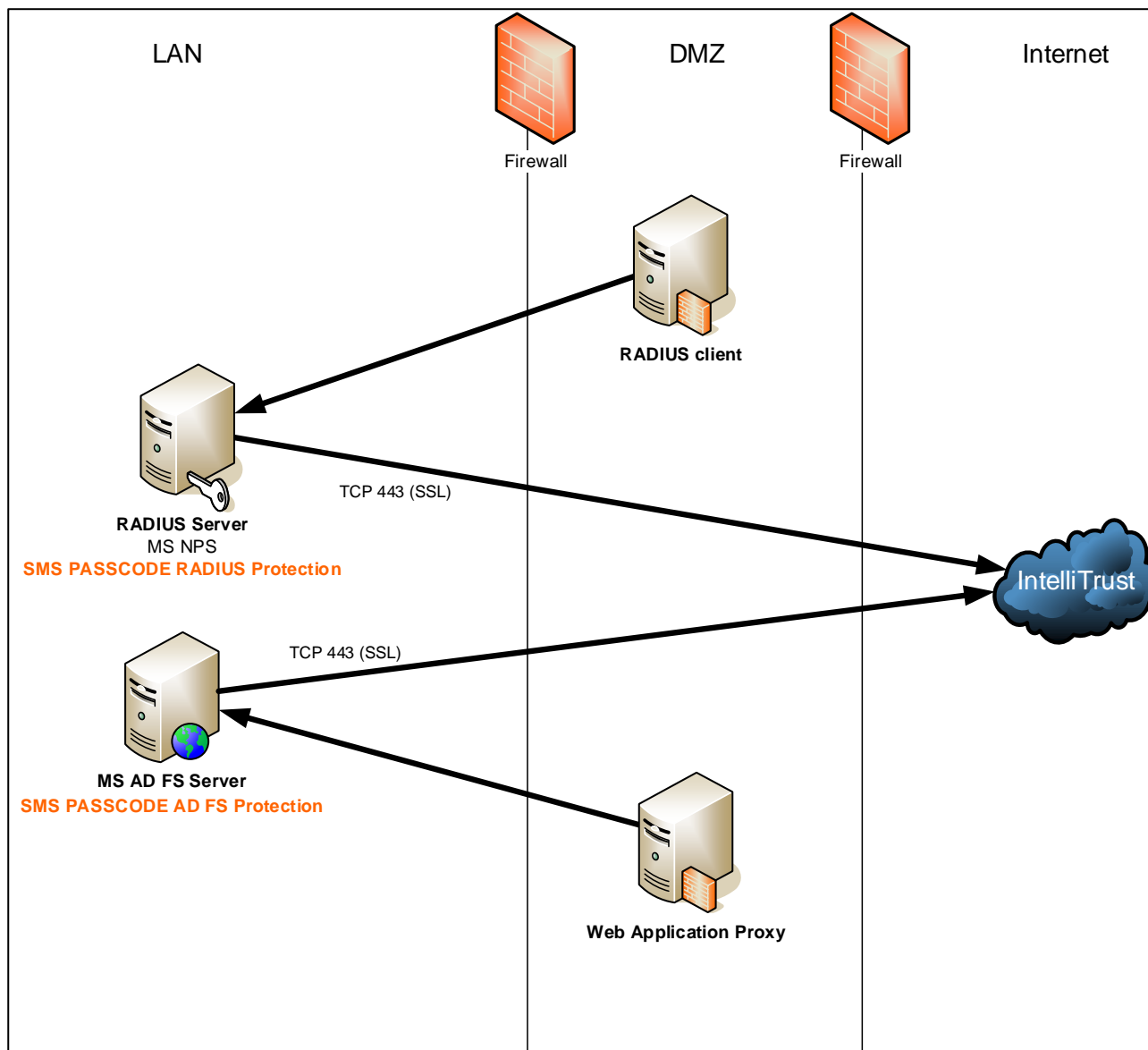
The usage of the different TCP ports is also illustrated using network diagrams in the following sections (e.g. the network diagram in section 11.6, page 52, gives a good overview). Section 23.4 (page 345) contains Password Reset Module specific network diagrams illustrating the communication between the Password Reset Website and Password Reset Backend Service components.

You can change the default TCP ports during an installation (or afterwards), in case they conflict with other applications.

¹² In SMS PASSCODE 2020 SP1, only the Citrix Web Interface protection and Secure Device Provisioning are not supported in a **Cloud Setup**. Also, SMS PASSCODE Windows Logon Protection supports **Cloud Setup** only for Windows versions newer than Windows 7 / Windows Server 2008 R2.

11.2 Cloud Setup

This section illustrates a **Cloud Setup** of SMS PASSCODE. In this case, **RADIUS Protection** and **AD FS Protection** is configured to communicate directly with the IntelliTrust™ cloud service. No SMS PASSCODE core components are installed in this case:

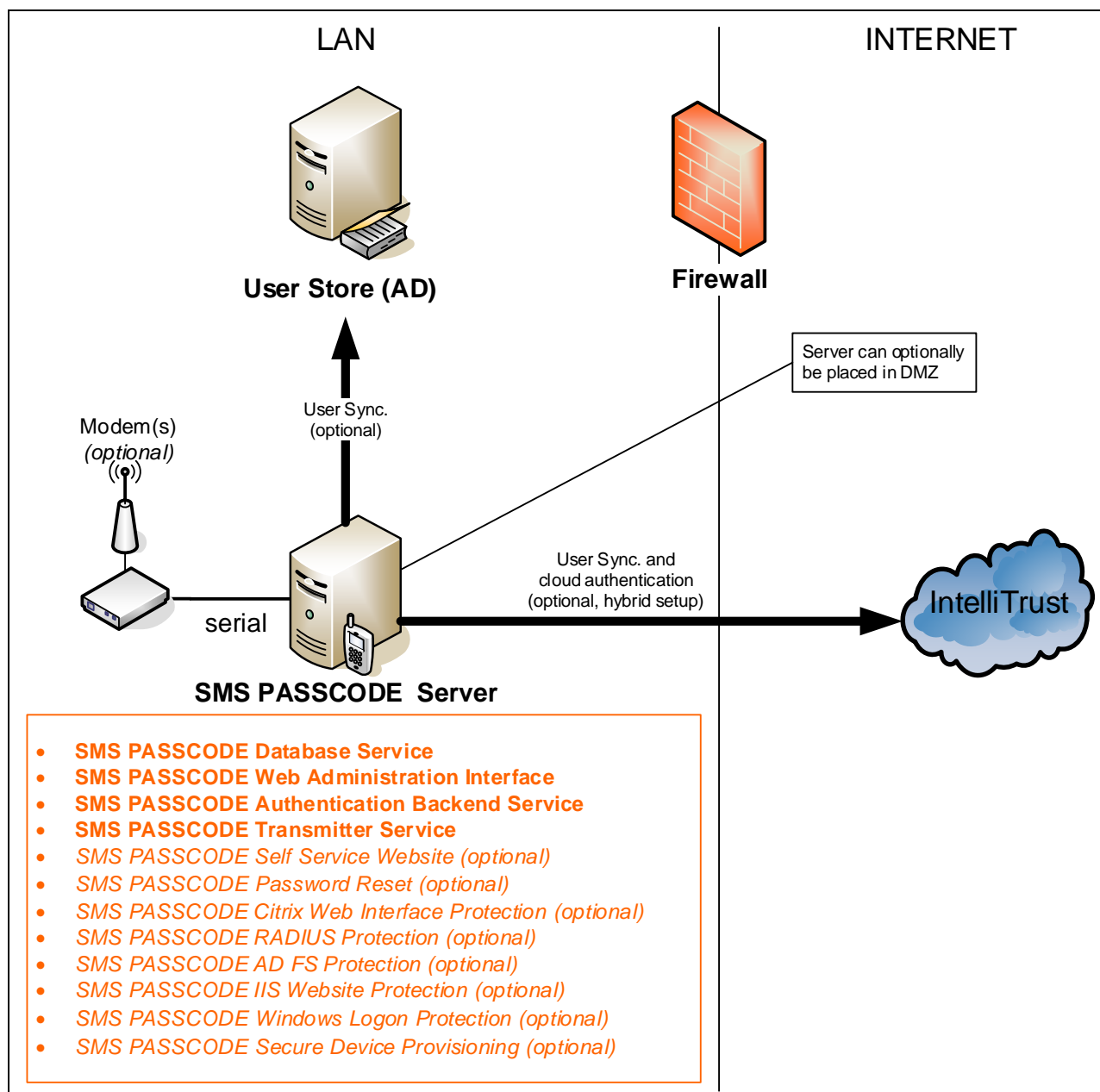


11.3 On-premise Single Server Installation

The simplest form of an On-premise (or Hybrid) SMS PASSCODE installation is to install all required components on a single server. The following (required) components must always be installed during this type of installation:

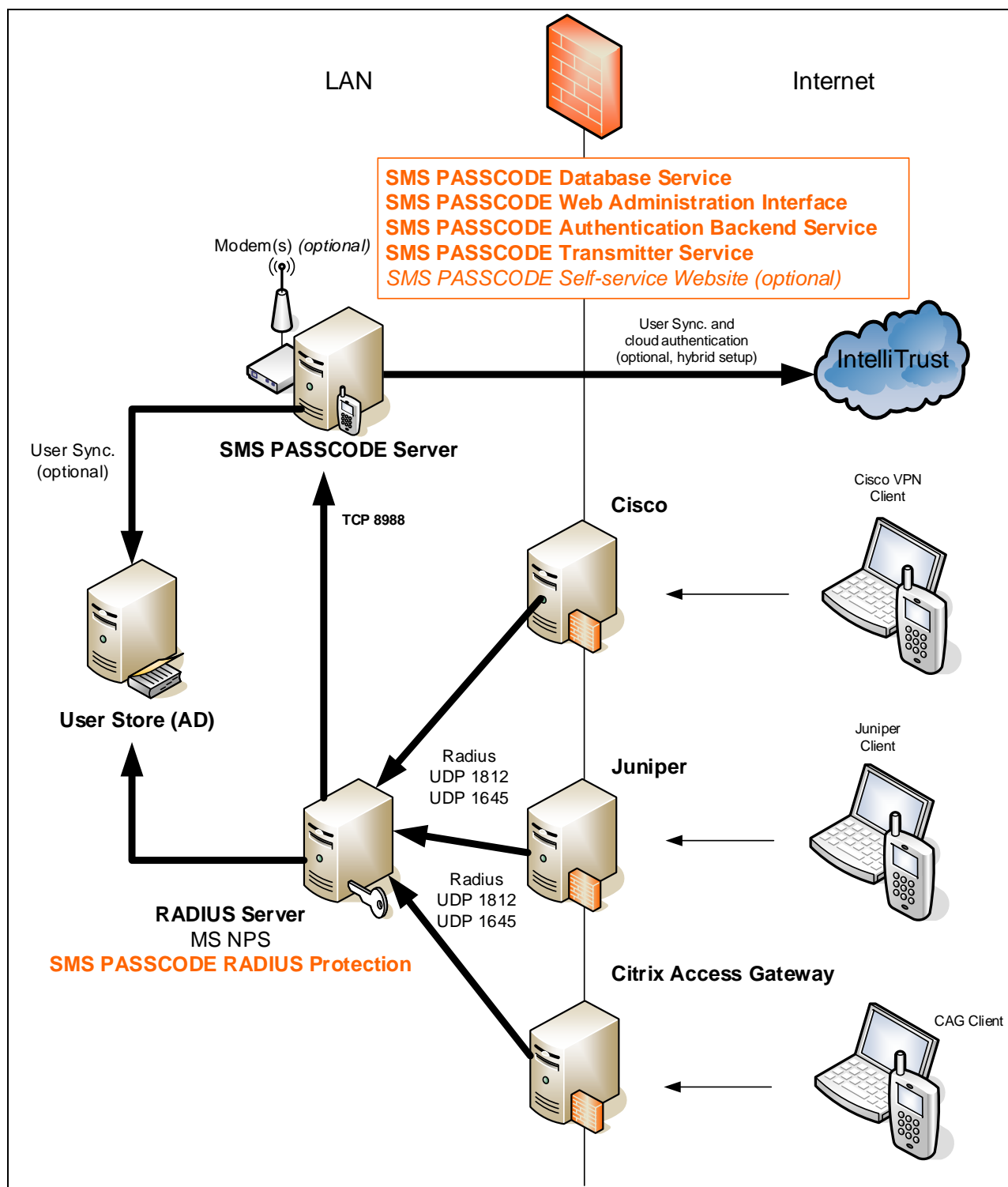
- **Database Service**
- **Web Administration Interface**
- **Authentication Backend Service**
- **Transmitter Service**

The remaining components are optional.

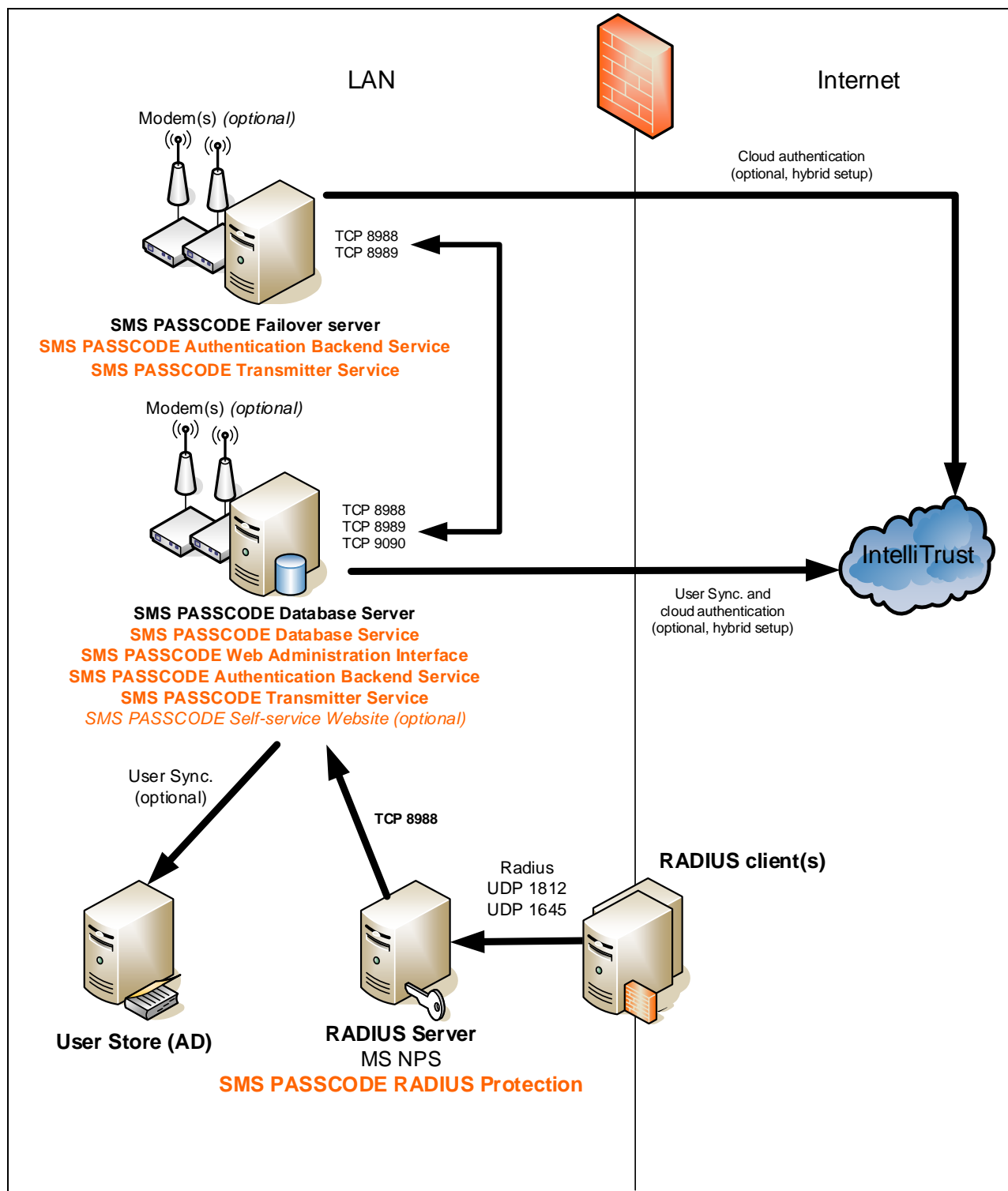


11.4 RADIUS Clients

In this section, an on-premise (or hybrid) installation example is shown with SMS PASSCODE being used for RADIUS authentication. Whereas a possibility is to install all necessary SMS PASSCODE components on the RADIUS server itself, the example below illustrates another scenario where the **RADIUS Protection** component is installed on the RADIUS server and the remaining components are installed on a separate server:



For failover reasons it would be better to have several **Authentication Backend Service** and **Transmitter Service** components installed, to ensure that if any **Authentication Backend Service** would become unavailable for some reason, then the RADIUS server can communicate with another one. In addition, each **Authentication Backend Service** instance will automatically perform intelligent load balancing and failover between all available Transmitter Services, according to the Dispatch Policies, that you define. You can install as many Authentication Backend Services and Transmitter Services as you like. The example below illustrates the usage of two instances of each:



For further failover, you could additionally decide to deploy several RADIUS servers, each with SMS PASSCODE RADIUS Protection.

11.5 Enterprise Setup

SMS PASSCODE supports enterprise environments with 24x7 uptime demands. This is achieved by supporting failover on all levels of the SMS PASSCODE infrastructure:

- **Failover on the database level:**
The Database Service continuously pushes all data changes to all Authentication Backend Services. All data is cached locally which means that all Authentication Backend Services have access to all data even in case the Database Service becomes unavailable¹³.
- **Failover on the Transmitter service level:**
Each Authentication Backend Service continuously monitors all Transmitter Services and ensures an intelligent load balancing of all message requests between all available Transmitter Services. The failover/load balancing algorithm is customizable using **Dispatch Policies**. Using these policies, it is possible to define in detail, how incoming message requests should be distributed according to customizable Dispatch Policy Rules. Please refer to section 17.18 (page 271) for more information regarding this.
- **Failover on the modem level:**
Up to 32 modems can be connected to each Transmitter Service in a modem pool. The Authentication Backend Services ensure intelligent load balancing between all available modems across Transmitter Services. In case a modem becomes unavailable, requests are automatically redirected to other modems in the modem pool. By using SIM cards of different telco operators, you can even achieve failover on the operator level.
- **Failover on the message dispatching level:**
If you have users that cannot receive one-time-passcodes (OTPs) by SMS, you can define policies to allow authentication by other means (e.g. send OTPs by email, voice calls or SMS PASSCODE Mobile app, or enable push authentication, or allow authentication using hardware tokens, software tokens or time-constrained personal passcodes).
- **Failover on the authentication client level:**
Each *SMS PASSCODE Authentication client* can be configured to redirect its requests to a prioritized list of Authentication Backend Services. If any of the listed services becomes unavailable, then requests are automatically redirected to the services being available. Please notice that the list of services can be changed **on-the-fly** during operation without any downtime.

For **optimal** failover, your SMS PASSCODE On-premise (or Hybrid) installation should include:

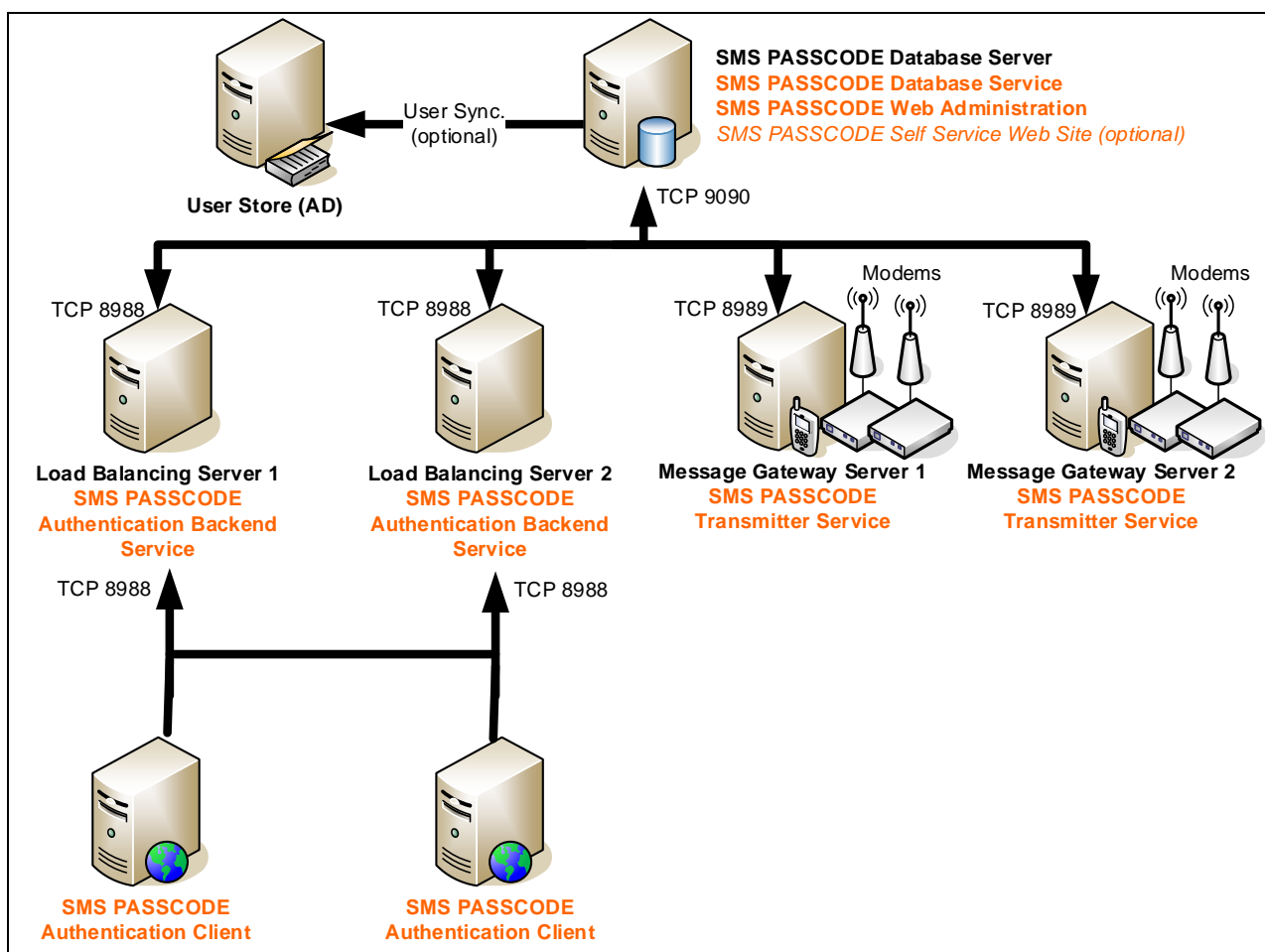
- At least two Authentication Backend Services.
- At least two Transmitter Services.
- At least two different dispatch mechanisms assigned to every Transmitter Service (e.g. two modems, or 1 modem and 1 Dispatch Connector allowing message requests to be forwarded to an external message provider). In a Hybrid Setup, one dispatch mechanism

¹³ The only exception to this is that the database must be running, in order for OATH token authentication to succeed.

might be sufficient, as you will then have failover between the IntelliTrust™ cloud service and the on-premise Transmitter Service.

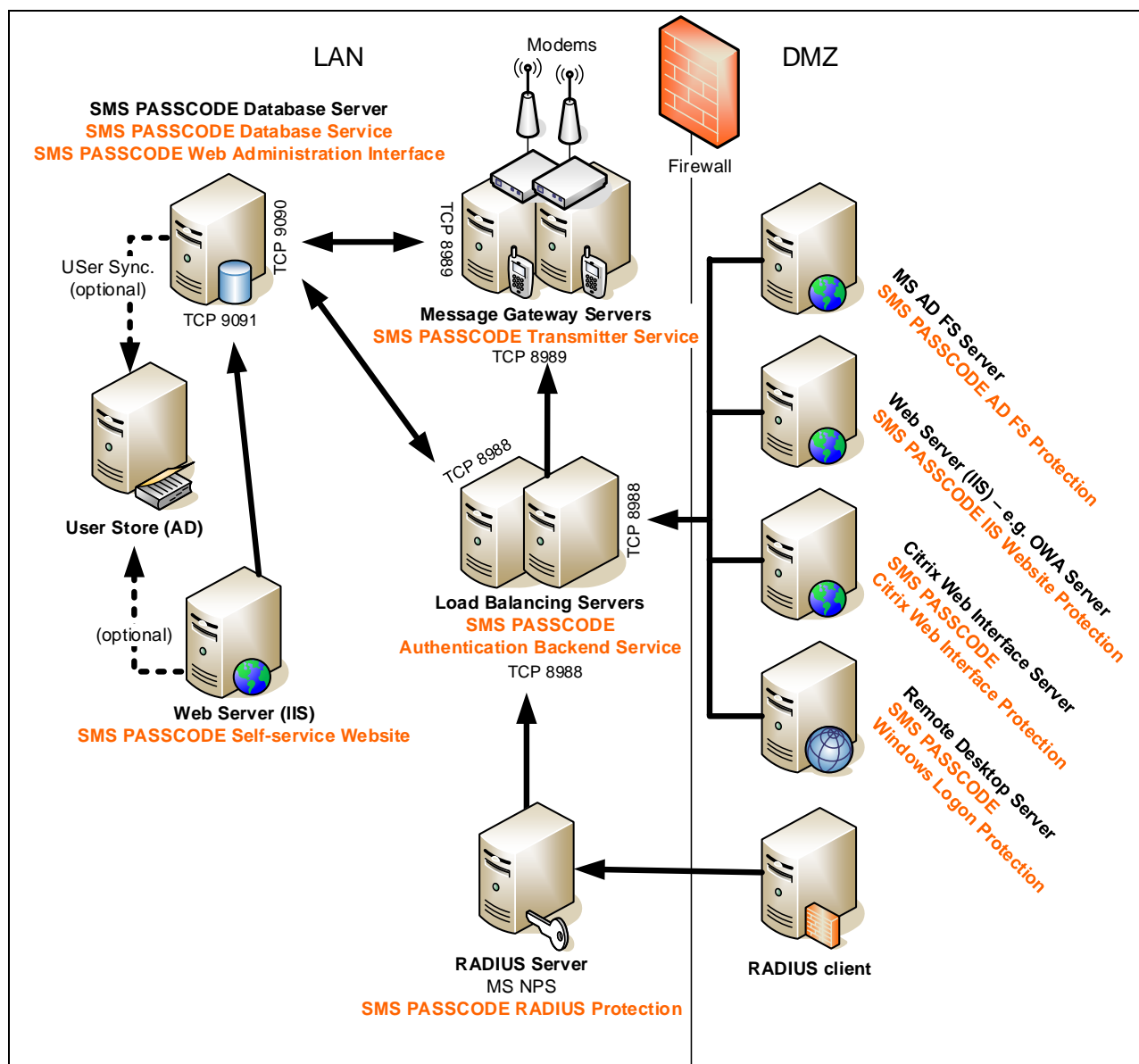
- Each *SMS PASSCODE Authentication client* should redirect requests to at least two Authentication Backend Services.

The following diagram illustrates an example of a minimum setup for optimal failover. In practice, you would most probably consolidate the four servers running **Authentication Backend Service** and **Transmitter Service** on two servers, since an Authentication Backend Service and a Transmitter Service may run on the same server.



11.6 Total Distribution

In this section, a last installation example is shown. This example illustrates how it is possible to distribute all components on separate servers, during an On-premise (or Hybrid) setup:



12 PRE-INSTALLATION ACTIONS

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

12.1 Check SIM Cards

This section only applies for On-premise and Hybrid Setups, and only if you are using GSM modems with SIM cards for message transmission. In this case, please ensure that all SIM cards are working correctly.

Important: It is strongly recommended to check each SIM card according to the instructions below BEFORE the SMS PASSCODE installation is started.

The procedure for checking a SIM card is described below. It is recommended to perform the check at the location where the GSM modem, for which the SIM card is intended, is located.

For each SIM card, perform the following actions:

1. Insert the SIM card into a cell phone.
2. Enter PIN code if the SIM card requires this.
3. Wait until the cell phone has been registered on the mobile network.
4. Enter a new SMS and send it to another cell phone. Check that the transmission succeeds and that the SMS is received correctly on the other cell phone.

If the above check is not successful, it is usually caused by one of the following:

- **The SIM card is not active or has been closed:** Contact your cell phone operator and request activation of the SIM card.
- **There is no GSM coverage at the location in question:** You have the following possibilities in this case:
 - Move the server together with the GSM modem(s) to another location
 - Lengthen the antenna of the modem (e.g. to the roof of the building)
 - Move the GSM modem(s) to another location by installing the **Transmitter Service** on another server at a different location
 - Move the GSM modem(s) to another location by connecting them to a serial port server (e.g. Moxa NPort) connected to the network

For further information regarding external modem antennas or serial port servers please contact your SMS PASSCODE reseller.

12.2 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 10 (page 31).

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 12.2.1 (page 55)

- **AD FS Protection**

If you are planning to install the **AD FS Protection** component, then the AD FS server role must be installed on the relevant server beforehand. It is also recommended to configure any (cloud) applications beforehand and ensure that standard AD FS authentication works without SMS PASSCODE. For more details, please read section 25.3 (page 400).

- **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 25.4 (page 407) 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 / 2012 R2 / 2016 / 2019:** Either protect the RD Web Access Site using the SMS PASSCODE IIS Website Protection component (cf. section 12.2.2, page 55), or protect each RD Session Host using the SMS PASSCODE Windows Logon Protection component (cf. section 12.2.3, page 62).
- **Windows Server 2012:** Protect each RD Session Host using the SMS PASSCODE Windows Logon Protection component (cf. section 12.2.3, page 62).

- **Secure Device Provisioning**

If you are planning to install SMS PASSCODE Secure Device Provisioning, then it is important to read section 24.2 (page 364) before performing such installation.

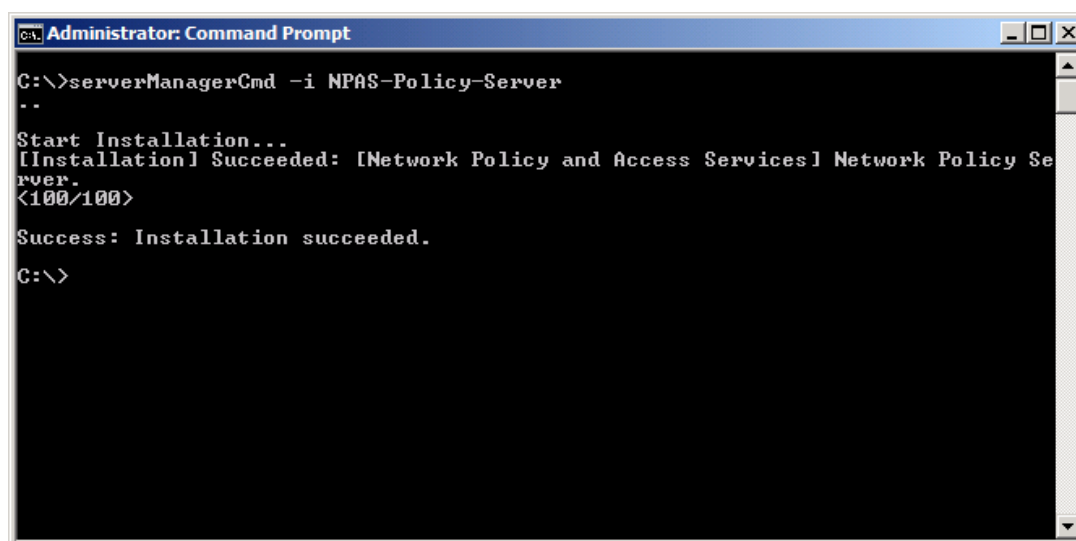
12.2.1 Installation of NPS

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

Windows Server 2008 R2

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

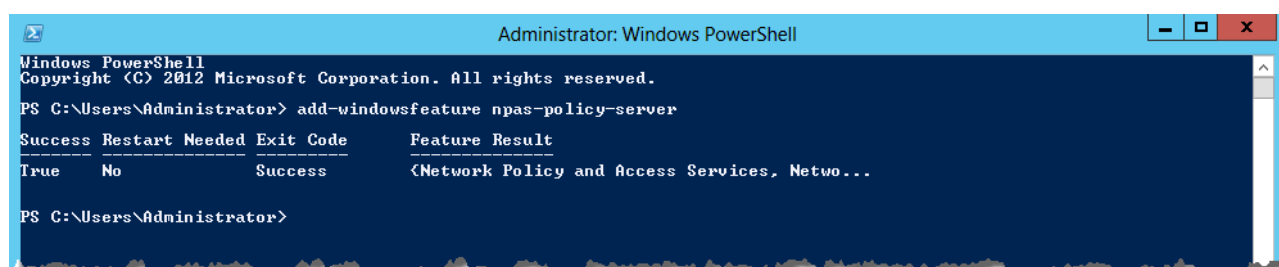
```
ServerManagerCmd -i NPAS-Policy-Server
```



Windows Server 2012 (R2) / 2016 / 2019

To install NPS on a Windows Server 2012 (R2) / 2016 / 2019, please use the Server Manager or run the following command in a PowerShell console:

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

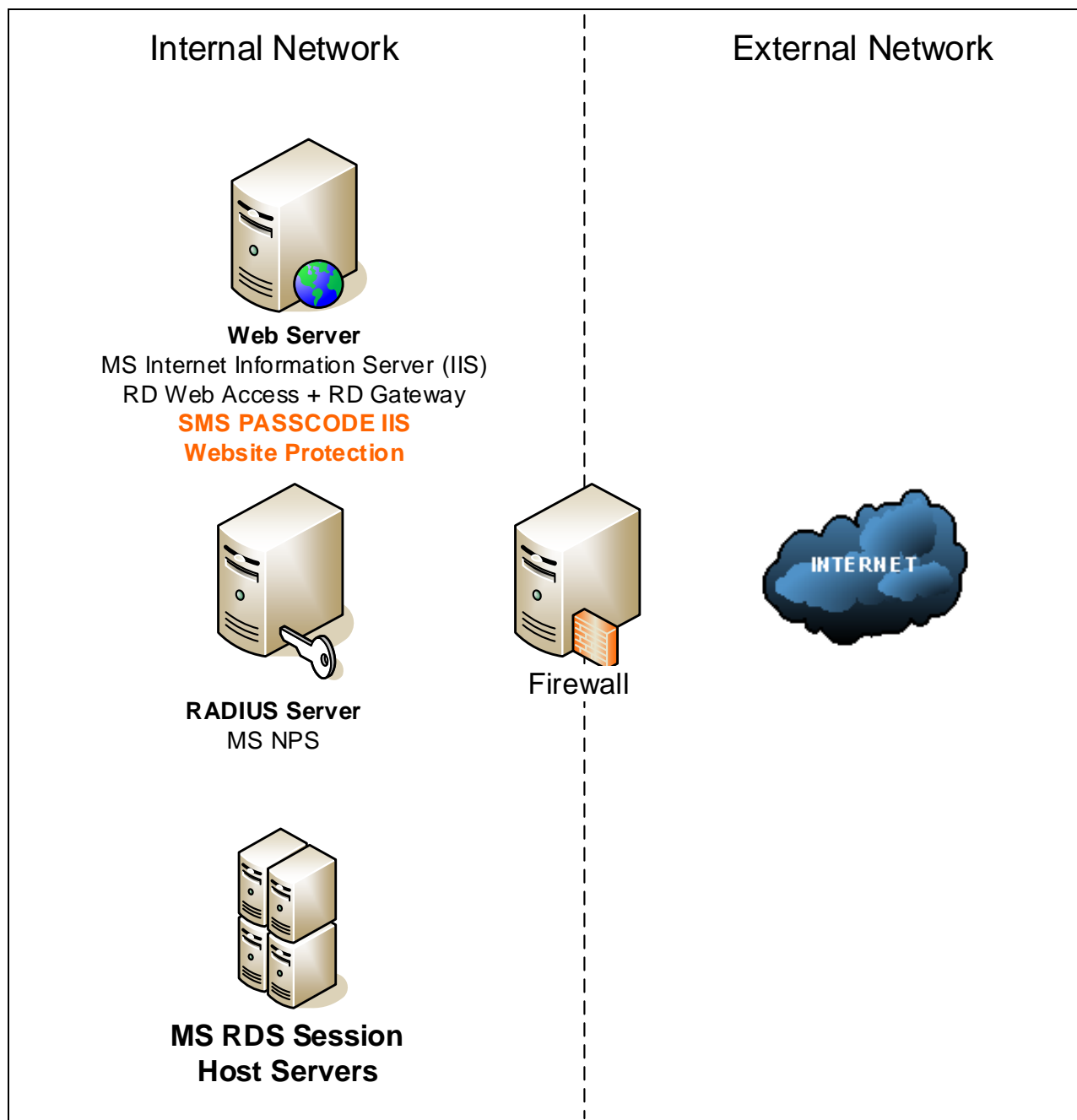


12.2.2 Protection of RD Web Access using IIS Website Protection

This section describes how to protect the Remote Desktop Web Access Site on a Windows Server 2008 R2 / 2012 R2 / 2016 / 2019.

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). You may install any other SMS PASSCODE components on the Web Server as well.
- It is mandatory, that the RD Web Access site and RD Gateway site reside on the same 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 / 2016 / 2019: 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).

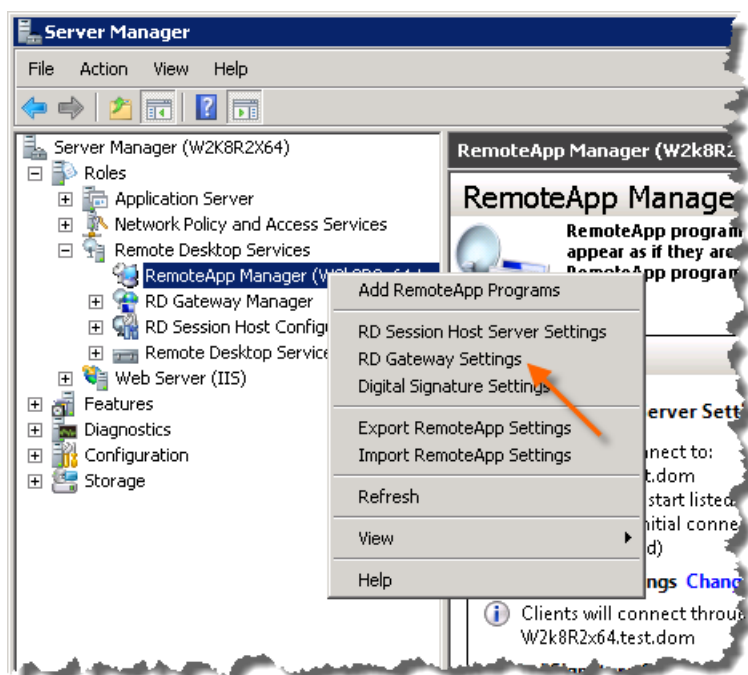
- Windows Server 2008 R2: Section 12.2.2.1 (below).
- Windows Server 2012 R2 / 2016 / 2019: Section 12.2.2.2 (page 61).

12.2.2.1 Protecting RD Web Access (Windows Server 2008 R2)

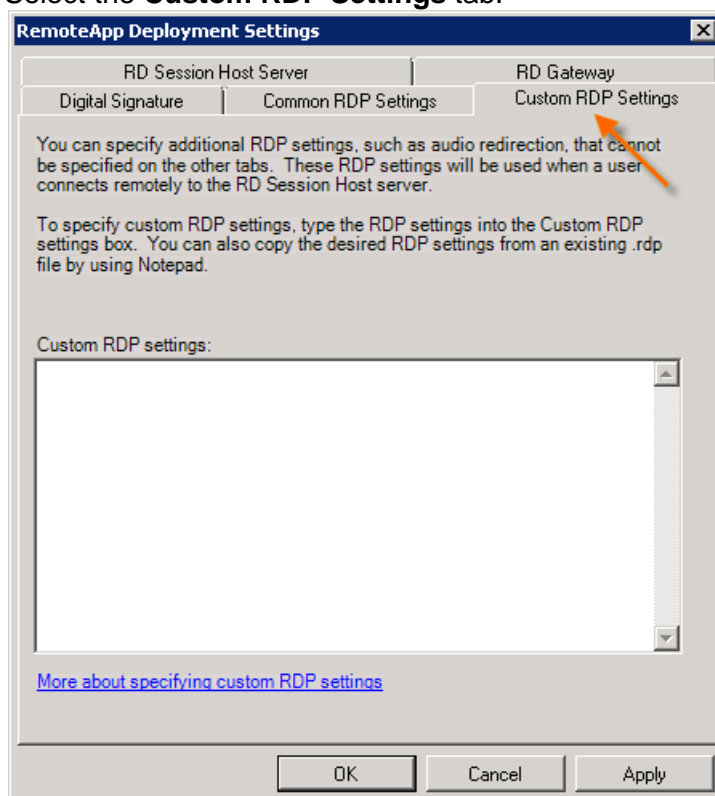
To protect the RD Web Access Site using SMS PASSCODE multi-factor authentication on a Windows Server 2008 R2, please follow the instructions below:

1. 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.
2. 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:

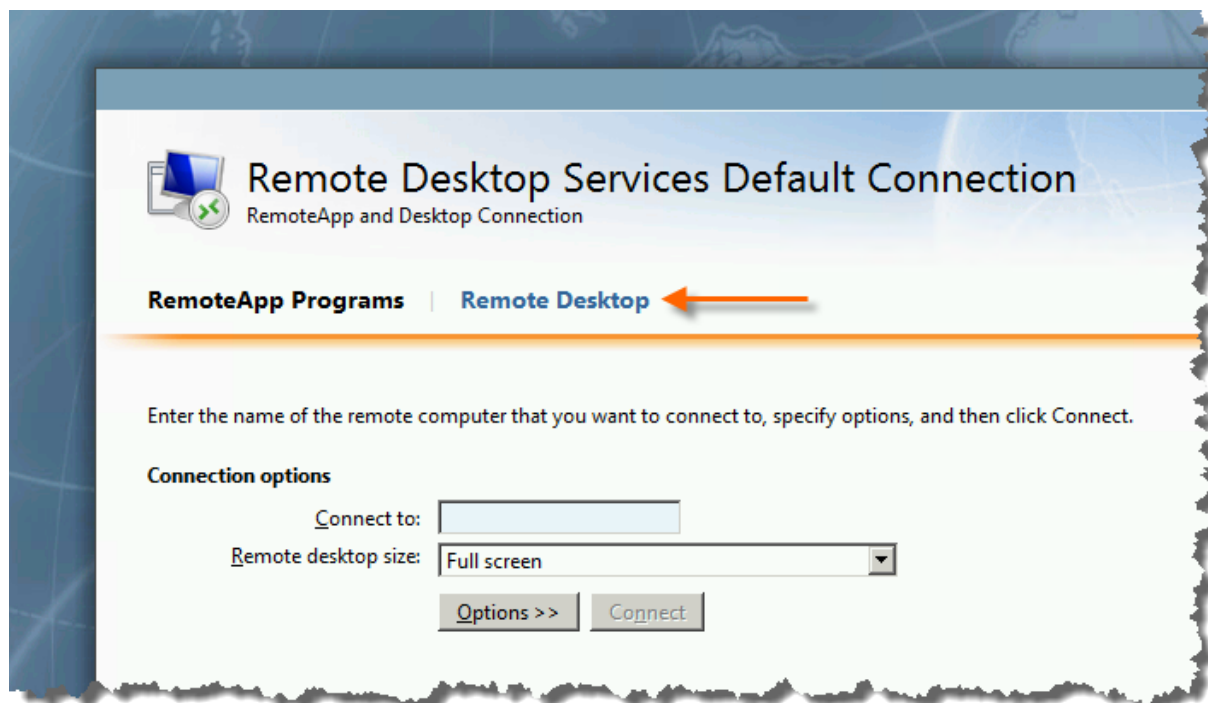


6. Test that SMS PASSCODE authentication works as expected.

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.

12.2.2.1.1 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, and 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 must 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...

```
RDPtr += "authentication level:i:2\n";
```

...with the following two lines...

```
RDPtr += "require pre-authentication:i:1\n";
RDPtr += "pre-authentication server address: s: https://fqdn/rdroot\n";
```

...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).

3. Save the changes to the desktops.aspx file.
4. Test that Remote Desktops can be accessed through the SMS PASSCODE protected RD Web Access Site.

12.2.2.2 Protecting RD Web Access (Windows Server 2012 R2 / 2016 / 2019)

To protect the RD Web Access Site using SMS PASSCODE multi-factor authentication on a Windows Server 2012 R2 / 2016 / 2019, please follow the instructions below:

1. 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.
2. 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”

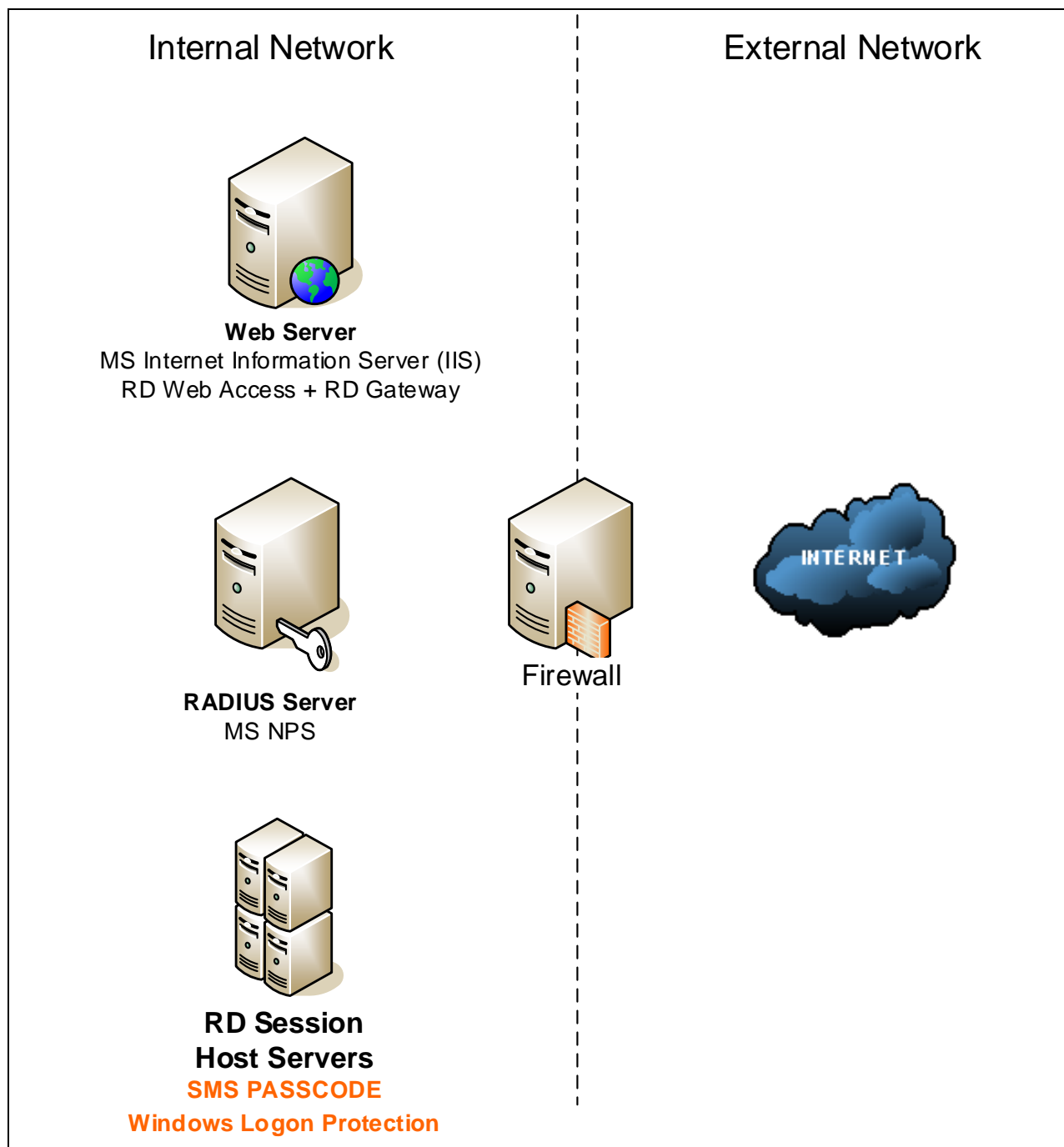
...then please read section 28.9 (page 441) for solving this issue.
 - b. On Windows Server 2016 / 2019, if single sign-on (SSO) does not work, meaning the user has to re-authenticate on the RD Session Host, then please read section 28.9 (page 441) for solving this issue.

This completes the procedure for protecting the RD Web Access Site on a Windows Server 2012 R2 / 2016 / 2019, using SMS PASSCODE multi-factor authentication.

12.2.3 Protection of RD Session Hosts using Windows Logon Protection

On Windows Server 2008 R2 / 2012 (R2) / 2016 / 2019 the RDS infrastructure can be protected using SMS PASSCODE multi-factor authentication by installing the **SMS PASSCODE Windows Logon Protection** component on each 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:

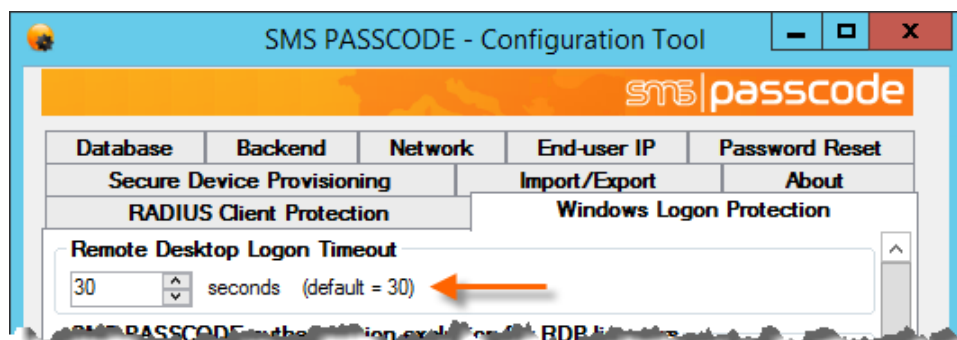
- The SMS PASSCODE **RADIUS protection** component cannot be installed on the RADIUS server.
- The Web Server and RADIUS server could be consolidated to a single server (installing both NPS and IIS on the same server).
- The SMS PASSCODE **Windows Logon Protection** component must be installed on each RD Session Host Server. You may install any other SMS PASSCODE components on these servers as well (but this is not recommended).
- 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 external 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 without 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 each 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 several options for this:
 - a. Only require multi-factor authentication for requests originating from the RD Gateway. This can be configured using Authentication Policies by setting up a filter on the IP address of the RD Gateway. Please refer to section 17.8, page 193, for more details regarding Authentication Policies.
 - b. 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 25.5.3, page 416, for more details how to set up and configure RDP Listener exclusion.

12.2.4 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 26.3, page 428, for more details).

13 UPGRADE

You can upgrade the following versions of SMS PASSCODE directly to version 2020 SP1:

- SMS PASSCODE 9.0
- SMS PASSCODE 9.0 SP1
- SMS PASSCODE 9.0 SP2
- SMS PASSCODE 2018
- SMS PASSCODE 2020

To perform an upgrade, just run the SMS PASSCODE 2020 SP1 installation like a “First-time installation” (cf. section 14). Do not uninstall any previous version of SMS PASSCODE before installing version 2020 SP1. The installation package will automatically upgrade the previous version and convert the database as needed.

In case of an On-premise or Hybrid Setup, you must obtain a new license key, before starting the upgrade unless you are upgrading from SMS PASSCODE 2020. In case of version 2020, license keys are compatible with 2020 SP1 version.

When upgrading, you must upgrade SMS PASSCODE on all servers containing any SMS PASSCODE components (both core components and authentication clients).

IMPORTANT (On-premise and Hybrid Setup):

If upgrading from 9.x and 2018 versions a new license key is required for SMS PASSCODE 2020 SP1. If you have a valid Software Assurance agreement or a valid Subscription agreement, you should already have received an email by now, explaining how to proceed to get the new license key. If not, please request a new license key from support@entrustdatacard.com.

After a successful upgrade, you should consider the impact of new features in SMS PASSCODE 2020 SP1, and whether you need to do some manual configurations. Relevant considerations are described in the next section.

13.1 Upgrade Considerations

If you are upgrading from SMS PASSCODE version 2018 or 2020, the upgrade is straight-forward. Please take into account, that SMS PASSCODE TMG Website Protection is not supported anymore. After the upgrade, you can optionally decide, whether you want to enable a Hybrid Setup, enabling IntelliTrust™ cloud service features (cf. section 17.3.4, page 119).

However, if you are upgrading from SMS PASSCODE version 9.x, then there are a number of additional considerations to take into account that were introduced since SMS PASSCODE 2018. The following sub-sections summarize these considerations.

13.1.1 Email and Dispatch Plugins Always Allowed for Dispatching

In SMS PASSCODE 9.x, notifications could always be sent via Email Connectors (SMTP) or Dispatch Connectors (Dispatch Plugin Modules), whereas OTP messages were only allowed to be transmitted by SMS via local modems, unless explicitly permitted to be transmitted otherwise in the general settings. It meant, that by default, Dispatch Policy rules referring to Email Connectors or Dispatch Connectors were previously skipped, when transmitting OTP messages.

For improved convenience, both notifications and OTP messages can now always be transmitted using any dispatch mechanism. You can still create distinct Dispatch Policies, in case you want notifications and OTP messages to be transmitted differently. And every type of notification can be assigned to a specific Dispatch Policy.

If you had previously NOT allowed OTP messages to be transmitted via Email Connectors or Dispatch Connectors, then you should carefully evaluate, whether any of your existing Dispatch Policies will now use such mechanisms for OTP message transmission (as no Dispatch Policy rules are skipped anymore due to the type of transmission).

13.1.2 Default Dispatch Connector

The system now automatically creates a default Dispatch Connector for the SMS PASSCODE Cloud Service. This default Dispatch Connector does NOT occupy a dispatch license.

If you had previously created your own Dispatch Connector for the same purpose, then you can proceed as follows to free up a dispatch license:

- On the previously created Dispatch Connector, click on “References” to get an overview, on which Dispatch Policy rules it is in use.
- On every such Dispatch Policy rule, change the dispatch mechanism to use the default dispatch connector.
- Now, “References” on the previously created Dispatch Connector should show, that it is not in use anywhere, anymore. It is therefore safe to delete it, to free up a dispatch license.

13.1.3 New Behavior for Dispatch Policies

In SMS PASSCODE 9.x, the last rule of every Dispatch Policy had a fixed behavior, and you could not delete this rule. Now, this rule is editable just as every other rule of a Dispatch Policy.

During the upgrade, all “fixed rules” are converted to editable rules with the same behavior as previously. It means, that your Dispatch Policies will behave as before. However, it is recommended to evaluate all your Dispatch Policies and consider, whether you want to adapt the rule sequence, now that you can edit the last rule as well.

13.1.4 Secure Device Provisioning

If you are upgrading the Secure Device Provisioning feature from SMS PASSCODE 9.x, please consider, that this component was redesigned considerably since SMS PASSCODE 2018. You should carefully plan the consequences of the following:

- “Configurable workflows” are not supported anymore.
- “Auto-approval” of ActiveSync devices is not supported anymore.

Please read section 24 (page 363) for more details on the redesigned Secure Device Provisioning feature.

13.1.5 IIS Website Protection

In SMS PASSCODE 9.x, any IIS websites NOT listed in the configuration file (config.xml) of the SMS PASSCODE IIS Website Protection component were automatically protected with SMS PASSCODE multi-factor authentication. Starting from SMS PASSCODE 2018, any website NOT listed in the configuration file is not protected with SMS PASSCODE multi-factor authentication anymore. Instead, ordinary access is granted.

In SMS PASSCODE 2020 SP1 IIS Website protection has been changed to use native HTTP module instead of ISAPI filter.

Therefore, please verify that all websites present in the IIS on a server where SMS PASSCODE IIS Website Protection has been upgraded, are protected by SMS PASSCODE as expected.

14 FIRST-TIME INSTALLATION

To install SMS PASSCODE, you must complete three steps:

1. Install local hardware, if needed (section 14.1, page 67).
2. Install software (section 14.2, page 67).
3. Configure SMS PASSCODE (section 16, page 95).

These three steps are described in the specified sections.

14.1 Installation of Hardware

NOTE: This section only applies to SMS PASSCODE installations in the **On-premise** or **Hybrid Setup**. For a **Cloud Setup**, hardware is not involved.

If you have acquired any modem hardware for handling message transmissions, then it is recommended to connect all such hardware to your servers, before starting the installation of the SMS PASSCODE software. You can request an up-to-date list of supported hardware from support@entrustdatacard.com.

14.2 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 8 (page 24), 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.

A valid **On-premise** or **Hybrid Setup** must fulfill the following requirements:

- A single **Database Service** must be installed on a server.
- A single **Web Administration interface** must be installed on the same server as the **Database Service**.
- At least one **Authentication Backend Service** must be installed on a server.

Additionally, an **On-premise** service must also fulfill the requirements below, whereas a **Hybrid Setup** does not need to, but it is recommended:

- At least one **Transmitter Service** must be installed on a server.
- At least one modem, Email Connector or Dispatch Connector must be connected to a **Transmitter Service**, to handle message transmissions. A Default Dispatch Connector is automatically created during installation. This Default Dispatch Connector ensures that message delivery works out-of-the-box. For subscription and trial customers, out-of-the-box message delivery is SMS-based, via the SMS PASSCODE Cloud Service; for other customers, out-of-the-box message delivery is performed using the SMS PASSCODE Mobile app.

The procedure for an SMS PASSCODE installation is to run the installation package on each involved machine and select the components to be installed on this machine. The recommended order of actions for an **On-premise** or **Hybrid Setup** is:

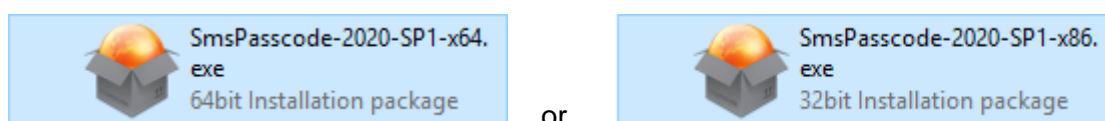
1. First, install the **Database Service** component on a server (the database server). If other SMS PASSCODE components are planned to be installed on the same server, then also include these components during this installation. It is mandatory to include the **Web Administration interface** component.
2. Configure SMS PASSCODE using the **Web Administration Interface** (cf. section 17). At this time, you should already create all planned Authentication Backend Service hosts, Transmitter Service hosts, and dispatch mechanisms (modems, Email Connectors and/or Dispatch Connectors) in the database.
3. Now install the **Authentication Backend Service** component on all those servers where this component is planned for installation. If other SMS PASSCODE components are planned to be installed on some of these servers, then also include these components during installation. Please note: In case you have already installed the **Authentication Backend Service** component on a server during step 1, do not run the installation again on that server.
4. Now install the **Transmitter Service** component on all those servers where this component is planned for installation. If other SMS PASSCODE components are planned to be installed on some of these servers, then also include these components during installation. Please note: In case you have already installed the **Transmitter Service** component on a server during step 1 or 3, do not run the installation again on that server.
5. Finally install *SMS PASSCODE Authentication clients* on the machines where these are planned for installation.
Please note: In case you have already installed some of these components during step 1, 3 or 4, do not run the installation again on those machines.

The procedure for a **Cloud Setup** is much simpler. In this case, only step 5 above is required (as steps 1-4 can be skipped, because no SMS PASSCODE core components are involved).

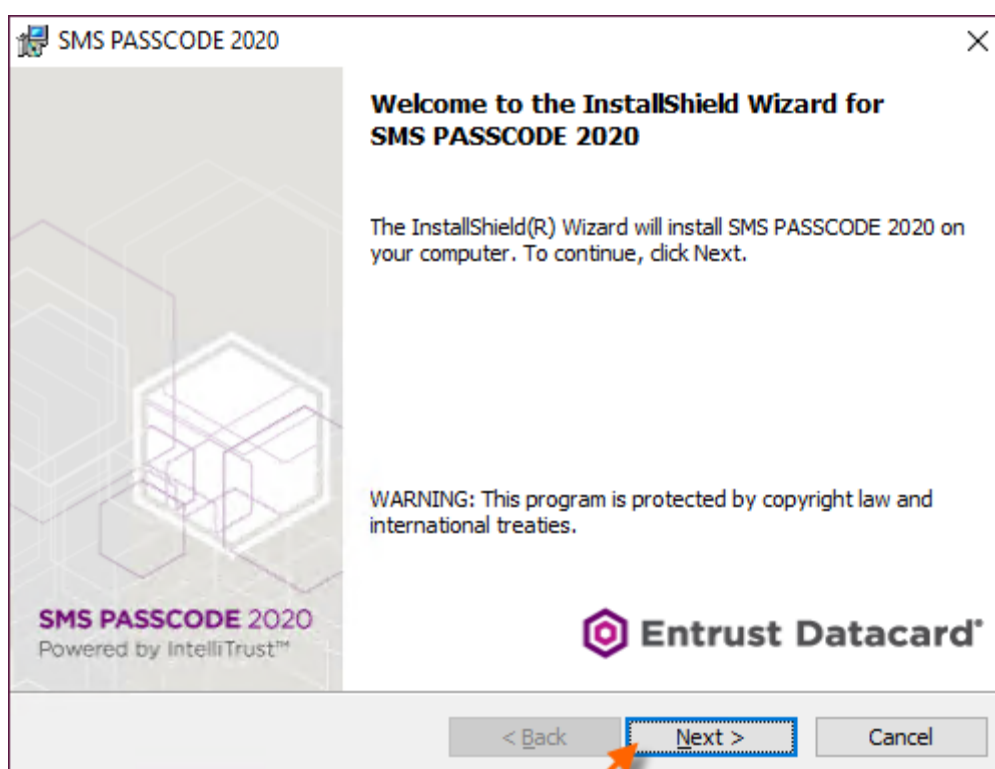
The actions for installing components on a machine are listed below. Please repeat these actions on each machine being part of the SMS PASSCODE installation.

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-2020-SP1-x86.exe** (32-bit) or **SmsPasscode-2020-SP1-x64.exe** (64-bit) to a local path on the machine.
3. Start the installation by double-clicking the setup file:

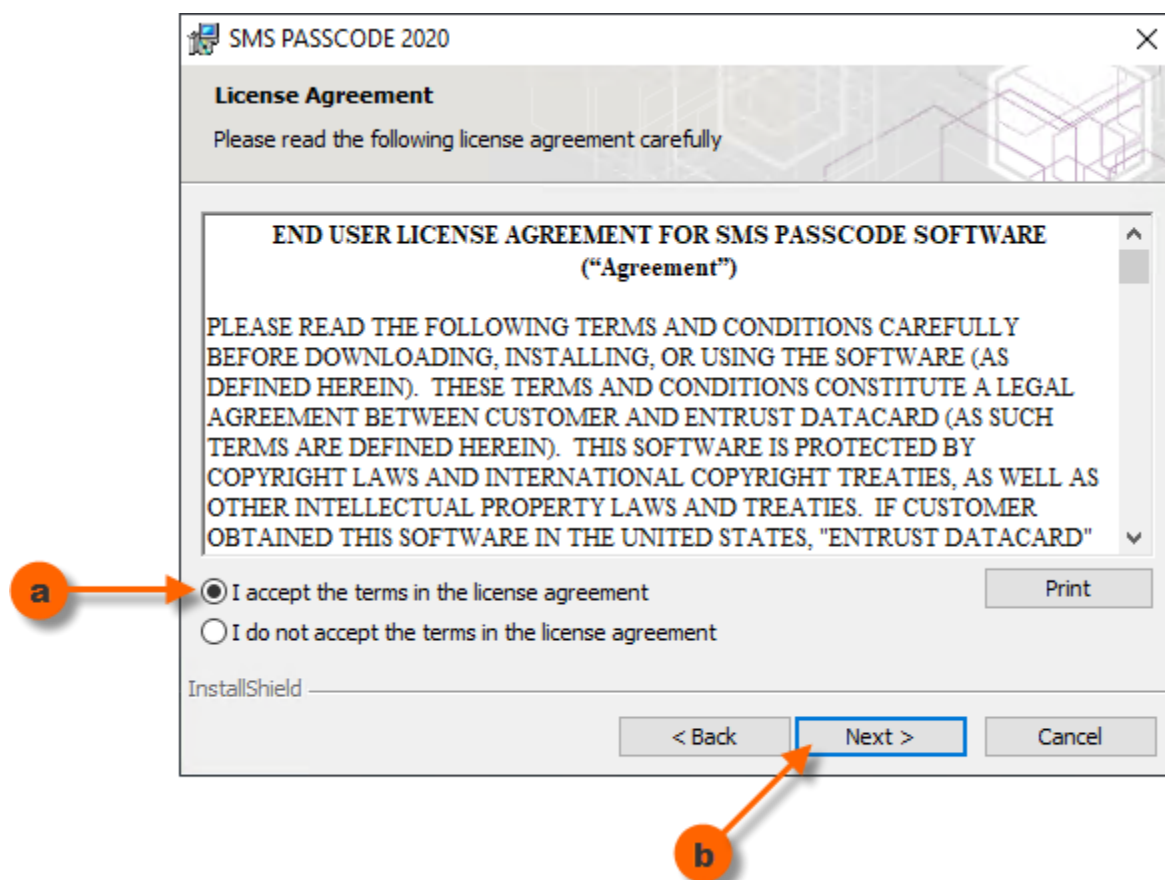


4. A Welcome dialog appears. Click the **Next** button.



(During an upgrade from an earlier version of SMS PASSCODE a notice that an upgrade is about to occur will appear in this window)

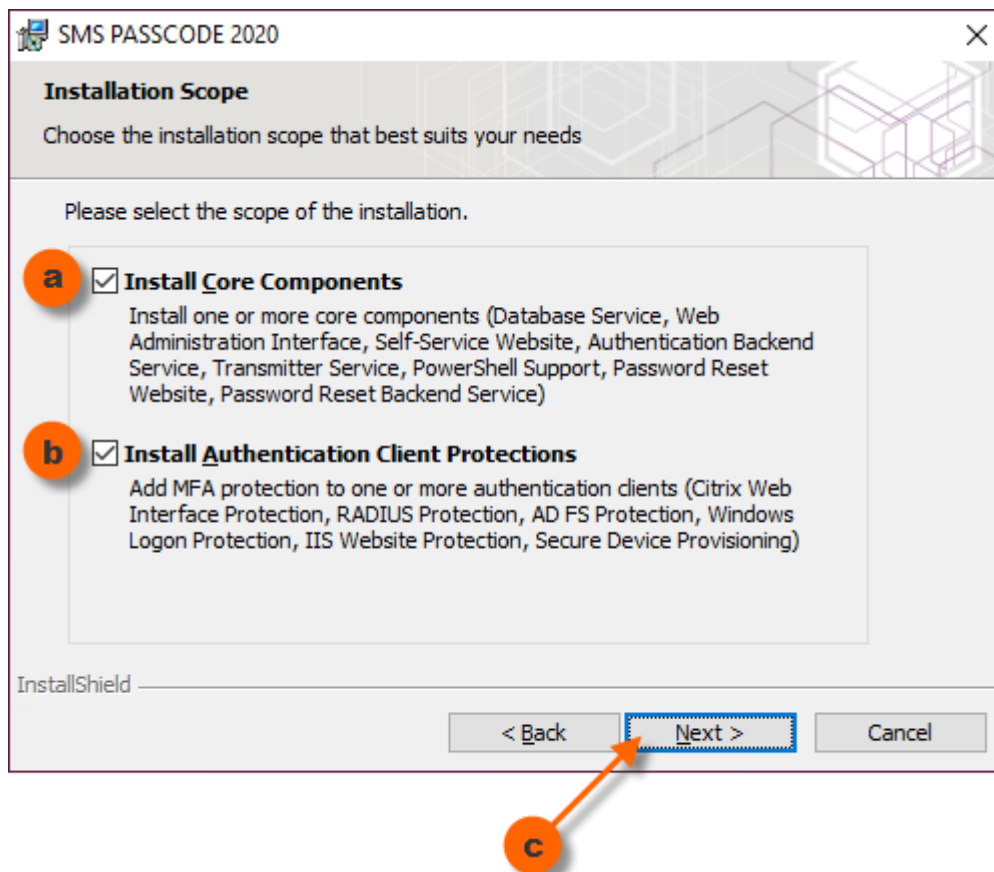
5. An End-User License Agreement (EULA) appears. Please read the agreement carefully. If you accept the EULA:
 - a. Click on **I accept the terms in the license agreement**.
 - b. Click the **Next** button.



6. A dialog for setting the scope of the installation appears. Select one or both available options:
 - a. Select **Install Core Components**, only in case you are planning to install any of the components listed.
 - b. Select **Install Authentication Client Protections**, only in case you are planning to install any of the MFA protections listed.

NOTE: For a **Cloud Setup**, select (b) only.

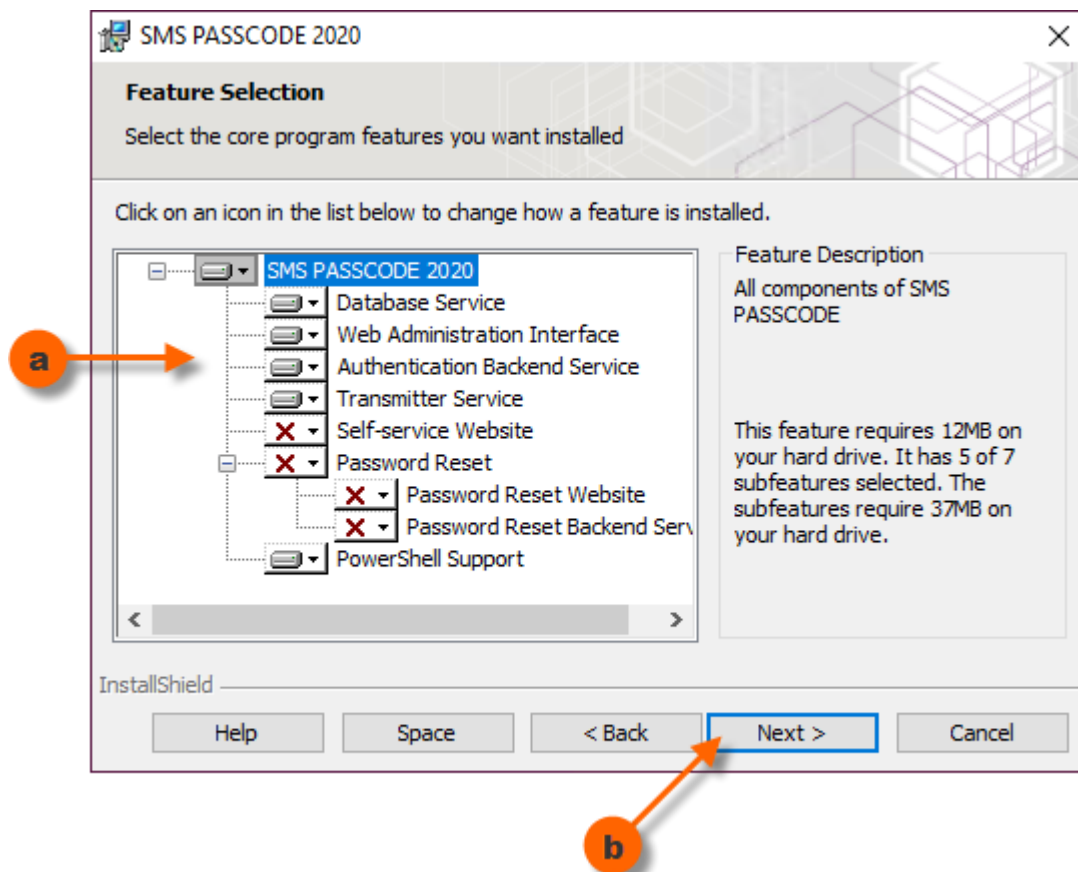
- c. Click the **Next** button.



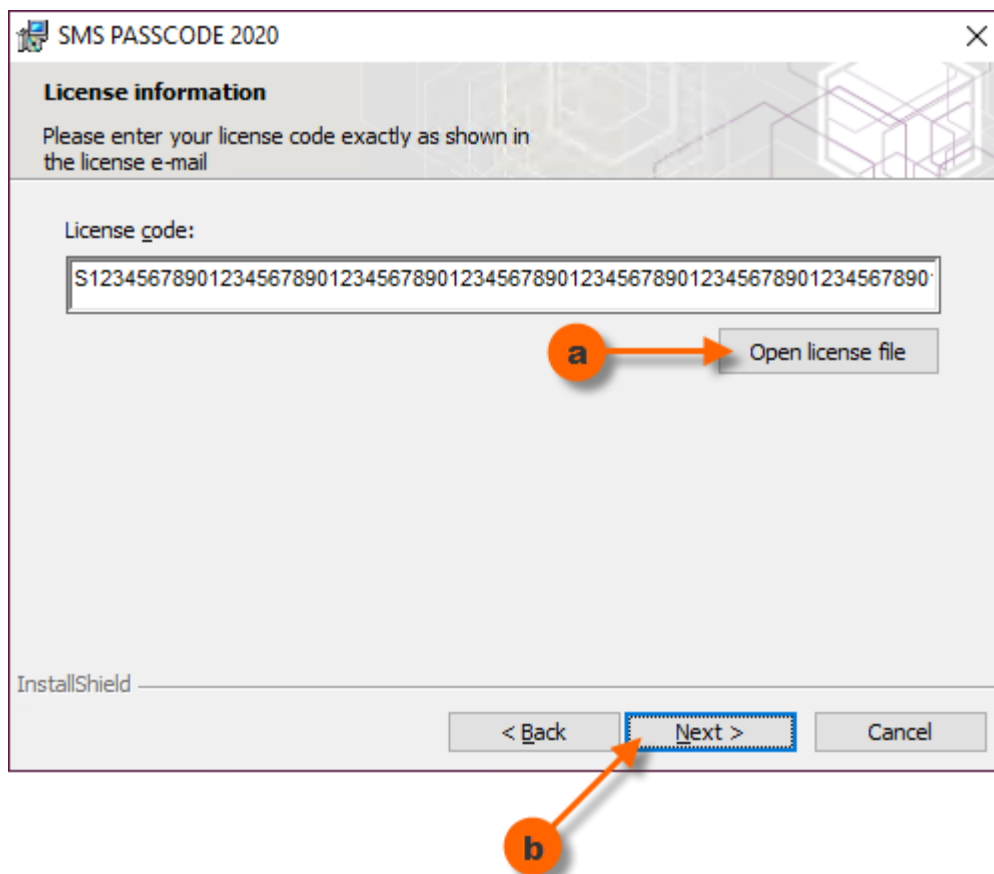
7. If a dialog for feature selection appears, this is where you decide which core components are to be installed on the current machine.
 - a. Make your component selections.

Please note: The selections you make are not permanent. You can always run the installation again afterwards and change your selections (cf. section 15).

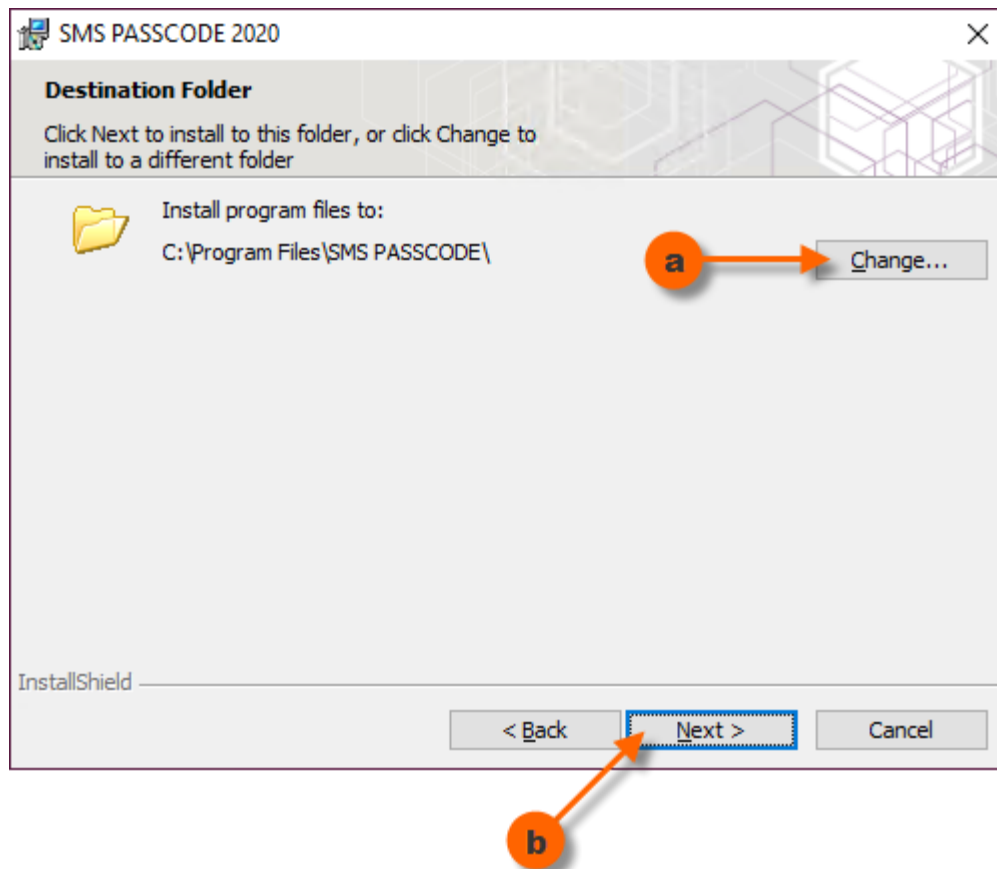
- b. Click the **Next** button.



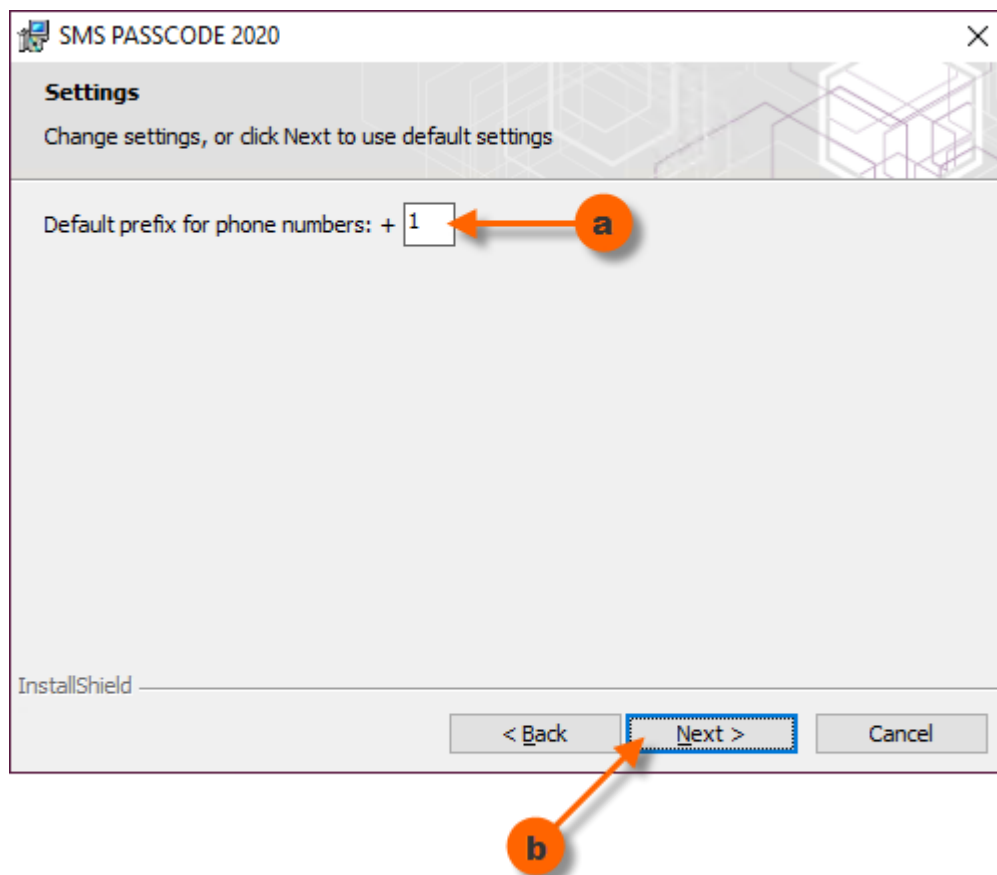
8. If a dialog appears, for entering license information:
 - a. Click the **Open license file** button and select the **License.txt** file that was attached to your SMS PASSCODE license email. The installer will automatically read the license code from the license file and insert it to the **License code** textbox (alternatively you can also manually copy&paste the license code from the **License.txt** file).
 - b. Click the **Next** button.



9. If 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.

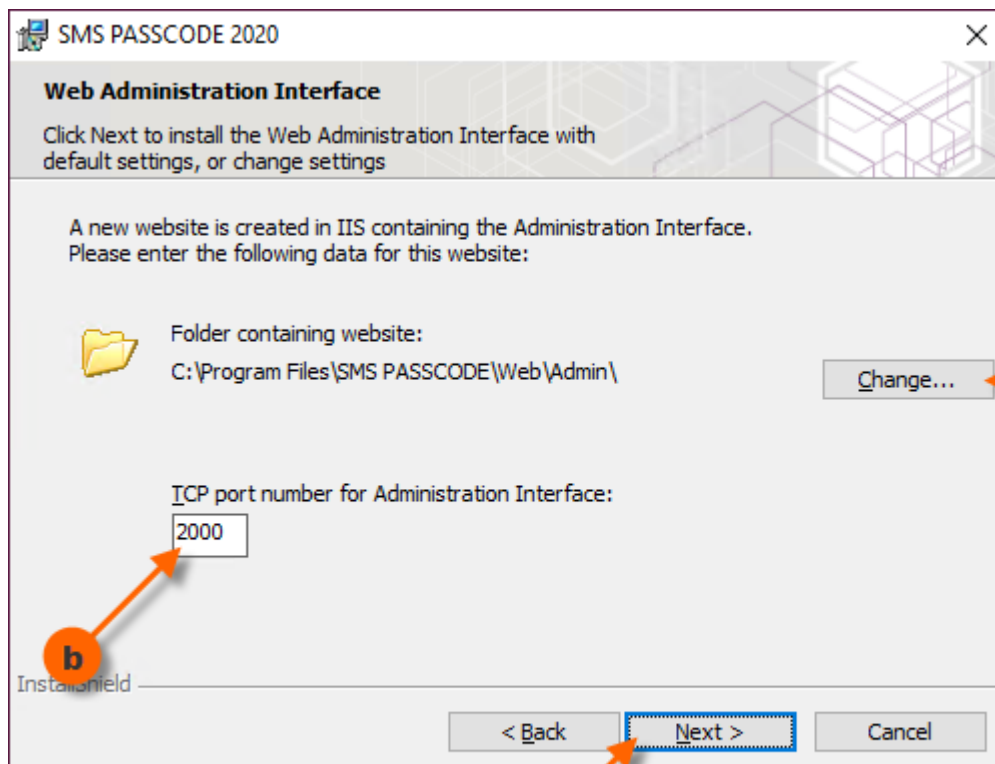


10. If a dialog appears, for specifying the default prefix:
 - a. Specify the default prefix for phone numbers. All phone numbers without an explicit prefix will have this prefix automatically added.
 - b. Click the **Next** button.

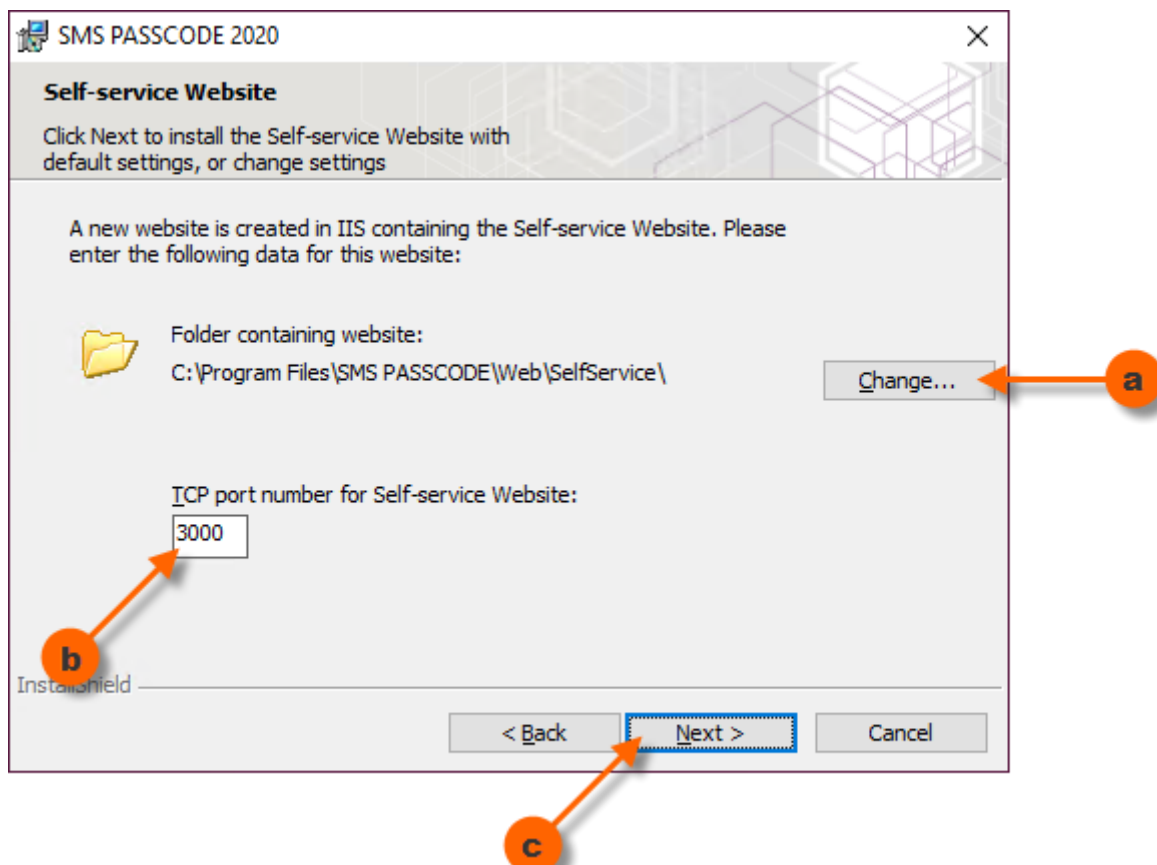


11. If a dialog appears, for setting up the **Web Administration Interface**:

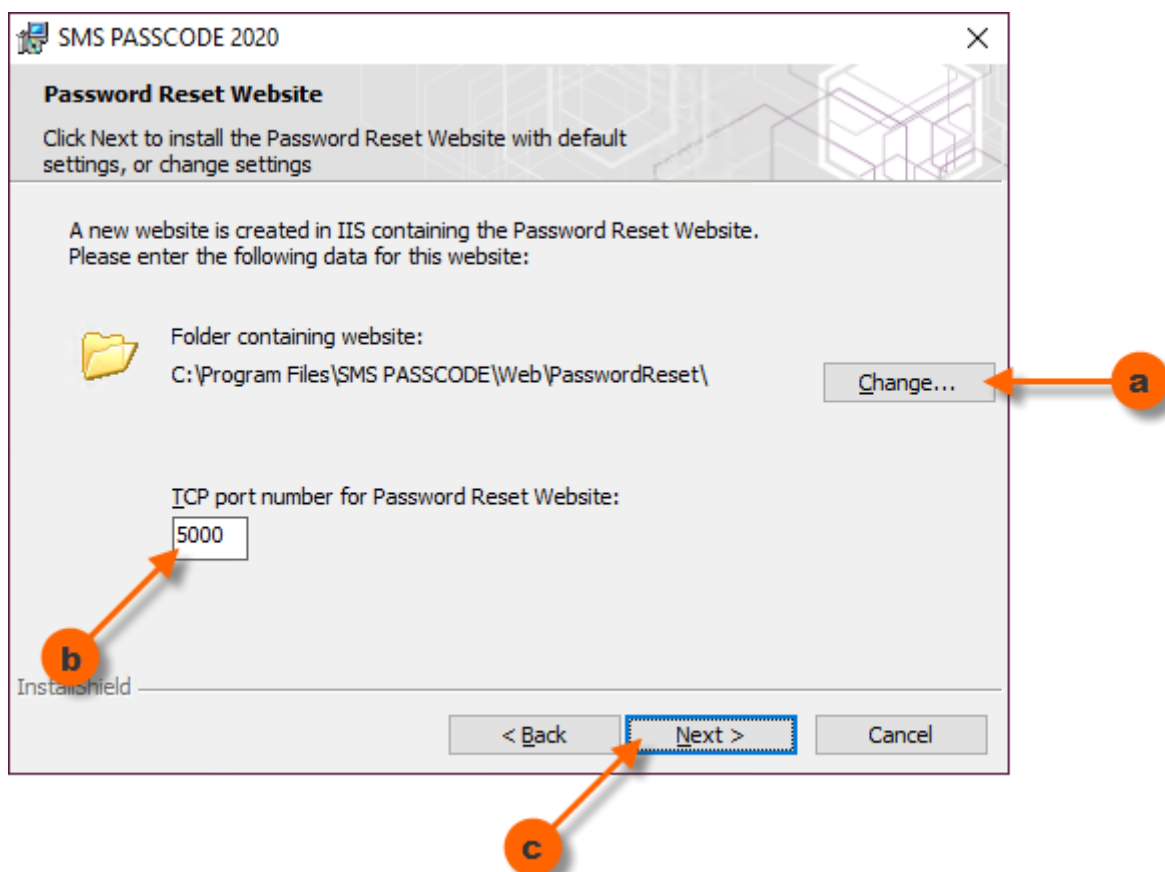
- a. It is recommended to use the proposed default path for the **Web Administration Interface** installation folder. If you want to change the path anyhow: Click the **Change** button and select a new path.
- b. It is recommended to use the proposed default TCP port for the **Web Administration Interface** site. If you want to change the TCP port anyhow, e.g. because of a port conflict with another application or another website, then enter a different TCP port.
- c. Click the **Next** button.



12. If a dialog appears, for setting up the **Self-service Website**:
- It is recommended to use the proposed default path for the **Self-service Website** installation folder. If you want to change the path anyhow:
Click the **Change** button and select a new path.
 - It is recommended to use the proposed default TCP port for the **Self-service Website**. If you want to change the TCP port anyhow, e.g. because of a port conflict with another application or another website, then enter a different TCP port.
 - Click the **Next** button.



13. If a dialog appears, for setting up the **Password Reset Website**:
- It is recommended to use the proposed default path for the **Password Reset Website** installation folder. If you want to change the path anyhow: Click the **Change** button and select a new path.
 - It is recommended to use the proposed default TCP port for the **Password Reset Website**. If you want to change the TCP port anyhow, e.g. because of a port conflict with another application or another website, then enter a different TCP port.
 - Click the **Next** button.



14. If a dialog for selecting **Authentication Clients** appears.
- Select the protection(s) that you would like to install on this machine. Please read section 8 (page 24) for more details on each component. You may also 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 15).

NOTE:

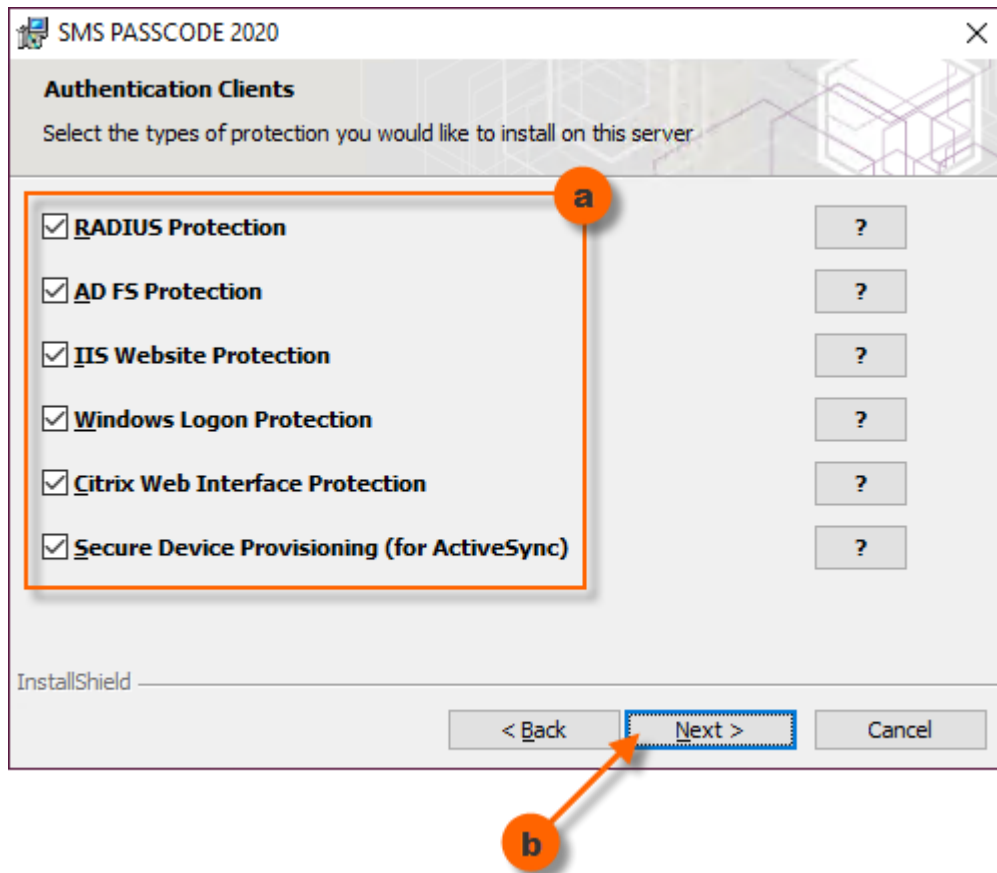
If a component is disabled for selection, this is caused by system requirements not being fulfilled for this component (cf. section 10, page 31)

IMPORTANT (Cloud Setup):

For a **Cloud Setup**, only select among the following authentication clients

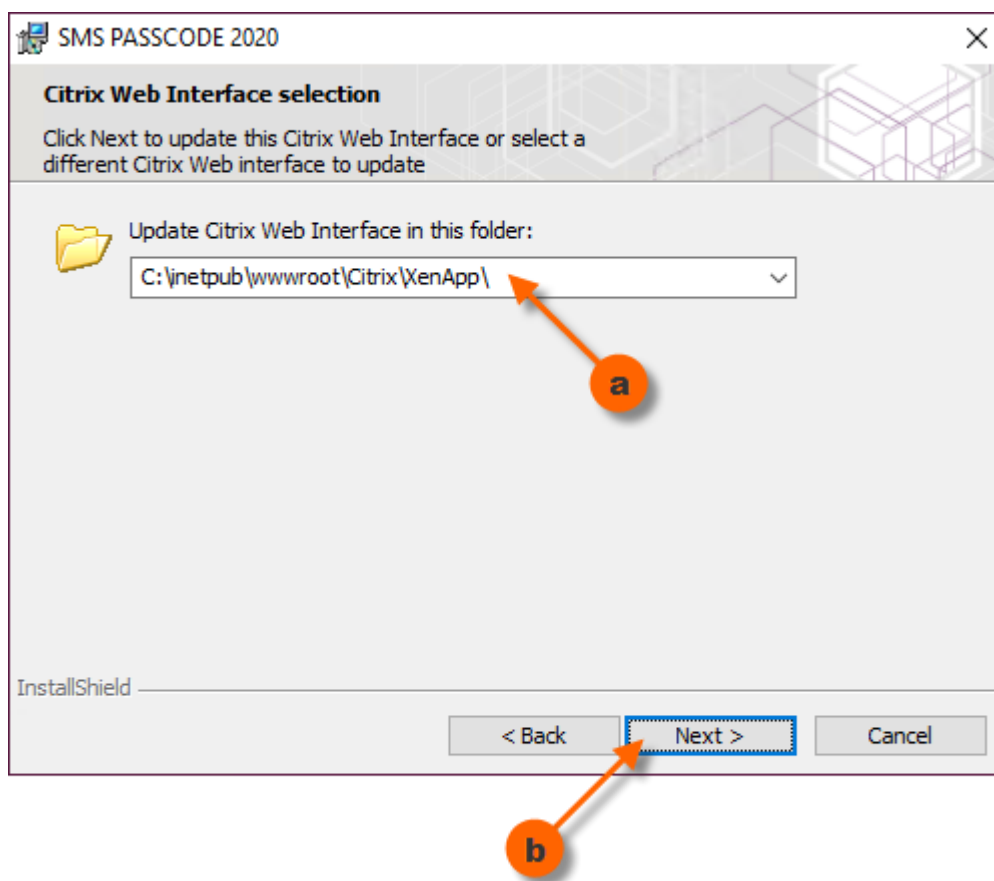
RADIUS Protection, AD FS Protection, IIS Website Protection and Windows Logon Protection.

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



15. If a dialog appears, for selecting the Citrix Web Interface to protect using SMS PASSCODE:

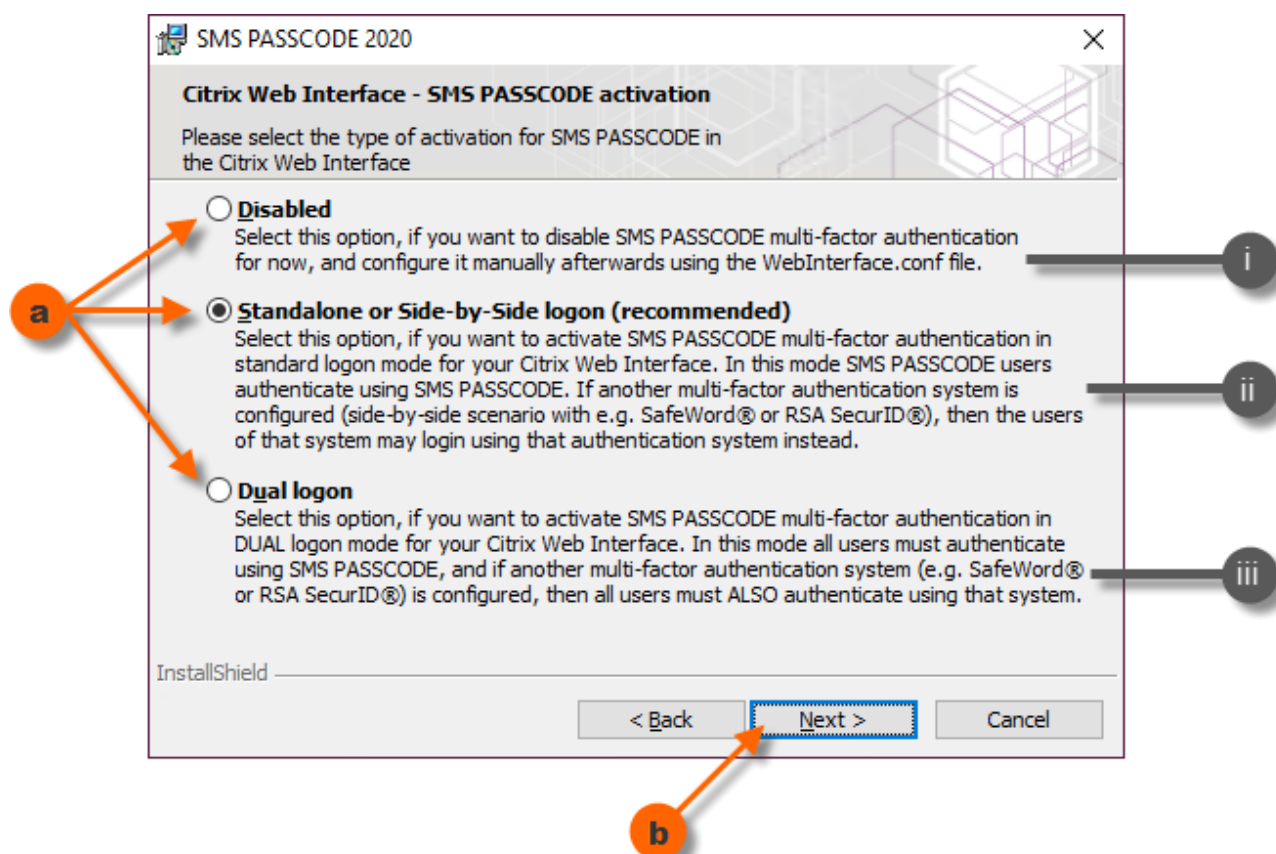
- a. Please select the physical path for the Citrix Web Interface¹⁴ to be protected by SMS PASSCODE authentication.
- b. Click the **Next** button.



¹⁴ 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@entrustdatacard.com for instructions on how to do this.

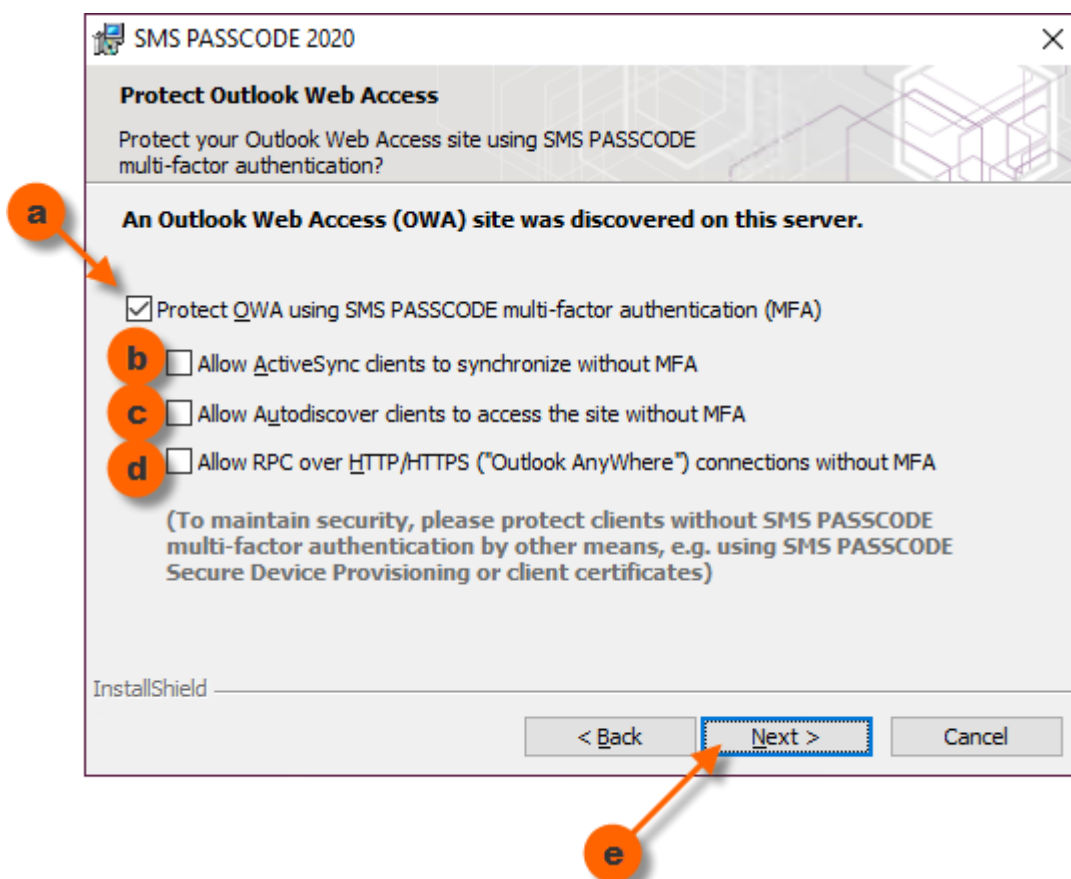
16. If a dialog appears, for selecting the scenario you would like to use for the protection of the Citrix Web Interface with SMS PASSCODE:

- 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 25.1).
 - ii. **Standalone or Side-by-Side logon:** Select this option (recommended) to activate standard SMS PASSCODE authentication. If no other kind of multi-factor 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.

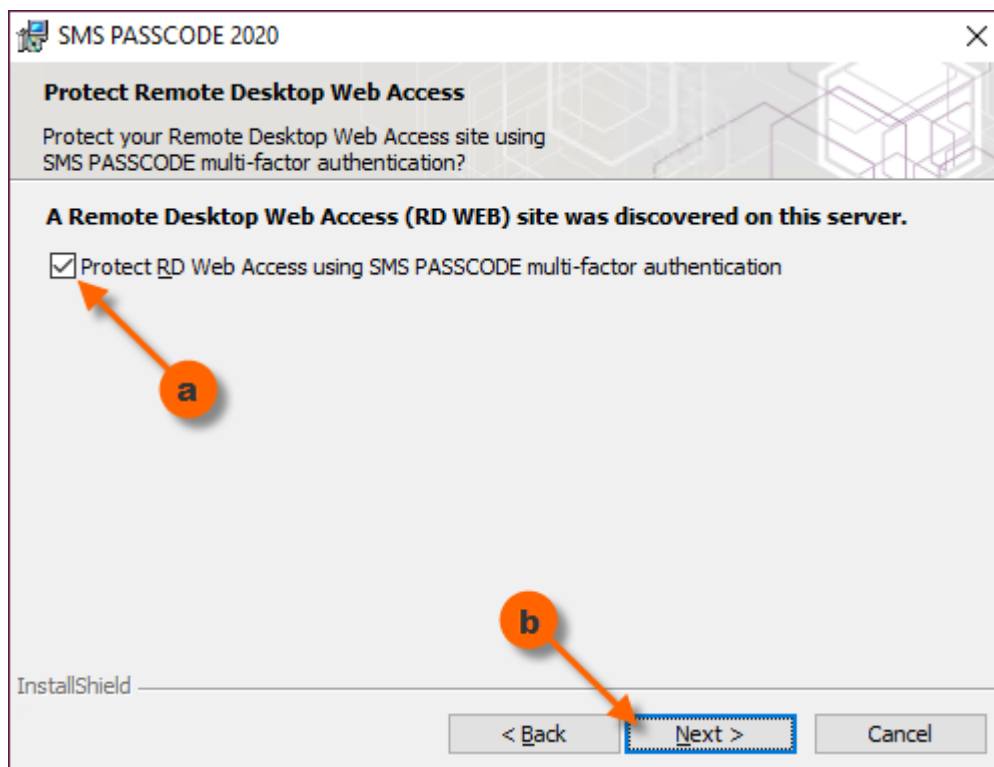


17. If a dialog appears, for configuring SMS PASSCODE protection of an OWA site:

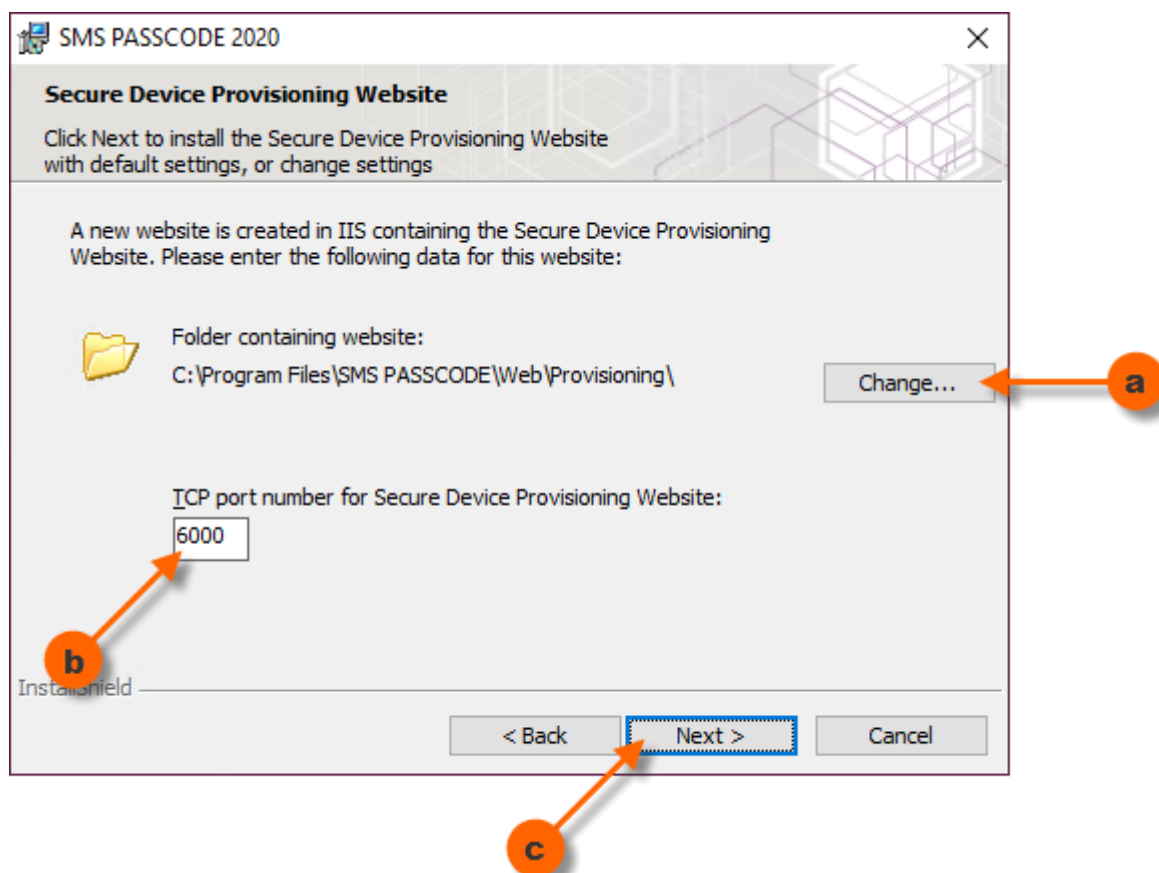
- a. Select this option if the OWA site on the server should be protected using SMS PASSCODE authentication.
- b. Select this option to allow ActiveSync clients to synchronize using the OWA site on this server. In this case, SMS PASSCODE authentication will be disabled for ActiveSync requests. Please maintain security by protecting the ActiveSync clients by other means, e.g. using the SMS PASSCODE Secure Device Provisioning component.
- 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.



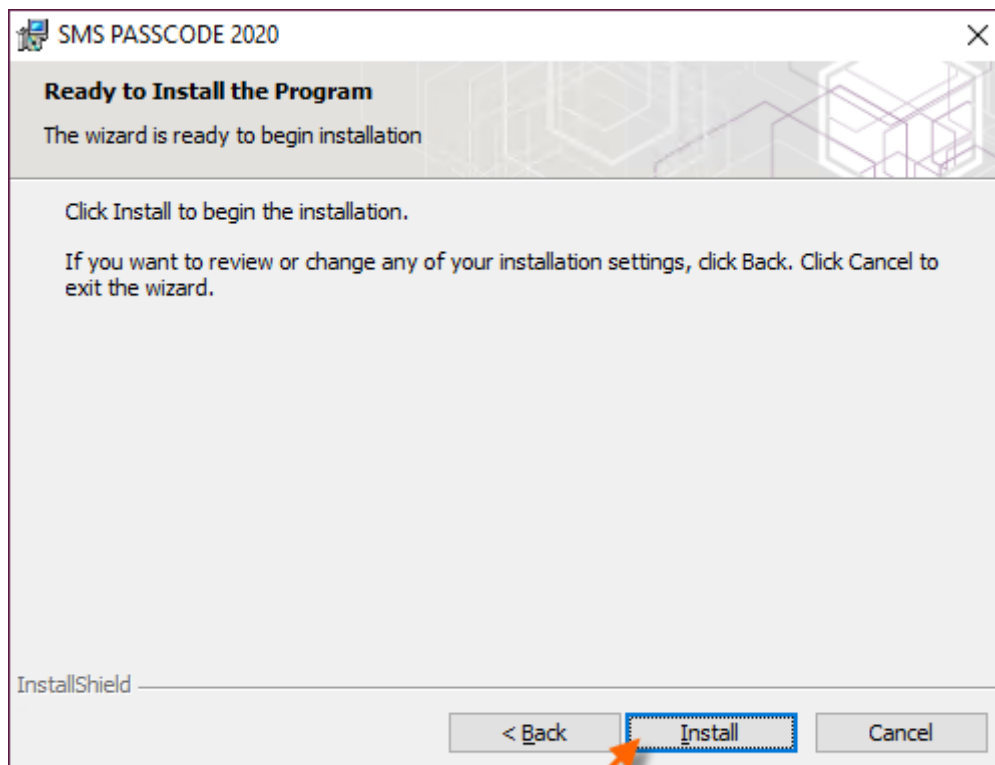
18. If a dialog appears, for configuring SMS PASSCODE protection of an RD Web Access site (only supported on Windows Server 2008 R2, 2012 R2 and 2016, cf. section 10.2, page 36):
- Select this option if the RD Web Access site on the server should be protected using SMS PASSCODE authentication.
 - Click the **Next** button.



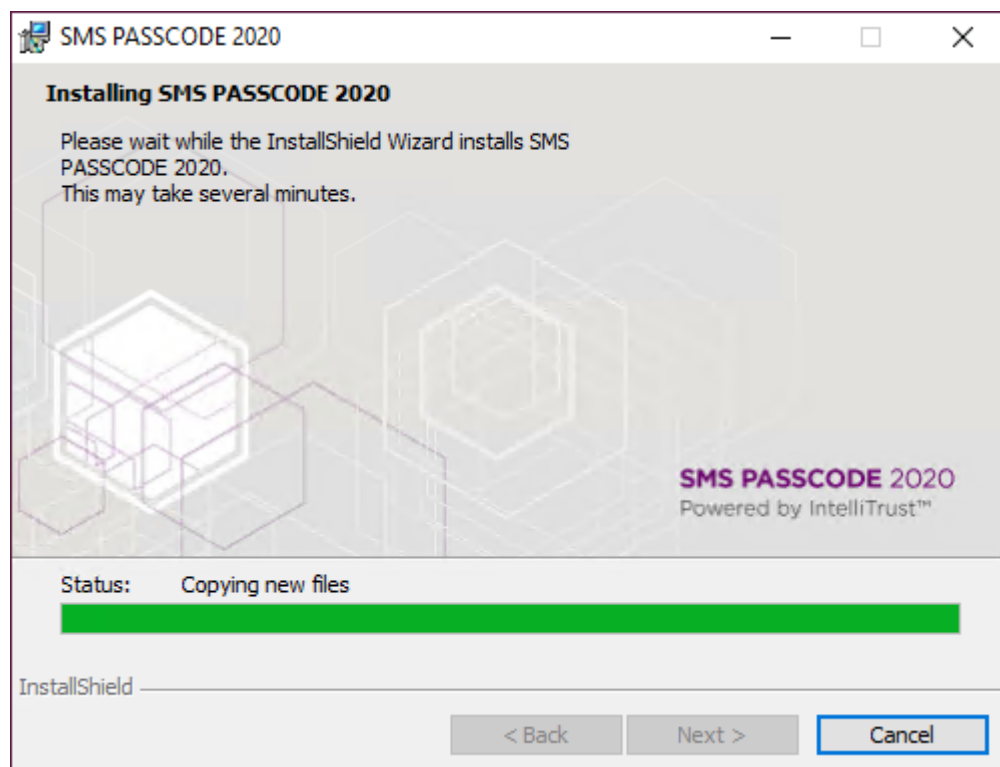
19. If a dialog appears, for setting up the **Secure Device Provisioning Website**:
- It is recommended to use the proposed default path for the **Secure Device Provisioning Website** installation folder. If you want to change the path anyhow: Click the **Change** button and select a new path.
 - It is recommended to use the proposed default TCP port for the **Secure Device Provisioning Website**. If you want to change the TCP port anyhow, e.g. because of a port conflict with another application or another website, then enter a different TCP port.
 - Click the **Next** button.



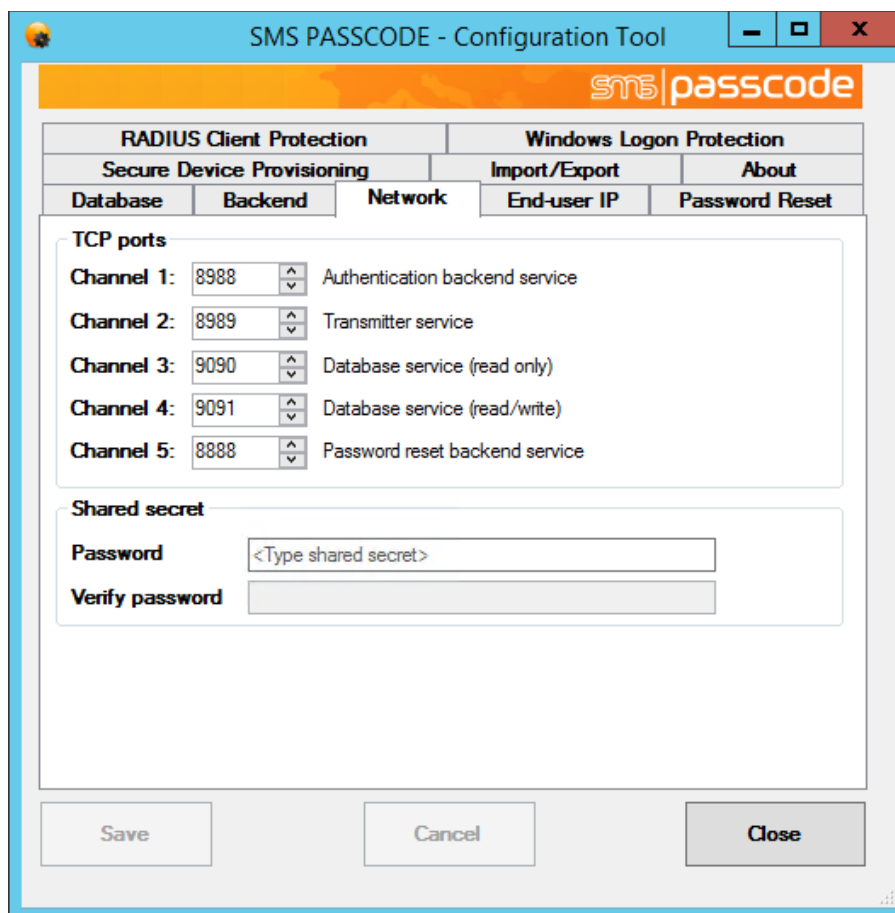
20. You are now ready to perform the installation according to the choices you have made. Click the **Install** button.



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



22. At some stage during the installation, the **SMS PASSCODE Configuration Tool** is automatically started (except during an upgrade, because in this case the settings from the previous installation are preserved):

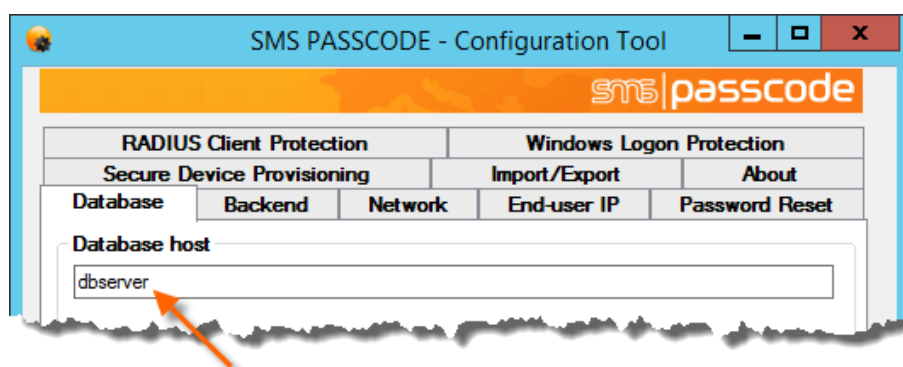


This tool is used, among others, for configuring the SMS PASSCODE infrastructure, i.e. you use this tool to specify where the different SMS PASSCODE components are located and how they should communicate with each other. You may not see all the tabs shown in the picture above because the user interface of the **SMS PASSCODE Configuration Tool** is automatically adapted according to the components installed on the current machine.

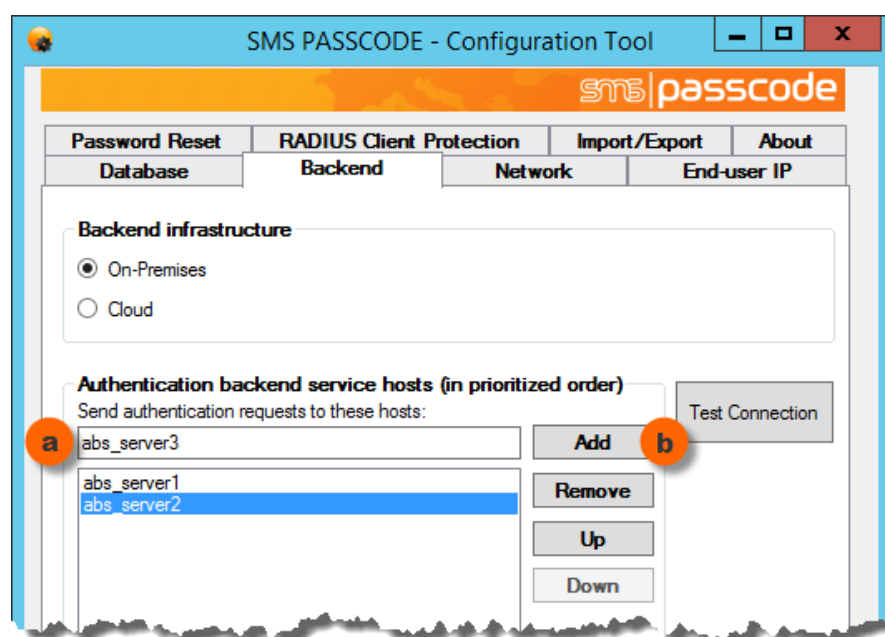
You must now configure the SMS PASSCODE infrastructure and save the settings before the SMS PASSCODE installation is complete. Please follow the instructions below.

On-premise or Hybrid Setup:

- a. In case you have installed **Authentication Backend Service**, **Transmitter Service**, **Self-service Website** or **PowerShell Support** on the current machine, and the **Database Service** component is not installed on the current machine, you must specify where the database server is located. To do this, please specify the host name of the database server in the field **Database host** on the **Database** tab:



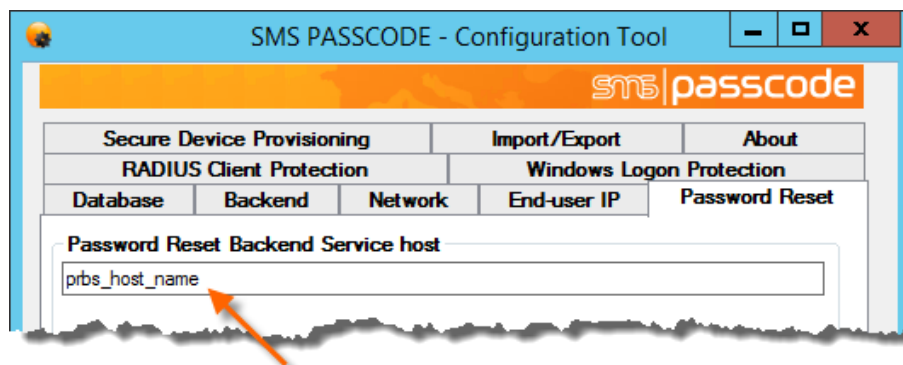
- b. If you have installed the **Password Reset Backend Service** or an *SMS PASSCODE Authentication Client* on the current machine, you must specify where Authentication Backend Services are located. These services are used to handle authentication sessions and request message transmissions. You can specify a list of one or more Authentication Backend Service hosts. This is configured on the **Backend** tab. To specify a list of such hosts, enter the host name of the servers running the **Authentication Backend Service**. Specify the host name of each server (a) and add it to the list by clicking the **Add** button (b):



The authentication client will always try to locate an **Authentication Backend Service** in the specified order, i.e. the order of the hosts in the list is of importance.

In case of communication problems with the higher prioritized hosts, the authentication client will automatically communicate with lower prioritized hosts (failover).

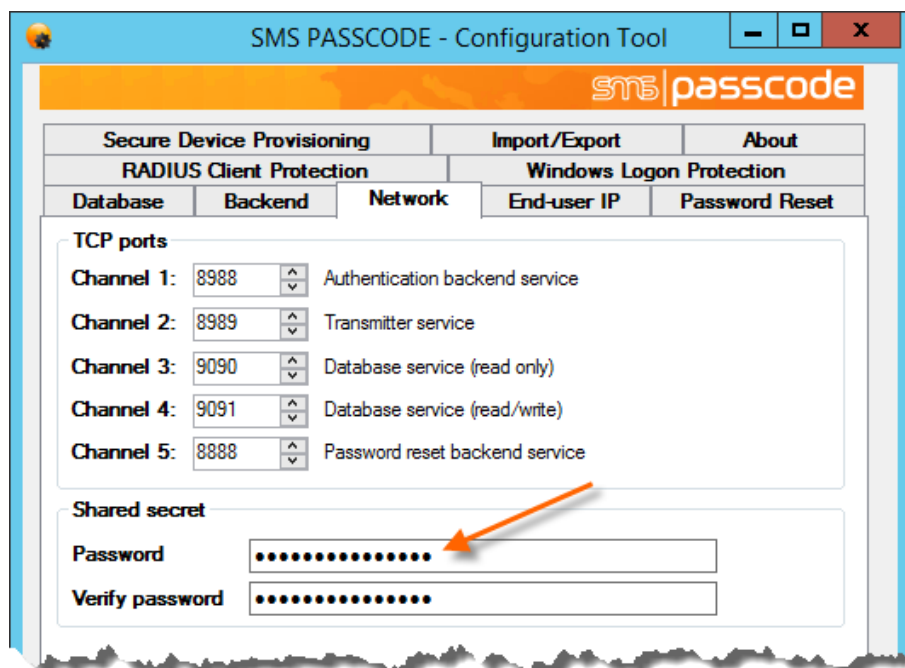
- c. If you have installed the SMS PASSCODE **Password Reset Website** on the current machine, then you must specify where a **Password Reset Backend Service** is located. To do this, please specify the host name of the PRBS server in the field **Password Reset Backend Service host** on the **Password Reset** tab:



- d. The **Network** tab lists the TCP ports used for communication between the SMS PASSCODE components (cf. section 11.1, page 44). If some TCP port fields are disabled and cannot be changed, this is because they are not in use by the current machine. It is recommended to use the default TCP ports proposed. However, in case of TCP port conflicts with other applications you may change some TCP ports on this tab.

Important: The TCP ports must match each other on all machines having SMS PASSCODE components installed. If you plan to change one or more TCP ports, please change these TCP ports in the same manner on all machines. If this is not observed, then communication will fail.

Finally, you must enter a **Shared Secret** on the **Network** tab. This is a secret password that is used for encrypting all messages exchanged between the SMS PASSCODE components. To ensure that security is not compromised, a password with a minimum length of 15 characters is required. It is recommended to use letters, digits, and special characters in the password:



Important: Always remember to specify a Shared Secret.

Please enter the same **Shared Secret** on all machines having SMS PASSCODE components installed. If this is not observed, then communication will fail.

- e. Click the **Save** button.

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

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

Cloud Setup:

- a. To switch to **Cloud Setup**, on the **Backend** tab set the **Backend infrastructure** to **Cloud** (a). Then enter the URL of the IntelliTrust™ tenant to which you want to connect (b). Finally, enter the IDs that uniquely identify the Application(s) of type “Authentication API” within your IntelliTrust™ tenant that your SMS PASSCODE Authentication Clients must use to connect to the IntelliTrust™ cloud service (c). You can either use the same IDs for all your SMS PASSCODE Protections, or decide to use separate ones. It is only recommended to use separate ones, in case you wish to be able to define separate authentication flows (“Resource rules”) in IntelliTrust™ per SMS PASSCODE Authentication client.

Finally, click the **Test Connection** button (d) to test the validity of your entries¹⁵.

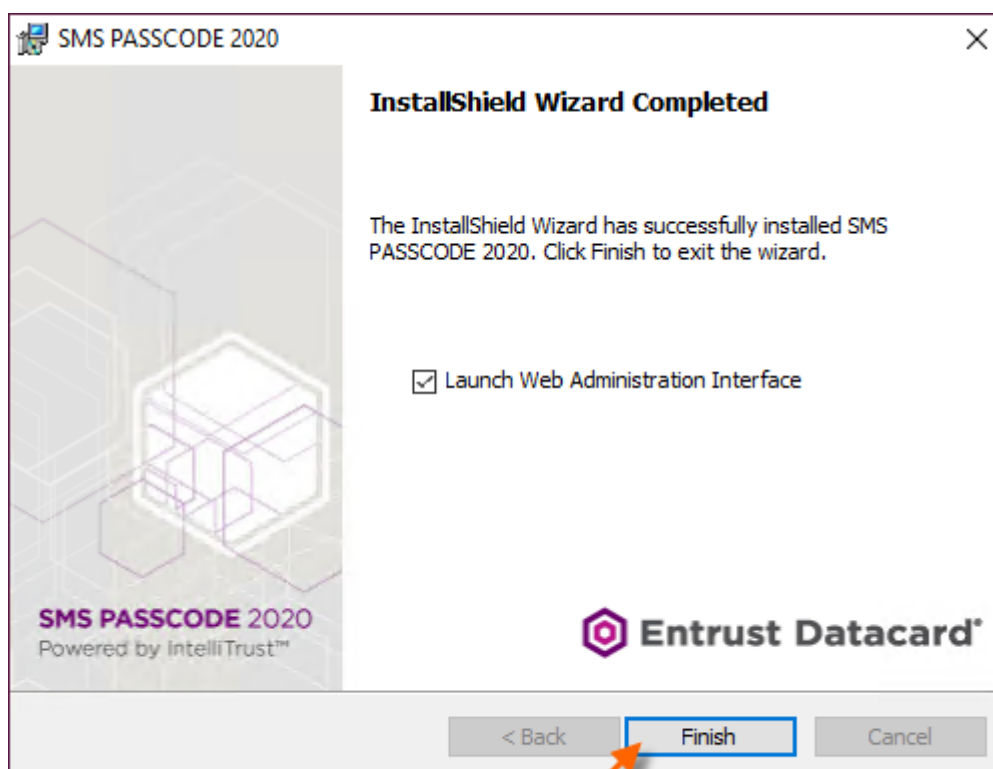
- b. Click the **Save** button.

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, then you can always run the **SMS PASSCODE Configuration Tool** again manually. A shortcut to this tool is created in the Windows Start menu.

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



24. The installation of SMS PASSCODE is now complete on the current machine. You should now perform any necessary configurations of this machine (cf. section 16). This is especially important if you have just installed the **Database Service** and **Web Administration Interface** on the current machine. In this case, you should now start the **Web Administration Interface** and...

- a. authorize all servers planned to run the **Transmitter Service**
- b. authorize all servers planned to run the **Authentication Backend Service**
- c. create modems, Email Connectors and Dispatch Connectors, as needed, in the database.

25. If more machines are part of the installation: Please go back to step 1 (page 69) and follow the same instructions for the next machine.

14.3 Unattended Installation and Uninstallation

NOTE: This section only applies to SMS PASSCODE installations in the **On-premise** or **Hybrid Setup**.

SMS PASSCODE has support for fully unattended installation and uninstallation.

Unattended install/uninstall support is provided by means of two PowerShell scripts, provided in the SMS PASSCODE download package in the "SilentInstall" folder:

- `Install-Smspc.ps1`: Used for unattended install (or unattended modify of an existing installation).
- `Uninstall-Smspc.ps1`: Used for unattended uninstall.

To get more details on the usage of these scripts, please use the "help" command in PowerShell. I.e. to get full help, use the following commands (commands must be executed from within the path, where the scripts are located):

```
Get-Help .\Install-Smspc -Full
```

```
Get-Help .\Uninstall-Smspc -Full
```

Below are some examples on the usage of the PowerShell scripts:

- Example 1: Unattended installation of the SMS PASSCODE Database Service, Authentication Backend Service, Transmission Service, Web Administration Interface and Self-service Website on the same server:

```
.\Install-Smspc -InstallComponent DbService,  
AuthenticationBackendService,TransmitterService,WebAdminInterface,  
SelfServiceWebsite -SharedSecret [SharedSecret]  
-LicenseCode [LicenseCode] -Action Execute
```

- Example 2: Unattended installation of SMS PASSCODE RADIUS Protection only:

```
.\Install-Smspc -InstallProtection Radius -SharedSecret [SharedSecret]  
-Action Execute
```

- Example 3: Unattended uninstall:

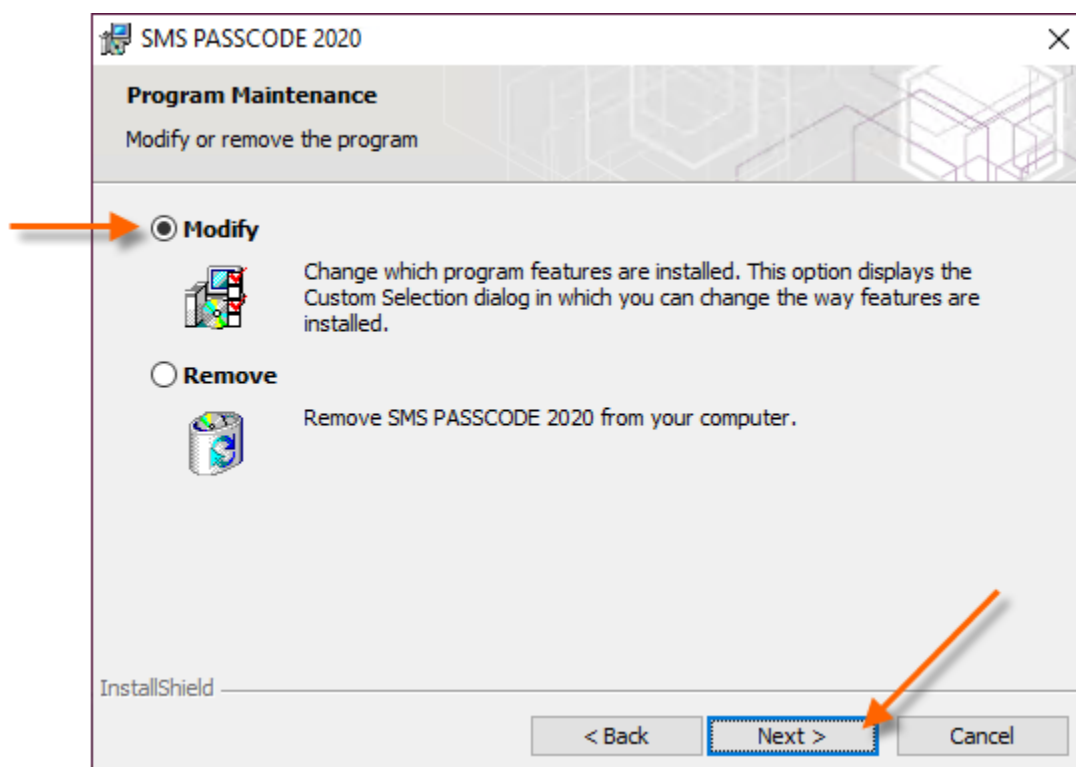
```
.\Uninstall-Smspc -Action Execute
```

If you want to combine unattended installation with unattended configuration, then note that you can call the SMS PASSCODE Configuration Tool from the command line to import and apply SMS PASSCODE settings (cf. section 26.3, page 428). Additionally, you can use SMS PASSCODE PowerShell cmdlets to automate administrator tasks (cf. section 18, page 308).

15 ADD/REMOVE COMPONENTS

If you wish to add or remove some components from an 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 core components and/or *SMS PASSCODE Authentication Clients*.

To add/remove components, 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.

16 POST-INSTALLATION ACTIONS

After having completed the SMS PASSCODE installation, you should perform some configurations, before SMS PASSCODE is ready for use:

Cloud Setup:

- Configuration of the **RADIUS Protection** component.
Please read section 25.2 (page 377).
- Configuration of the **AD FS Protection** component.
Please read section 25.3 (page 400).
- Configuration of the **IIS Website Protection** component
Please read section 25.4 (page 407)
- Configuration of the **Windows Logon Protection** component
Please read section 25.5 (page 415)

On-premise or Hybrid Setup:

- 1) Use the **Web Administration Interface** for the following tasks:
 - a. Configuring general SMS PASSCODE settings
 - b. Configuring SMS PASSCODE policies
 - c. Maintaining SMS PASSCODE user settings
 - d. Maintaining the SMS PASSCODE transmission and authentication infrastructure

Please read section 17 for a detailed description of the SMS PASSCODE Web Administration Interface.

NOTE: Remember to enable required General Settings

It is recommended to review the options on all tabs of the **General Settings** page in the **Web Administration Interface** carefully after installation. Initially, the product is installed with all advanced options disabled. You might miss out important features that could be valuable to you (AD Integration, IntelliTrust™ integration, Authentication Monitoring, Geo-IP, MFA bypassing, and more).

General settings are described in section 17.3 (page 108).

In case you decide to enable IntelliTrust™ integration, e.g. to make use of *push authentication*, please read section 16.2 (page 99) for details on important configuration actions.

- 2) Configuration of *SMS PASSCODE Authentication Clients*:
 - a. Configuration of the **Citrix Web Interface Protection** component.
Please read section 25.1 (page 376).
 - b. Configuration of the **RADIUS Protection** component.
Please read section 25.2 (page 377).

- c. Configuration of the **AD FS Protection** component.
Please read section 25.3 (page 400).
 - d. Configuration of the **IIS Website Protection** component.
Please read section 25.4 (page 407).
 - e. Configuration of the **Windows Logon Protection** component.
Please read section 25.5 (page 415).
 - f. Configuration of the **Secure Device Provisioning** component.
Additional steps are required after installation of the Secure Device Provisioning component before it is ready for use. Please read section 24 (page 363), in particular subsection 24.2.
- 3) Optionally configure the **SMS PASSCODE Self-service Website** to use form-based authentication.
Please read section 22.5 (page 328).
 - 4) Complete setup of the **SMS PASSCODE Password Reset Website**.
Additional steps are required after installation of the PRWS component before it is ready for use. Please read section 23.6 (page 349).
 - 5) Complete setup of the **SMS PASSCODE Password Reset Backend Service**.
Additional steps are required after installation of the PRBS component before it is ready for use. Please read section 23.7 (page 350).

Additionally, the **SMS PASSCODE Configuration Tool** allows you to perform various tasks, like re-configuring the SMS PASSCODE infrastructure and changing settings for some authentication clients. Please read section 25.5.5 (page 420) for more details regarding the configuration tool.

Finally, for enhanced security you might decide to enable *location and behavior aware authentication*. Please note, that this is an advanced topic, and the related features are disabled by default. If you are new to SMS PASSCODE, then it is recommended to get the SMS PASSCODE system up and running first, without *location and behavior aware authentication* enabled. Then afterwards, study the features related to *location and behavior aware authentication* and consider, whether and how to make use of them. The following subsection introduces the concept of *location and behavior aware authentication* and gives you an overview regarding the possibilities.

16.1 Overview: Location and Behavior Aware Authentication

NOTE: This section only applies to SMS PASSCODE installations in the **On-premise** or **Hybrid Setup**. For a **Cloud Setup**, authentication behavior is configured in the IntelliTrust™ admin portal.

SMS PASSCODE contains patented technology that optionally lets you enable advanced features for even stronger security. The common term for these features is *location and behavior aware authentication*. This section explains the purpose of these features. Please note that these advanced features are disabled by default, thereby ensuring that the SMS PASSCODE system works out-of-the-box without the necessity to get familiar with the advanced settings, before you decide to.

Location and behavior aware authentication actually refers to two different, but related features that can enhance security during authentication attempts:

- *Location aware authentication*: Refers to the fact that the SMS PASSCODE system can determine facts about the location, from which a user is attempting to perform a login. These facts are determined from the end-user's IP address. Currently the SMS PASSCODE system can determine the **country** of the IP address and the name of the **organization** owning the IP address.
- *Behavior aware authentication*: Refers to the fact that the SMS PASSCODE system can remember the history of earlier used end-user IP addresses and thereby identify whether new logon attempts comply with earlier behavior or not.

The pre-requisites for using *location and behavior aware authentication* are:

- The SMS PASSCODE authentication client used must support *location and behavior aware authentication*. Please check the requirements in section 10.1 (page 35).
- Collection of end-user IP addresses must have been enabled for the authentication client(s) in question. This is configured using the SMS PASSCODE Configuration Tool (cf. section 26.2, page 424).
- The setting **Geo IP and IP history** must have been enabled on the **General Settings** page of the SMS PASSCODE Web Administration interface (cf. section 17.3.1, page 109).

When these pre-requisites are fulfilled, a lot of additional features and possibilities for customization become available. In that case, you should understand the following concepts and terms:

- **User IP History**
The SMS PASSCODE system will start recording an individual history of IP addresses used during authentication attempts by each user.

The *User IP History* feature is described in more detail in 17.10.2 (page 247).

- **IP Trust Level**
Each end-user IP address listed in a user's *User IP History* is assigned a *Trust Level*. This level is zero initially but can be configured to increase on each successful multi-factor authentication completed from the IP address. By default, the *Trust Level* increases by 1 on each successful multi-factor authentication, but this is customizable using the **Authentication Policy** assigned to the user. If you do not wish to make use of *behavior aware authentication*, then you should configure the Authentication Policy NOT to increase the *Trust Level*.
- **Trusted IP address**
An IP address is treated as a *Trusted IP* when its *Trust Level* has reached a specific value, called the *Trust Level Threshold*. This threshold is defined by the **Authentication Policy** assigned to the user. An IP address is treated as *Non-Trusted*, until it becomes *Trusted*.
- **Passcode Policy**
Using **Passcode Policies**, you may define the exact content to be shown in the passcode messages sent to users during SMS PASSCODE multi-factor authentication. For example, you may define whether location specific information should be shown in the messages (country and/or organization). This is the *location aware* part. Additionally, Passcode Policies let you define distinct message content for authentication requests originating from

Trusted or *Non-Trusted* end-user IP addresses, respectively. This is the *behavior aware* part. All in all this makes more contextual information available for users during authentication, thereby giving them the chance to become alerted in case of any irregularities.

Passcode Policies are described in more detail in section 17.7 (page 184).

- **Learning mode**

Learning mode is an optional feature that lets you define an initial temporary period where specific message content is shown in the passcode messages sent to a user. This allows you to override the message content for an initial period, until the system has become aware of *Trusted* and *Non-Trusted* IP addresses of the user. *Learning Mode* is configured on the **Authentication Policy** assigned to the user.

- **Authentication Policy**

As stated above, **Authentication Policies** allow you to define *Trust Level Threshold*, increase of IP address *Trust Level* during authentications, and *Learning Mode* activation. Additionally, Authentication Policies allow you to customize the authentication behavior itself using *Authentication Rules*, thereby making authentications *location and behavior aware*. An example could be to deny authentications from specific locations. Additionally, Authentication Policies allow you to override the effective Dispatch Policy and Passcode Policy to use depending on the actual authentication context. This is also called *adaptive message dispatching*.

Authentication Policies are described in more detail in section 17.8 (page 193).

16.2 Overview: IntelliTrust™ Integration

NOTE: This section only applies to an SMS PASSCODE installation that is going to be configured as a **Hybrid Setup**.

SMS PASSCODE allows you optionally to integrate with the IntelliTrust™ cloud service, which allows you to utilize additional cloud authentication mechanisms. Among others it provides push authentication, and a risk-based authentication engine. Please read section 3 for more details on the IntelliTrust™ cloud service.

The required steps for enabling IntelliTrust™ authentication are described below:

Hybrid Setup:

1. Enable IntelliTrust™ integration on the **General Settings** page of the Web Administration Interface, thereby connecting your SMS PASSCODE backend to a dedicated IntelliTrust™ tenant (cf. section 17.3.4.1, page 119).
2. Verify that all SMS PASSCODE users are synchronized successfully to your IntelliTrust™ tenant (see section 17.10.6, page 252).
3. Log in to the IntelliTrust™ tenant, and configure it. At least, you need to:
 - a. Create an application of type **Authentication API**. You can use this guide:

https://entrust.us.trustedauth.com/documentation/help/admin/index.htm#t=Resources%2FManaging_API_Integrations%2FAdd_Authentication_API_application_to_IntelliTrust.htm

IMPORTANT: When creating the Application, set the setting **Source of the Client IP Address for Risk Conditions** to the value **Provided in the API**. This will allow SMS PASSCODE to forward end-user IPs to the risk-engine of IntelliTrust™ during authentication attempts.

- b. Add a **Resource Rule** to the Application created above, that defines the authentication behavior according to your needs. For more information, see:

https://entrust.us.trustedauth.com/documentation/help/admin/index.htm#t=Security%2FEnter_resource_rule_general_settings.htm

In the Resource Rule, set the **First Factor** to **External Password**, to allow SMS PASSCODE to perform password validation. If you optionally want to bypass multi-factor authentication in some cases, e.g. in the “Low Risk” category, you must clear all checkboxes in the **Second Factors** list.

4. Configure via your SMS PASSCODE **Authentication Policies** when to make use of IntelliTrust™ authentication (see section 17.8.2.5, page 204).

17 WEB ADMINISTRATION INTERFACE

NOTE: This section only applies to SMS PASSCODE installations in the **On-premise** or **Hybrid Setup**.

The SMS PASSCODE **Web Administration Interface (WAI)** provides a graphical user interface, where you can:

- Configure SMS PASSCODE settings
 - General settings
 - License information
- Configure SMS PASSCODE policies
 - User Integration Policies
 - User Group Policies
 - Authentication Policies
 - Passcode Policies
 - Dispatch Policies
 - Token Policies
- Maintain SMS PASSCODE user settings
- Maintain hosts
 - Maintain Authentication Backend Service hosts
 - Maintain Transmitter Service hosts
- Maintain SMS PASSCODE transmission settings
 - Maintain message dispatchers (Modems, Email Connectors, Dispatch Connectors)
 - Maintain modem groups
- Monitor current and past authentication attempts
- Monitor status of all modems

In the following subsections, **WAI** is used as a shorthand for **Web Administration Interface**, and **WAI server** designates the server on which **WAI** is installed.

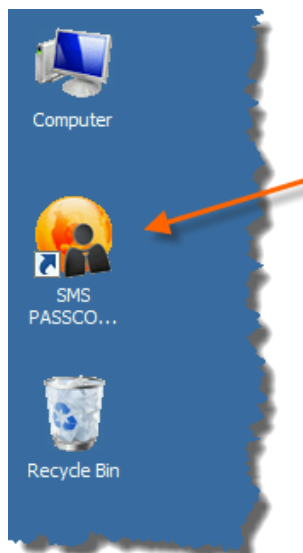
By default, only members of the Administrators group have permissions to access the WAI. Non-administrators can be granted permission to access the WAI by adding them to the local Windows user group "SMS PASSCODE Administrators". Furthermore, distinct permissions within the WAI can be assigned to different administrator roles (cf. section 20 for more details on this).

Please note, that many administrator tasks can also be performed using PowerShell scripts, which can for example be advantageous in case of automation. PowerShell support is described in section 18 (page 308).

17.1 Starting the Web Administration Interface

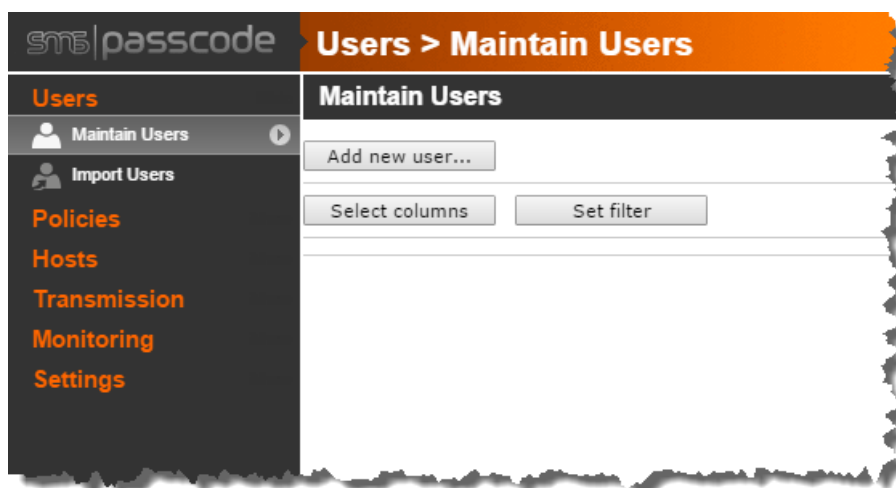
You can start the **WAI** in three different ways:

1. You can start the **WAI** using a shortcut created on the desktop of the **WAI server**:



2. You can start the **WAI** using the shortcut **Web Admin** created in the SMS PASSCODE folder in the Windows Start Menu of the **WAI server**.
3. The **WAI** is also available from any computer on the network using a web browser if this computer can connect to the **WAI server** on TCP port 2000¹⁶. Connect to the **WAI** using the URL <http://ip-address:2000>, where *ip-address* is the IP address of the **WAI server**. By default, only administrators of the **WAI server** have access to the **WAI** using a web browser.

The following user interface is shown on the first startup of the **WAI**:



¹⁶ Port 2000 is the default TCP port for the **Web Administration Interface**. The port may be changed during installation.

The left part of the user interface is a **navigation menu**. Please notice, that this navigation menu is dynamically adapted according to the different data and settings in the **WAI**, and according to role-based permissions (cf. section 20).

The complete list of possible menu items is:

Users

- **Maintain users**
Maintain SMS PASSCODE users, i.e. create, edit and delete users.
Please read section 17.10 (page 234) for details.
- **Import users**
Import SMS PASSCODE users from a comma-separated file.
Please read section 17.11 (page 253) for details.

Policies

- **User Integration Policies**
Maintain policies for automatic synchronization of SMS PASSCODE users from one or more Active Directories or other types of LDAP directories. This menu item is only available, when User Store Integration has been enabled in the general settings. Please read section 17.5 (page 126) for details.
- **User Group Policies**
Maintain user settings on a user group basis.
Please read section 17.6 (page 156) for details.
- **Authentication Policies**
Maintain policies and rules affecting user authentication behavior.
Please read section 17.8 (page 193) for details.
- **Passcode Policies**
Maintain passcode specific settings, like passcode length, composition and lifetime; and maintain passcode message templates using the *MessageDesigner*.
Please read section 17.7 (page 184) for details.
- **Dispatch Policies**
Maintain policies and rules for message transmission load distribution and failover.
Please read section 17.18 (page 271) for details.
- **Token Policies**
Maintain policies describing the types of tokens allowed in your organization. This menu item is only available when token authentication has been allowed in the general settings.
Please read section 17.9 (page 221) for details.

Hosts

- **Authentication Backend Service Hosts**
Maintain Authentication Backend Service hosts, e.g. authorize new Authentication Backend Service hosts. Please read section 17.13 (page 258) for details.
- **Transmitter Hosts**
Maintain Transmitter servers, e.g. authorize new Transmitter Service hosts. Please read section 17.12 (page 255) for details.

Transmission

- **Modems**
Maintain modem settings. Please read section 17.14 (page 261) for details.
- **Modem Groups**
Maintain modem groups, which are used by Dispatch Policies. Please read section 17.17 (page 269) for details.
- **Email Connectors**
Maintain settings for email dispatching. Please read section 17.15 (page 263) for details.
- **Dispatch Connectors**
Maintain settings for message dispatching using plugin modules. Plugin modules allow alternative message dispatching mechanisms, like SMS and voice call using external web services, and to connect to the SMS PASSCODE Cloud Service. Please read section 17.16 (page 265) for details.

Monitoring

- **Authentications**
Inspect current and past authentication attempts on any SMS PASSCODE protected authentication clients. Both live monitoring of current authentication attempts, as well as reporting and exporting of past authentication attempts is supported. This menu item is only available when **Authentication monitoring** has been enabled in the general settings. Please read section 17.19 (page 296) for details.
- **Modems**
Inspect the current live status of all modems. Please read section 17.20 (page 307) for details.

Settings

- **General**
Maintain general settings, e.g. enable **User Store Integration** or **IntelliTrust™** integration. Please read section 17.3 (page 108) for details.
- **License**
Monitor license usage, and maintain license information, e.g. when additional licenses have been acquired. Please read section 17.4 (page 122) for details.

After installation of SMS PASSCODE, the recommended order of actions is:

1. Configure the general settings.
2. User store integration enabled in step 1?
 - a. Yes: Configure User Integration Policies.
 - b. No: Create users manually (or import from comma-separated file).
3. Configure User Group Policies.
4. Configure your transmission infrastructure.
 - a. Optionally authorize additional Authentication Backend Service hosts, if failover is required between more such services.
 - b. Optionally authorize additional Transmitter servers, if failover is required between more such services.
 - c. Create required dispatching entities, e.g. create modems, Email Connectors and/or Dispatch Connectors, according to your message transmission requirements.

Note: If you are a trial or subscription customer, then SMS-based message dispatching works out-of-the-box, using the SMS PASSCODE Cloud Service. In this case you do not need to create any dispatching entities, unless you would like to configure additional message dispatching mechanisms, e.g. for failover reasons.

- d. Optionally create modem groups and/or Dispatch Policies, if you have advanced failover and/or scalability requirements for message transmission.

When the SMS PASSCODE system is up and running, you may additionally decide to enable and configure *location and behavior aware authentication* for even stronger security. Please read section 16.1 (page 96) to get a short overview about this topic.

17.2 Overview of Policy Types

SMS PASSCODE includes several types of **Policies**:

- User Integration Policies
- User Group Policies
- Authentication Policies
- Passcode Policies
- Dispatch Policies
- Token Policies

This section gives an overview regarding these policies and explains their intended usage and relationship to each other.

A **User Integration Policy** (UIP) is used to define a periodic synchronization of users from a user store (Active Directory or different type of LDAP directory) into the SMS PASSCODE database. Each UIP keeps important user attributes up-to-date in the SMS PASSCODE database according to any changes in the underlying user store, like (mobile) phone number(s), email address and full name. By creating several UIPs, you can synchronize users from several user groups of a user store, and/or from user groups from several user stores.

Each user in the SMS PASSCODE database has a lot of individual settings and permissions that can be customized by administrators. However, to make it easier for administrators to manage these settings across large amounts of users, **User Group Policies** were introduced to make it possible to maintain common settings for *groups* of users. The methodology is simple: Each user is

assigned a specific User Group Policy (UGP) and *inherits* all the settings defined by this policy. Most of the settings can additionally be overridden on individual users, if any deviations from the inherited settings are required. Any overridden setting can afterwards be reset again, to fall back to the inherited value.

Among the settings of a UGP are the following sub-policies:

- **Authentication Policy:**
Defines authentication behavior, e.g. whether and how a user is allowed to authenticate from specific locations.
- **Passcode Policy:**
Defines settings regarding the random one-time-passcodes generated for a user and defines the content of passcode messages (using message templates).
- **Dispatch Policy:**
Defines prioritized rules for determining the dispatchers to use to send messages to a user.
- **Token Policy:**
Defines the types of tokens being used within your organization (in case token authentication has been allowed)

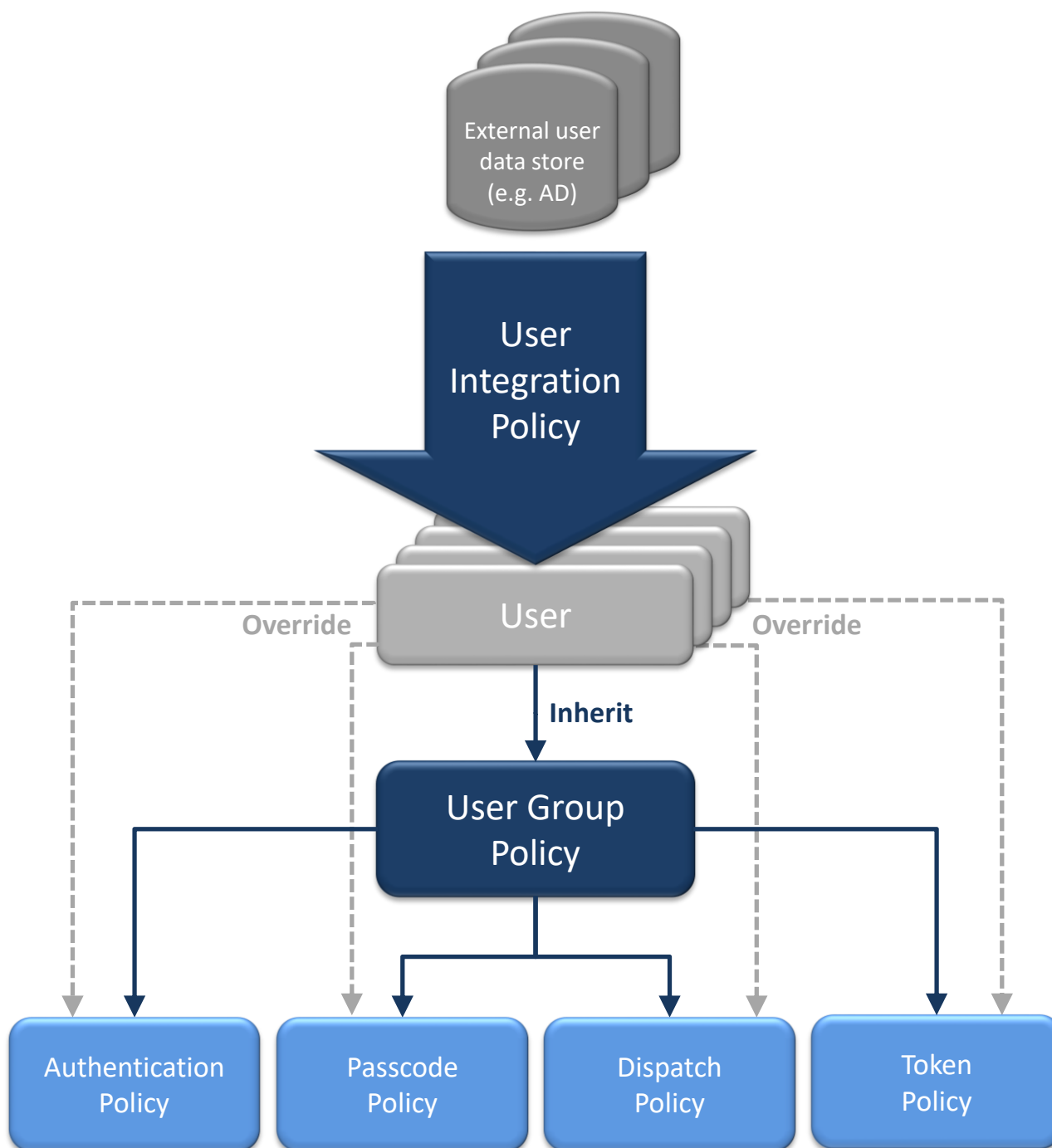
17.2.1 Static Relationship between Policy Types

Each user belongs to exactly one policy of each policy type. The *static relationship* between the different types of policies defines how the different policies are assigned to a user.

The static relationship between the different policies is as follows:

- Each **User Integration Policy** defines the **User Group Policy** to assign to the users being imported.
- Each user is assigned a single, specific **User Group Policy**. Either automatically by a User Integration Policy, or manually.
- Each **User Group Policy** refers to a particular **Authentication Policy**, **Passcode Policy**, **Dispatch Policy** and **Token Policy**. These four policies are inherited by all the users to which the User Group Policy is assigned. However, each of the policies can be overridden individually on any user.

The static relationship of the policies is illustrated by the diagram below:



Each of the policies is explained in more detail in subsequent sections:

- User Integration Policies: Section 17.5 (page 126)
- User Group Policies: Section 17.6 (page 156)
- Passcode Policies: Section 17.7 (page 184)
- Authentication Policies: Section 17.8 (page 193)
- Dispatch Policies: Section 17.18 (page 271)
- Token Policies: Section 17.9 (page 221)

17.2.2 Runtime Relationship between Policy Types

The *runtime relationship* between policy types defines how policies are used during a user's authentication attempt.

User Integration Policies are not part of the *runtime relationship*, since they are not directly having any influence on an authentication attempt. Instead, User Integration Policies are, as part of the static relationship, defining which other policies belong to a user, and thereby indirectly influencing the authentication behavior (as described in the previous section).

The authentication behavior for a specific user is determined in the following way:

- First, the **Authentication Policy** assigned to the user is determined. The Authentication Policy determines, whether the user can log in at all. If the user is allowed to log in, the outcome might be either to use or bypass multi-factor authentication.

In case the user is denied access, or access is allowed with multi-factor authentication bypassed, the remaining policy types are ignored.

Otherwise, multi-factor authentication is performed according to the remaining policy types, as described below.

- The **Passcode Policy** assigned to the user determines among others the format of the OTP to be sent to the user, and the content of the OTP message. Normally, the Passcode Policy is assigned statically to the user, i.e. either inherited from the user's User Group Policy, or overridden on the user itself.

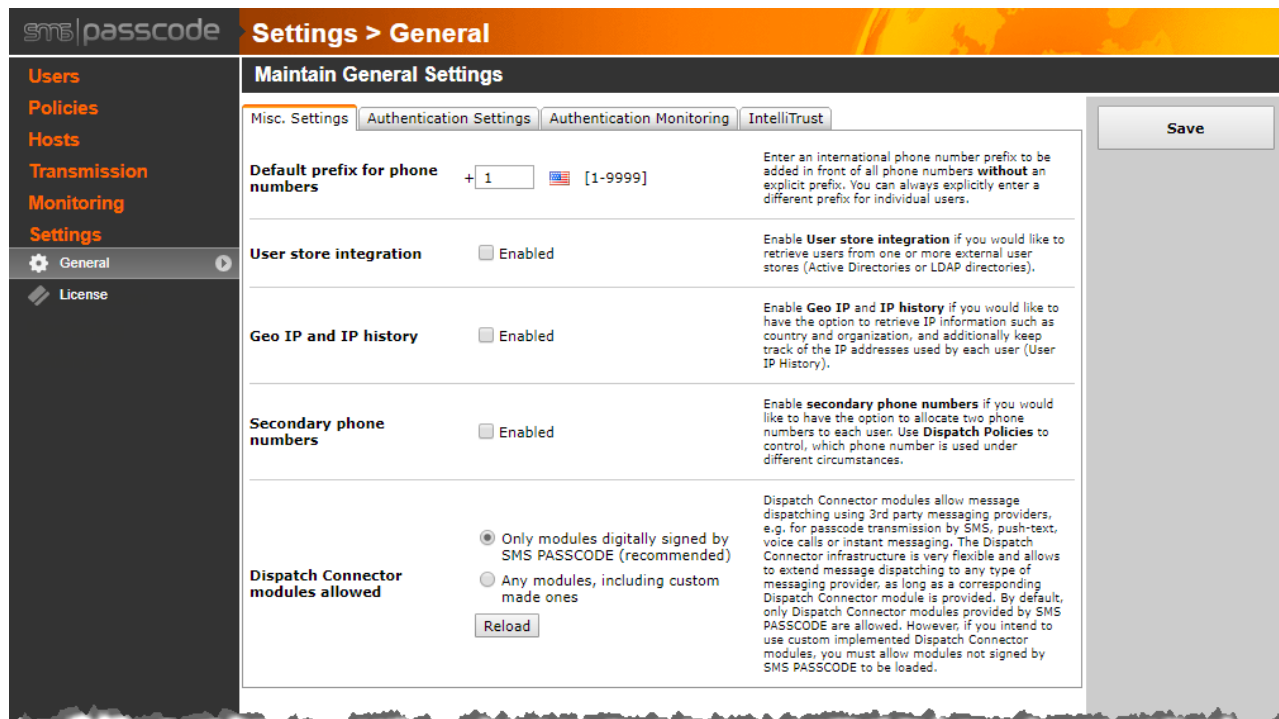
However, the Passcode Policy might also be determined dynamically at runtime by the authentication policy during step 1, allowing for *adaptive contextual message dispatching* (advanced feature). Please read section 17.8.2.5 (page 204) for more details about this.

- Finally, the user's **Dispatch Policy** determines how OTP messages are sent to the user (which type of message to send, which dispatcher to use, which target to send to). The Dispatch Policy is normally assigned statically to the user, i.e. either inherited from the user's User Group Policy, or overridden on the user itself.

However, the Dispatch Policy might also be determined dynamically at runtime by the Authentication Policy during step 1, allowing for *adaptive contextual message dispatching* (advanced feature). Please read section 17.8.2.5 (page 204) for more details about this.

17.3 General Settings

The **General** settings page allows configuration of important system-wide settings:



Changes do not take effect until you click the **Save** button.

As shown in the screenshot above, the settings are divided into 4 tabs:

- **Misc. Settings**

This tab contains miscellaneous important system-wide settings.

Please read section 17.3.1 below for a detailed description of these settings.

- **Authentication Settings**

This tab contains system wide settings that indicate whether non-standard authentication types are activated and allowed to be used during user authentication attempts. You are only advised to enable any of these settings, in case standard SMS authentication is not sufficient.

Please read section 17.3.2 below for a detailed description of the different *Authentication settings*.

- **Authentication Monitoring**

This tab contains settings concerning authentication monitoring, e.g. whether to enable authentication monitoring at all.

Please read section 17.3.3 below for a detailed description of the *Authentication Monitoring settings*.

- **IntelliTrust**

This tab contains settings that are used to enable integration of the SMS PASSCODE backend with the IntelliTrust™ cloud service, thereby achieving a **Hybrid Setup**.

Please read section 17.3.4 below for a detailed description of configuring a Hybrid Setup.

The subsections below describe the settings of all four tabs in more detail.

17.3.1 Miscellaneous Settings

This section describes the settings available on the **Misc. Settings** tab on the **General** settings page of the WAI. The settings are described in detail in the table below.

Setting	Explanation
Default prefix for phone numbers	This prefix is automatically added to the beginning of each user's phone number if no <u>explicit</u> international prefix is specified. You can always explicitly specify a different prefix for individual users.
User store integration	<p>When this setting is enabled, users are imported from one or more external user stores, typically a single Active Directory, and are kept up-to-date via periodic synchronizations.</p> <p>Synchronization of users from user stores is defined using a User Integration Policy. Please read section 17.5 (page 126) for more details on setting up User Integration Policies.</p>
Geo IP and IP history	<p>This setting controls whether <i>location and behavior aware authentication</i> is enabled for strengthened security. When enabled, end-user IP address usage is recorded in the SMS PASSCODE database and Geo IP data is looked up by IP addresses to determine geo-location information.</p> <p>You should only enable this setting if at least one of your authentication clients fulfills the requirements for collecting end-user IP addresses correctly (cf. section 10.1, page 35).</p> <div> <p>IMPORTANT: Allow outgoing network HTTP/HTTPS traffic</p> <p>Please note that when Geo IP lookups are enabled, you must allow outgoing HTTP/HTTPS traffic from the SMS PASSCODE Database Service, Web Administration Interface and Authentication Backend Service. This is required, since these services will contact a 3rd party Geo IP database during Geo IP data lookups, and additionally they will periodically contact an SMS PASSCODE web service to check for any required updates ensuring correct Geo IP lookups.</p> </div>
Secondary phone numbers	When this setting is enabled, you can optionally allocate a secondary phone number to each user. Secondary phone numbers can be used during configuration of Dispatch Policies for failover scenarios.

Setting	Explanation
Dispatch Connector modules allowed	<p>By default, only the dispatch plugin-modules provided by SMS PASSCODE can be used for message transmissions using Dispatch Connectors. However, you may implement your own dispatch plugin module(s) in case of special message transmission requirements and use such custom modules for transmission of messages. For security reasons, you must allow the SMS PASSCODE system to load such custom modules.</p> <p>Note: The "Reload" button allows you to reload the plugin modules currently located in the "Plugins" folder without restarting the Database Service, for example if you have added new modules or updated existing modules.</p>

17.3.2 Authentication Settings

The **Authentication Settings** tab contains settings that allow you to customize the mechanisms allowed for user authentications. Some mechanisms might lower security but might be required to support the challenges met because of global diversities, or due to the need for improved convenience and flexibility.

SMS PASSCODE Settings > General

Maintain General Settings

Misc. Settings | **Authentication Settings** | Authentication Monitoring | IntelliTrust

By default, the SMS PASSCODE system requires **multi-factor authentication** for all SMS PASSCODE protected authentication clients, where **session-specific one-time-passcodes** are generated in realtime and sent as passcode messages to each user. On this page you can allow different authentication mechanisms, for greater flexibility and convenience. Please note that you may decrease security by enabling some of these options.

Token	<input type="checkbox"/> Allowed	Allow authentication using OATH Tokens (incl. software tokens) or USB keys 3rd party Token / USB key option for users without a mobile phone, or users using software tokens.
Personal passcode	<input type="checkbox"/> Allowed	Allow authentication using personal passcodes Low security option for non-critical users, or failover in case of emergency.
Multi-factor authentication bypassing	<input type="checkbox"/> Allowed	Allow multi-factor authentication bypassing (conditional) Allow bypassing, if you would like to have the possibility to bypass multi-factor authentication under certain circumstances (as defined by Authentication Policies)
PIN codes	<input type="checkbox"/> Allowed	Allow usage of PIN codes during authentications (not recommended) Allow PIN codes if you would like to have the option to require users to enter a PIN code in front of each passcode during authentications.

Save

The **Authentication Settings** tab contains settings that control the types of authentications allowed. By default, only message-based multi-factor authentication is allowed.










Setting	Explanation
Token	<p>Enable this setting to allow selected users to authenticate using tokens.</p> <p>Token authentication is very different from the message-based authentication types, which SMS PASSCODE provides by default. All message-based authentication types will not generate a random OTP, until a request has been made (<i>“challenge based”</i>) and will generate an OTP for the specific authentication (<i>“session specific OTP”</i>). Contrary to this, a token has a unique, but pre-determined sequence of OTPs.</p> <p>Token authentication is useful for users that cannot authenticate by any of the stronger, message-based authentication types for some reason.</p> <p>SMS PASSCODE supports several types of tokens:</p> <ul style="list-style-type: none"> • All OATH compliant tokens <ul style="list-style-type: none"> ✓ Including both hardware and software tokens ✓ Including event-based tokens (HOTP) ✓ Including time-based tokens (TOTP) • YubiKeys (proprietary USB Keys from a 3rd-party provider called Yubico). This provider also hosts a web service for which you need to sign up¹⁷. Communication with the web service is performed using HTTPS (SSL encrypted network traffic). <p><u>NOTE regarding RADIUS authentication using MS-CHAP v2:</u></p> <ul style="list-style-type: none"> • OATH token authentication works with MS-CHAP v2 as well • USB Key authentication is not guaranteed to function properly with RADIUS clients using MS-CHAP v2. This depends on the specific RADIUS client implementation / manufacturer. The RADIUS client is required to return the passcode in clear text as a response to the challenge request. <p>For more information regarding token authentication, please read section 17.9 (page 221).</p>

¹⁷ If you intend to make use of YubiKey authentication, then you must acquire USB Keys from our selected 3rd-party USB Key provider (Yubico). These USB Keys have a user-friendly feature that allows entering the complete OTP by a single push of a button on the USB Key.

Please contact SMS PASSCODE support (support@entrustdatacard.com) to receive the document [“Yubico USB Key Authentication Guide for SMS PASSCODE”](#). This document describes the steps necessary to implement USB Keys in SMS PASSCODE.

Setting	Explanation
Personal passcode	<p>Enable this setting to allow selected users to authenticate (temporarily) using an encrypted personal passcode.</p> <p>Personal passcodes are meant to be used in case of emergency (ICE). They provide a last resort to allow users to authenticate using a temporary assigned personal passcode, if everything else should fail. The code can be set by the administrator, or by the user through the SMS PASSCODE Self-service Website. The personal passcode is stored encrypted and is not visible to the administrator or anyone else.</p> <p>Note: This setting only controls, whether Personal Passcodes can be used as a replacement for a one-time passcode during authentication client logins (ICE). Usage of Personal Passcodes as a replacement for the user <u>password</u>, when logging in to the SMS PASSCODE Password Reset Website, is always allowed.</p> <p>It is possible to allow users to maintain Personal Passcodes themselves, using the SMS PASSCODE Self-service Website (cf. section 17.6.1.2, page 163). Personal Passcodes can also be imported from AD (cf. section 17.5.4.3, page 140) or set using PowerShell script (cf. section 18.1, page 309).</p>
Multi-factor authentication bypassing	<p>This is a system wide setting that controls whether any users should be allowed to bypass SMS PASSCODE multi-factor authentication under specific circumstances. "Bypassing" means that the user authenticates only using username and password, i.e. without entering a passcode. Allowing this must be done with great care, since it lowers the security level. When allowed, the conditions for bypassing are defined using Authentication Rules (cf. section 17.8.2.5, page 204). An example could be to allow bypassing for convenience, when the user is observed to be in a trusted login context.</p> <p>Proof-of-Concept (PoC) Mode: When allowing "multi-factor authentication bypassing", an additional checkbox appears below the setting that allows you to enable PoC mode. When PoC mode is enabled, users without any SMS PASSCODE license assigned can log in using standard authentication, i.e. without using SMS PASSCODE multi-factor authentication. This provides the possibility to test the SMS PASSCODE product with only a few SMS PASSCODE licenses, without affecting the login behavior for the remaining users.</p> <p>NOTE: Even when PoC mode is enabled, any user must still be imported into the SMS PASSCODE database to be allowed to log in to any SMS PASSCODE protected authentication client.</p> <div> <p>WARNING: For security reasons, please only enable PoC Mode during a product evaluation / Proof-of-Concept period.</p> </div>
PIN codes	<p>Enable this setting to allow the usage of PIN codes during authentication client logins. This will allow the administrator to set individual PIN codes on each user, which must be entered in front of the one-time passcodes during authentication.</p> <p>It is possible to allow users to maintain PIN codes themselves, using the SMS PASSCODE Self-service Website (cf. section 17.6.1.2, page 163). PIN codes can also be set using PowerShell script (cf. section 18.1, page 309).</p>

The extra authentication types described above all introduce a lower level of security, than ordinary SMS-based multi-factor authentication. The table below compares the security rating of the different types of authentication:

Authentication type	Challenge based and session specific OTP	End-to-end out-of-band dispatching	Security Rating	Convenience
SMS OTP	Yes	Yes		<ul style="list-style-type: none"> ✓ Support for flash SMS ✓ Support for memoPasscodes™
SMS PASSCODE Mobile app (Encrypted push notifications)	Yes	No, but end-to-end encrypted		<ul style="list-style-type: none"> ✓ Support for memoPasscodes™ ✓ End-to-end encryption of messages
Alternative dispatch types to augment secure dispatching (the alternatives provide a security level below the level of SMS OTP and SMS PASSCODE Mobile app)				
Dispatch plugin OTP (SMS)	Yes	No ¹⁹		<ul style="list-style-type: none"> ✓ Most likely supports memoPasscodes™ (depends on the provider) ✓ Might support flash SMS (depends on the provider)
Email OTP (secure/closed network) ¹⁸	Yes	No		<ul style="list-style-type: none"> ✓ Support for memoPasscodes™
Dispatch plugin OTP (Voice call)	Yes	No ¹⁹		<ul style="list-style-type: none"> ✓ Allows calls to landline phones
Token OTP	No	-		<ul style="list-style-type: none"> ✓ OTP entered automatically when using YubiKeys
Email OTP (non-secure) ²⁰	Yes	No		<ul style="list-style-type: none"> ✓ Support for memoPasscodes™
Temporary personal passcode	No	-		-
Bypassing MFA	No	-		-

¹⁸ When e-mail access is well-protected, e.g. only accessible by a personal device

¹⁹ A dispatch plugin module will typically make use of a 3rd-party web service that is called using HTTPS, i.e. using SSL encrypted network traffic.

²⁰ When e-mail access is not well-protected, e.g. accessible from anywhere using ordinary authentication with a user name and password

17.3.3 Authentication Monitoring

This section describes the settings available on the **Authentication Monitoring** tab on the **General** settings page of the WAI.

SMS PASSCODE Settings > General

Maintain General Settings

Misc. Settings | Authentication Settings | **Authentication Monitoring** | IntelliTrust

Authentication monitoring ☒ Enabled

Enable **Authentication monitoring** if you would like the system to record all authentication attempts. Among others, this will provide a complete login history per user.

Archive destination

Archive records of old authentication attempts to:

- ☒ CSV files
- ☐ XML files
- ☐ SQL table

To limit the size of the internal database, old authentication attempts are periodically removed from the database and archived externally. Choose whether you would like entries to be archived as CSV files, XML files, or added to an SQL table of an existing SQL server.

Archive Path

C:\Program Files\SMS PASSCODE\DB\Archive

Specify the path of the folder, where archive files will be stored.

Archiving threshold 10000

The maximum number of authentication attempt records to keep in the internal database. When this threshold is exceeded, oldest authentication attempts are removed and archived. NOTE: Please note, that authentication attempts performed within the last week are never removed and archived, even though the threshold has been exceeded. This is to ensure, that most recent authentication attempts are always readily available as live data.

Statistics Show statistics...

Click the link to show statistics regarding live entries and archived entries of the authentication monitor.

Save

© Entrust Datacard

These settings all relate to the SMS PASSCODE **Authentication Monitoring** feature. Please note, that authentication monitoring is disabled by default, i.e. you must enable it explicitly on this page, in case you would like to make use of it. When enabled, administrators can get access to the **Authentication Monitoring** page, which allows monitoring, reporting and exporting authentication attempts across all users and SMS PASSCODE protected authentication clients. Please read section 17.19 (page 296) for more details regarding the Authentication Monitoring page.

The settings are described in detail in the table below.

Setting	Explanation
Authentication monitoring	<p>This setting controls, whether the SMS PASSCODE system should record every authentication attempt in the SMS PASSCODE database, across all users and SMS PASSCODE protected authentication clients, for reporting and monitoring afterwards.</p> <p>The setting is disabled by default, i.e. authentication attempts are not recorded in the SMS PASSCODE database by default.</p> <p>Enable the setting, in case you would like to make use of the advanced authentication monitoring features on the Authentication Monitoring page of the WAI (cf. section 17.19, page 296).</p> <p>NOTE: The remaining settings described in this table will only become visible in the WAI, when the Authentication monitoring setting is enabled.</p>
Archive destination	<p>When authentication monitoring is enabled, every authentication attempt is recorded and stored in the SMS PASSCODE database. Eventually, this will grow the SMS PASSCODE database unnecessary big and could reduce system responsiveness. To avoid this, SMS PASSCODE includes an auto-archiving feature that will automatically archive and remove the oldest authentication attempts from the SMS PASSCODE database.</p> <p>Please note, that archived authentication attempts remain available for reporting and export on the Authentication Monitoring page.</p> <p>The Archive destination setting allows you to specify, how archived data should be stored. The following options are available:</p> <ul style="list-style-type: none">• CSV Archived data is stored as CSV files in a specific folder in the file system• XML Archived data is stored as XML files in a specific folder in the file system• SQL Archived data is inserted into a specific table in a specific database of an SQL Server. The SQL server must have been installed beforehand. Currently, Microsoft SQL Server 2005, 2008 and 2012 are supported for SQL archiving. <p>Please read the notes following this table for additional information regarding the Archive destination setting.</p>

Setting	Explanation
Archiving threshold	<p>Specifies the number of authentication attempt records to keep in the internal SMS PASSCODE database. When the number of records in the database exceeds the specified threshold, then the auto-archiving feature will start to remove and archive the oldest authentication attempts, to keep the number of entries below the threshold.</p> <p>The default threshold is 10.000 records.</p> <p>NOTE: The auto-archiving feature has a built-in rule, that it will never archive authentication attempts that have occurred within the recent week. I.e. even if the threshold setting is low compared to the number of logins per day in your organization, you are guaranteed always to have the recent week of authentication attempts readily available in the internal SMS PASSCODE database for monitoring and reporting.</p>
Statistics	<p>Click the Show statistics... link to open a new window containing statistics regarding number of authentication attempt entries, for both the internal SMS PASSCODE database and the archive:</p> <ul style="list-style-type: none"> • Number of entries • Date and time of the oldest record • Date and time of the newest record

IMPORTANT:

The SMS PASSCODE system supports one authentication **archive** at a time. I.e. if you change the type or destination of the archive at any time, then no data of the previous archive will be available for retrieval on the **Authentication Monitoring** page anymore.

Notes regarding **Archive destination**, type = CSV or XML

Using CSV files or XML files for archiving is the easiest option. You only need to select a specific folder in the file system, which the SMS PASSCODE database has write access to, and you are done. If the folder does not exist, the SMS PASSCODE database will automatically create the folder, if allowed to.

By default, the subfolder "Database\Archive" of the SMS PASSCODE installation folder is used for archiving.

CSV or XML files are supported by many 3rd party analysis systems, like e.g. Microsoft Excel, which allow you to perform further analysis of the archived authentication attempts. Please note, that if you wish to consolidate several of the files in the archive into one file or wish to select only a subset of the attributes in the files, you can easily select and filter the archived data on the **Authentication Monitoring** page and export the filtered data into new consolidated CSV or XML files.

Please remember to back up the files in the archive destination folder if you want to be able to recover them in case of data loss.

Notes regarding **Archive destination**, type = **SQL**

Archiving authentication attempts to an SQL Server is more complex than the CSV/XML files option, but might be advantageous to you, in case you already have an SQL Server running in your organization, and/or because you have special data analysis systems available for analyzing data in the SQL Server.

The screenshot below shows the settings that must be specified, when SQL archiving is selected:

The screenshot shows the 'Archive destination' settings for SQL archiving. The settings are as follows:

- Archive destination:** Archive records of old authentication attempts to:
 - ☐ CSV files
 - ☐ XML files
 - ☒ SQL table
- SQL Server:** MySQLServer (labeled a)
- Database name:** MyDatabase (labeled b)
- Table name:** SMSPASSCODE (labeled c)
- Authentication Type:** SQL Authentication (labeled d)
- Credentials:** User name: (labeled e), Password: (labeled e)
- Additional Connection String Parameters:** (labeled f)
- Test Connection:** (labeled g)

To limit the size of the internal database, old authentication attempts are periodically removed from the database and archived externally. Choose whether you would like entries to be archived as CSV files, XML files, or added to an SQL table of an existing SQL Server.

Name or IP address of the SQL Server to use for archiving

Name of the destination database within the SQL Server

Name of the table in the SQL database, where authentication attempts should be archived to. Enter the name of a non-existing table to automatically create a new one with the correct data structure.

Select the type of authentication to use to connect to the SQL Server

Credentials for connecting to the SQL Server

Optional: Enter any additional connection string parameters. The string entered here is directly appended to the auto-built connection string.

	Setting	Explanation
(a)	SQL Server	<p>Name or IP address of the SQL Server to use for archiving. The SQL Server must have been installed beforehand.</p> <p>Currently, MS SQL Server 2005, 2008 and 2012 are supported.</p>
(b)	Database name	<p>Name of the destination database within the selected SQL Server. The database must have been created beforehand. You can either create a new dedicated database or use an existing database to which the SMS PASSCODE system should add a new table.</p> <p>You must also assign an SQL User Account or Windows User Account to the database. This account must have permissions to create a new table, as well as read/write access to this new table.</p>
(c)	Table name	Name of a table within the selected SQL database, where authentication attempts should be stored. It is recommended to enter a name of a non-existing table – this will cause the SMS PASSCODE database service to create the table automatically, with the required data structure.
(d)	Authentication Type	Specify, whether the SMS PASSCODE database service should make use of a dedicated SQL User Account or Windows User Account to access the SQL database.
(e)	Credentials	Specify the credentials of the user account that the SMS PASSCODE database service should use for accessing the SQL database. Enter the credentials of either an SQL User Account or Windows User Account, depending on the selection of the previous setting (d).
(f)	Additional Connection String Parameters	This option is only for advanced use. It allows you to specify additional parameters that should be appended to the connection string used for accessing the SQL Server.
(g)	Test Connection	Click this button to test, whether all the previous settings have been entered correctly, and to verify, that the SMS PASSCODE database service is able and allowed to connect to the specified SQL database.

Please remember to back up the SQL table used for archiving if you want to be able to recover the table in case of data loss.

17.3.4 IntelliTrust Settings

This section describes the settings available on the **IntelliTrust** tab on the **General** settings page of the WAI. The main purpose of the **IntelliTrust** tab is to allow you to optionally enable the integration of SMS PASSCODE with the IntelliTrust™ cloud service, thereby activating a **Hybrid Setup**, which extends the SMS PASSCODE backend with additional cloud-based authentication services. The main two features that become active, when IntelliTrust™ integration is enabled, are:

- **User sync:** All relevant user data will immediately be synced to the IntelliTrust™ cloud service – and will continue to stay in sync afterwards.
- **Authentication:** SMS PASSCODE Authentication Policies will allow additional configuration options, which allow authentication requests to be forwarded conditionally to the IntelliTrust™ cloud service, e.g. depending on the context. This is described in more detail in section 17.8.2.5 (page 204).

If you want to make use of a **Hybrid Setup**, the recommended order of actions is described in section 16.2, page 99. The first action is to enable the IntelliTrust™ cloud service integration, thereby connecting your SMS PASSCODE backend to a dedicated IntelliTrust™ tenant. This is described in section 17.3.4.1 below.

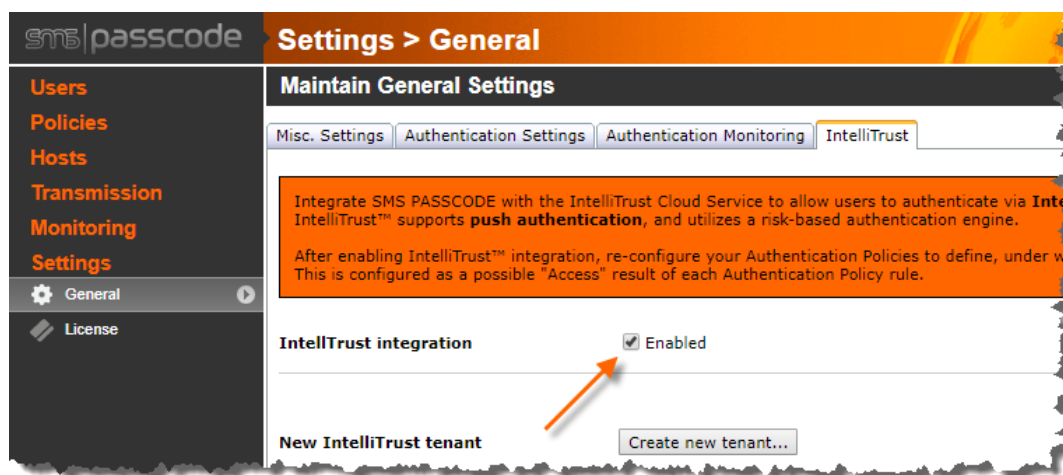
17.3.4.1 Connecting SMS PASSCODE to an IntelliTrust Tenant

To connect your SMS PASSCODE backend to an IntelliTrust™ tenant, please proceed as follows:

IMPORTANT: User sync starts immediately

As soon as IntelliTrust™ integration has been enabled, SMS PASSCODE will immediately start syncing all SMS PASSCODE users to the selected IntelliTrust™ tenant. The synchronization status can be inspected on the **User Maintenance** page (cf. section 17.3.4, page 119).

1. On the **IntelliTrust** tab, select the **Enabled** option:

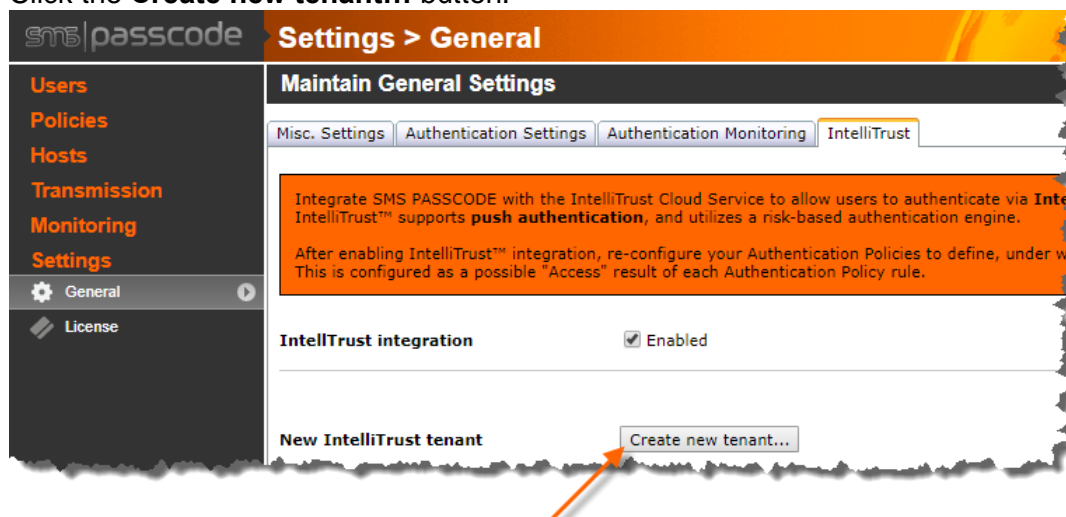


2. You now have to specify, whether you want to connect to a new IntelliTrust™ tenant, or an existing one. During a fresh installation, you will typically want to connect to a new, empty tenant. However, you might want to connect to an existing tenant, e.g. if you have performed a re-installation of SMS PASSCODE and would like to connect to a previously created IntelliTrust™ tenant. Both options are described below.

Connecting to a new tenant:

IMPORTANT: Before connecting to a new tenant, make sure that you have created a user account within the SMS PASSCODE Database that you want to become the IntelliTrust™ admin account. You must select this user as the admin, when creating the new tenant (see below).

- a. Click the **Create new tenant...** button:



- b. A dialog pops up, asking you to enter required data for the new tenant:

Create new IntelliTrust™ tenant

This form allows you to create a new IntelliTrust™ tenant and associate it with your current SMS PASSCODE installation - one license code entitles one IntelliTrust™ tenant.

Select a user to become tenant administrator	<input type="text" value="Type to search for a user..."/>	The user selected will become administrator for the newly created IntelliTrust™ tenant. The user is required.
Company name	<input type="text" value="Enter company name"/>	The name of the company that will own this account. This value is required.
Country	<input type="text" value="Type to search for a country..."/>	The country of the company that will own this account. This value is required.
Tenant name	<input type="text" value="Enter tenant name"/> .de.trustedauth.com	Tenant name is the name of your tenant and how it will appear in the URL. This value is required.
Data Center location	<input type="text" value="Germany"/>	Location of the IntelliTrust™ data center. This value is required.
Terms Of Use	<input type="checkbox"/> I agree to the noted service terms and conditions	

By checking the box, you hereby acknowledge that you have read, understood and agreed to the [following service terms and conditions](#).

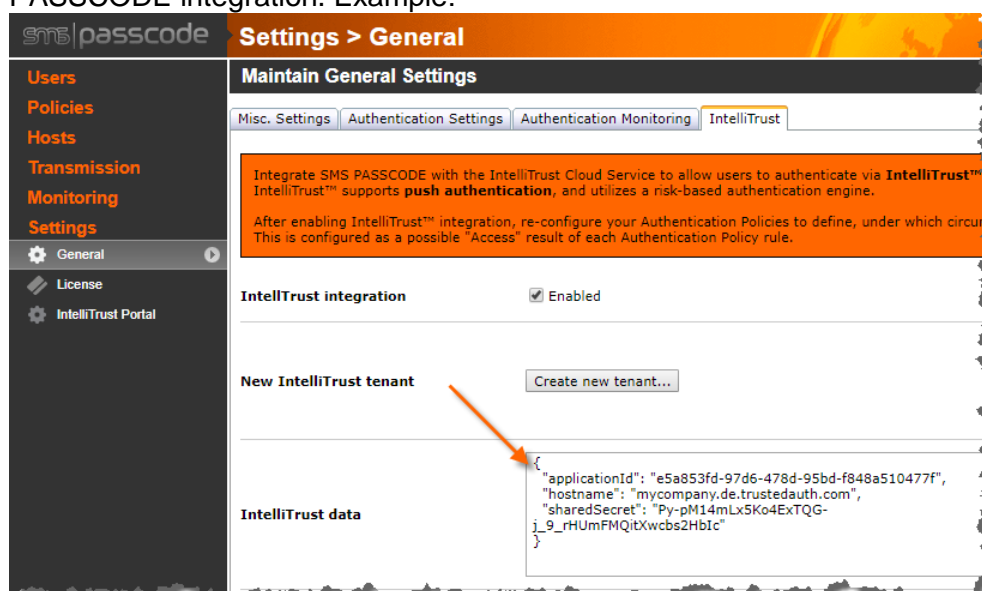
Fill in the required data, read and accept the terms of use, and then click the **Create** button. In case of any error messages, please correct the error, and click the **Create** button again.

- c. A new IntelliTrust™ tenant was now created, with which your SMS PASSCODE system integrates.

Connecting to an existing tenant:

IMPORTANT: To connect to an existing tenant, you must prove that you are the rightful owner of the tenant. This is done by inserting the JSON code that uniquely identifies the **Administration API** in your existing tenant. If you have not stored such JSON code, you can re-create it. See below.

- In the **IntelliTrust data** field, insert the JSON code that uniquely identifies the **Administration API** of your IntelliTrust™ tenant to be used for the SMS PASSCODE integration. Example:



- Recommended: Click the **Verify settings** button to verify that the JSON data is correct.
- Click the **Save** button.

If you do not have the JSON data for your existing IntelliTrust™ tenant available, you can re-create it using the following procedure:

- Log in to your existing IntelliTrust™ tenant using an administrator account.
- Create a new **Application** of type **Administration API**. You can use this guide: [https://entrust.us.trustedauth.com/documentation/help/admin/index.htm#t=Resources%2FAdd Administration API to IntelliTrust.htm](https://entrust.us.trustedauth.com/documentation/help/admin/index.htm#t=Resources%2FAdd%20Administration%20API%20to%20IntelliTrust.htm).

IMPORTANT:

Make sure to set the **Role** of the application to "Super Administrator".

On the last page, before clicking the **DONE** button, make sure to click the **COPY TO CLIPBOARD** button, to copy the JSON code to the clipboard, so that you can paste it into the **IntelliTrust data** field in SMS PASSCODE, as described above. You might also click the **DOWNLOAD** button in the IntelliTrust™ portal to download the JSON code and store it in a safe place. Then you have it ready, if you should ever need to reinstall SMS PASSCODE and reconnect to the tenant again.

IMPORTANT: Keep the JSON code in a **safe place**, as anyone getting access to this JSON code can connect to your tenant with “Super Administrator” permissions (at least until the shared secret of the application is regenerated, or the application is deleted).

17.4 License Information

The **WAI** has a page for inspecting and maintaining license information.

[illegible]

Use the **License** page to inspect the current, overall license allocation status, e.g. to check whether you are running low on licenses. The **In use** column in the **License statistics** section indicates the current number of licenses that have been allocated. In case you have run out of any licenses, this will be shown in the **Missing** column.

You will typically only perform any changes on this page in the following cases:

1. When you have received a new license key, because you have acquired more CALs or dispatch licenses. Section 17.4.1 below describes how to enter a new license key.
2. In case you wish to enable **License limits** (advanced feature). This is described in section 17.4.2 below.

17.4.3 License Management

In some cases, you might need different kinds of overviews regarding the actual license allocations across users and user groups. Besides the total license overview shown on the **License page** itself, you also have several other options:

- On the **Maintain Users** page, you can inspect license information across all users. You can (a) enable columns with license related information to be shown, and (b) use row filtering to filter on license related information. For example, you may enable a filter that shows only users with Password Reset CALs granted, but not allocated.

Users > Maintain Users

Maintain Users

Add new user...

a Select columns **b** Set filter

Display name	Login SAM	Login UPN	Phone num ⁺
Alex	mycompany\alex	alex@mycompany.com	+47 3040
Jane	mycompany\jane	jane@mycompany.com	+1 200 36
John	mycompany\john	john@mycompany.com	+45 1026

- When maintaining the settings of a specific user, you may go to the **License** tab to inspect the license status of this user (cf. section 17.10.1.6, page 246).
- On the **User Group Policies** page, you can inspect license information across all User Group Policies. You can (a) enable columns with license related information to be shown, and (b) use row filtering to filter on license related information. For example, you may enable a filter that shows only User Group Policies granting Password Reset CALs.

Policies > User Group Policies

Maintain User Group Policies

Add new User Group Policy...

a Select columns **b** Set filter

Name	Description	Authentication Policy	Passcode Policy	Dispatch Policy
Default User Group Policy	Default User Group Policy	Default Authentication Policy	Default Passcode Policy	Default Dispatch Policy
Restricted Users	Users with restricted access	Restricted Access	Default Passcode Policy	Advanced failover

- When maintaining the settings of a specific User Group Policy, you may go to the **License** tab to inspect the license status of this particular User Group Policy (cf. section 17.6.1.4, page 181).

17.5 User Integration Policies

User Integration Policies let you define, how users are imported from other user stores, like Microsoft Active Directory (AD), OpenLDAP or AD LDS, to the SMS PASSCODE database. Not only are the users imported, they are also kept in sync with the external user store, using periodic synchronizations. As a result, you can maintain SMS PASSCODE users in the external user store(s), as you are used to, making administration of SMS PASSCODE users easy.

The most common scenario is to import users from Active Directory. No schema extension of the AD is necessary in this case. Import from other LDAP directories²¹ are also possible, for example OpenLDAP and AD LDS.

User Integration Policies support several advanced features:

- **Multi sync support:** It is possible to import users from one or several user stores, for example one or more ADs.
- **General LDAP support:** It is possible to import users from ADs, or from general LDAP directories, for example OpenLDAP or AD LDS.
- **Configurable protocol:** Synchronization can occur using the LDAP protocol; and in case of AD also using the Global Catalog (GC) protocol.

Optionally, SSL/TLS encryption can also be enabled to encrypt the network communication between the SMS PASSCODE database service and the user store.

- **Flexible user selection:** When importing users from a user store, you can define which subset of users to import. The easiest option is to import all users belonging to a specific user group. Alternatively, you may select users using an LDAP filter (advanced).
 - **Group nesting:** When importing users that are member of a specific user group, the chosen group may contain other groups in a nested hierarchy. Users of such nested groups are also imported, thereby making administration of SMS PASSCODE users even easier.
 - **Child domains and trusted domains:** When importing users from an AD, and using nested groups, such groups and/or users in the group hierarchy that are located in child domains and/or trusted domains are also imported.

²¹ Importing users from a non-AD directory is useful, if you are planning to authenticate such non-AD users using SMS PASSCODE. The SMS PASSCODE RADIUS Protection component allows authentication of non-AD users using LDAP authentication (cf. section 25.2.2.1, page 385).

- **Configurable import of user properties:** When importing users, you may customize which user properties to import. Login names and full name are always imported, when available. Additionally, you can decide to import any of the following user properties from the user store:
 - (Primary) phone number
 - Secondary phone number
 - Email address
 - Token ID
 - Personal passcode

Imported properties cannot be edited in the SMS PASSCODE database after import, since they are supposed to be maintained in the user store, and will be kept in sync, whenever a change occurs in the user store. In case any of the above properties are configured NOT to be imported from the user store, then they can be maintained manually in the SMS PASSCODE database by the administrator.

The administrator might grant users permission to maintain some of the above properties themselves using the SMS PASSCODE Self-service Website (SSWS). For example, users might maintain their phone numbers themselves. Please note, that the SSWS is only available for users imported from an AD, not for users imported from other types of LDAP directories. When users are granted permission to maintain some of the properties, any changes will be written back to the SMS PASSCODE database or directly to the user store, depending on whether the corresponding property was imported from the user store (AD) or not, respectively.

- **Configurable LDAP attribute mapping:** Each imported user property is retrieved from an LDAP attribute of the corresponding user in the user store. You configure, exactly which LDAP attribute to use for every user property in your specific organization. You might even configure a prioritized list of LDAP attributes to perform a prioritized search through multiple attributes of each user in the user store.
- **Data transformations:** Optionally apply data transformations to imported user properties, before they are stored in the SMS PASSCODE database.

Using nested group from child domains / trusted domains

Please note, when importing users from an AD, that to make use of nested groups from Child Domains and/or Trusted Domains, an AD user account that has read-access to all involved domains must exist. If the SMS PASSCODE **Database Service** is not started using this user account, the credentials of this user account must be specified as part of the User Integration Policy.

Alternatively, instead of using nested groups from child/trusted domains, you can create multiple User Integration Policies with separate settings (credentials) for each child/trusted domain explicitly.

In most cases, you will only need to create a single User Integration Policy (UIP), to define a single user sync from a single user store. When importing users from an AD by group membership, this might span several AD domains, because the selected group might contain nested groups, including nested groups from child domains and trusted domains. All users from nested groups are synchronized as well.

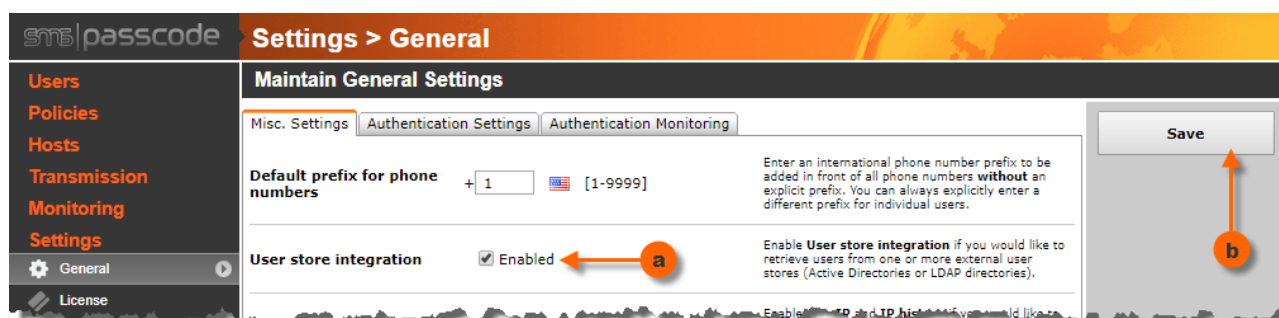
Optionally, you can create several User Integration Policies. For example, this can be relevant in the following cases:

- For hosting providers that are hosting multiple separate domains for different customers and wish to import the users of every customer using a separate UIP.
- For enterprise customers that wish to assign different User Group Policies to different subsets of the users. This can be achieved by letting each UIP assign a distinct User Group Policy to the imported users.
- For enterprise customers that wish to import users from both AD(s) and general LDAP directories.

17.5.1 Enable User Store Integration

Synchronization of users from an external user store is disabled by default. To enable it, please follow the simple procedure described below:

1. Select the **General** settings page.
2. Enable **User store Integration**:
 - a. Select the **Enabled** option.
 - b. Click the **Save** button.



17.5.2 Simple Setup (AD)

In the simplest case, if the SMS PASSCODE database service is running on a domain member server (or domain controller), and you wish to import users from this AD domain, and no child or trusted domains are involved, you will typically only need to enable User Store Integration, as described above, and after this, **User store integration** is ready for use – simply create a group called **SMS PASSCODE USERS** in your AD and add users or nested groups to this group.

Note: The simple setup will import users' (mobile) phone numbers from the default LDAP attribute "mobile", and email addresses from the default LDAP attribute "mail". Please read the "Advanced setup" section below, in case you want to import other user attributes as well, or in case you want to import phone numbers or email addresses from different LDAP attributes.

17.5.3 Advanced Setup

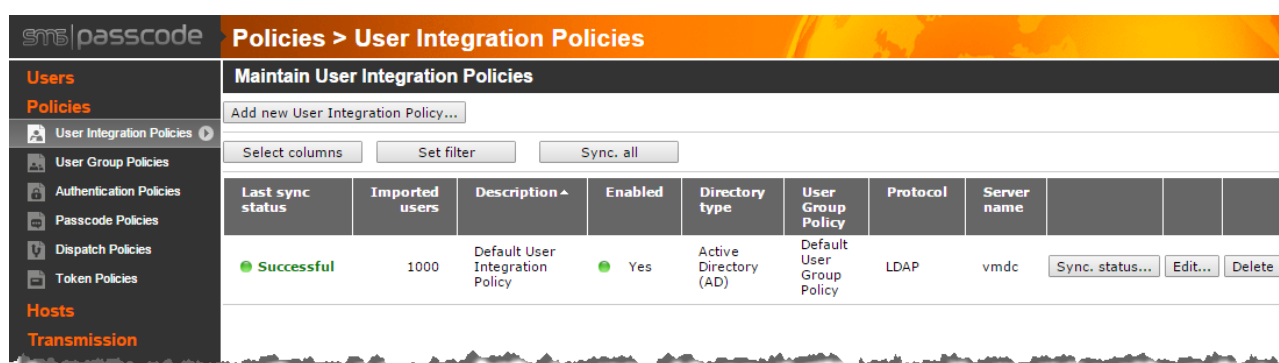
In more complex cases, where...

- The SMS PASSCODE database service is NOT running on a domain member server, or
- Nested groups from child domains or trusted domains are involved, or
- You need to import users from a non-AD LDAP directory, or
- You need to change some of the more advanced settings (e.g. because you plan to use Password Reset)

...then you will need to edit the Default User Integration Policy and configure it according to your specific requirements. Additionally, you can create additional User Integration Policies to define multiple user synchronizations running in parallel, with distinct settings. For example, to:

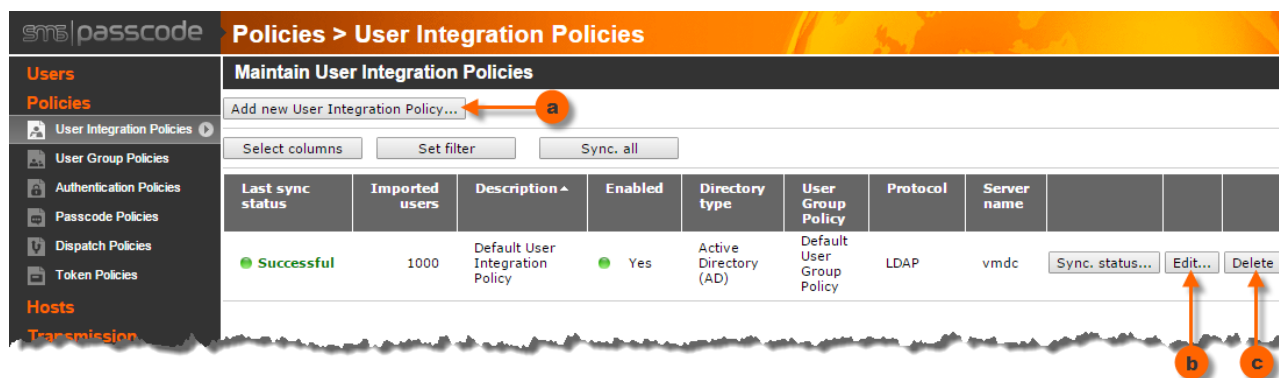
- Import users from multiple user groups, or
- Import users from multiple user stores, or
- Assign different User Group Policies to imported users

UIPs are maintained on the **User Integration Policies** page. The first time you enter this page, it will show an *UIP grid* looking similar to this:



Initially, the SMS PASSCODE database will only contain a single UIP called *Default User Integration Policy*. You can create any number of additional UIPs. To maintain UIPs, proceed as follows:

- To add a new UIP, click the **Add new User Integration Policy...** button.
- To edit a UIP, click the **Edit...** button on the policy.
- To delete a UIP, click the **Delete** button on the policy.



WARNING: Deleting a UIP will also remove all users imported through this UIP from the SMS PASSCODE database.

When editing a UIP, settings of the UIP are shown inside a tab control:

The screenshot shows the 'Edit User Integration Policy' page in the SMS PASSCODE web interface. The page is titled 'Policies > User Integration Policies' and 'Edit User Integration Policy: Default User Integration Policy (test.dom)'. The interface includes a sidebar with navigation links: Users, Policies (selected), User Group Policies, Authentication Policies, Passcode Policies, Dispatch Policies, Token Policies, Hosts, Transmission, Monitoring, and Settings. The main content area has a tab control with five tabs: General Settings (selected), Data Source, Data Mapping, Data Filtering, and Data Transformations. The General Settings tab contains the following settings:

- Directory type:** Radio buttons for 'Active Directory (AD)' (selected) and 'General LDAP'. Description: 'Select whether to synchronize users from a Microsoft Active Directory (AD) or from a general LDAP directory (advanced).'.
- Refresh interval:** A text input field with '5' and a label 'minutes'. Description: 'Specify how often to perform a synchronization. The entry must be in the interval [1-1440]. Default: 1.'.
- Default prefix:** Radio buttons for 'Use system default' (selected) and 'Default prefix: +' followed by a text input field. Description: 'Specify, which international phone number prefix to add in front of all phone numbers that do not have an explicit prefix beforehand.'.
- User Group Policy:** A dropdown menu with 'Default User Group Policy' selected. Description: 'Select the User Group Policy to assign to the imported users.'.
- AD lockout check interval:** A text input field with '15' and a label 'seconds'. Description: 'Specify how often to check for user lockouts in AD in order to send out AD lockout notifications. The entry must be in the interval [15-86400]. Default: 15.'.

On the right side of the page, there is a 'Save' button and a 'Show sync. status...' link.

The tab control contains five tabs, each containing different UIP settings:

- **General Settings**
Described in section 17.5.4.1, page 131.
- **Data Source**
Described in section 17.5.4.2, page 133.
- **Data Mapping**
Described in section 17.5.4.3, page 140.
- **Data Filtering**
Described in section 17.5.4.4, page 153
- **Data Transformations**
Described in section 17.5.4.5, page 154

IMPORTANT: Changes do not take effect until you click the **Save** button.

17.5.4 Settings of a User Integration Policy

17.5.4.1 UIP: General Settings

The **General Settings** tab contains various basic settings of the UIP:

Policies > User Integration Policies

Edit User Integration Policy: Default User Integration Policy (test1.local)

General Settings | Data Source | Data Mapping | Data Filtering | Data Transformations

a **Description** (Optional) Enter a description for your own reference.

b **Enabled** ☒ You can disable this user synchronization temporarily. All users previously imported will stay in the SMS PASSCODE database.

c **Directory type** ☒ Active Directory (AD) ☐ General LDAP Select whether to synchronize users from a Microsoft Active Directory (AD) or from a general LDAP directory (advanced).

d **Refresh interval** minutes Specify how often to perform a synchronization. The entry must be in the interval [5-1440]. Default: 5.

e **Default prefix** ☒ Use system default ☐ Default prefix: + Specify, which international phone number prefix to add in front of all phone numbers that do not have an explicit prefix beforehand.

f **User Group Policy** Select the User Group Policy to assign to the imported users.

g **Priority** Specify the priority of this user synchronization. In case a user is imported by several User Integration Policies, the user is assigned to the policy with highest priority.

h **AD lockout check interval** seconds Specify how often to check for user lockouts in AD in order to send out AD lockout notifications. The entry must be in the interval [15-86400]. Default: 15.

Save **Cancel** **Create copy of...** **Show sync. status...**

The settings are described in the table below:

	Setting	Explanation
(a)	Description	You can assign a description to each UIP. This description is shown in the <i>UIP grid</i> and is useful for identification when you have many UIPs. It can also be used when searching for specific UIPs using the Set filter button (located above the <i>UIP grid</i>).
(b)	Enabled	Using this option, you can enable or disable a UIP. When you disable a UIP, the users of the UIP stay in the SMS PASSCODE database, but no synchronizations will be performed anymore, until the policy is enabled again.
(c)	Directory type	Select, whether you want to import/synchronize users from an Active Directory (AD), or from a general LDAP directory (e.g. OpenLDAP).
(d)	Refresh interval	Enter into this field how often the synchronization engine should check for changes in the user store. The default value is every 5 minutes.

	Setting	Explanation
(e)	Default prefix	Specify the international phone number prefix to add in front of all imported phone numbers NOT having an explicit prefix specified already. Select Use system default to use the default prefix specified on the General Settings page.
(f)	User Group Policy	Select the User Group Policy to be assigned by default to all imported users. The User Group Policy determines several important settings for the users – please read section 17.6 (page 156) for more details regarding User Group Policies.
(g)	Priority	<p>This setting is only relevant, in case you have created multiple UIPs importing users from user groups within the <u>same</u> user store. In this case, you might have the potential conflict, that the same user is a member of several of the user groups. This raises the question, which UIP will eventually import the user, and which settings will consequently be applied to the user?</p> <p>To resolve this issue, the Priority setting can be used to prioritize the UIPs. You just need to enter a number into the field, indicating the priority of the UIP. A higher number means higher priority. If a user could be imported using several UIPs, the UIP with the highest priority (i.e. highest number) will import the user. In case you assign the same priority to several conflicting UIPs, then the winning UIP is chosen in an unpredictable way (not recommended).</p> <p>You can ignore this setting, if you have not created multiple UIPs importing users from the <u>same</u> user store.</p>
(h)	AD logout check interval	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Note: This setting is only available, when the setting Directory type has been set to Active Directory (AD). </div> <p>Enter into this field how often to check for AD lockouts. This setting is only relevant, in case you have enabled <i>AD Account Lockout</i> notifications for some of the users imported by this UIP (cf. section 17.6.1.3.3, page 175). Otherwise, the setting is ignored.</p> <p>It is recommended to keep the default setting of 15 seconds, since this will guarantee a fast response, resulting in fast notifications after AD lockouts occur.</p> <p>Note: The SMS PASSCODE system has intelligent logic for checking for AD lockouts. Consequently, even if you set the UIP to check for AD lockouts often, you should not see any heavy load on your domain controllers.</p>

17.5.4.2 UIP: Data Source

The **Data Source** tab of the UIP contains settings used to define, where and how to find the users to synchronize into the SMS PASSCODE database:

Policies > User Integration Policies

Edit User Integration Policy: Default User Integration Policy (test1.local)

General Settings | **Data Source** | Data Mapping | Data Filtering | Data Transformations

a Protocol

☒ LDAP
☐ Global Catalog
☐ Encrypt communication using SSL

Select whether to retrieve users from AD using LDAP or Global Catalog.

b Server name (Optional)

Specify the host name or IP address of a domain controller, or specify a domain name. If this policy is used for user synchronization only, and the database service runs on a domain member server, then you can leave this entry empty to synchronize from the same domain.

c Credentials (Optional)

Login:
 Password:

Specify credentials for AD authentication. If this policy is used for user synchronization only, and the database service account has AD read access to the relevant domain, then you can leave this entry empty.

d User selection

☒ Group membership (default)
☐ Custom LDAP filter (advanced)

Import users that are direct or indirect members of the group specified below.

Group name:
 SMS PASSCODE Users

Select how to retrieve users from the data source. You can either retrieve all users that are direct or indirect members of a specific user group, or retrieve users according to an LDAP filter (advanced).

Specify the name of the AD group (security or distribution group) containing the SMS PASSCODE users. The default group is "SMS PASSCODE Users". In case a group does not have a unique name within an AD forest, or there is no authorization to perform a search for the group from the root domain naming context, then please specify the complete distinguished name (DN) of the group.

e Connection test

Verify settings

Click the button to perform a connection test, verifying the settings above.

The settings are described in the table below:

	Setting	Explanation
(a)	Protocol	<ul style="list-style-type: none"> Directory type = Active Directory: When importing users from an AD, this setting allows you to select the protocol for synchronization. LDAP is normally recommended, but the Global Catalog protocol might provide performance advantages in environments with one or more child domains, because all information can be collected from the Global Catalog server instead of contacting each child domain controller sequentially. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> IMPORTANT (Global Catalog) When using Global Catalog, please note that you must ensure that the LDAP attributes specified on the Data mapping tab of the UIP are replicated²² to the Global Catalog. </div> <ul style="list-style-type: none"> Directory type = General LDAP: When importing users from a general LDAP directory, no selection is possible, since LDAP is always used in this case. <p>Optionally select the Encrypt communication using SSL checkbox to encrypt the network communication between the SMS PASSCODE database service and the user store using SSL/TLS.</p>
(b)	Server name	<ul style="list-style-type: none"> Directory type = Active Directory: If the SMS PASSCODE Database Service is running on a domain member server (or domain controller), then you can leave this field empty. The database service will then automatically locate a domain controller of the domain, to which it belongs. You may specify the host name or IP address of a domain controller anyhow, if you would like the synchronization always to occur with a specific domain controller. <p>On the other hand, if you would like to synchronize users outside the current domain, or if the SMS PASSCODE Database Service is NOT running on a domain member server (or domain controller), then you must specify either the DNS name of a domain, or the host name or IP address of a domain controller that should be used for synchronization.</p> <ul style="list-style-type: none"> Directory type = General LDAP: In this case, it is mandatory to specify the host name or IP address of the LDAP directory server containing the users to synchronize.

²² For more information about how to add attributes to the Global Catalog, please read <https://support.microsoft.com/da-dk/help/248717/how-to-modify-attributes-that-replicate-to-the-global-catalog>

	Setting	Explanation
(c)	Credentials	<ul style="list-style-type: none"> • Directory type = Active Directory: By default, the SMS PASSCODE Database Service will connect to a domain controller using the permissions of the user account executing the database service. If this is sufficient, e.g. because the database service is running on a domain member server or a domain controller, then you can leave this field empty. Credentials are normally only necessary if the SMS PASSCODE Database Service is NOT running on a domain member server (or domain controller), or if a specific user account is needed for read access to child domains and/or trusted domains. In this case, you should specify credentials (user name and password) for a user account having read access to all involved Active Directories. • Directory type = General LDAP: In this case, it is mandatory to specify credentials of a user having read access to the LDAP directory server containing the users to synchronize.
(d)	User selection	<p>This setting defines which subset of the users in the user store to synchronize. In the default case, when importing users from a selected user group in an AD, you only need to specify the name of this group. The default group name is SMS PASSCODE Users, but you may enter the name of a different group.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: User Group Search Issues (AD) When the synchronization engine tries to locate the specified user group, it will search for the specified user group by name, starting the search from the root domain naming context. In simple domains, this will typically work without any problems. However, in scenarios that are more complex, the group name might not be unique, or a search from the root domain naming context might fail due to lack of permissions. In such cases, you must enter the unique distinguished name (DN) of the user group, which will allow the synchronization engine to look up the user group directly. Here is an example of a distinguished name of a user group:</p> <p>CN=SMS PASSCODE Users,OU=DepartmentEast,DC=domainX,DC=com</p> </div> <p>When using the more advanced option "Custom LDAP Filter" for selecting users, or when importing users from a general LDAP directory, more options must be defined. This is explained in section 17.5.4.2.1 below.</p>
(e)	Connection test	<p>Finally, you can perform a test of the specified settings by clicking the Verify settings button. This will perform an authentication test and verify whether your Data source settings are correct. The test verifies:</p> <ul style="list-style-type: none"> • If a user store can be located. • If it is possible to authenticate and read data from the located user store. • If the specified user group can be found (in case User selection is set to Group membership)

IMPORTANT: When using UIP Settings for Password Reset

If you are planning to use the Password Reset module, then please note that the Password Reset component can be configured to use the UIP Data Source settings for performing the actual password reset operations for the users imported by such UIP. In this case, note the following:

- LDAP is always used for password reset operations, even when users are imported using the Global Catalog protocol.
- It is mandatory to explicitly specify Server/Domain (b) and credentials (c) in this case.
- Password Reset only works when **Directory type** is set to Active Directory on the **General Settings** tab of the UIP.

For more details on this, please read section 23.7.2.1, page 357.

17.5.4.2.1 User Selection (Advanced)

This section describes the settings relevant for defining **User selection** on the **Data Source** tab, in advanced scenarios. Advanced scenarios are:

- Synchronize users from AD or a general LDAP directory, using an LDAP filter for user selection
- Synchronize users from a general LDAP directory, using group membership for user selection

The relevant settings of the different scenarios are described below.

Synchronize users from AD or a general LDAP directory, using an LDAP filter for user selection

When synchronizing users using an LDAP filter (advanced), the required **User selection** settings are identical, when synchronizing from an AD or from a general LDAP directory, respectively.

Policies > User Integration Policies

Edit User Integration Policy: Default User Integration Policy (test1.local)

General Settings | **Data Source** | Data Mapping | Data Filtering | Data Transformations

Protocol

☒ LDAP
☐ Global Catalog
☐ Encrypt communication using SSL

Select whether to retrieve users from AD using LDAP or Global Catalog.

Server name
(Optional)

Specify the host name or IP address of a domain controller. If a domain name is specified, the database service runs on the member server, then this entry empty, then the database service runs on the same domain controller.

Important: Entry in this policy is also used for password reset.

Credentials
(Optional)

Login:
Password:

Specify credentials for authentication. If this policy is used for user synchronization and the database service has AD read access, then you can leave this entry empty.

Important: Entry in this policy is also used for password reset. Please make sure to provide credentials of an account with password reset permissions for relevant users that are managed by this policy.

User selection

☐ Group membership (default)
☒ Custom LDAP filter (advanced)

Import users according to the LDAP filter specified below.

a LDAP filter baseDN:
dc=my-domain,dc=local

Specify the distinguished name (DN) of the directory entry where to start the search to import.
Example: dc=my-domain,dc=local

b LDAP filter:
(&(objectClass=organizationalPerson)(memberOf=cn=SMS_PASSCODE Users,cn=Users,dc=my-domain,dc=local))

Specify an LDAP filter to select the users to import.
Example: (&(objectClass=organizationalPerson)(memberOf=cn=SMS_PASSCODE Users,cn=Users,dc=my-domain,dc=local))

	Setting	Explanation
(a)	LDAP filter baseDN	This setting defines the “root” of the search for users. You must specify the distinguished name (DN) of the node in the user store, from where to synchronize users. I.e. only users below this node (incl. sub nodes) will be collected, according to the LDAP filter (b).
(b)	LDAP filter	<p>This setting defines which users to synchronize. You must specify the filter condition using LDAP filter syntax (advanced). For example, you can choose only to collect users with a specific attribute having a specific value.</p> <p>Please ensure that only “user objects” are collected, for example by including a condition on the object class.</p>

When all settings have been specified, please use the **Verify settings** button to verify the correctness of the settings.

Synchronize users from a general LDAP directory, using group membership for user selection

When synchronizing users from a general LDAP directory, by group membership, several additional settings need to be defined compared to a synchronization from an AD. This is because in the general LDAP scenario the SMS PASSCODE system does not know, how user and group objects are defined, and how the “group membership” between such objects are defined. The following settings are used to define this:

User selection

☒ Group membership (default)
☐ Custom LDAP filter (advanced)

Import users that are direct or indirect members of the group specified below.

a Group name:

b Name of group members attribute:

c Name of group member lookup attribute:

d Object class for users:

e Object class for group(s):

Select from the either the direct or indirect members of the group specified below.
 Specify the group. It can be a complex DN of the group.
 Example: cn=SMS PASSCODE Users,cn=domain,
 Specify the attribute. The attribute lists the group. The "member" attribute lists the group members.
 Then specify the attribute value. The value lists the member's "entryDN" or "UID".
 Specify the object class for the user.
 Specify the object class for the group(s) to import.

	Setting	Explanation
(a)	Group name	<p>This setting specifies the user group containing the users to synchronize. It is mandatory to specify the complete distinguished name (DN) of the user group.</p> <p>The group can contain nested groups. In this case, users of all nested groups are synchronized as well.</p>
(b)	Name of group members attribute	This setting defines the name of the LDAP attribute containing group members. It is used to identify the group members of the group (a), as well as group members of any nested groups.
(c)	Name of group member lookup attribute	<p>This setting defines how group members are determined from the group members attribute (b). You must specify the name of the LDAP attribute on group <u>members</u> that matches the content of attribute (b) on a group. "Group members" means users, but possibly also nested groups.</p> <p><u>Example 1:</u> If setting (b) contains a list of DN's, then setting (c) must specify the name of the LDAP attribute on each group member that contains the DN.</p> <p><u>Example 2:</u> If setting (b) contains a list of unique IDs, then setting (c) must specify the name of the LDAP attribute on each group member that contains such unique ID.</p>
(d)	Object class for users	This setting defines the object class name of users in the user store. This is needed to identify users, since a group might contain other types of group member objects as well.
(e)	Object class for group(s)	This setting defines the object class name of groups in the user store. This is needed to identify nested groups, since a group might contain other types of group member objects as well.

When all settings have been specified, please use the **Verify settings** button to verify the correctness of the settings.

17.5.4.3 UIP: Data Mapping

The **Data Mapping** tab of the UIP contains settings to define the user properties to collect for each imported user, and from which LDAP attributes to import such properties. The number of settings depend on the scenario, whether users are being synchronized from an AD or a general LDAP directory, respectively.

Synchronizing users from AD (Directory type = AD)

When importing users from an AD, the following settings are displayed on the **Data Mapping** tab:

Policies > User Integration Policies

Edit User Integration Policy: Default User Integration Policy (test1.local)

General Settings | Data Source | **Data Mapping** | Data Filtering | Data Transformations

For each user property listed below, please specify whether to maintain it manually ("Do not import") or maintain it maintained in AD, please additionally specify, which LDAP attribute the property must be imported from. You may search multiple attributes in prioritized order.

a	Phone number Primary	Import from attribute(s) ▼	mobile	Optional: Specify one or several
b	Phone number Secondary	Do not import ▼		Optional: Specify one or several
c	Email	Import from attribute(s) ▼	mail	Optional: Specify one or several
d	Token assignment	Do not import ▼		Optional: Specify one or several
e	Personal passcode	Do not import ▼		Optional: Specify one or several

NOTE: LDAP attribute names

A list of valid LDAP attribute names can be found here:

[http://msdn.microsoft.com/en-us/library/ms683980\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms683980(VS.85).aspx)

The settings are described in the table below:

	Setting	Explanation
(a)	(Primary) phone number	<p>This setting specifies whether to extract (primary) phone numbers from the AD and assign them to the users imported from the AD.</p> <p><u>Import from AD:</u> If you want to extract users' (primary) phone numbers from the AD, then select Import from attribute(s) in the drop-down list. In this case, (primary) phone numbers are maintained in the AD and administrators are not allowed to change the imported phone numbers in the WAI. Users may, if allowed to, change the phone numbers using the SMS PASSCODE Self-service Website, but any changes are then written directly back to the AD.</p> <p>When Import from attribute(s) is selected, the textbox to the right of the drop-down list changes its border to a green color. Enter into this textbox the LDAP attribute name of the AD user attribute that contains the (primary) phone number to be extracted for each user. You can even specify multiple attributes separated by commas. In this case, the synchronization engine will perform a prioritized search for the phone number. E.g. if you enter "mobile, otherMobile", then the synchronization engine will first look for each user's phone number in the user attribute <code>mobile</code>. If this field does not contain any phone number, then the field <code>otherMobile</code> is searched.</p> <p><u>Do not import from AD:</u> If you want to maintain users' (primary) phone numbers in the SMS PASSCODE database only, then select Do not import in the drop-down list. In this case, users are imported from the AD without extracting any (primary) phone numbers. Instead, administrators can maintain the phone numbers manually in the WAI, or alternatively allow users to maintain the phone numbers themselves using the SMS PASSCODE Self-service Website. In either case, phone numbers are not written back to the AD, but stay in the SMS PASSCODE database only (which might be desirable due to privacy, e.g. in case private phone numbers are used).</p> <p><u>Default settings:</u> By default, (primary) phone numbers are imported from the AD and extracted from the LDAP attribute "mobile".</p>

	Setting	Explanation
(b)	Secondary phone number	<p>This setting specifies whether to extract secondary phone numbers from the AD and assign them to the users imported from the AD. Assigning secondary phone numbers to users might be useful, e.g. to provide mobile phone (receiver) failover using Dispatch Policies.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: This setting is only available, if Secondary phone numbers have been enabled on the General Settings page (cf. section 17.3.1, page 109).</p> </div> <p><u>Import from AD:</u> If you want to extract secondary phone numbers from the AD and assign to users, then select Import from attribute(s) in the drop-down list. In this case, secondary phone numbers are maintained in the AD and administrators are not allowed to change the imported secondary phone numbers in the WAI. Users may, if allowed to, change the secondary phone numbers using the SMS PASSCODE Self-service Website, but any changes are then written directly back to the AD.</p> <p>When Import from attribute(s) is selected, the textbox to the right of the drop-down list changes its border to a green color. Enter into this textbox the LDAP attribute name of the AD user attribute that contains the secondary phone number to be extracted for each user. You can even specify multiple attributes separated by commas. In this case, the synchronization engine will perform a prioritized search for the phone number. E.g. if you enter "pager, otherMobile", then the synchronization engine will first look for each user's secondary phone number in the user attribute pager. If this field does not contain any phone number, then the field otherMobile is searched.</p> <p><u>Do not import from AD:</u> If you want to maintain users' secondary phone numbers in the SMS PASSCODE database only, then select Do not import in the drop-down list. In this case, users are imported from the AD without extracting any secondary phone numbers. Instead, administrators can maintain the secondary phone numbers manually in the WAI, or alternatively allow users to maintain the secondary phone numbers themselves using the SMS PASSCODE Self-service Website. In either case, secondary phone numbers are not written back to the AD but stay in the SMS PASSCODE database only (which might be desirable due to privacy, e.g. in case private phone numbers are used).</p> <p><u>Default settings:</u> Secondary phone numbers are not imported from AD by default. If you enable the import, you must select an available LDAP attribute of own choice.</p>

	Setting	Explanation
(c)	Email	<p>This setting specifies whether to extract email addresses from the AD and assign them to the users imported from the AD.</p> <p><u>Import from AD:</u> If you want to extract users' email addresses from the AD, then select Import from attribute(s) in the drop-down list. In this case, email addresses are maintained in the AD and administrators are not allowed to change the email addresses in the WAI. Users may, if allowed to²³, change the email addresses using the SMS PASSCODE Self-service Website, but any changes are then written directly back to the AD.</p> <p>When Import from attribute(s) is selected, the textbox to the right of the drop-down list changes its border to a green color. Enter into this textbox the LDAP attribute name of the AD user attribute that contains the email address to be extracted for each user. You can even specify multiple attributes separated by commas. In this case, the synchronization engine will perform a prioritized search for the email address. E.g. if you enter "mail,otherMailBox", then the synchronization engine will first look for each user's email address in the user attribute <code>mail</code>. If this field does not contain any email address, then the field <code>otherMailBox</code> is searched.</p> <p>Note: Since email addresses can be imported from any LDAP attributes, this allows for the usage of external email addresses, e.g. to use email messages for failover.</p> <p><u>Do not import from AD:</u> If you want to maintain users' email addresses in the SMS PASSCODE database only, then select Do not import in the drop-down list. In this case, users are imported from the AD without extracting any email addresses. Instead, administrators can maintain the email addresses manually in the WAI, or alternatively allow users to maintain the email addresses themselves using the SMS PASSCODE Self-service Website. In either case, email addresses are not written back to the AD, but stay in the SMS PASSCODE database only (which might be desirable due to privacy, e.g. in case private email addresses are used).</p> <p><u>Default settings:</u> By default, email addresses are imported from the AD, and extracted from the LDAP attribute "mail".</p>

²³ A built-in rule will deny users to change their e-mail address in the SMS PASSCODE Self Service Website, in case the default LDAP attribute "mail" is used, even if an administrator allows users to change their e-mail address in the Self Service Website. It is mandatory to use a non-default LDAP attribute for the e-mail addresses, or alternatively disable import of e-mail addresses, if users should be allowed to maintain their e-mail address by themselves.

	Setting	Explanation
(d)	Token ID	<p>This setting specifies whether to extract token IDs from the AD and assign them to the users imported from the AD.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: This setting is only available, if token authentication has been allowed on the General Settings page (cf. section 17.3.2 page 110).</p> </div> <p><u>Import from AD:</u> If you want to extract token IDs²⁴ from the AD and assign to users, then select Import from attribute(s) in the drop-down list. In this case, token IDs are maintained in the AD and administrators are not allowed to change the imported token IDs in the WAI. Users may, if allowed to, change the token IDs using the SMS PASSCODE Self-service Website, but any changes are then written directly back to the AD.</p> <p>When Import from attribute(s) is selected, the textbox to the right of the drop-down list changes its border to a green color. Enter into this textbox the LDAP attribute name of the AD user attribute that contains the token ID to be extracted for each user. You can even specify multiple attributes separated by commas. In this case, the synchronization engine will perform a prioritized search for the token ID. E.g. if you enter "pager, otherPager", then the synchronization engine will first look for each user's token ID in the user attribute pager. If this field does not contain any token ID, then the field otherPager is searched.</p> <p><u>Do not import from AD:</u> If you want to maintain users' token IDs in the SMS PASSCODE database only, then select Do not import in the drop-down list. In this case, users are imported from the AD without extracting any token IDs. Instead, administrators can maintain the token IDs manually in the WAI, or alternatively allow users to maintain the token IDs themselves using the SMS PASSCODE Self-service Website. In either case, token IDs are not written back to the AD, but stay in the SMS PASSCODE database only.</p> <p><u>Default settings:</u> Token IDs are not imported from AD by default. If you enable the import, you must select an available LDAP attribute of own choice.</p>

²⁴ If a user is assigned to a Token Policy that uses token seed files, then the UIP will not import the token ID from AD, but instead import the public token S/N, and then determine the private token ID via the token seed mapping.

	Setting	Explanation
(e)	Personal Passcode	<p>This setting specifies whether to extract personal passcodes from the AD and assign them to the users imported from the AD.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: This setting is only available, if the usage of personal passcodes has been allowed on the General Settings page (cf. section 17.3.2 page 110).</p> </div> <p><u>Import from AD:</u> If you want to extract personal passcodes from the AD and assign them to users, then select Import from attribute(s) in the drop-down list. In this case, personal passcodes are maintained in the AD and administrators are not allowed to change the imported personal passcodes in the WAI. Users may, if allowed to, change their personal passcodes using the SMS PASSCODE Self-service Website, but any changes are then written directly back to the AD.</p> <p>When Import from attribute(s) is selected, the textbox to the right of the drop-down list changes its border to a green color. Enter into this textbox the LDAP attribute name of the AD user attribute that contains the personal passcode to be extracted for each user. You can even specify multiple attributes separated by commas. In this case, the synchronization engine will perform a prioritized search for the personal passcode.</p> <p><u>Do not import from AD:</u> If you want to maintain users' personal passcodes in the SMS PASSCODE database only, then select Do not import in the drop-down list. In this case, users are imported from the AD without extracting any personal passcodes. Instead, administrators can maintain the personal passcodes manually in the WAI, or alternatively allow users to maintain their personal passcodes themselves using the SMS PASSCODE Self-service Website. In either case, personal passcodes are not written back to the AD, but stay in the SMS PASSCODE database only.</p> <p><u>Default settings:</u> Personal passcodes are not imported from AD by default. If you enable the import, you must select an available LDAP attribute of own choice. It is possible to apply transformations to the imported personal passcodes, e.g. only retrieving the last 4 digits of an employee number. Transformations are described in section 17.5.4.5, page 154.</p>

Please note: Users not having any valid phone number in any of the specified LDAP attributes, or not having any valid email address in any of the specified LDAP attributes, might be skipped during AD synchronization due to **Data Filtering** settings. This is described in section 17.5.4.4.

Synchronizing users from a general LDAP directory (Directory type = General LDAP)

When importing users from a general LDAP directory, the following settings are displayed on the **Data Mapping** tab:

Policies > User Integration Policies

Edit User Integration Policy: Default User Integration Policy (test1.local)

General Settings | Data Source | **Data Mapping** | Data Filtering | Data Transformations

For each user property listed below, please specify whether to maintain it manually ("Do not import") or maintain it in the LDAP directory. For each property maintained in the LDAP directory, please additionally specify, which LDAP attribute the property must be imported from.

a	UserID	entryUUID	Please enter the name of an LDAP attribute (GUIDs). Typically called "entryUUID" (Novell).
b	Username (SAM)	Do not import	Optional: Specify an LDAP attribute. "Username (SAM)" field in the LDAP directory.
c	Username (UPN)	Do not import	Optional: Specify an LDAP attribute.
d	Display name	Import from attribute(s) displayName	Optional: Specify an LDAP attribute.
Regarding the properties below: You may enter a single LDAP attribute or a comma-separated list of LDAP attributes to search for.			
e	Phone number Primary	Import from attribute(s) mobile	Optional: Specify one or several numbers.
f	Phone number Secondary	Do not import	Optional: Specify one or several numbers.
g	Email	Import from attribute(s) mail	Optional: Specify one or several addresses.
h	Token assignment	Do not import	Optional: Specify one or several token assignments.
i	Personal passcode	Do not import	Optional: Specify one or several passcodes.

The settings are described in the table below.

	Setting	Explanation
(a)	UserID	This mandatory setting specifies the name of the LDAP attribute that uniquely identifies every user. It should be a permanent, unique, non-changing ID. SMS PASSCODE uses this ID to track changes of a specific user object during synchronizations.

	Setting	Explanation
(b)	Username (SAM)	<p>This setting specifies whether to extract usernames from the user store and assign them to the field "Username (SAM)" in the SMS PASSCODE database.</p> <p><u>Import from the user store:</u> If you want to extract usernames from the user store into the "Username (SAM)" field, then select Import from attribute(s) in the drop-down list. In this case, usernames (of type SAM) are maintained in the user store and administrators are not allowed to change the imported usernames in the WAI.</p> <p>When Import from attribute(s) is selected, the textbox to the right of the drop-down list changes its border to a green color. Enter into this textbox the LDAP attribute name of the user attribute that contains the username to be extracted for each user. You can even specify multiple attributes separated by commas. In this case, the synchronization engine will perform a prioritized search for the username through the list of attributes.</p> <p><u>Do not import from the user store:</u> If you want to maintain usernames (of type SAM) in the SMS PASSCODE database only, then select Do not import in the drop-down list. In this case, users are imported from the user store without extracting any usernames into the "Username (SAM)" field. Instead, administrators can maintain the usernames (of type SAM) manually in the WAI. Changes are not written back to the user store but stay in the SMS PASSCODE database only.</p>
(c)	Username (UPN)	<p>This setting specifies whether to extract usernames from the user store and assign them to the field "Username (UPN)" in the SMS PASSCODE database.</p> <p><u>Import from the user store:</u> If you want to extract usernames from the user store into the "Username (UPN)" field, then select Import from attribute(s) in the drop-down list. In this case, usernames (of type UPN) are maintained in the user store and administrators are not allowed to change the imported usernames in the WAI.</p> <p>When Import from attribute(s) is selected, the textbox to the right of the drop-down list changes its border to a green color. Enter into this textbox the LDAP attribute name of the user attribute that contains the username to be extracted for each user. You can even specify multiple attributes separated by commas. In this case, the synchronization engine will perform a prioritized search for the username through the list of attributes.</p> <p><u>Do not import from the user store:</u> If you want to maintain usernames (of type UPN) in the SMS PASSCODE database only, then select Do not import in the drop-down list. In this case, users are imported from the user store without extracting any usernames into the "Username (UPN)" field. Instead, administrators can maintain the usernames (of type UPN) manually in the WAI. Changes are not written back to the user store but stay in the SMS PASSCODE database only.</p>

	Setting	Explanation
(d)	Display name	<p>This setting specifies whether to extract the display names (full names) from the user store and assign them to the users imported from the user store.</p> <p><u>Import from the user store:</u> If you want to extract display names from the user store, then select Import from attribute(s) in the drop-down list. In this case, display names are maintained in the user store and administrators are not allowed to change the imported display names in the WAI.</p> <p>When Import from attribute(s) is selected, the textbox to the right of the drop-down list changes its border to a green color. Enter into this textbox the LDAP attribute name of the user attribute that contains the display name to be extracted for each user. You can even specify multiple attributes separated by commas. In this case, the synchronization engine will perform a prioritized search for the display name through the list of attributes.</p> <p><u>Do not import from the user store:</u> If you want to maintain display names in the SMS PASSCODE database only, then select Do not import in the drop-down list. In this case, users are imported from the user store without extracting any display names. Instead, administrators can maintain display names manually in the WAI. Changes are not written back to the user store but stay in the SMS PASSCODE database only.</p>
(e)	(Primary) phone number	<p>This setting specifies whether to extract (primary) phone numbers from the user store and assign them to the imported users.</p> <p><u>Import from the user store:</u> If you want to extract users' (primary) phone numbers from the user store, then select Import from attribute(s) in the drop-down list. In this case, (primary) phone numbers are maintained in the user store and administrators are not allowed to change the imported phone numbers in the WAI.</p> <p>When Import from attribute(s) is selected, the textbox to the right of the drop-down list changes its border to a green color. Enter into this textbox the LDAP attribute name of the user attribute that contains the (primary) phone number to be extracted for each user. You can even specify multiple attributes separated by commas. In this case, the synchronization engine will perform a prioritized search for the phone number. E.g. if you enter "mobile, otherMobile", then the synchronization engine will first look for each user's phone number in the user attribute <code>mobile</code>. If this field does not contain any phone number, then the field <code>otherMobile</code> is searched.</p> <p><u>Do not import from the user store:</u> If you want to maintain users' (primary) phone numbers in the SMS PASSCODE database only, then select Do not import in the drop-down list. In this case, users are imported from the user store without extracting any (primary) phone numbers. Instead, administrators can maintain the phone numbers manually in the WAI. Changes are not written back to the user store but stay in the SMS PASSCODE database only.</p>

	Setting	Explanation
(f)	Secondary phone number	<p>This setting specifies whether to extract secondary phone numbers from the user store and assign them to the imported users. Assigning secondary phone numbers to users might be useful, e.g. to provide mobile phone (receiver) failover using Dispatch Policies.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: This setting is only available, if Secondary phone numbers have been enabled on the General Settings page (cf. section 17.3.1, page 109).</p> </div> <p><u>Import from the user store:</u> If you want to extract secondary phone numbers from the user store and assign to users, then select Import from attribute(s) in the drop-down list. In this case, secondary phone numbers are maintained in the AD and administrators are not allowed to change the imported secondary phone numbers in the WAI.</p> <p>When Import from attribute(s) is selected, the textbox to the right of the drop-down list changes its border to a green color. Enter into this textbox the LDAP attribute name of the user attribute that contains the secondary phone number to be extracted for each user. You can even specify multiple attributes separated by commas. In this case, the synchronization engine will perform a prioritized search for the phone number. E.g. if you enter "pager, otherMobile", then the synchronization engine will first look for each user's secondary phone number in the user attribute pager. If this field does not contain any phone number, then the field otherMobile is searched.</p> <p><u>Do not import from the user store:</u> If you want to maintain users' secondary phone numbers in the SMS PASSCODE database only, then select Do not import in the drop-down list. In this case, users are imported from the user store without extracting any secondary phone numbers. Instead, administrators can maintain the secondary phone numbers manually in the WAI. Changes are not written back to the user store but stay in the SMS PASSCODE database only.</p>

	Setting	Explanation
(g)	Email	<p>This setting specifies whether to extract email addresses from the user store and assign them to the imported users.</p> <p><u>Import from the user store:</u> If you want to extract users' email addresses from the user store, then select Import from attribute(s) in the drop-down list. In this case, email addresses are maintained in the user store and administrators are not allowed to change the email addresses in the WAI.</p> <p>When Import from attribute(s) is selected, the textbox to the right of the drop-down list changes its border to a green color. Enter into this textbox the LDAP attribute name of the user attribute that contains the email address to be extracted for each user. You can even specify multiple attributes separated by commas. In this case, the synchronization engine will perform a prioritized search for the email address. E.g. if you enter "mail, otherMailBox", then the synchronization engine will first look for each user's email address in the user attribute <code>mail</code>. If this field does not contain any email address, then the field <code>otherMailBox</code> is searched.</p> <p><u>Do not import from the user store:</u> If you want to maintain users' email addresses in the SMS PASSCODE database only, then select Do not import in the drop-down list. In this case, users are imported from the user store without extracting any email addresses. Instead, administrators can maintain the email addresses manually in the WAI. Changes are not written back to the user store but stay in the SMS PASSCODE database only.</p>

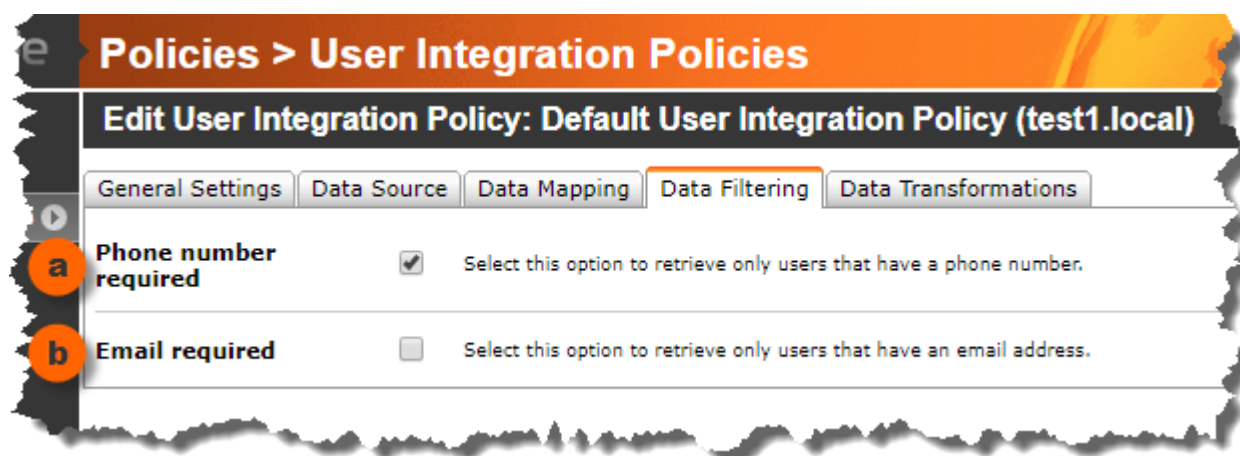
	Setting	Explanation
(h)	Token ID	<p>This setting specifies whether to extract token IDs from the user store and assign them to the imported users.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: This setting is only available, if token authentication has been allowed on the General Settings page (cf. section 17.3.2 page 110).</p> </div> <p><u>Import from the user store:</u> If you want to extract token IDs²⁵ from the user store and assign to users, then select Import from attribute(s) in the drop-down list. In this case, token IDs are maintained in the user store and administrators are not allowed to change the imported token IDs in the WAI.</p> <p>When Import from attribute(s) is selected, the textbox to the right of the drop-down list changes its border to a green color. Enter into this textbox the LDAP attribute name of the user attribute that contains the token ID to be extracted for each user. You can even specify multiple attributes separated by commas. In this case, the synchronization engine will perform a prioritized search for the token ID. E.g. if you enter "pager, otherPager", then the synchronization engine will first look for each user's token ID in the user attribute pager. If this field does not contain any token ID, then the field otherPager is searched.</p> <p><u>Do not import from the user store:</u> If you want to maintain users' token IDs in the SMS PASSCODE database only, then select Do not import in the drop-down list. In this case, users are imported from the user store without extracting any token IDs. Instead, administrators can maintain the token IDs manually in the WAI. Changes are not written back to the user store but stay in the SMS PASSCODE database only.</p>

²⁵ If a user is assigned to a Token Policy that uses token seed files, then the UIP will not import the token ID from AD, but instead import the public token S/N, and then determine the private token ID via the token seed mapping.

	Setting	Explanation
(i)	Personal Passcode	<p>This setting specifies whether to extract personal passcodes from the user store and assign them to the imported users.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: This setting is only available, if the usage of personal passcodes has been allowed on the General Settings page (cf. section 17.3.2 page 110).</p> </div> <p><u>Import from the user store:</u> If you want to extract personal passcodes from the user store and assign them to users, then select Import from attribute(s) in the drop-down list. In this case, personal passcodes are maintained in the user store and administrators are not allowed to change the imported personal passcodes in the WAI.</p> <p>When Import from attribute(s) is selected, the textbox to the right of the drop-down list changes its border to a green color. Enter into this textbox the LDAP attribute name of the user attribute that contains the personal passcode to be extracted for each user. You can even specify multiple attributes separated by commas. In this case, the synchronization engine will perform a prioritized search for the personal passcode.</p> <p><u>Do not import from the user store:</u> If you want to maintain users' personal passcodes in the SMS PASSCODE database only, then select Do not import in the drop-down list. In this case, users are imported from the user store without extracting any personal passcodes. Instead, administrators can maintain the personal passcodes manually in the WAI. Changes are not written back to the user store but stay in the SMS PASSCODE database only.</p> <p><u>Note:</u> It is possible to apply transformations to the imported personal passcodes, e.g. only retrieving the last 4 digits of an employee number. Transformations are described in section 17.5.4.5, page 154.</p>

17.5.4.4 UIP: Data Filtering

The **Data Filtering** tab of the UIP contains settings defining whether some users should be skipped during import:



The settings are described in the table below:

	Setting	Explanation
(a)	Phone number required	<p>Select this option if only users having a valid phone number should be imported from the user store or clear this option to allow import of users not having any phone number. Importing users without any phone number might make sense in the following cases:</p> <ul style="list-style-type: none"> The users without any phone numbers are going to authenticate using an authentication type not requiring any phone number, e.g. by Email OTP. You are planning to let the users enter their phone numbers by themselves, using the SMS PASSCODE Self-service Website (cf. section 22, page 325) – this is only possible, when importing users from AD.
(b)	Email required	<p>Select this option, if only users having a valid email address should be imported from the user store or clear this option to allow import of users not having any email address. Importing users without any email address might make sense in the following cases:</p> <ul style="list-style-type: none"> The users without any email address are going to authenticate using an authentication type not requiring any email address, e.g. by SMS OTP. You are planning to let the users enter their email addresses by themselves, using the SMS PASSCODE Self-service Website (cf. section 22, page 325) – this is only possible, when importing users from AD.

17.5.4.5 UIP: Data Transformations

When importing users from user stores (or custom CSV-files), it might sometimes be useful to apply data transformations to some of the imported user attributes. For example, all phone numbers in a user store might be prefixed with a zero ("0") due to some technical reasons for calling the number from the office. In this case, it would be useful to apply a data transformation that would remove any leading zeroes from all phone numbers. This is possible using the data transformation feature of SMS PASSCODE.

Data transformations can be applied to imported usernames, phone numbers, email addresses and personal passcodes. Transformations are specified using regular expression syntax (please read [http://msdn.microsoft.com/en-us/library/6wzad2b2\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/6wzad2b2(VS.85).aspx) or www.regular-expressions.info for a detailed description of regular expressions).

Data transformations are configured as part of a UIP. When maintaining a UIP, the data transformation settings are displayed on the **Data Transformations** tab:

Policies > User Integration Policies

Edit User Integration Policy: Default User Integration Policy (test1.local)

General SettingsData SourceData MappingData FilteringData Transformations

Phone number transform

Phone number search pattern

Phone number replacement pattern

Test transform:

Test

Optional (advanced): Transform imported phone numbers by applying the search pattern (regular expression) to each phone number and replacing the first search pattern match, if any, with the replacement string.

Username transform SAM

Username (SAM) search pattern

Username (SAM) replacement pattern

Test transform:

Test

Optional (advanced): Transform imported SAM usernames by applying the search pattern (regular expression) to each SAM username and replacing the first search pattern match, if any, with the replacement string.

Username transform UPN

Username (UPN) search pattern

Username (UPN) replacement pattern

Test transform:

Test

Optional (advanced): Transform imported UPN usernames by applying the search pattern (regular expression) to each UPN username and replacing the first search pattern match, if any, with the replacement string.

Email transform

Email search pattern

Email replacement pattern

Test transform:

Test

Optional (advanced): Transform imported email addresses by applying the search pattern (regular expression) to each email address and replacing the first search pattern match, if any, with the replacement string.

Personal passcode transform

Personal passcode search pattern

Personal passcode replacement pattern

Test transform:

Test

Optional (advanced): Transform imported personal passcodes by applying the search pattern (regular expression) to each personal passcode and replacing the first search pattern match, if any, with the replacement string.

The procedure for applying a data transformation to usernames, phone numbers or personal passcodes is the same. In any case, you enter a search pattern and a replacement string. During the import of new data, the search pattern will be applied to the data being imported, and in case any search pattern matches, the matching pattern will be replaced according to the replacement string. Any username, phone number or personal passcode not matching the search pattern will be imported unaltered.

Below are some data transformation examples:

- **Example 1:** Changing the domain name for imported users from “mydomain” to “yourdomain”:
 - Search pattern: ^mydomain\\(.*)\$
 - Replacement string: yourdomain\\\$1
 - Transformation example:
mydomain\alex → yourdomain\alex
- **Example 2:** Removing any leading zeroes from phone numbers:
 - Search pattern: ^(0*)(.*)\$
 - Replacement string: \$2
 - Transformation examples:
234 456 → 234 456
0 234 456 → 234 456
00 234 456 → 234 456
- **Example 3:** Removing parentheses and dashes from phone numbers in the format “(xxxx) xxxx-xxxx”:
 - Search pattern: ^(\((\d*)\))?\s*(\d*)\s*-\s*(\d*)\$
 - Replacement string: \$2 \$3 \$4
 - Transformation examples:
(461) 345-456 → 461 345 456
345 456 → 345 456
- **Example 4:** Removing parentheses, dashes or dots from phone numbers in the format “(xxx)xxx-xxxx”, “xxx.xxx.xxxx” or “xxx-xxx-xxxx”:
 - Search pattern: ^(\\$(?(\d*)\$)?)?(-?|¥.?)¥s*(\d*)¥s*(-?|¥.?)¥s*(\d*)\$
 - Replacement string: \$2 \$4 \$6
 - Transformation examples:
(123)123-4567 → 123 123 4567
123.456.7890 → 123 456 7890
123-456-7890 → 123 456 7890

17.6 User Group Policies

User Group Policies make it easy for administrators to manage user settings. The idea is that every user is assigned to a User Group Policy (UGP) and automatically inherits the settings specified by this policy. I.e. if the administrator would like to change a specific setting for all users assigned to a specific UGP, the administrator only needs to change this setting once on the UGP in question, and all users assigned to this UGP will instantly inherit the new setting. For example, the administrator could change the Dispatch Policy, Passcode Policy, SMS type (flash/standard) or Self-service Website permissions. At the same time, maximum flexibility is preserved, since most

settings of a UGP can be *overridden* on each individual user. This means if an exception needs to be defined for a specific user, the administrator can just override one or more settings on this specific user – no need to create a new UGP for this specific case.

Overall, this means you can manage user settings on a *group basis* using UGPs, or on an *individual user basis* by overriding UGP settings on any user.

UGPs can be assigned to users either manually or automatically during user synchronizations. Each User Integration Policy (UIP) specifies the UGP to assign to the imported users (cf. section 17.5, page 126). If you wish to assign different UGP's to users imported from a user store, you can proceed as follows:

- Group your users in several user groups in the user store (one group per UGP)
- Enable **User store integration** on the **General settings** page (cf. section 17.3.1, page 109)
- Create a UIP for each user group. Set each UIP to import users from a specific group and assign a specific UGP.

UGPs are maintained on the **User Group Policies** page. The first time you enter this page, it will look similar to this:

The screenshot displays the 'Policies > User Group Policies' interface. On the left is a sidebar with navigation links: Users, Policies (selected), User Integration Policies, User Group Policies (active), Authentication Policies, Passcode Policies, Dispatch Policies, and Token Policies. The main area is titled 'Maintain User Group Policies' and includes a button to 'Add new User Group Policy...'. Below this are 'Select columns' and 'Set filter' buttons. A table lists the policies:

Name	Description	Authentication Policy	Passcode Policy	Dispatch Policy	Users assigned	CAL allocation status		
Default User Group Policy	Default User Group Policy	Default Authentication Policy	Default Passcode Policy	Default Dispatch Policy	1053	Success	Edit...	Delete

Initially, the SMS PASSCODE database will only contain a single UGP called *Default User Group Policy*. This policy cannot be deleted and will always be assigned to users that are not assigned to

any other UGP. You can create any number of additional UGPs. To maintain UGPs, proceed as follows:

- To add a new UGP, click the **Add new User Group Policy...** button.
- To edit a UGP, click the **Edit...** button on the policy.
- To delete a UGP, click the **Delete** button on the policy.

Policies > User Group Policies

Maintain User Group Policies

Add new User Group Policy... **a**

Select columns Set filter

Name	Description	Authentication Policy	Passcode Policy	Dispatch Policy	Users assigned	CAL allocation status All CAL types		
Default User Group Policy	Default User Group Policy	Default Authentication Policy	Default Passcode Policy	Default Dispatch Policy	1003	Success	Edit...	Delete
Sales personnel	Policy for all sales personnel	Default Authentication Policy	Default Passcode Policy	Default Dispatch Policy	50	Success	b Edit...	c Delete

NOTE: The built-in **Default User Group Policy** is a special policy, which is assigned to users by default. You can edit, but not delete this policy.

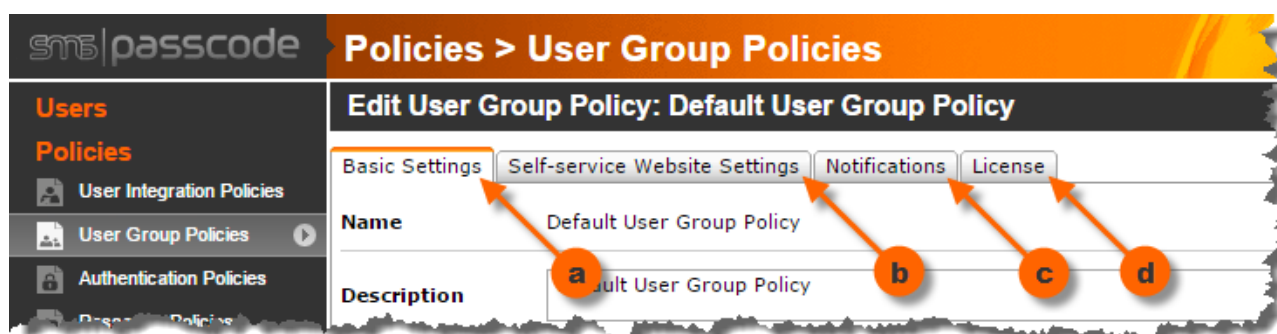
WARNING: When deleting a UGP, all users assigned to this UGP will be re-assigned to the *Default User Group Policy*.

The subsection below explains the different settings of a UGP in detail. Please note that the available settings of a UGP are adapted dynamically depending on other settings in SMS PASSCODE. This means, you might not see all the settings described in the next section.

17.6.1 Settings of a User Group Policy

When creating a new UGP or maintaining an existing UGP, a tab control is shown for configuring the different settings of the UGP. The settings are divided into four categories:

- a. **Basic Settings**
The main settings of the UGP, among others defining authentication behavior.
- b. **Self-service Website Settings**
Settings defining permissions and requirements regarding the SMS PASSCODE Self-service Website. These settings are only relevant, if you intend to make use of the SMS PASSCODE Self-service Website.
- c. **Notifications**
Settings defining whether to send out different types of user notifications automatically.
- d. **License**
License management settings, i.e. settings defining which CALs to grant to the users of the UGP.



The different settings are described in detail in the following subsections. When making changes to a UGP please remember to click the **Save** button to store the changes permanently.

17.6.1.1 User Group Policy: Basic Settings

This section describes the settings available on the **Basic Settings** tab while maintaining a UGP.

The screenshot shows the 'Policies > User Group Policies' interface. The main heading is 'Edit User Group Policy: Sales personnel'. Below this are four tabs: 'Basic Settings' (selected), 'Self-service Website Settings', 'Notifications', and 'License'. The 'Basic Settings' tab contains the following fields and options:

- Name:** A text input field containing 'Sales personnel' (labeled a).
- Description:** A text input field containing 'Policy for all sales personnel' (labeled b).
- Authentication Policy:** A dropdown menu showing 'Default Authentication Policy' (labeled c).
- Passcode Policy:** A dropdown menu showing 'Default Passcode Policy' (labeled d).
- Dispatch Policy:** A dropdown menu showing 'Default Dispatch Policy' (labeled e).
- Token Policy:** A dropdown menu showing 'Default Token Policy' (labeled f).
- Passcode type:** Radio buttons for 'One-time passcode (OTP)' (selected) and 'Personal passcode' (labeled g).
- SMS type:** Radio buttons for 'Flash SMS' (selected) and 'Standard SMS' (labeled h).
- Token authentication:** Radio buttons for 'Allow' and 'Deny' (selected) (labeled i).

	Setting	Explanation
(a)	Name	The name used to identify the UGP. Giving the UGP a unique name is mandatory.
(b)	Description	Optional description explaining the purpose of the UGP.
(c)	Authentication Policy	The Authentication Policy to assign to the users assigned to this UGP. An Authentication Policy defines the rules regarding authentication attempts of the user. Please read section 17.8 (page 193) for more details regarding Authentication Policies.

	Setting	Explanation
(d)	Passcode Policy	<p>The Passcode Policy to assign to the users assigned to this UGP. A Passcode Policy defines the dynamic content of passcode messages.</p> <p>Please read section 17.7 (page 184) for more details regarding Passcode Policies.</p>
(e)	Dispatch Policy	<p>The Dispatch Policy to assign to the users assigned to this UGP. A Dispatch Policy defines how passcode messages and notifications will be sent to users.</p> <p>Please read section 17.18 (page 271) for more details regarding Dispatch Policies.</p>
(f)	Token Policy	<p>The Token Policy to assign to the users assigned to this UGP. A Token Policy defines the type of tokens users are using (if any).</p> <p>Please read section 17.9 (page 221) for more details regarding Token Policies.</p> <p>Note: This setting is only available, if Token Authentication has been allowed on the General Settings page (cf. section 17.3.2 page 110).</p>
(g)	Passcode type	<p>The type of passcode to use for authenticating the users assigned to this UGP. One-time passcodes are strongly recommended.</p> <p>Note: This setting is only available, if personal passcodes have been allowed on the General Settings page (cf. section 17.3.2 page 110). Otherwise one-time-passcodes (OTPs) are always used.</p> <p>IMPORTANT: <i>Personal passcodes</i> are only recommended in case of emergency. Selecting this option reduces the security from multi-factor to one-factor authentication.</p> <p>Note: <i>Personal passcodes</i> cannot be used in case of emergency, when IntelliTrust™ authentication is in use (Hybrid Setup). In this case, configure the equivalent feature in IntelliTrust™, called Temporary Access Code.</p>
(h)	SMS type	<p>This setting specifies the type of SMS message to send to the users assigned to this UGP in case one-time passcodes are sent by SMS. Flash SMS has the advantage that on most mobile phones it will pop up automatically and will not be stored on the phone after usage. Flash SMS is recommended, unless it is not supported by your mobile phone or Telco²⁶.</p> <p>Note: This setting is ignored when one-time passcodes are not sent by SMS, or when they are sent by SMS using a Dispatch connector that does not support flash SMS.</p>

²⁶ You may disable flash SMS on individual users (user settings override), in case any specific users experience problems (cf. section 17.10.1.2, page 242)

	Setting	Explanation
(i)	Token authentication	<p>This setting specifies whether users assigned to this UGP are <u>allowed</u> to authenticate using a token. Please note that you must additionally <u>allocate</u> a unique token to each user to allow the user to authenticate successfully using a token. This is done by entering the ID of the user's token on the user's settings page (cf. section 17.10.1.1, page 237), or by granting the user permission to self-enroll by way of entering the token ID in the SMS PASSCODE Self-service Website.</p> <p>Note: This setting is only available, if Token authentication has been allowed on the General Settings page (cf. section 17.3.2 page 110).</p>

When *Personal Passcodes* are enabled for a UGP (*Passcode type* = **Personal passcode**), some additional settings appear on the page:

	Setting	Explanation
(j)	Personal passcode	<p>Enter the passcode that the users assigned to this UGP must enter to perform a successful authentication.</p> <p>Note: This setting is only available, if personal passcodes have been allowed for authentication on the General Settings page (cf. section 17.3.2 page 110).</p> <p>IMPORTANT: Please note that the personal passcode can be overridden by individual users. If you plan to make use of personal passcodes, then it is recommended to let the relevant users create a user-specific personal passcode beforehand using the SMS PASSCODE Self-service Website (this can be allowed on the Self-service Website Settings tab, cf. section 17.6.1.2 below). In this way, a user-specific personal passcode will already be in place, in case you decide to switch the <i>Passcode type</i> from OTP to Personal Passcode for the UGP.</p>
(k)	Personal passcode duration	<p>This option specifies for how long the personal passcode is valid for usage. When the personal passcode becomes invalid, the UGP will automatically switch back to Passcode type = One-time passcode.</p> <p>Note: This setting is only available, if personal passcodes have been allowed for authentication on the General Settings page (cf. section 17.3.2 page 110).</p>

Please note that most settings on the **Basic Settings** tab can be overridden by individual settings for each user (cf. section 17.10.1.2, page 242).

17.6.1.2 User Group Policy: Self-service Website Settings

This section describes the settings available on the **Self-service Website Settings** tab while maintaining a UGP. You only need to maintain settings on this tab if you intend to make use of the SMS PASSCODE Self-service Website (described in section 22). Otherwise, just keep the standard settings that will deny access to the Self-service Website (SSWS).

Policies > User Group Policies

Edit User Group Policy: Default User Group Policy

Basic Settings
Self-service Website Settings
Notifications
License

Permission		Allow	Deny
Access to Self-service		<input type="radio"/>	<input type="radio"/>
Permission	Mandatory*	Read/Write	Read-only
Username			<input type="radio"/>
Dispatch Policy		<input type="radio"/>	<input type="radio"/>
SMS type		<input type="radio"/>	<input type="radio"/>
Primary phone number	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
Secondary phone number	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
Email	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
Personal passcode	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
Passcode type			<input type="radio"/>
PIN	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
Token Policy		<input type="radio"/>	<input type="radio"/>
Token assignment	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
Permission		Allow	Deny
Resync token		<input type="radio"/>	<input type="radio"/>

*Data is only mandatory, if the user is actually allowed to change it.

Minimum length requirement

Min. required length, if the user makes an entry:
PIN:
Personal passcode:

	Setting	Explanation
(a)	Permissions	<p>The permission table specifies the rights for the users assigned to this UGP regarding the SMS PASSCODE Self-service Website (SSWS). The following permissions can be set:</p> <p><u>Access to Self-service</u> Specifies whether the user is allowed to log in to the SSWS at all. If this setting is set to Deny, then all other settings on this tab are ignored.</p> <p>Note: Only AD users can access the SSWS (either created manually in the SMS PASSCODE database or imported using a User Integration Policy with Directory type set to Active Directory).</p> <p><u>Usernames</u> Specifies whether to display the usernames of the user in the SSWS.</p> <p><u>Dispatch Policy</u> Specifies whether the user is allowed to override and change the <i>Dispatch Policy</i> for sending (passcode) messages to the user. For example, you can create Dispatch Policies with preference for SMS or voice call, respectively, and then let the users choose themselves.</p> <p><u>SMS type</u> Specifies whether the user is allowed to override and change the <i>SMS type</i> (Flash or Standard SMS) used when sending one-time passcodes to the user by SMS.</p> <p><u>(Primary/Secondary) phone number</u> Specifies whether the user is allowed to change his phone number(s).</p> <p>Note: The permission to change secondary phone number is only shown if secondary phone numbers have been enabled on the General settings page (cf. section 17.3.1, page 109).</p> <p><u>Email</u> Specifies whether the user is allowed to change his email address.</p> <p>Note: If a specific user has been imported from an AD into the SMS PASSCODE database by a User Integration Policy, and the user's email address was determined by the default email attribute in AD (LDAP attribute "mail"), then the user will NOT be allowed to change his email address in the Self-service Website, regardless of the permission set by the Email option.</p> <p><u>Personal passcode</u> Specifies whether the user is allowed to override and set/change a personal passcode that can be used in case the administrator sets authentication to use personal passcodes, or in case the user accesses the SMS PASSCODE Password Reset Website.</p> <p><u>Passcode type</u> Specifies whether to display the currently set <i>Passcode type</i> of the user in the SSWS.</p> <p>Note: This setting is only available, if personal passcodes have been allowed on the General Settings page (cf. section 17.3.2 page 110). Otherwise one-time-passcodes (OTPs) are always used.</p>

	Setting	Explanation
		<p><u>PIN</u> Specifies whether the user is allowed to override and set/change a personal PIN code that can be used during authentication.</p> <p>Note: This option is only available if the usage of PIN codes has been allowed on the General settings page (cf. section 17.3.2, page 110).</p> <p><u>Token Policy</u> Specifies whether the user is allowed to override and select a Token Policy of own choice. In this way the user might decide by himself which kind of token to use – which might make sense in case of software tokens. For example, the user might choose between two Token Policies called “MS Authenticator” and “Google authenticator”.</p> <p>Note: This option is only available if Token authentication has been allowed on the General settings page (cf. section 17.3.2, page 110).</p> <p><u>Token assignment</u> Specifies whether the user is allowed to set/change the token assigned to him. This is recommended, in case you would like users to self-enroll their tokens.</p> <p>Note: This option is only available if Token authentication has been allowed on the General settings page (cf. section 17.3.2, page 110).</p> <p><u>Resync token</u> Specifies whether the user is allowed to perform a complete resynchronization of his token in case it has come out of sync. When allowed to, a button for resynchronizing the token appears in the SSWS.</p> <p>As an administrator, you may always perform a resynchronization of user's token (cf. section 17.10.1.1, page 237).</p> <p>Note: This option is only available if Token authentication has been allowed on the General settings page (cf. section 17.3.2, page 110).</p>

	Setting	Explanation
(b)	Mandatory data	<p>Specifies the data that the user is required to enter in the SSWS. The user will not be able to save any changes in the SSWS before all required data has been entered.</p> <p>Please note that any data is only really required, if the user has also been granted the permission to change the data in question. For example, if Personal Passcode is set to required, but the Personal Passcode permission has been set to Deny, then the user cannot enter any Personal Passcode in the SSWS, and therefore cannot be forced to do so.</p> <p>You can require the users to enter their (mobile) phone numbers. This is especially useful in case the phone numbers have not been collected yet at all – just let the users do the job themselves.</p>
(c)	Minimum length requirement	This setting allows setting a minimum required length for the PIN code and/or personal passcode, in case the users have been allowed to change any of these. This ensures that the users will not enter too simple PIN codes or personal passcodes.

17.6.1.3 User Group Policy: Notifications

This section describes the settings available on the **Notifications** tab while maintaining a UGP. The **Notifications** tab is used to enable or disable different types of automatic user notifications:

Notification type	Description
Self-service	When enabled, a welcome notification is sent to a user, which informs about the usage of the Self-service Website. Additionally, reminder notifications can be sent to the user, if mandatory data is missing to be filled out on the Self-service Website.
SMS PASSCODE Lockout	When enabled, a notification is sent to a user whenever he is locked out in the SMS PASSCODE system.
AD Account Lockout	When enabled, a notification is sent to a user whenever he is locked out in the AD.
Before Password Expiration	When enabled, a notification is sent to a user whenever his AD password will expire soon.
On Password Expiration	When enabled, a notification is sent to a user whenever his AD password has just expired.

The purpose of the **Self-service** notifications is to make new users aware of the possibilities of the SMS PASSCODE Self-service Website. For example, the notifications can be configured to contain the URL of the Self-service Website.

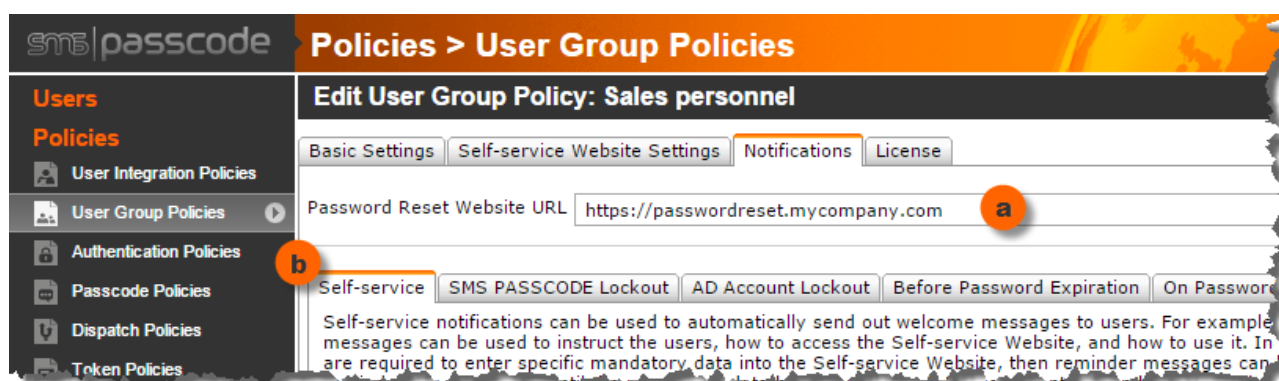
The **SMS PASSCODE Lockout** and **AD Account Lockout** notifications both have two purposes:

- Strengthen security:
Since the user is notified immediately about the lockout, he can take immediate counter-actions, in case the lockout was unexpected, e.g. due to a hacker attempting to compromise the user's login credentials.
- Improve "password reset" convenience:
A lockout may occur, because a user has forgotten his password and triggered a lockout in the process of guessing the forgotten password. A convenient feature is that the lockout notification text can be configured to contain the URL of the SMS PASSCODE Password Reset Website. Consequently, the user is automatically reminded about the possibility to reset the password by himself, thereby being able to continue work without interruptions.

The **Before Password Expiration** and **On Password Expiration** notifications both have the purpose of reminding the user about the need of renewing the existing AD password. Again, the notification text can be configured to contain the URL of the SMS PASSCODE Password Reset Website, thereby providing a very convenient way of resetting the password immediately. If the notification is received on a smartphone, the password reset process can be performed right away on the smartphone itself, just by clicking the URL (hyperlink).

By default, every notification is sent according to the Dispatch Policy of the user (as set on the **Basic Settings** tab of the UGP, unless it has been overridden on the user). However, it is possible per notification type to select a different Dispatch Policy, for example a policy sending notifications by email.

The screenshot below shows the settings on the **Notifications** tab:



	Setting	Explanation
(a)	Password Reset Website URL	<p>This setting specifies the URL that the users must use to access the Password Reset Website. By default, this URL is shown in Self-service notifications and password related notifications sent to users.</p> <p>Please enter https:// in front of the URL. If the Password Reset Website has been published for external access, then please enter the public URL.</p> <div style="border: 1px solid black; padding: 5px; background-color: #f9f9f9;"> <p>Note: This setting is only available, in case any Password Reset CALs have been acquired.</p> </div>
(b)	Notifications	A sub tab displays the individual settings for each types of notification. The settings of each sub tab are described below.

17.6.1.3.1 Self-service Notification

The **Self-service** tab contains the settings regarding **Self-service welcome** and **Self-service reminder** notifications:

A good way to get users started using the SMS PASSCODE Self-service Website is to send them a message, informing them about how to access it. This is exactly what the **Self-service** notifications can do automatically for you.

Self-service notifications can be used for two purposes:

- **Welcome notifications:** Informing new SMS PASSCODE users, that they have access to the SMS PASSCODE Self-service Website – and how to access it.
- **Reminder notifications:** Sending periodic reminders to existing users in case they have forgotten to enter any mandatory data in the SMS PASSCODE Self-service Website.

The settings available for configuring the **Self-service** notifications are described below:

Policies > User Group Policies

Edit User Group Policy: Sales personnel

Basic Settings | Self-service Website Settings | **Notifications** | License

Password Reset Website URL

Self-service | SMS PASSCODE Lockout | AD Account Lockout | Before Password Expiration | On Password Expiration

Self-service notifications can be used to automatically send out welcome messages to users. For example, such messages can be used to instruct the users, how to access the Self-service Website, and how to use it. In case users are required to enter specific mandatory data into the Self-service Website, then reminder messages can be used to remind users about this, until the mandatory data has been entered. Message content can be changed by linking to customized message template files.

Note: Self-service notifications are only sent to users that have been granted access to the Self-service Website

a ☒ Send a welcome notification to users
☐ Only if any mandatory data is missing

b ☒ Send a reminder notification to users that have not entered mandatory data yet
The reminder notification will be sent every days at (time of DB server), until the mandatory data has been entered.

c Dispatch Policy
☒ Standard (determined by the actual user)
☐ Override - always use:

d Message content
The URL that will be displayed in notifications to allow users to access the Self-service Website:

e Welcome notifications - filename of template file:

f Reminder notifications - filename of template file:

	Setting	Explanation
(a)	Enable welcome notifications	<p>Select the checkbox “Send a welcome notification to users” to enable welcome notifications. When enabled, users assigned to the UGP will receive a welcome notification, which can contain important information about SMS PASSCODE in general and about the usage of the Self-service Website (SSWS) in particular.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: Welcome notifications are only sent to <u>AD</u> user accounts that have been <u>granted</u> access to the SSWS (users, either created manually in the SMS PASSCODE database, or imported using a User Integration Policy with Directory type set to Active Directory).</p> </div> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>WARNING: When you enable welcome notifications and save the UGP, the system will immediately start transmission of welcome notifications to the users assigned to the UGP. If you have many users assigned to the UGP, then carefully consider, how many messages will be sent, and consider whether the correct Dispatch Policy has been set. It is recommended to create a dedicated Dispatch Policy and assign this in setting (c). Moreover, it is recommended that such dedicated Dispatch Policy should send messages by email, or alternatively, if sending messages via SMS, to set an extended transmission timeout, since sending long messages by SMS takes more time, than sending short OTP messages.</p> </div> <p>Welcome notifications are sent to...</p> <ul style="list-style-type: none"> • New users that are assigned to this UGP. • Existing users, in case they are re-assigned from a different UGP to this UGP. • Existing users, already assigned to this UGP, in case they have not received the welcome notification previously (applies, when you enable welcome notifications for a UGP that already has users assigned). <p>Welcome notifications are only sent once to each user. However, in case you need to resend a welcome notification to a specific user, you can force this on the user maintenance page (cf. section 17.10.1.4, page 244).</p> <p>Optionally, you may limit welcome notifications only to be sent to users that have mandatory data missing to be filled out in the SSWS. This is achieved by selecting the checkbox “Only if any mandatory data is missing”.</p> <p>The content of welcome notifications will contain the URL of the SSWS by default, according to setting (d), but the content of the notifications can be customized according to setting (e).</p>

	Setting	Explanation
(b)	Enable reminder notifications	<p>Select the checkbox “Send a reminder notification to users that have not entered mandatory data yet” to enable reminder notifications. When enabled, all users assigned to the UGP will receive a reminder notification, if they have been granted access to the SSWS, and any data marked as “mandatory” is missing to be filled out.</p> <p>Additionally, you can specify, how often to resend reminders, and at what time of the day reminders must be sent. Every user of the UGP will continue to receive reminder notifications, until the relevant mandatory data has been entered on the SSWS. For example, this can be used to motivate users to enter their phone numbers or personal passcodes.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: Reminder notifications are only sent to <u>AD</u> user accounts that have been <u>granted</u> access to the SSWS (users, either created manually in the SMS PASSCODE database, or imported using a User Integration Policy with Directory type set to Active Directory).</p> </div> <p>The content of reminder notifications will contain the URL of the SSWS by default, according to setting (d), but the content of the notifications can be customized according to setting (f).</p>
(c)	Dispatch Policy	<p>By default, welcome and reminder notifications are sent using the Dispatch Policy assigned to each user, meaning in the same way as passcode messages are sent to the user. In case you prefer to send Self-service notifications in a different way, you may override the Dispatch Policy to use. For example, selecting a Dispatch Policy that always sends messages by email.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>IMPORTANT: It is recommended to set a dedicated Dispatch Policy for Self-service notifications. Moreover, it is recommended that such dedicated Dispatch Policy is configured to send messages by email, or alternatively, if sending messages via SMS, to set an extended transmission timeout, since sending long messages by SMS takes more time, than sending short OTP messages.</p> </div>
(d)	Self-service Website URL	<p>Specifies the URL that the users must use to access the SSWS. By default, this URL will be shown in both welcome and reminder notifications. However, the notification content can be customized – cf. settings (e) and (f) below.</p> <p>Please enter http:// or https:// in front of the URL, depending on the fact whether the SSWS is protected with Windows Authentication or Form-based authentication, respectively (cf. section 22.5, page 328).</p>

	Setting	Explanation
(e)	Welcome notification – template file	<p>Specifies the path to the message template file that defines the content of welcome notifications.</p> <div> Note: Only enter the name of the template file. The template file must be located in the “Templates” folder, which is located in the SMS PASSCODE installation folder on the SMS PASSCODE database server. </div> <p>If you need to customize the content of welcome notifications, then it is recommended to make a copy of the default message template file, apply changes to the content of the copied file, and then reference the copied file in setting (e).</p> <p>Please note that the default message template file has the “Read-only” file attribute set, to avoid unintended changes. When you make a copy, you must remove the “Read-only” attribute on the new file, to be able to modify it.</p>
(f)	Reminder notification – template file	<p>Specifies the path to the message template file that defines the content of reminder notifications.</p> <div> Note: Only enter the name of the template file. The template file must be located in the “Templates” folder, which is located in the SMS PASSCODE installation folder on the SMS PASSCODE database server. </div> <p>If you need to customize the content of reminder notifications, then it is recommended to make a copy of the default message template file, apply changes to the content of the copied file, and then reference the copied file in setting (f).</p> <p>Please note that the default message template file has the “Read-only” file attribute set, to avoid unintended changes. When you make a copy, you must remove the “Read-only” attribute on the new file, to be able to modify it.</p>

17.6.1.3.2 SMS PASSCODE Lockout Notification

The **SMS PASSCODE Lockout** tab contains settings regarding **SMS PASSCODE Lockout** notifications:

Policies > User Group Policies

Edit User Group Policy: Sales personnel

Basic Settings | Self-service Website Settings | **Notifications** | License

Password Reset Website URL:

Self-service | **SMS PASSCODE Lockout** | AD Account Lockout | Before Password Expiration | On Password Expiration

a ☒ Send out a notification when a user is locked out from SMS PASSCODE Reset template

Dispatch Policy

b ☒ Standard (determined by the actual user)
☐ Override - always use:

c Message content

WARNING!
 Your SMS PASSCODE account has been locked out.
 Reason: [REASON]
 Lockout duration: [DURATION]
 {You may reset your password here: [PRS URL]}
 Please contact your system administrator, if this lockout is unexpected.
 [LICENSEE]

d Estimated length of message: 206 - 345 characters

e Email subject

Your SMS PASSCODE account has been locked out!

Allowed macros

{...}	Conditional text for Password Reset info. The characters '{' and '}' are <u>always</u> removed from any message. The text between these characters is only shown in the message, in case the user is locked out due to entering incorrect passwords, <u>and</u> the user has been allocated a Password Reset CAL.
[USERNAME]	Name of the user receiving the notification
[REASON]	Reason for the user lockout
[DURATION]	Duration of the user lockout
[PRS URL]	URL of the Password Reset Web Site
[LICENSEE]	Owner of the license of the SMS PASSCODE system

	Setting	Explanation
(a)	Notification enabled	<p>Select the checkbox “Send out a notification when a user is locked out from SMS PASSCODE” to enable SMS PASSCODE lockout notifications (recommended). When enabled, all users of the UGP will receive a notification whenever they are locked out by the SMS PASSCODE system.</p> <p>SMS PASSCODE lockout notifications are enabled by default.</p>

	Setting	Explanation
(b)	Dispatch Policy	By default, lockout notifications are sent using the Dispatch Policy assigned to each user, meaning in the same way as passcode messages are sent to the user. In case you prefer to send lockout notifications in a different way, you may override the Dispatch Policy to use.
(c)	Message content	<p>Specifies the message content of the notification. You can enter static text, but also macros (placeholders) that will be substituted with relevant content when sending the notification. A list of allowed macros is shown at the bottom of the web page.</p> <p><u>Password Reset tip:</u> Any text put between the characters "{" and "}" is treated as conditional text, that is only included in the lockout notification message, in case the following conditions are all fulfilled:</p> <ul style="list-style-type: none"> • The user was locked out due to a password brute-force attempt (i.e. a wrong password was entered several times in a row). • A Password Reset CAL has been allocated to the user <p>Note: The macros "{...}" and "[PRS URL]" are only available, in case any Password Reset CALs have been acquired.</p>
(d)	Estimated length of message	Shows the estimated length of the lockout notification content after macro substitutions. If the estimated length is more than 160 characters, then please take the information regarding "Notification message length" in section 17.6.1.3.6 (page 181) into account.
(e)	Email subject	This setting is only relevant when the lockout notification is sent by email. In this case, the setting specifies the content of the email subject. Macros are allowed here, too.

17.6.1.3.3 AD Account Lockout Notification

The **AD Account Lockout** tab contains settings regarding **AD Account Lockout** notifications:

Policies > User Group Policies

Edit User Group Policy: Sales personnel

Basic Settings | Self-service Website Settings | **Notifications** | License

Password Reset Website URL:

Self-service | SMS PASSCODE Lockout | **AD Account Lockout** | Before Password Expiration | On Password Expiration

a ☒ Send out a notification when a user is locked out from AD Reset template

b Dispatch Policy

☒ Standard (determined by the actual user)
☐ Override - always use:

c Message content

WARNING!
Your Windows account has been locked out.
You may reset your password here: [PRS URL]
Please contact your system administrator, if this lockout is unexpected.
[LICENSEE]

d Estimated length of message: 200 characters

e Email subject

Allowed macros

[USERNAME]	Name of the user receiving the notification
[PRS URL]	URL of the Password Reset Web Site
[LICENSEE]	Owner of the license of the SMS PASSCODE system

	Setting	Explanation
(a)	Notification enabled	<p>Select the checkbox “Send out a notification when a user is locked out from AD” to enable AD account lockout notifications. When enabled, any user assigned to the UGP will receive a notification whenever his account becomes locked out in AD.</p> <div> <p>IMPORTANT: Password Reset CAL required Please note that a user will only receive an AD account lockout notification if a Password Reset CAL has been allocated to the user.</p> <p>IMPORTANT: UIP required AD account lockout notifications only work for users imported into the SMS PASSCODE database through a User Integration Policy (UIP) with Directory type set to <u>Active Directory</u>. The UIP has a setting specifying how often to check for AD lockouts (AD lockout check interval, cf. section 17.5.4.1, page 131).</p> </div> <p>AD account lockout notifications are disabled by default. It is recommended to enable them if you are using the SMS PASSCODE Password Reset module.</p>
(b)	Dispatch Policy	By default, lockout notifications are sent using the Dispatch Policy assigned to each user, meaning in the same way as passcode messages are sent to the user. In case you prefer to send lockout notifications in a different way, you may override the Dispatch Policy to use.
(c)	Message content	Specifies the message content of the notification. You can enter static text, but also macros (placeholders) that will be substituted with relevant content when sending the notification. A list of allowed macros is shown at the bottom of the web page.
(d)	Estimated length of message	Shows the estimated length of the notification content after macro substitutions. If the estimated length is more than 160 characters, then please take the information regarding “Notification message length” in section 17.6.1.3.6 (page 181) into account.
(e)	Email subject	This setting is only relevant when the notification is sent by email. In this case, the setting specifies the content of the email subject. Macros are allowed here, too.

17.6.1.3.4 “Before Password Expiration” Notification

The **Before Password Expiration** tab contains settings regarding **Password Pre-expiration** notifications:

Policies > User Group Policies

Edit User Group Policy: Sales personnel

Basic Settings | Self-service Website Settings | **Notifications** | License

Password Reset Website URL:

Self-service | SMS PASSCODE Lockout | AD Account Lockout | **Before Password Expiration** | On Password Expiration

a ☒ Send out a notification when a user's password will expire soon

b Send notification days before password expiration Reset template

c Dispatch Policy

☒ Standard (determined by the actual user)

☐ Override - always use:

d Message content

SERVICE MESSAGE:
Your password will expire in [REMAINING] days.
You can set a new password here: [PRS URL]
[LICENSEE]

e Estimated length of message: 129 characters

f Email subject

Allowed macros

[USERNAME]	Name of the user receiving the notification
[REMAINING]	Number of days until the password expires
[PRS URL]	URL of the Password Reset Web Site

	Setting	Explanation
(a)	Notification enabled	<p>Select the checkbox “Send out a notification when a user’s password will expire soon” to enable password pre-expiration notifications. When enabled, any user assigned to the UGP will receive a notification whenever his AD password will expire soon.</p> <div> <p>IMPORTANT: Password Reset CAL required Please note that a user will only receive a password pre-expiration notification if a Password Reset CAL has been allocated to the user.</p> <p>IMPORTANT: UIP required Password pre-expiration notifications only work for users imported into the SMS PASSCODE database through a User Integration Policy (UIP) with Directory type set to <u>Active Directory</u>. The pre-expiration check is done as part of every AD sync.</p> </div> <p>Password pre-expiration notifications are disabled by default. It is recommended to enable them if you are using the SMS PASSCODE Password Reset module.</p>
(b)	Pre-notification period	Specifies how early a user will be notified, before the AD password expires. E.g. if you enter a value of “3” days, then any user of the UGP is notified, when his password will expire within the next 3 days. After this, the same user will not receive another password pre-expiration notification again, before a new password has been set and expires.
(c)	Dispatch Policy	By default, password pre-expiration notifications are sent using the Dispatch Policy assigned to each user, meaning in the same way as passcode messages are sent to the user. In case you prefer to send the notifications in a different way, you may override the Dispatch Policy to use.
(d)	Message content	Specifies the message content of the notification. You can enter static text, but also macros (placeholders) that will be substituted with relevant content when sending the notification. A list of allowed macros is shown at the bottom of the web page.
(e)	Estimated length of message	Shows the estimated length of the notification content after macro substitutions. If the estimated length is more than 160 characters, then please take the information regarding “Notification message length” in section 17.6.1.3.6 (page 181) into account.
(f)	Email subject	This setting is only relevant when the notification is sent by email. In this case, the setting specifies the content of the email subject. Macros are allowed here, too.

17.6.1.3.5 “On Password Expiration” Notification

The **On Password Expiration** tab contains settings regarding **Password Expiration** notifications:

Policies > User Group Policies

Edit User Group Policy: Sales personnel

Basic Settings | Self-service Website Settings | **Notifications** | License

Password Reset Website URL:

Self-service | SMS PASSCODE Lockout | AD Account Lockout | Before Password Expiration | **On Password Expiration**

a ☒ Send out a notification when a user's password has expired Reset template

b Dispatch Policy

☒ Standard (determined by the actual user)
☐ Override - always use:

c Message content

WARNING!
 Your password has expired and you need to set a new one.
 You can set a new password here: [PRS URL]
 [LICENSEE]

d Estimated length of message: 141 characters

e Email subject

Allowed macros

[USERNAME]	Name of the user receiving the notification
[PRS URL]	URL of the Password Reset Web Site
[LICENSEE]	Owner of the license for the SMS PASSCODE system

	Setting	Explanation
(a)	Notification enabled	<p>Select the checkbox “Send out a notification when a user’s password has expired” to enable password expiration notifications. When enabled, any user assigned to the UGP will receive a notification whenever his AD password has just expired.</p> <div> <p>IMPORTANT: Password Reset CAL required Please note that a user will only receive a password expiration notification if a Password Reset CAL has been allocated to the user.</p> <p>IMPORTANT: UIP required Password expiration notifications only work for users imported into the SMS PASSCODE database through a User Integration Policy (UIP) with Directory type set to <u>Active Directory</u>. The expiration check is done as part of every AD sync.</p> </div> <p>Password expiration notifications are disabled by default. It is recommended to enable them if you are using the SMS PASSCODE Password Reset module.</p>
(b)	Dispatch Policy	By default, password expiration notifications are sent using the Dispatch Policy assigned to each user, meaning in the same way as passcode messages are sent to the user. In case you prefer to send the notifications in a different way, you may override the Dispatch Policy to use.
(c)	Message content	Specifies the message content of the notification. You can enter static text, but also macros (placeholders) that will be substituted with relevant content when sending the notification. A list of allowed macros is shown at the bottom of the web page.
(d)	Estimated length of message	Shows the estimated length of the notification content after macro substitutions. If the estimated length is more than 160 characters, then please take the information regarding “Notification message length” in section 17.6.1.3.6 (page 181) into account.
(e)	Email subject	This setting is only relevant when the notification is sent by email. In this case, the setting specifies the content of the email subject. Macros are allowed here, too.

17.6.1.3.6 Long Message Content

WARNING: Consequences of long SMS message content (> 160 characters)

When notifications are sent by email, the length of the message content is not important. On the other hand, when notifications are sent by SMS, then please note the following consequences of long message content: Longer message content generally means longer message transmission time as well. But more importantly, if the resulting content of a notification message exceeds **160 characters**, this will have the following consequences:

- If the SMS message is sent using a modem, the message will be split into several messages²⁷ that are sent sequentially and merged by the receiving mobile phone into a single message again. This means
 - Longer transmission time (because of several message transmissions)
 - Possibly higher transmission cost (because of several message transmissions)
- If the SMS message is sent using a Dispatch Connector, the corresponding service provider might only support messages up to a specific maximum length. Content of messages exceeding such maximum length will be cut off. Limitations of specific Dispatch Connectors are shown on the Dispatch Connector maintenance page (cf. section 17.16.1, page 267).

17.6.1.4 User Group Policy: License

This section describes the settings available on the **License** tab while maintaining a UGP. The **License** tab contains settings to control which types of Client Access Licenses (CALs) are assigned to the users of the UGP. Before describing the details on this tab, it is important first to understand the terms used for license management:

- **License Grants:** As an administrator, you may *grant* CALs to users. Whenever you grant a specific CAL to a specific user, it means that you *intend* to allocate this particular type of CAL to this particular user. However, the CAL might or might not become allocated to the user, for different reasons to be described below. One reason could be, that you are granting more CALs than you have actually acquired.
- **License Allocations:** The SMS PASSCODE database service internally contains a *License Manager* process. This process continuously monitors data changes in the database affecting licensing. Whenever license grants are added or removed, the License Manager will (re-)allocate CALs in the most appropriate way. You can rely on the fact, that whenever a CAL was successfully allocated to a user, the License Manager will not remove the license allocation from this user again, unless you explicitly remove the license grant from this user, or otherwise explicitly decrease the number of available CALs.

To conclude, as an administrator you have control of the license grants given to users, whereas the corresponding license allocations are handled internally by the *License Manager* process.

²⁷ Each message containing up to 155 characters, because 5 characters are “lost” per message part due to some extra header data.

Using the license tab, you can control license grants and inspect license allocations:

Policies > User Group Policies

Edit User Group Policy: Sales personnel

Basic Settings | Self-service Website Settings | Notifications | **License**

Number of users assigned to this policy: 1050 (a)

License type (b)	Granted (c)	License allocations		
		Actual (e)	Missing (f)	Limit (d)
MFA Standard CAL MFA Standard CALs allow users to authenticate using SMS PASSCODE® multi-factor authentication through one or more of the following SMS PASSCODE® components: Citrix Web Interface Protection, RADIUS Protection, IIS Website Protection, Custom Protection, Windows Logon Protection, TMG Website Protection, AD FS Protection, ActiveSync Device Provisioning	<input checked="" type="checkbox"/>	1050	0	1500
Password Reset CAL Password Reset CALs allow users to reset their own AD password using the SMS PASSCODE® Password Reset Website	<input checked="" type="checkbox"/>	1050	0	1500

	Setting	Explanation
(a)	Number of users assigned to this policy	Shows the total number of users currently assigned to the UGP.
(b)	License type	This column lists the types of CALs that have been acquired according to the license key entered on the License page (cf. section 17.4, page 122).
(c)	Granted	<p>For each row of license types, this column contains a checkbox that lets you control whether the corresponding license type should be granted to the users of the UGP.</p> <p>Select/clear a checkbox to grant or not grant the license type of the row to the users of the UGP, respectively.</p>
(d)	Limit	<p>For each row of license types, this column contains a textbox that optionally lets you enter the maximum number of licenses to allocate to the users of the UGP.</p> <p>Leave the textbox empty to define no explicit limit for the license type of the row.</p> <p>Enter a specific number, in case you would like to limit the number of license allocations for the license type of the row. This is useful, in case the number of users assigned to the UGP may change over time, outside your control. E.g. if you are a hosting partner, and the users of every customer are assigned to a customer-specific UGP, where the customer is in control of adding/removing users that are imported from AD through a User Integration Policy.</p> <div> Note (Advanced feature): The Limit column is not visible by default. You need to enable License limits on the License page in order to make it visible (cf. section 17.4, page 122). </div>

	Setting	Explanation
(e)	Actual	<p>For each row of license types, this column shows the total number of CALs that have actually been <u>allocated</u> to users of the UGP.</p> <p>Normally you would expect when <u>granting</u> a license type, that the license type will be <u>allocated</u> to all users of the UGP. This means that you would normally expect the number in this column to be identical to (a), i.e. the total number of users assigned to the UGP. However, the actual number of license allocations might differ due to several reasons:</p> <ul style="list-style-type: none"> • The license key does not contain enough CALs of the corresponding license type ("Out of licenses"). Resolution: Acquire more CALs of the license type in question or remove some of the users from the UGP. • A limit has been set for the license type in column (d), and the limit has been reached. Resolution: Increase the limit or remove some of the users from the UGP. • The granting of the license type has been removed by an override on individual users of the UGP (cf. section 17.10.1.6, page 246). <p>On the other hand, if a license type has NOT been granted, then you would normally expect the number in this column to be zero. The actual number of license allocations might in this case only differ, due to the license type being granted to selected users of the UGP via individual overrides (cf. section 17.10.1.6, page 246).</p>
(f)	Missing	<p>For each row of license types, this column shows the total number of users of the UGP that have been <u>granted</u> the corresponding license type, but have not been <u>allocated</u> a corresponding CAL.</p> <p>Normally you would not expect any allocations to be missing, meaning the column should show a total number of zero missing allocations, and show a green light.</p> <p>On the other hand, if any CAL allocations are missing, due to missing CALs in the license key ("Out of licenses"), or due to an explicitly defined license limit (d), then the column will show a red light to warn about the issue.</p>

Note: In case any license allocations have failed, then the **License** tab will clearly indicate this using red text and an exclamation icon:

Policies > User Group Policies

Edit User Group Policy: Sales personnel

Basic Settings | Self-service Website Settings | Notifications | **License** ⚠

Number of users assigned to this policy: 1050

License type	Granted	License allocations	
		Actual	Missing
MFA Standard CAL MFA Standard CALs allow users to authenticate using SMS PASSCODE® multi-factor authentication through one or more of the following SMS PASSCODE® components: Citrix Web Interface Protection, RADIUS Protection, IIS Website Protection, Custom Protection, Windows Logon Protection, TMG Website Protection, AD FS Protection, ActiveSync Device Provisioning	<input checked="" type="checkbox"/>	1050	0
Password Reset CAL Password Reset CALs allow users to reset their own AD password using the SMS PASSCODE® Password Reset Website	<input checked="" type="checkbox"/>	1000	50

In case you need to get a better overview of CAL grants and allocations across several UGPs, you have several options for achieving this:

- Go to the **License** page to see the overall statistics for license allocations (cf. section 17.4, page 122).
- Use other license management options (cf. section 17.4.3, page 125).

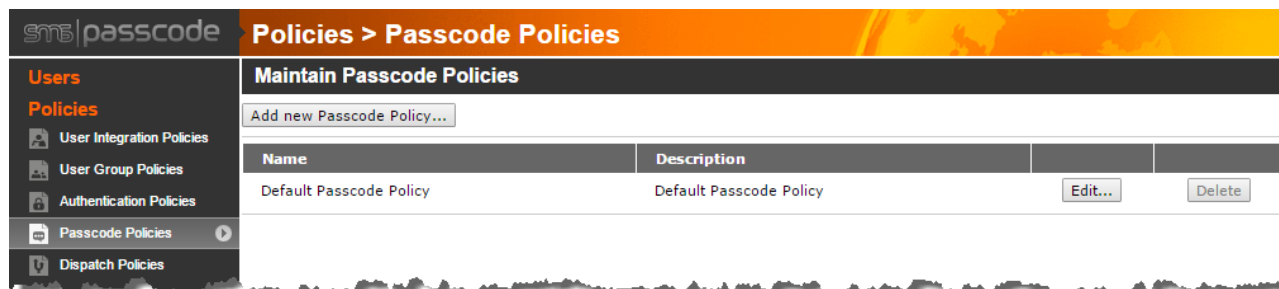
17.7 Passcode Policies

Passcode Policies are used to define basic settings related to the passcodes themselves, i.e. the length and composition of the random generated one-time-passcodes. Furthermore, Passcode Policies define the content of passcode messages using the **MessageDesigner**.

Each user is assigned to a particular Passcode Policy, which then controls the generation of one-time-passcodes for the user during authentication attempts and controls the content of the passcode messages sent to the user. The Passcode Policy is normally assigned to the user through the User Group Policy assigned to the user (since each User Group Policy specifies a Passcode Policy), but it is also possible to override this on the individual user and assign a specific Passcode Policy²⁸. You may create any number of Passcode Policies, thereby having required combinations of passcode settings ready for different groups of users.

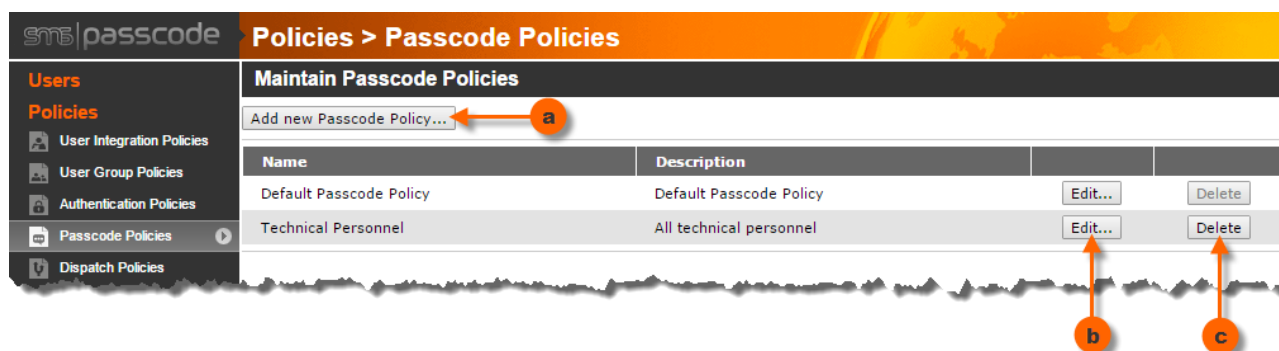
²⁸ As an advanced feature, it is also possible to define Authentication Policies that will dynamically override the Passcode Policy of a user during a login attempt; this is called *adaptive contextual message dispatching*. Please refer to section 17.8.2.5 (page 203).

Passcode Policies are maintained on the **Passcode Policies** page. The first time you enter this page, it will look like this:



Initially, the SMS PASSCODE database will only contain a single Passcode Policy called *Default Passcode Policy*. This policy cannot be deleted and will always be assigned to users that are not assigned to any other Passcode Policy. You can create any number of additional Passcode Policies. To maintain Passcode Policies, proceed as follows:

- To add a new Passcode Policy, click the **Add new Passcode Policy...** button.
- To edit a Passcode Policy, click the **Edit...** button on the policy.
- To delete a Passcode Policy, click the **Delete** button on the policy.



NOTE: The built-in **Default Passcode Policy** is a special policy, which is assigned to User Group Policies and users by default. You can edit, but not delete this policy.

IMPORTANT: Please note when deleting a Passcode Policy that all User Group Policies, users and Authentication Policies referring to this Passcode Policy will be set to refer to the **Default Passcode Policy** instead.

The subsection below explains the different settings of a Passcode Policy in detail.

17.7.1 Settings of a Passcode Policy

When creating a new Passcode Policy or maintaining an existing Passcode Policy, a tab control is shown for configuring the different settings of the policy. The settings are divided into 2 tabs:

- a. **Basic Settings**
The main settings, for example concerning the passcode generation.
- b. **MessageDesigner**
Settings defining the content of the passcode messages using *message templates* and *macro placeholders*.



The different settings are described in detail in the following subsections. When making changes to a Passcode Policy please remember to click the **Save** button to store the changes permanently.

17.7.1.1 Passcode Policy: Basic Settings

This section describes the settings available on the **Basic Settings** tab while maintaining a Passcode Policy.

Policies > Passcode Policies

Edit Passcode Policy: Technical Personnel

Basic Settings | MessageDesigner

Name (a)

Description (b)

Passcode length (c) [5-20] Default: 6

Passcode composition (d)

- ☐ Digits only
- ☐ Digits + lower case letters
- ☐ Digits + upper case letters
- ☒ memoPasscodes™

Default: memoPasscodes™

Passcode lifetime (e) seconds [1-3600] Default: 120

	Setting	Explanation
(a)	Name	The name used to identify the Passcode Policy. Giving the Passcode Policy a unique name is mandatory.
(b)	Description	Optional description of the Passcode Policy, for your own records. Here you can describe the purpose of the Passcode Policy.
(c)	Passcode length	<p>This setting controls the length of the generated passcodes, i.e. the number of characters in each passcode.</p> <p>Longer passcodes mean higher security because the probability of guessing a passcode decreases. Shorter passcodes are easier to enter for the users, on the other hand.</p> <p>The default setting is: 6. Allowed range: 5-20.</p>

	Setting	Explanation
(d)	Passcode type	<p>This setting defines whether the generated passcodes are only allowed to contain digits, or a combination of digits and letters.</p> <p>Passcodes containing only digits are usually easier to enter for the users. Passcodes containing both digits and letters, on the other hand, are more secure because there are more combinations, meaning less probability of guessing a passcode.</p> <p>SMS PASSCODE offers a unique option called memoPasscodes™. memoPasscodes™ are constructed in a special way, making them easier for users to memorize, thereby providing improved user convenience during authentication. At the same time, memoPasscodes™ still offer maximum security by building the passcodes using random patterns.</p> <p>memoPasscodes™ is the recommended passcode type.</p> <p>The default setting is: memoPasscodes™</p>
(e)	Passcode lifetime	<p>This setting controls the default lifetime of a passcode, after it has been sent. However, according to the Dispatch Policy used for sending the passcode, the lifetime might be shortened or prolonged according to the settings of the Dispatch Policy rule applied (cf. section 17.18.2.3.4, page 284).</p> <p>The default setting is 120 seconds = 2 minutes. Allowed range: 1-3600 seconds (3600 seconds = 1 hour)</p>

IMPORTANT (Dispatch Connector limitations):

Please note when sending passcode messages using Dispatch Connectors (cf. section 17.16, page 265) that some of these have limitations regarding the supported formats of passcodes. For example, some 3rd party service providers might only support passcodes of a specific minimum or maximum length, or might only support passcodes containing digits. In such cases, the limitations of a Dispatch Connector take precedence over the settings of the applied Passcode Policy.

The passcode formats supported by the different Dispatch Connectors are shown on the Dispatch Connector maintenance page (cf. section 17.16.1, page 267).

17.7.1.2 Passcode Policy: MessageDesigner

This section describes the settings available on the **MessageDesigner** tab while maintaining a Passcode Policy. Using the *MessageDesigner* you can create your own message templates that define the content of passcode messages sent to your users during multi-factor authentication. Both the content of SMS and email messages can be defined, independent of each other.

IMPORTANT:

The number of message templates available on the **MessageDesigner** tab depend on the fact whether the setting **Geo IP and IP History** has been enabled on the **General Settings** page (cf. section 17.3.1, page 109).

If the setting **Geo IP and IP History** is disabled on the **General Settings** page, then the *MessageDesigner* is in *simple mode*, allowing maintenance of a single message template. On the

other hand, if the setting is enabled, then the *MessageDesigner* is in *advanced mode*, allowing maintenance of four different message templates. The difference between these modes is explained in the table below:

Mode	Explanation
Simple mode	In <i>simple mode</i> , each Passcode Policy defines a single message template defining the content of the passcode messages sent to users. You can define different content of messages sent by SMS and email, respectively – and you can define different message templates for different groups of users by assigning distinct Passcode Policies to them. However, it is not possible for a single user to receive different, contextual specific message content depending on the specific authentication context. Such <i>location and behavior aware</i> differentiation according to the exact context is only possible, when the <i>MessageDesigner</i> is in the <i>advanced mode</i> .
Advanced mode	<p>In <i>advanced mode</i>, each Passcode Policy defines 4 different message templates, where each template is used in different contexts. The 4 available message templates are:</p> <p><u>Unknown IP:</u> This message template is used whenever a user requests an authentication, and the end-user IP is unknown (either because the authentication client in question is not able to collect end-user IP addresses, or because collection of end-user IP addresses has not been enabled in the SMS PASSCODE Configuration Tool – cf. section 26.2, page 424).</p> <p><u>Learning Mode:</u> This message template is used whenever a user with <i>Learning Mode</i> activated requests an authentication (and the end-user IP is known). Please read section 17.8.2.3 (page 201) for more details regarding <i>Learning Mode</i>.</p> <p><u>Trusted IP:</u> This message template is used whenever a user requests an authentication from an IP recognized as a <i>Trusted IP</i> (and <i>Learning Mode</i> is not active). Please read section 17.8.2.3 (page 201) for more details regarding the definition of a <i>Trusted IP</i>.</p> <p><u>Non-Trusted IP:</u> This message template is used whenever a user requests an authentication from an IP recognized as a <i>Non-Trusted IP</i> (and <i>Learning Mode</i> is not active). Please read section 17.8.2.3 (page 201) for more details regarding the definition of a <i>Non-Trusted IP</i>.</p> <p>Additionally, more types of dynamic content (<i>macro placeholders</i>) are available in <i>advanced mode</i>. For example, the message templates Learning Mode, Trusted IP and Non-Trusted IP allow dynamic content like the name of the country from which an authentication request originates, or the name of the organization owning the end-user IP from which the request originates.</p> <p>The main idea of having different message templates is to give the user the opportunity during an authentication attempt to recognize irregularities and to become alerted in this case. E.g. if the user gets the content of the Non-trusted IP message template, when this was not expected, or if a message template shows a country or organization name, that was not expected.</p>

The screenshot below shows how the **MessageDesigner** tab looks in *simple mode*:

Policies > Passcode Policies

Edit Passcode Policy: Technical Personnel

Basic Settings | **MessageDesigner**

Trusted IP | Non-Trusted IP | **Message format** | Learning Mode

SMS message **a**

PASSCODE: [PASSCODE]
[LICENSEE]

Estimated length of message: 21 characters

Email subject **b**

SMS PASSCODE: [PASSCODE]

Email body **c**

PASSCODE: [PASSCODE]
[LICENSEE]

Allowed macros **d**

[LICENSEE]	Owner of the license of the SMS PASSCODE system
[PASSCODE]	Random, session-specific One-time passcode
[USERNAME]	Name of the user receiving the passcode

The different sections are explained in the table below:

	Setting	Explanation
(a)	SMS message	Message template for passcode messages sent by SMS. This template is also used for all non-email messages, for example, when a Dispatch Connector is sending a message by voice call, using text-to-speech (speech synthesis).
(b)	Email subject	Template for the subject of passcode messages sent by email
(c)	Email body	Template for the body of passcode messages sent by email
(d)	Allowed macros	List of macro placeholders permitted in the message templates

Any static text entered into any of the message template fields is copied unchanged to the passcode messages sent to users. The section **Allowed macros** lists the placeholders that you may enter into the message templates for dynamic content. These placeholders will then be replaced with the correct contextual content whenever a message is generated. E.g. wherever you put the macro **[USERNAME]** in a message template, the name of the actual user receiving a message will appear.

In *advanced mode*, the **MessageDesigner** looks like this:

Policies > Passcode Policies

Edit Passcode Policy: Technical Personnel

Basic Settings | **MessageDesigner**

Trusted IP | Non-Trusted IP | Unknown IP | Learning Mode

SMS message

TRUSTED LOCATION
PASSCODE: [PASSCODE]
[LICENSEE]

Estimated length of message: 38 characters

Email subject

SMS PASSCODE: [PASSCODE]

Email body

TRUSTED LOCATION
Dear [USERNAME]
Please enter the passcode below to complete your authentication.
PASSCODE: [PASSCODE]
{Country: [COUNTRYNAME]}
Org: [ORG]
[LICENSEE]

Allowed macros

{...}	Conditional text for authentications from deviating countries. The characters '{' and '}' are <u>always</u> removed from any message templates. Text content between '{' and '}' characters will be removed as well, unless the determined source country <u>deviates</u> from the country of the user's international phone number prefix.
[COUNTRYCODE]	Country code of the end-user IP address
[COUNTRYNAME]	Country name of the end-user IP address

In this case, the **MessageDesigner** shows four tabs (**Trusted IP**, **Non-Trusted IP**, **Unknown IP** and **Learning Mode**). Each tab allows you to define message templates, in the same manner as in *simple mode*. The different message templates are used under different circumstances, as explained previously.

Please note, that additional macro placeholders are available in *advanced mode*. On each of the four tabs the bottom section **Allowed macros** lists the placeholders that are permitted.

Another important feature, only present in *advanced mode*, is the possibility of having *conditional text*:

- Any text between the characters “{” and “}” is displayed conditionally in messages sent to users. The text is displayed only, when the country determined from the international prefix of the user’s phone number differs from the country determined from the end-user IP address from which the authentication originates.

In case a user has no phone number assigned, or no country could be determined from the originating end-user IP address, the countries are assumed to differ; i.e. the conditional text is displayed in this case.

You may ask what the purpose of having conditional text is. The idea is that most users will typically log in from an IP address located in their “home country”, i.e. the country corresponding to the international prefix of their phone number. Since this is the typical scenario, it might be undesired to show repetitive information in the passcode messages each time. Especially getting informed about the name of the originating country during every such authentication attempt might be irrelevant. We want the users to be alerted, in case of irregularities. Hence, it makes more sense to display the name of the originating country only when it deviates from the “home country”. This is exactly what you may achieve using conditional text.

Wrapping up the two different modes: *Simple mode* allows you to adapt the content of the passcode messages per Passcode Policy, e.g. to localize the content or add specific required data, like for example the phone number to the internal helpdesk. Whereas *advanced mode* additionally allows you to send more detailed contextual information to the user, both depending on location and behavior, thereby giving the user the chance to get alerted in case of any irregularities.

WARNING: Consequences of long SMS message content (> 160 characters)

When customizing the content of SMS messages (**SMS message** templates) it is recommended to keep the message content relatively short and concise. One thing to notice is that longer message content generally means longer message transmission time as well. But more importantly, if the resulting content of an SMS passcode message exceeds **160 characters**, this will have the following consequences:

- If the SMS message is sent using a modem, the message will be split into several messages²⁹ that are sent sequentially and merged by the receiving mobile phone into a single message again. This means
 - Longer transmission time (because of several message transmissions).
 - Possibly higher transmission cost (because of several message transmissions).
 - No support for flash SMS, i.e. the message is sent as a standard SMS, even though the user was configured to receive a flash SMS.
- If the SMS message is sent using a Dispatch Connector, the corresponding service provider might only support messages up to a specific maximum length. Content of messages exceeding such maximum length will be cut off. Limitations of specific Dispatch Connectors are shown on the Dispatch Connector maintenance page (cf. section 17.16.1, page 267).

²⁹ Each message containing up to 155 characters, because 5 characters are “lost” per message part due to some extra header data.

17.8 Authentication Policies

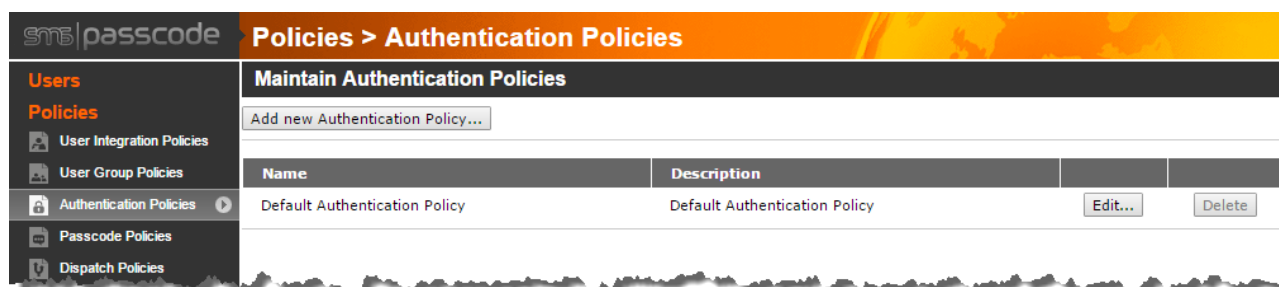
By default, all users created in the SMS PASSCODE database can log in to any authentication client protected by SMS PASSCODE, unless access is denied natively by the authentication client itself. Moreover, every user must log in using strong, secure authentication, meaning SMS PASSCODE multi-factor authentication. *Authentication Policies* optionally allow you to customize this default authentication behavior³⁰, either making access more or less restrictive under certain circumstances. Examples could be:

- Deny users to log in from specific continents or countries (because this is not expected)
- Allow specific groups of users to only have access to a subset of the SMS PASSCODE protected authentication clients
- Allow users logging in from specific continents or countries to only have access to a subset of the SMS PASSCODE protected authentication clients
- Allow users logging in from specific “trustworthy” IP scopes (e.g. internal LAN or branch offices) to have simple access without requiring SMS PASSCODE multi-factor authentication.

Additionally, Authentication Policies are used to define a number of other settings, like settings regarding brute-force attacks, and settings controlling *Learning Mode* and how quickly IP addresses become *Trusted*. This is all explained in more detail in the following subsections.

Each user is assigned to a particular Authentication Policy. The policy is normally assigned to the user through the User Group Policy assigned to the user (since each User Group Policy specifies an Authentication Policy), but it is also possible to override this on the individual user and assign a specific Authentication Policy. You may create any number of Authentication Policies, thereby having different authentication behaviors ready for different groups of users.

Authentication Policies are maintained on the **Authentication Policies** page. The first time you enter this page, it will look like this:

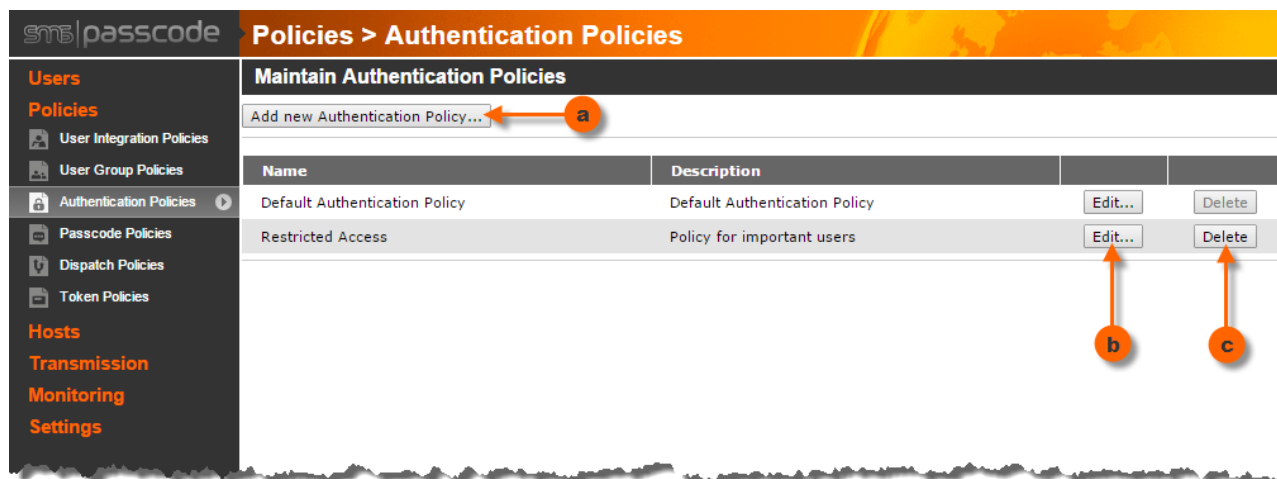


Initially, the SMS PASSCODE database will only contain a single Authentication Policy called *Default Authentication Policy*. This policy cannot be deleted and will always be assigned to users

³⁰ Besides Authentication Policies, default authentication behavior is also affected by the CALs allocated to a user, and whether proof-of-concept (PoC) mode is enabled. Please refer to section 9.1, page 27, for details.

that are not assigned to any other Authentication Policy. You can create any number of additional Authentication Policies. To maintain Authentication Policies, proceed as follows:

- a. To add a new Authentication Policy, click the **Add new Authentication Policy...** button.
- b. To edit an Authentication Policy, click the **Edit...** button on the policy.
- c. To delete an Authentication Policy, click the **Delete** button on the policy.



NOTE: The built-in **Default Authentication Policy** is a special policy, which is assigned to User Group Policies and users by default. You can edit, but not delete this policy.

IMPORTANT: Please note when deleting an Authentication Policy that all User Group Policies and/or users referring to this Authentication Policy will be set to refer to the **Default Authentication Policy** instead.

The configuration of Authentication Policies is very flexible and allows for many different setups. The following subsections describe in detail, how Authentication Policies are configured and maintained.

First section 17.8.1 explains the overall idea of having a *sequence* of Authentication Rules. Then section 17.8.2 explains how to maintain Authentication Policies, i.e. create new ones or edit existing ones. In particular, subsection 17.8.2.4 explains how to maintain the sequence of Authentication Rules of an Authentication Policy. At last, section 17.8.3 lists some examples on the usage of Authentication Policies.

17.8.1 Authentication Rule Sequence

Each Authentication Policy defines a **sequence** of prioritized Authentication Rules, e.g. a specific sequence could consist of Authentication Rules 1 to 5. Whenever an authentication request is received from a user, the SMS PASSCODE system will evaluate the sequence of Authentication Rules to determine the action to be taken. The sequence is always evaluated in strict order from the first to the last rule. I.e. if the sequence consists of n Authentication Rules, then the rules are evaluated in this order:

- Authentication Rule 1
- Authentication Rule 2
- Authentication Rule 3
- ...
- Authentication Rule $n-1$
- Authentication Rule n

The evaluation of the sequence is stopped as soon as the first **matching** Authentication Rule is found. I.e. the Authentication Rule sequence can be seen as an “if-then-else” chain:

- **IF** Authentication Rule 1 applies **THEN** use Authentication Rule 1
- **ELSE IF** Authentication Rule 2 applies **THEN** use Authentication Rule 2
- **ELSE IF** Authentication Rule 3 applies **THEN** use Authentication Rule 3
- ...
- **ELSE IF** Authentication Rule $n-1$ applies **THEN** use Authentication Rule $n-1$
- **ELSE** use Authentication Rule n

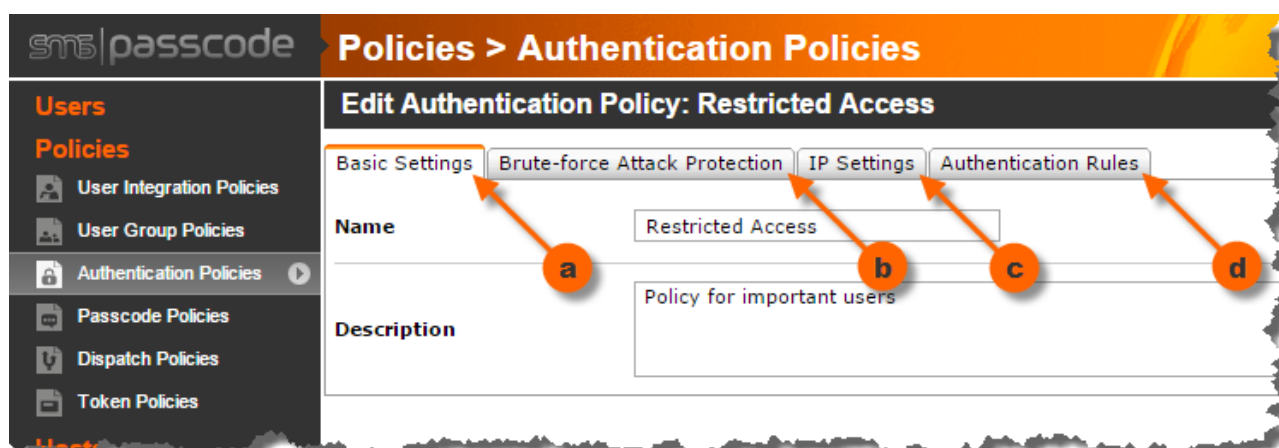
Please note, that the last Authentication Rule of the sequence will always be a **built-in default Authentication Rule** that applies to all authentication requests. This is to ensure, that every authentication request is handled even though no other Authentication Rule of the sequence would apply.

The possibilities using Authentication Rules are very wide-ranging. You can create any number of Authentication Rules and you can re-arrange the order of them as needed afterwards.

17.8.2 Settings of an Authentication Policy

When creating a new or editing an existing Authentication Policy in the SMS PASSCODE database, a tab control is shown for configuring the different settings of the Authentication Policy. The settings are divided into 4 tabs:

- a. **Basic Settings**
Settings for identifying the Authentication Policy
- b. **Brute-force Attack Protection**
Settings defining how to react to brute-force attack attempts
- c. **IP Settings**
Settings regarding *behavior aware authentication*, i.e. settings regarding *Trusted IPs* and *Learning mode*
- d. **Authentication Rules**
The sequence of Authentication Rules specifying the authentication behavior of the Authentication Policy



The different settings are described in detail in the following subsections. When making changes to an Authentication Policy please remember to click the **Save** button at last to store the changes permanently. Otherwise, all changes will be lost.

17.8.2.1 Authentication Policy: Basic Settings

This section describes the settings available on the **Basic Settings** tab while maintaining an Authentication Policy. The **Basic Settings** are only used for identifying and describing the Authentication Policy:

The screenshot shows the 'Edit Authentication Policy: Restricted Access' form in the SMS Passcode interface. The form has four tabs: 'Basic Settings', 'Brute-force Attack Protection', 'IP Settings', and 'Authentication Rules'. The 'Basic Settings' tab is active. It contains two main fields: 'Name' (labeled 'a') with the value 'Restricted Access' and 'Description' (labeled 'b') with the value 'Policy for important users'. On the right side of the form, there are 'Save' and 'Cancel' buttons, and a 'Create copy of...' link. The left sidebar shows a navigation menu with 'Users' and 'Policies' sections, where 'Authentication Policies' is selected.

	Setting	Explanation
(a)	Name	The name used to identify the Authentication Policy. Giving the Authentication Policy a unique name is mandatory.
(b)	Description	Optional description of the Authentication Policy, for your own records. Here you can describe the purpose of the Authentication Policy.

17.8.2.2 Authentication Policy: Brute-force Attack Protection

This section describes the settings available on the **Brute-force Attack Protection** tab while maintaining an Authentication Policy. These settings are used to define, how the SMS PASSCODE system should react to *brute-force attacks*, i.e. attacks where a hacker tries to determine a user's password or passcode simply by performing a large number of authentication attempts with different guesses. The solution is to limit the number of brute-force attempts a hacker is allowed to perform, thereby making it very unlikely that a hacker would guess the right password or passcode:

Users

Policies

- User Integration Policies
- User Group Policies
- Authentication Policies
- Passcode Policies
- Dispatch Policies
- Token Policies

Hosts

Transmission

Monitoring

Settings

Policies > Authentication Policies

Edit Authentication Policy: Restricted Access

Basic Settings | **Brute-force Attack Protection** | IP Settings | Authentication Rules

	Password entries	Passcode entries	Description
Max. attempts	a <input type="text" value="3"/>	d <input type="text" value="3"/>	Specifies the number of <u>consecutive</u> incorrect entries that will cause the system to lock out the user according to the settings below.
Initial temporary lockout duration	b <input type="text" value="5"/> minutes	e <input type="text" value="5"/> minutes	Specifies the duration for the initial temporary lockout period of a user, when the allowed number of <u>consecutive</u> incorrect entries has been exceeded. Hereafter the duration of temporary lockout periods is doubled if the user keeps entering incorrect entries.
Max. temporary lockout duration	c <input type="text" value="20"/> minutes	f <input type="text" value="20"/> minutes	Specifies the maximum duration allowed for a temporary lockout. If a temporary lockout period exceeds this value, then the user is locked out permanently from SMS PASSCODE, until an administrator manually unlocks the user again.

	Setting	Explanation
(a)	Max. attempts (Password)	<p>Specifies the number of <u>consecutive</u> incorrect password entries that will cause the SMS PASSCODE system to lock out the user.</p> <p>The first time a lockout happens, the user is locked out temporarily for a duration specified by setting (b). When this duration has expired, the user is allowed to attempt a single authentication again. If another incorrect password is entered this time, the user is locked out temporarily once more, this time for a doubled duration compared to the previous temporary lockout. The procedure continues like this, i.e. if the user keeps entering an incorrect password after each temporary lockout, a new temporary lockout occurs with a doubled duration compared to the previous one. However, setting (c) specifies a threshold for the maximum allowed duration of a temporary lockout. If this threshold is exceeded, the user is locked out permanently.</p> <p>In case the user is locked out, he will not be able to log in to any SMS PASSCODE protected authentication client³¹, until an administrator has unlocked the user's SMS PASSCODE account.</p> <p>Please note, that the user must enter incorrect passwords <u>consecutively</u> for the procedure above to apply. In case the user enters a correct password before the permanent lockout, then the procedure starts all over, i.e. the user is again allowed to enter incorrect passwords multiple times as specified by setting (a).</p> <div> <p>IMPORTANT: The value of this setting should be <i>calibrated</i> with the lockout threshold setting of the AD Group Policy assigned to the user. It is recommended to set the lockout threshold in SMS PASSCODE to a value <u>lower</u> than the lockout threshold of the AD account. This will ensure that a password brute-force attack will lock out the SMS PASSCODE user account before the corresponding AD user account gets locked out.</p> </div> <div> <p>IMPORTANT: Please note that some authentication clients perform AD password validation <u>before</u> the corresponding SMS PASSCODE integration is allowed to kick in. In such cases, AD lockouts cannot be prevented. This applies in the following cases:</p> <ul style="list-style-type: none"> • SMS PASSCODE IIS Website Protection: Always. • SMS PASSCODE Windows Logon Protection: When RDP connections are validated using Network Level Authentication. • SMS PASSCODE AD FS Protection. </div>
(b)	Initial temporary lockout duration (Password)	<p>Specifies the duration of the first temporary lockout period, in case the user has entered more consecutive incorrect passwords than allowed according to setting (a).</p>

³¹ However, the user is still allowed to log in to the SMS PASSCODE Password Reset Website (PRWS) in this case. If the user succeeds logging in to the PRWS, then the user is automatically unlocked again, without any administrator required to take action.

	Setting	Explanation
(c)	Max. temporary lockout duration (Password)	Specifies the maximum allowed duration of a temporary lockout caused by entering incorrect passwords. If a new temporary lockout period with a longer duration is about to start, the user is locked out permanently instead. In this case, the user cannot log in to any SMS PASSCODE protected authentication client anymore, until an administrator has unlocked the user's SMS PASSCODE account, or the user unlocks his account by logging in to the SMS PASSCODE Password Reset Website.
(d)	Max. attempts (Passcode)	<p>Specifies the number of <u>consecutive</u> incorrect passcode entries that will cause the SMS PASSCODE system to lock out the user.</p> <p>The first time a lockout happens, the user is locked out temporarily for a duration specified by setting (e). When this duration has expired, the user is allowed to attempt a single authentication again. If another incorrect passcode is entered this time, the user is locked out temporarily once more, this time for a doubled duration compared to the previous temporary lockout. The procedure continues like this, i.e. if the user keeps entering an incorrect passcode after each temporary lockout, a new temporary lockout occurs with a doubled duration compared to the previous one. However, setting (f) specifies a threshold for the maximum allowed duration of a temporary lockout. If this threshold is exceeded, the user is locked out permanently.</p> <p>Please note, that the user must enter incorrect passcodes <u>consecutively</u> for the procedure above to apply. In case the user enters a correct passcode before the permanent lockout, then the procedure starts all over, i.e. the user is again allowed to enter incorrect passcodes multiple times as specified by setting (d).</p> <p>Furthermore, please note that a hacker will not be able to perform passcode brute-force attacks at all, unless he has stolen the user's password beforehand (since the correct password must be entered to trigger the transmission of a passcode).</p>
(e)	Initial temporary lockout duration	Specifies the duration of the first temporary lockout period, in case the user has entered more consecutive incorrect passcodes than allowed according to setting (d).
(f)	Max. temporary lockout duration	Specifies the maximum allowed duration of a temporary lockout period caused by entering incorrect passcodes. If a new temporary lockout period with a longer duration is about to start, the user is locked out permanently instead. In this case, the user cannot log in to any SMS PASSCODE protected authentication client anymore, until an administrator has unlocked the user's SMS PASSCODE account again.

17.8.2.3 Authentication Policy: IP Settings

This section describes the settings available on the **IP Settings** tab while maintaining an Authentication Policy.

Please note that the **IP Settings** tab is only available when the setting **Geo IP and IP history** is enabled on the **General Settings** page. Otherwise, the settings on this tab are not relevant.

The settings on this tab are only of importance if you would like to make use of *behavior aware authentication*. What this means is, whether you would like to have the SMS PASSCODE system learn by itself over time, which end-user IP addresses should be treated as *Trusted* and *Non-Trusted*, respectively. This distinction between *Trusted* and *Non-Trusted* end-user IP address categories allows the SMS PASSCODE system to:

- Send out different types of passcodes messages depending on the category (cf. Passcode Policies, section 17.7.1.2, page 188)
- Define different authentication behavior depending on the category (cf. Authentication Rules, section 17.8.2.5, page 204)

If you do not wish to make use of this type of distinction, then one possibility is to disable the setting **Geo IP and IP history** on the **General Settings** page. However, this will disable both *location and behavior aware authentication*. If you would like to make use of *location aware authentication* only, then you should ignore the settings on this tab, except disabling the *Learning mode* setting, and then ensure that no IP addresses will ever become *Trusted*. You can achieve this by ensuring that no Authentication Rules will ever increase the *Trust Level* of any end-user IP address (cf. section 17.8.2.5, page 204, regarding Authentication Rules). As a result, all passcode messages will then use the *Non-Trusted* message format of the Passcode Policy assigned to a user.

On the other hand, if you would like to make use of *behavior aware authentication*, then an issue might be, that you would not like users to become concerned about passcode messages informing about *Non-Trusted* logins, simply because the system has not learned yet, that a commonly used end-user IP address should be treated as *Trusted*. This is where the *Learning Mode* feature fits in. This feature allows the SMS PASSCODE system to put a user into a special state for a temporary period, during which the system can identify *Trusted* end-user IP addresses. During this *Learning Period*, the system will use the *Learning Mode* message template of a Passcode Policy instead of the *Trusted* and *Non-Trusted* message templates (cf. section 17.7.1.2, page 188).

Users

Policies

- User Integration Policies
- User Group Policies
- Authentication Policies**
- Passcode Policies
- Dispatch Policies
- Token Policies

Hosts

Transmission

Monitoring

Settings

Policies > Authentication Policies

Edit Authentication Policy: Restricted Access

Basic Settings | Brute-force Attack Protection | **IP Settings** | Authentication Rules

Trusted IP threshold Specifies the required trust level of a user IP address before it is treated as a "Trusted IP".

User IP expiration days Specifies the maximum age of an IP address entry in a user's IP history. I.e. any IP address is removed from a user IP history, whenever it has not been in use for a period of the specified duration.

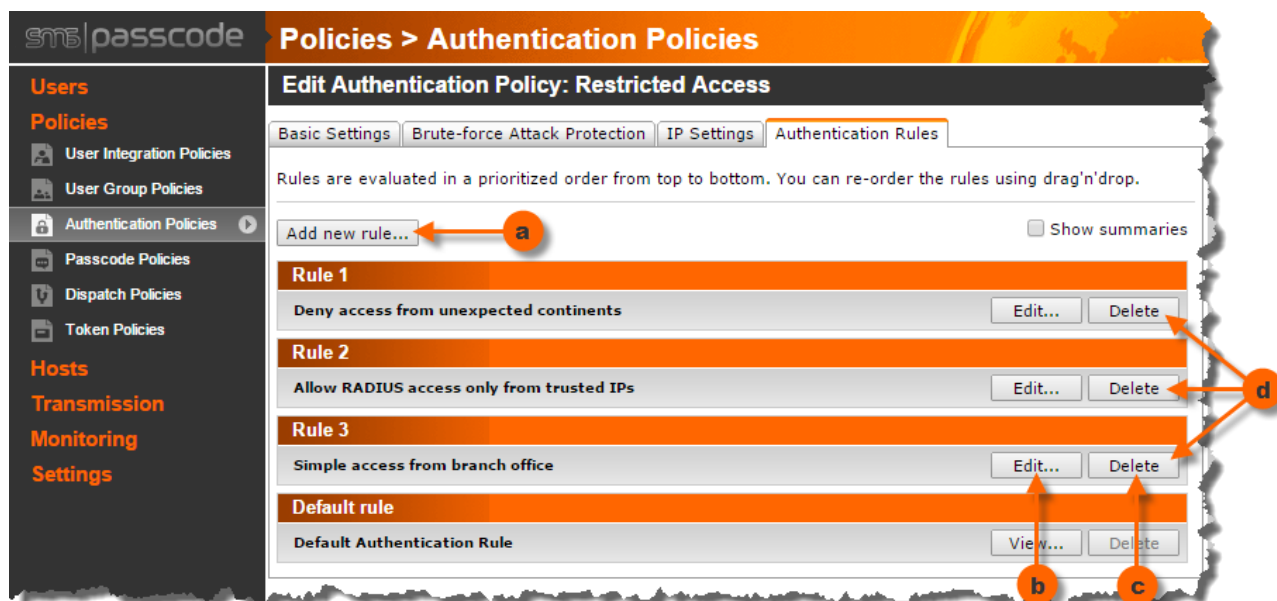
Learning mode ☒ Enabled Specifies whether "learning mode" is enabled. "Learning mode" allows users to receive passcode messages with a different content for the first number of successful logins. This is for example useful to let the system learn trusted IP addresses before starting to send out passcode messages with content targeted specifically for trusted and non-trusted IP addresses.

Learning mode threshold logins Specifies the number of successful MFA logins that a user must have completed, before the "learning mode" ends.

	Setting	Explanation
(a)	Trusted IP threshold	<p>Whenever a user performs an authentication from a <u>new</u> end-user IP address, i.e. an IP address not listed in the user's IP history yet, the IP address starts with a <i>Trust Level</i> of zero. By default, the <i>Trust Level</i> increases by 1 on every successful multi-factor authentication originating from the same end-user IP address. However, this behavior can be adapted using Authentication Rules, thereby suppressing the increase of the <i>Trust Level</i> in specific cases, or alternatively increase the <i>Trust Level</i> by more than 1 in specific cases.</p> <p>The setting, Trusted IP threshold, defines the <i>Trust Level</i> an end-user IP address must obtain at least, before it is treated as a <i>Trusted</i> end-user IP address.</p>
(b)	User IP expiration	<p>Whenever a user performs an authentication from a <u>new</u> end-user IP address, i.e. an IP address not listed in the user's IP history yet, the IP address is recorded and added to the user's IP history, in case authentication succeeds. The time and date of the last usage of every such recorded end-user IP address is updated, whenever the user performs another successful authentication from it. However, if an end-user IP address is not used anymore for a long time, it is preferable to remove it completely from the user's IP history. The setting, User IP expiration, defines for how long an unused end-user IP address will stay in the user's IP history, before it is removed from the history.</p>
(c)	Learning mode	<p>This setting defines whether <i>Learning Mode</i> should be enabled for the users assigned to this Authentication Policy. Please note, that this setting can be overridden individually while maintaining users (cf. section 17.10.1.5, page 245).</p>
(d)	Learning mode threshold	<p>This setting defines the duration of the <i>Learning Period</i>, measured in number of successful multi-factor authentications that the user must complete, before the <i>Learning Mode</i> automatically ends (if <i>Learning Mode</i> was enabled).</p>

17.8.2.4 Authentication Policy: Authentication Rules

This section describes the **Authentication Rules** tab, where you can maintain the sequence of Authentication Rules of an Authentication Policy.

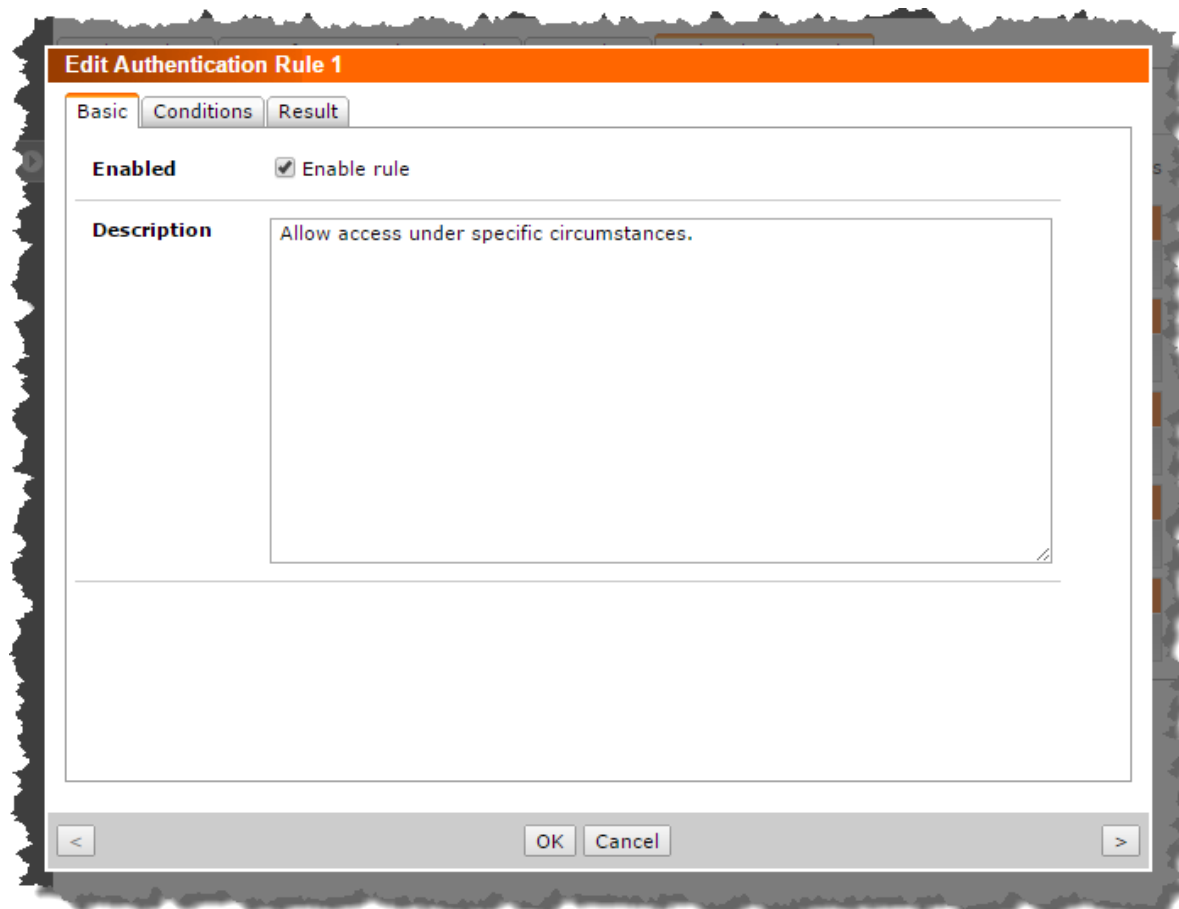


- a. Click the **Add new rule...** button to add a new Authentication Rule to the sequence.
- b. Click the **Edit...** button to edit the settings of an Authentication Rule.
- c. Click the **Delete** button to remove an Authentication Rule from the sequence.
- d. To re-arrange the order of the Authentication Rules: Click the title bar of an Authentication Rule without releasing the mouse button and drag the Authentication Rule to a new position in the sequence. Release the mouse button to drop the Authentication Rule in the new position.

Please note, that you can make any number of changes to the Authentication Rule sequence without affecting any current behavior. No changes will take effect until you click the **Save** button. I.e. as long as the **Save** button has not been clicked, you can undo all changes by leaving the page without clicking the **Save** button. However, when clicking the **Save** button, all changes are immediately pushed to all Authentication Backend Services on-the-fly and will take effect immediately.

17.8.2.5 Settings of an Authentication Rule

This section describes how to maintain the settings of each individual Authentication Rule in the Authentication Rule sequence of an Authentication Policy. When creating a new or editing an existing Authentication Rule, the following dialog appears:



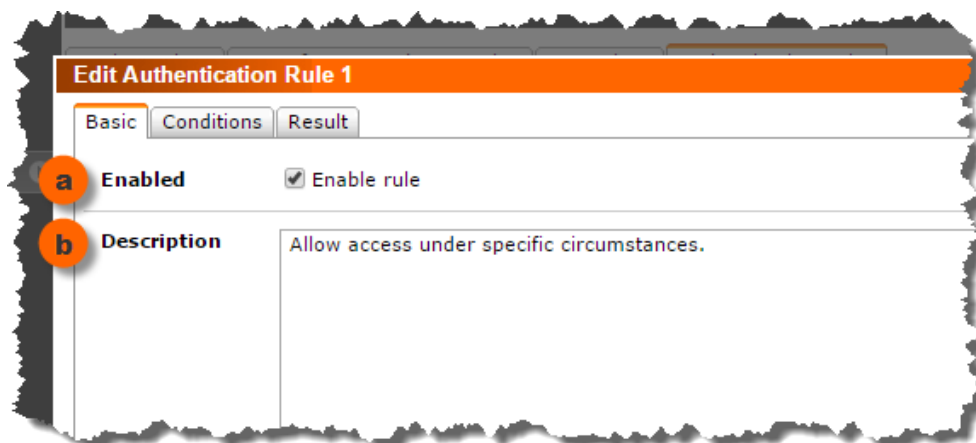
The dialog contains three tabs:

- **Basic:** This tab contains two basic settings for the rule
- **Conditions:** This tab is used to define under which conditions this rule applies.
- **Result:** This tab is used to define the outcome of the rule, in case it applies.

The settings of the three tabs are described below.

Basic:

The **Basic** tab contains the following two settings:



	Setting	Explanation
(a)	Enabled	The checkbox Enable rule specifies whether the rule is currently enabled (active) or not. If the rule is disabled, it will be skipped during evaluation of the Authentication Rule sequence, i.e. it will then not affect authentication behavior in any way. This might be useful for temporary de-activation of an Authentication Rule.
(b)	Description	A textbox for entering an optional informative text for your own records. You can use it to describe the purpose of the Authentication Rule.


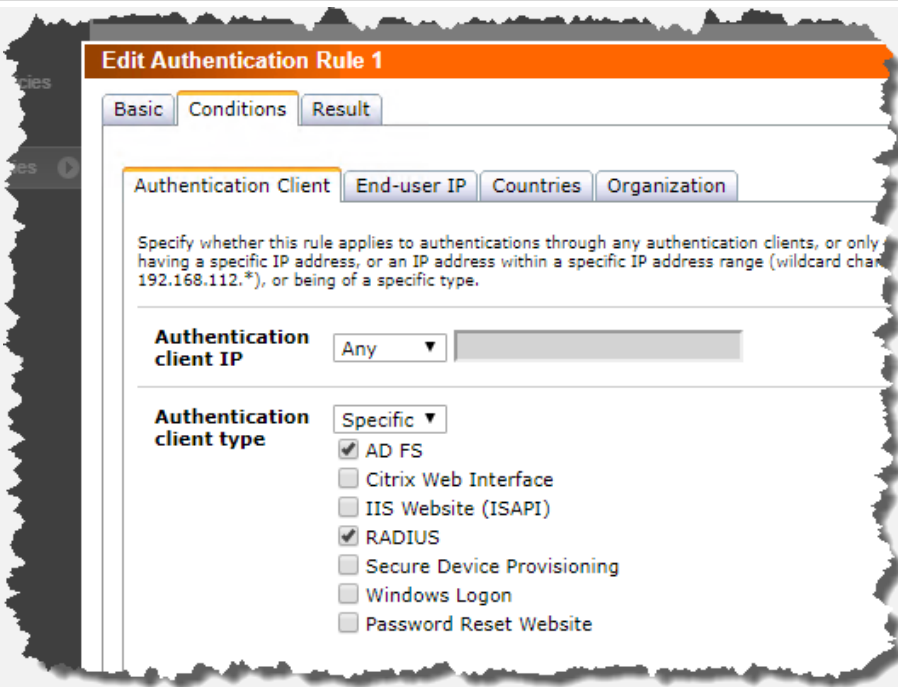
Conditions:

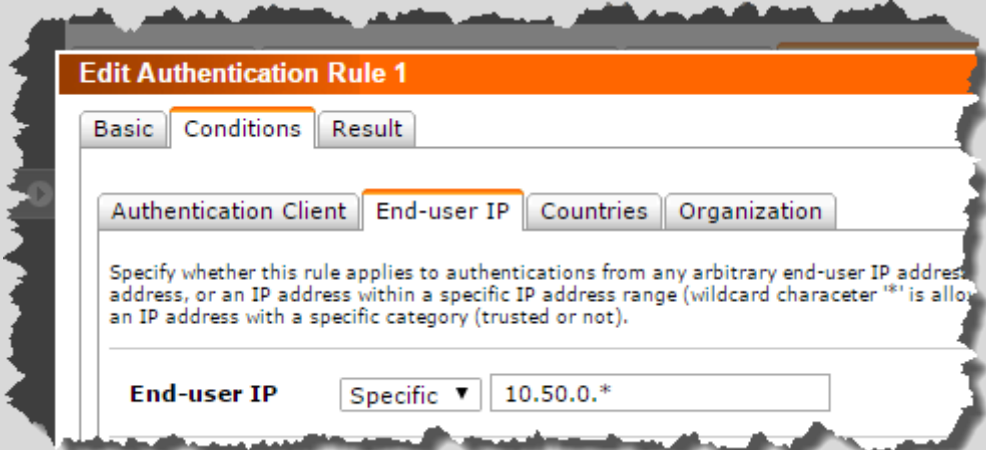
The **Conditions** tab groups all the settings defining the conditions when the Authentication Rule applies to an authentication attempt. By default, all settings are set to “Any”, meaning the Authentication Rule will apply to all authentication attempts. However, by changing one or more of the settings, you can customize the Authentication Rule to apply only under specific circumstances, according to your specific requirements. Please note that when several conditions are set, all of them must be fulfilled for the rule to apply.

Evaluation of Authentication Rules in case of *unknown data*

When evaluating the conditions of an Authentication Rule, sometimes it may occur that the data to be evaluated by a condition is not available (“unknown”). In such cases, the Authentication Rule will be skipped, and evaluation will continue at the next rule in the Authentication Rule sequence. Below, the descriptions of the individual condition settings highlight, when unknown data can occur, and what the consequences will be in each case.

The table below explains the settings of the **Conditions** tab in more detail.

Condition	Explanation
Authentication client IP	 <p>The Authentication client IP setting allows you to define whether the Authentication Rule must only apply in case authentication is attempted through an authentication client with a specific IP address. Wildcards are also allowed, making it possible to define the restriction on an IP-scope instead of a single IP address.</p> <p>This condition is useful if you would like to define specific authentication behavior for a specific subset of your authentication clients (determined by IP address).</p>
Authentication client type	 <p>The Authentication client type setting allows you to define whether the Authentication Rule must only apply in case authentication is attempted through an authentication client of a specific type. Checkboxes allow you to select the allowed types of authentication clients.</p> <p>This condition is useful if you would like to define specific authentication behavior for a specific subset of your authentication clients (determined by type).</p>

Condition	Explanation
End-user IP	<div data-bbox="406 257 1396 705">  </div> <p>The End-user IP setting allows you to define whether the Authentication Rule must only apply in case authentication is attempted from a specific end-user IP address. Wildcards are also allowed, making it possible to define the restriction on an IP-scope instead of a single IP address.</p> <p>This condition is useful if you would like to define specific authentication behavior for a specific subset of end-user IP addresses, e.g. authentication attempts from the internal LAN or from connected branch office networks.</p> <p><u>Note regarding Secure Device Provisioning (SDP)</u> In case of SDP, the end-user IP address is the IP address of the ActiveSync device, not the IP address of the browser logging in to the SDP website. These two IP addresses can be different, but will often be the same, since the user will most likely log in to the SDP website from the ActiveSync device itself. If you need to audit the IP address for the browser accessing the SDP website, then please inspect the Windows event log "SMS PASSCODE Provisioning" on the relevant Exchange CAS. This event log contains audit events with all relevant authentication information; including end-user IP addresses, in case end-user IP collection has been enabled for SDP in the SMS PASSCODE Configuration Tool on the CAS (cf. section 26.2, page 424).</p> <p><u>Note about "unknown end-user IP"</u> The end-user IP address might not be available during an authentication request. Either because an authentication client is configured not to collect it or does not support collecting it. If the end-user IP address is unknown during an authentication attempt and the End-user IP condition is set, then the Authentication Rule will be skipped during evaluation of the Authentication Rule sequence, i.e. the Authentication Rule will NOT apply to the authentication attempt (you can create another Authentication Rule taking care of the "unknown" end-user IP cases, by setting the Category of end-user IP condition to "Unknown", cf. next setting below).</p>

Condition

Explanation

Category of end-user IP

Please note, that this condition is only available, if the setting **Geo IP and IP history** is enabled on the **General Settings** page.

The screenshot shows the 'Edit Authentication Rule 1' window with the 'Conditions' tab active. Under the 'End-user IP' condition, the 'Category of end-user IP' dropdown is open, displaying the following options: Any, Trusted, Non-trusted, and Unknown. The 'Any' option is currently selected.

The **Category of end-user IP** setting allows you to define whether the Authentication Rule must only apply in case authentication is attempted from an unknown end-user IP address, or an end-user IP address that has been identified as *Trusted* or *Non-Trusted*, respectively.

This condition is useful if you would like to define specific authentication behavior for authentications from *Trusted* or *Non-Trusted* end-user IP addresses. For example, you may deny access to specific types of authentication clients from *Non-Trusted* IP addresses.

Note about "unknown end-user IP"

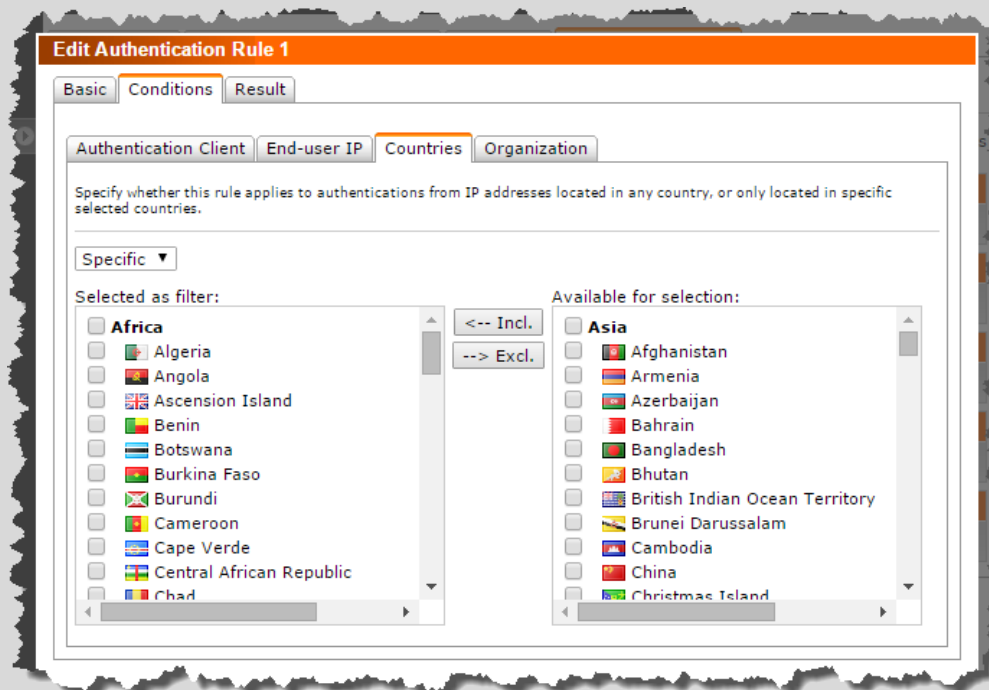
The end-user IP address might not be available during an authentication request. Either because an authentication client is configured not to collect it or does not support collecting it. If the end-user IP address is unknown during an authentication attempt and the **Category of end-user IP** condition is set to *Trusted* or *Non-Trusted*, then the Authentication Rule will be skipped during evaluation of the Authentication Rule sequence, i.e. the Authentication Rule will NOT apply to the authentication attempt.

Condition

Explanation

Countries

Please note, that this condition is only available, if the setting **Geo IP and IP history** is enabled on the **General Settings** page.



The **Countries** tab allows you to define whether the Authentication Rule must only apply in case authentication is attempted from an end-user IP address located in one or more specific countries or continents. To define the condition, select the required countries/continents in the **Available for selection** list and click the **Incl.** button. This will move the selected countries/continents to the **Selected as filter** list. If you want to remove any countries/continents from the condition again, select the countries/continents in question in the **Selected as filter** list, then click the **Excl.** button.

This condition is useful if you would like to define specific authentication behavior for authentications originating from specific countries or continents. E.g. from specific locations you may either deny access completely, or only allow restricted access to specific types of authentication clients.

Note about “unknown country of origin”

The country of origin might be unknown during an authentication request. Either because the end-user IP address is not available, due to the authentication client being configured not to collect it or not supporting collection of it; or because the end-user IP address is available, but it is not possible to determine the country of origin from the IP address; e.g. because the IP address is from a private IP scope. If the country of origin is unknown during an authentication attempt and the **Countries** condition is set, then the Authentication Rule will be skipped during evaluation of the Authentication Rule sequence, i.e. the Authentication Rule will NOT apply to the authentication attempt.

Condition

Explanation

Organization

Please note, that this condition is only available, if the setting **Geo IP and IP history** is enabled on the **General Settings** page



The **Organization** setting allows you to define whether the Authentication Rule must only apply in case authentication is attempted from an end-user IP owned by a specific organization. If plain text is entered into the filter textbox, then the Authentication Rule will apply as long as the organization name contains the text anywhere. E.g. if you enter the text "mycompany", then the rule will apply when authentication is attempted from an end-user IP address owned by for example "MyCompany Ltd.", "MyCompany Industries" or "CorporationMyCompany". However, you can also enter a **regular expression** into the filter textbox in case you need to define the matching condition more exactly. E.g. entering "^MyCompany\$" will only match IP addresses owned specifically by "MyCompany". Please note, that the evaluation of a match is always performed using a case-insensitive comparison.

This condition is useful if you would like to define specific authentication behavior for authentications originating from IP addresses owned by specific organizations.

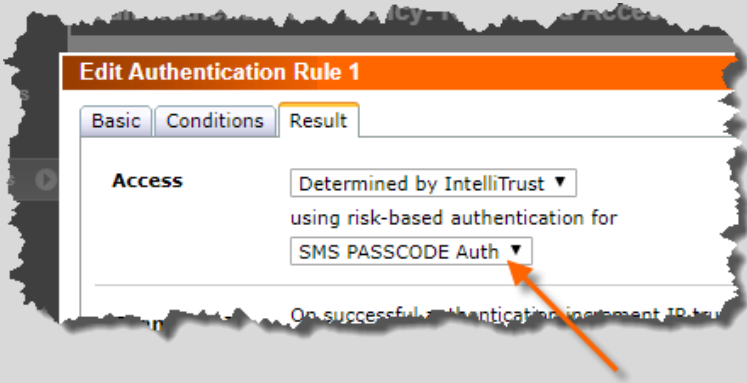
Note about "unknown organization"

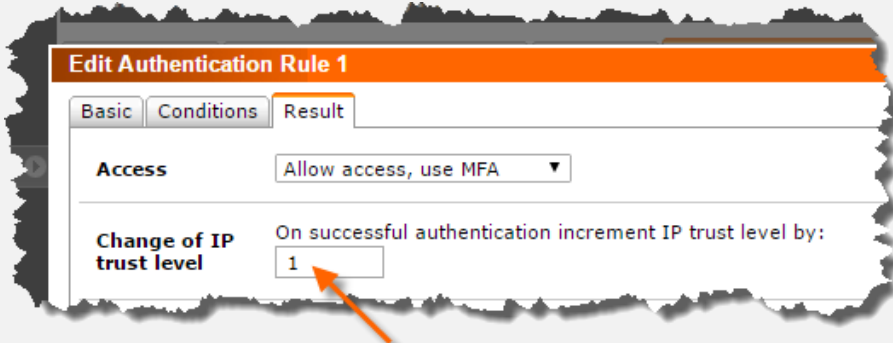
The name of the organization owning the end-user IP address might be unknown during an authentication request. Either because the end-user IP address is not available, due to the authentication client being configured not to collect it or not supporting collection of it; or because the end-user IP address is available, but it is not possible to determine the organization name from the IP address; e.g. because the IP address is from a private IP scope. If the organization name is unknown during an authentication attempt and the **Organization** condition is set, then the Authentication Rule will be skipped during evaluation of the Authentication Rule sequence, i.e. the Authentication Rule will NOT apply to the authentication attempt.

Result:

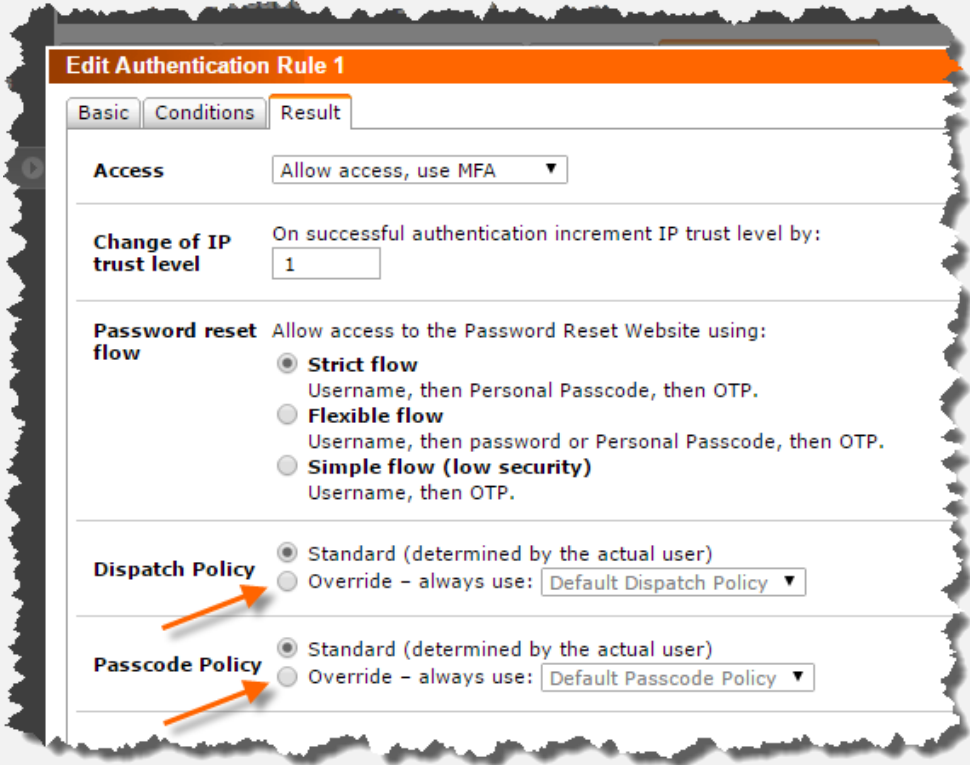
All the condition settings described above let you define, when an Authentication Rule applies to an authentication attempt. As explained previously, the **first** applying Authentication Rule in the rule sequence of an Authentication Policy is the rule that is selected for controlling the authentication behavior of an authentication attempt. The behavior or “outcome” of the selected rule is controlled by the settings on the **Result** tab.

Setting	Explanation
Access	<div data-bbox="405 524 1181 869"> </div> <p>The Access setting defines how an authentication attempt will be handled under the circumstances defined by the conditions of the rule. You may choose between the following four options:</p> <ul style="list-style-type: none"> • Allow access, use MFA: This is the default behavior. The user can log in, but must authenticate using strong, secure SMS PASSCODE multi-factor authentication. • Allow access, bypass MFA: This option allows the user to log in using standard “one-factor” authentication, i.e. by only entering user name and password. Use of this option should be treated with great care, since it lowers security considerably. However, it might make sense during logins from trustworthy locations, e.g. logins from the internal LAN. <div data-bbox="512 1308 1417 1438" style="border: 1px solid black; padding: 5px;"> <p>Note: The option Allow access, bypass MFA is only available if Multi-factor authentication bypassing has been allowed on the General Settings page. Otherwise, you will not see this option in the drop-down list.</p> </div> <div data-bbox="512 1469 1417 1720" style="border: 1px solid black; padding: 5px;"> <p>WARNING (concerning Password Reset Website): Bypassing MFA also applies to logins to the SMS PASSCODE Password Reset Website (PRWS). This is a new behavior in SMS PASSCODE that started from version 7.2. If you have upgraded from a version prior to 7.2 and have any authentication rules set to Allow access, bypass MFA, then please verify whether the login behavior for the PRWS is as expected. Otherwise, please create a distinct authentication rule for PRWS with the required behavior.</p> </div> <ul style="list-style-type: none"> • Deny access: This option will deny access, i.e. authentication will always fail immediately, after user name and password has been entered. No passcode will be sent. • Determined by IntelliTrust: This option will cause the SMS PASSCODE backend to forward each authentication request to the IntelliTrust™ cloud service, thereby allowing authentication to occur according to the behavior defined there.

Setting	Explanation
	<p>Note: The option Determined by IntelliTrust is only available if IntelliTrust integration has been enabled on the General Settings page. Otherwise, you will not see this option in the drop-down list.</p> <p>When this option is selected, another drop-down list will appear, listing the Applications of type "Authentication API" that have been created within your IntelliTrust™ tenant. This allows you to select the Application that determines the authentication behavior:</p>  <p>IMPORTANT: Set client type filter (recommended) The current release of SMS PASSCODE supports IntelliTrust™ authentication for the following SMS PASSCODE authentication clients: SMS PASSCODE AD FS Protection, SMS PASSCODE RADIUS Protection, SMS PASSCODE IIS Website Protection and SMS PASSCODE Windows Logon Protection. Any other type of client will currently fail authentication, if an authentication rule is applied, that is set to "Determined by IntelliTrust" as the result. Therefore, it is strongly recommended to set a client type filter on the Conditions tab, that will only apply such a rule, when a client of type RADIUS, AD FS, IIS Website Protection or Windows Logon is in use (cf. example 3 in section 17.8.3).</p> <p>As you can optionally create several authentication rules that determine authentication based on different IntelliTrust™ applications, this gives you the flexibility of configuring different authentication behavior for different contexts. Authentication behavior is configured using Applications and Resource rules in the IntelliTrust™ Administration Portal. For more information on this, please read section 16.2, page 99.</p> <p>IMPORTANT: IntelliTrust™ authentication takes full control When Access is set to Determined by IntelliTrust, <u>all</u> authentication behavior is delegated to IntelliTrust™. This means that special authentication behavior that is normally handled by the SMS PASSCODE backend, does not apply anymore. For example, SMS PASSCODE token authentication or personal passcode authentication cannot be used as a failover mechanism. Instead, you can configure similar behavior in IntelliTrust™, for example allowing Token OTP authentication or Temporary Access codes.</p> <p>NOTE: Although IntelliTrust™ takes full control of the authentication behavior, you will still see the outcome logged in the SMS PASSCODE authentication monitor (if enabled).</p>

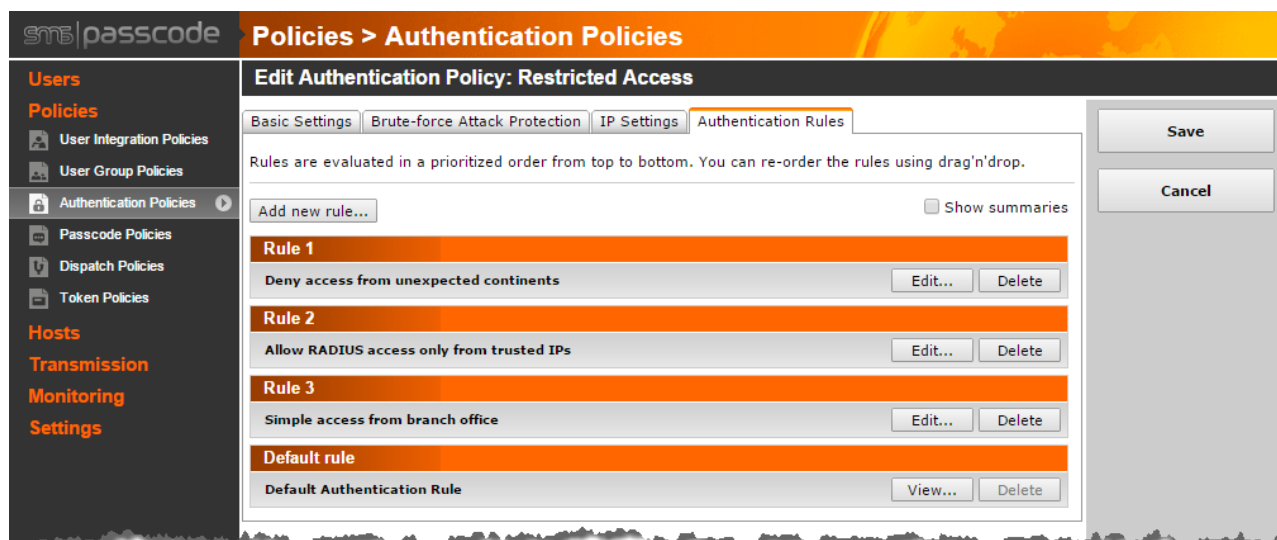
Setting	Explanation
Change of IP trust level	<div data-bbox="416 315 1434 385" style="border: 1px solid black; background-color: #f4a460; padding: 5px; margin-bottom: 10px;"> Please note, that this setting is only available, if the setting Geo IP and IP history is enabled on the General Settings page </div> <div data-bbox="405 416 1302 757" style="border: 1px solid black; background-color: #f4a460; padding: 10px; margin-bottom: 10px;">  </div> <p>The setting Change of IP trust level lets you define, how much the <i>Trust Level</i> of the end-user IP address must increase, in case the authentication attempt succeeds.</p> <div data-bbox="416 860 1434 1050" style="border: 1px solid black; background-color: #f4a460; padding: 5px; margin-bottom: 10px;"> <p>IMPORTANT:</p> <p>Please note that the <i>Trust Level</i> is only increased in case of a successful multi-factor authentication with Access set to Allow access, use MFA and a <i>real</i> multi-factor authentication succeeds. “Real” means that an OTP from a passcode message or token was used during authentication, as opposed to using a Personal Passcode.</p> </div> <p>It is recommended to either use the default setting of 1, or alternatively set it to zero, in case you have a specific authentication scenario that should not contribute to trusting IP addresses. For example, you might not want end-user IP addresses in foreign countries to become trusted ever.</p>

Setting	Explanation
Password reset flow	<div data-bbox="414 286 1439 416" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Password Reset only This setting is only relevant for the SMS PASSCODE Password Reset module and is hidden if you have not acquired any Password Reset CALs. You can just ignore this setting if you are not intending to make use of the Password Reset module. </div> <div data-bbox="406 443 1417 967" style="border: 1px solid black; padding: 10px; margin-bottom: 10px;"> <p>Edit Authentication Rule 1</p> <p>Basic Conditions Result</p> <p>Access Allow access, use MFA ▼</p> <p>Change of IP trust level On successful authentication increment IP trust level by: 1</p> <p>Password reset flow Allow access to the Password Reset Website using:</p> <ul style="list-style-type: none"> <input checked="" type="radio"/> Strict flow Username, then Personal Passcode, then OTP. <input type="radio"/> Flexible flow Username, then password or Personal Passcode, then OTP. <input type="radio"/> Simple flow (low security) Username, then OTP. </div> <p>The Password reset flow setting affects the login behavior of the SMS PASSCODE Password Reset Website. The effective login behavior is determined by a combination of the Access and the Password reset flow setting. Please read section 23.3.2 (page 343) for more details regarding the possible login flows.</p> <p>The most secure login flow is achieved by selecting Allow access, use MFA for the setting Access, and selecting Strict flow for the setting Password reset flow.</p> <p>However, by creating several authentication rules with different Password reset flow values depending on different login conditions (login context), you are able to create an adaptive login behavior, making the login less secure, but more convenient from trusted login contexts.</p>

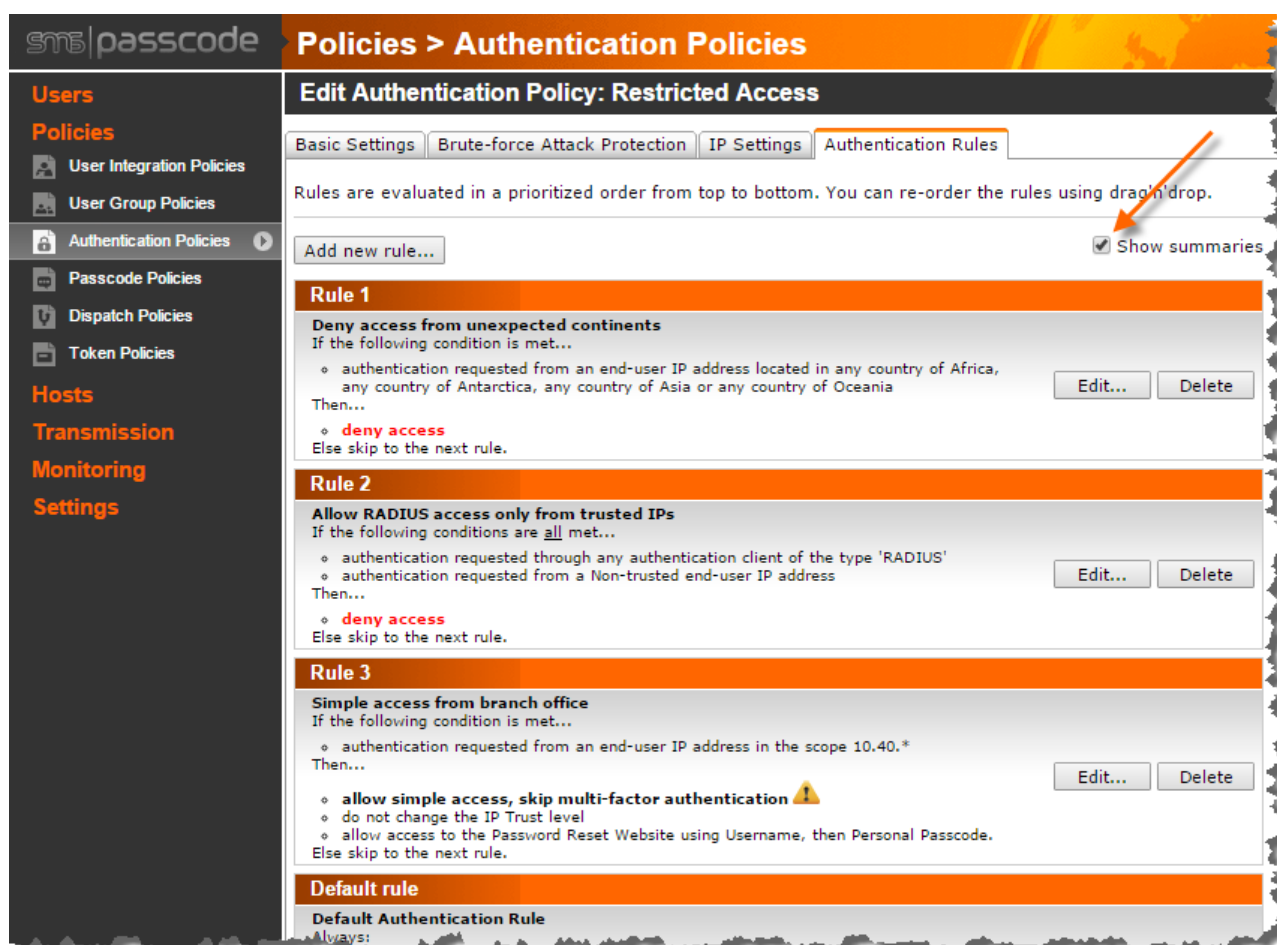
Setting	Explanation
Dispatch Policy & Passcode Policy	 <p>These settings only apply, when Access is set to Allow access, use MFA. By default, the Dispatch Policy and Passcode Policy used during an authentication attempt are determined <u>statically</u> by the configuration of the actual user – either by inheriting the policies from the User Group Policy, or by specific policy overrides on the user itself (cf. section 17.2.1, page 105). However, when an Authentication Rule applies to a specific authentication attempt, you may optionally introduce a <u>dynamic</u> override of those policies, which takes highest precedence. This means, you may introduce context aware switching to a Dispatch Policy and/or Passcode Policy that makes more sense in the specific context; also called <i>adaptive contextual message dispatching</i>. For example, switching to a Dispatch Policy that prefers voice calls before SMS, when logging in from specific countries, or switching to a Dispatch Policy that calls a landline phone number in a branch office (as the secondary phone number), when logging in from the branch office.</p> <p>To introduce a dynamic policy override, i.e. perform <i>adaptive contextual message dispatching</i>, select the corresponding Override radio button, then select the policy of choice from the drop-down list.</p>

17.8.2.6 Authentication Rule Summaries

When maintaining a sequence of Authentication Rules, by default, the **Authentication Rules** tab will only display the **Description** of each rule:



However, you may select the **Show summaries** checkbox to get a short summary of each Authentication Rule:



17.8.3 Authentication Policy Examples

This section shows different examples on how Authentication Policies can be applied usefully.

Example 1 (Limit access from specific countries):

An enterprise is located in Germany and its employees usually perform logins from Germany only. Any login from Germany should have full access to all authentication clients. Logins from other countries of Europe should have access to all clients, except RADIUS. Logins from outside Europe must not have any access at all. To achieve this, you need to create an Authentication Policy with the following four Authentication Rules (the last one being the built-in default Authentication Rule):

Authentication Rule

#1

Configuration

The first rule will allow access to everything, but from Germany only. Hence, the **Countries** condition is set to Germany, and **Access** is set to **Allow access, use MFA**:

Edit Authentication Rule 1

Basic Conditions Result

Authentication Client End-user IP Countries* Organization

Specify whether this rule applies to authentications from IP addresses located in any country, or only located in specific selected countries.

Specific ▾

Selected as filter:

☐ Europe

☐ Germany

<-- Incl. --> Excl.

Available for selection:

☐ Africa

- ☐ Algeria
- ☐ Angola
- ☐ Ascension Island
- ☐ Benin
- ☐ Botswana
- ☐ Burkina Faso
- ☐ Burundi
- ☐ Cameroon
- ☐ Cape Verde
- ☐ Central African Republic

Edit Authentication Rule 1

Basic Conditions Result

Access Allow access, use MFA ▾

Change of IP trust level On successful authentication increment IP trust level by:

1

Authentication Rule

#2

Configuration

The second rule will allow access to all clients, except RADIUS Protection, but only from countries within Europe. Hence the **Authentication client type** filter is set to all clients except RADIUS Protection, the **Countries** condition is set to all countries of Europe, and **Access** is set to **Allow access, use MFA**:

Edit Authentication Rule 2

Basic Conditions Result

Authentication Client End-user IP Countries Organization

Specify whether this rule applies to authentications through any authentication having a specific IP address, or an IP address within a specific IP address range (192.168.112.*), or being of a specific type.

Authentication client IP Any

Authentication client type Specific

- ☒ AD FS
- ☒ Citrix Web Interface
- ☒ IIS Website (ISAPI)
- ☐ RADIUS
- ☒ Secure Device Provisioning
- ☒ Windows Logon
- ☒ Password Reset Website

Edit Authentication Rule 2

Basic Conditions Result

Authentication Client* End-user IP Countries* Organization

Specify whether this rule applies to authentications from IP addresses located in any country, or only located in specific selected countries.

Specific

Selected as filter:

- ☐ Europe
 - ☐ Albania
 - ☐ Andorra
 - ☐ Austria
 - ☐ Belarus
 - ☐ Belgium

Available for selection:

- ☐ Africa
 - ☐ Algeria
 - ☐ Angola
 - ☐ Ascension Island
 - ☐ Benin
 - ☐ Botswana

<-- Incl. --> Excl.

Edit Authentication Rule 2

Basic Conditions Result

Access Allow access, use MFA

Change of IP trust level On successful authentication increment IP trust level by:

1

Authentication Rule	Configuration
#3	<div>Deny access in all other cases. I.e. create a rule without any conditions set, that has Access set to Deny access:</div> <div><div>Edit Authentication Rule 3</div><div><div>BasicConditionsResult</div><div><div>Access</div><div>Deny access</div></div><div><div>Change of IP trust level</div><div>On successful authentication increment IP trust level by:<div>0</div></div></div></div></div>

Example 2 (Skip MFA for internal access to OWA):

An enterprise has an Outlook Web Access (OWA) site that is protected using SMS PASSCODE IIS Website Protection and hosted on a specific server with the IP address 10.6.0.40. Any access to the OWA site from within the same network scope should be allowed without requiring SMS PASSCODE multi-factor authentication (MFA). However, any external access to the OWA site should still require MFA. To achieve this, you need to create an Authentication Policy with two Authentication Rules (the last one being the built-in default Authentication Rule):

Authentication Rule

Configuration

#1

The first rule will allow access without MFA, but only regarding access to the SMS PASSCODE IIS Website Protection component on the specific OWA server, and only regarding authentication requests coming from the same network scope. Hence, the **Authentication client IP** and **Authentication client type** conditions are set, and the **End-user IP** condition is set, and **Access** is set to **Allow access, bypass MFA**:

Edit Authentication Rule 1

Basic Conditions Result

Authentication Client End-user IP Countries Organization

Specify whether this rule applies to authentications through any authentication client having a specific IP address, or an IP address within a specific IP address range (wildcard character is allowed, e.g., 192.168.112.*), or being of a specific type.

Authentication client IP Specific ▼ 10.6.0.40

Authentication client type Specific ▼

- ☐ AD FS
- ☐ Citrix Web Interface
- ☒ IIS Website (ISAPI)
- ☐ RADIUS
- ☐ Secure Device Provisioning
- ☐ Windows Logon
- ☐ Password Reset Website

Edit Authentication Rule 1

Basic Conditions Result

Authentication Client* End-user IP* Countries Organization

Specify whether this rule applies to authentications from any arbitrary end-user IP address, or address, or an IP address within a specific IP address range (wildcard character "*" is allowed, e.g., 192.168.112.*), or being of a specific category (trusted or not).

End-user IP Specific ▼ 10.6.0.*

Category of end-user IP Any ▼

Edit Authentication Rule 1

Basic Conditions Result

Access Allow access, bypass MFA ▼

Change of IP trust level On successful authentication increment IP trust level by: 0

Example 3 (Hybrid Setup):

An enterprise wants to utilize a Hybrid Setup, where IntelliTrust™ authentication is used for AD FS and RADIUS clients, whereas traditional SMS PASSCODE authentications is used for all other clients. To achieve this, you need to create an Authentication Policy with two Authentication Rules (the last one being the built-in default Authentication Rule):

Authentication Rule

#1

Configuration

The first rule is set to utilize IntelliTrust™ authentication for clients of type AD FS and RADIUS only:

Edit Authentication Rule 1

Basic Conditions Result

Authentication Client End-user IP Countries Organization

Specify whether this rule applies to authentications through any authentication client having a specific IP address, or an IP address within a specific IP address range (with 192.168.112.*), or being of a specific type.

Authentication client IP Any

Authentication client type Specific

- ☒ AD FS
- ☐ Citrix Web Interface
- ☐ IIS Website (ISAPI)
- ☒ RADIUS
- ☐ Secure Device Provisioning
- ☐ Windows Logon
- ☐ Password Reset Website

Edit Authentication Rule 1

Basic Conditions Result

Access Determined by IntelliTrust

using risk-based authentication for SMS PASSCODE AUTH

17.9 Token Policies

While it is recommended to use session-specific, real-time authentication, some organizations nevertheless request support for token authentication as well. SMS PASSCODE supports side-by-side authentication using tokens, and even allows very flexible configuration of the actual types of tokens used by your organization; supporting both hardware and software tokens. If you do not plan to make use of tokens for authentication, then you may disregard this section.

Token Policies are used in SMS PASSCODE to specify the actual types of tokens used in your organization.

SMS PASSCODE supports the following types of tokens:

- All OATH compliant tokens, including time-based (TOTP) and event-based (HOTP) tokens
- Proprietary USB Keys from Yubico (YubiKeys)

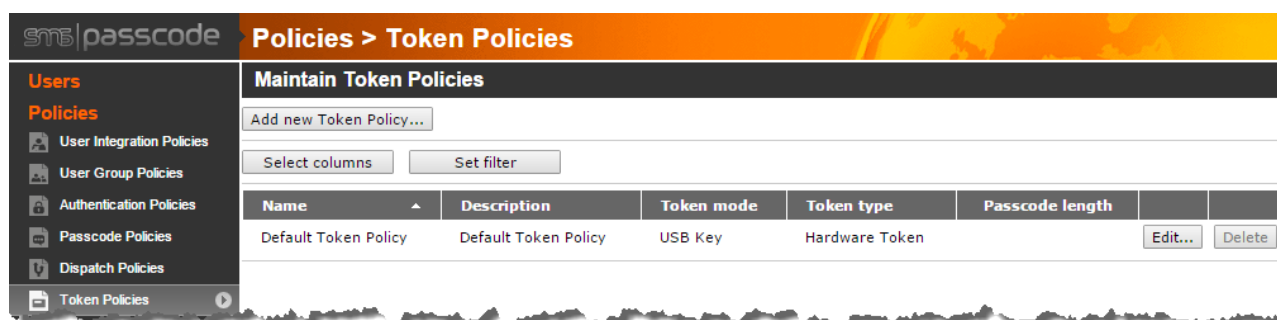
You can use any kind of OATH compliant token, including hardware and software tokens, since Token Policies let you specify the relevant token characteristics.

Token Policies also support import of **token seed files**, which are typically used in case of hardware tokens to import mappings from token serial numbers to token seeds.

Each user is assigned to exactly one Token Policy, which defines the characteristics of the token assigned to the user. If you allow different user groups to use tokens with different characteristics, then just create several Token Policies and assign them as needed. Typically, you will assign the different user groups to dedicated User Group Policies that assign the right Token Policy. Alternatively, you can permit users to choose the appropriate Token Policy by themselves using the SMS PASSCODE Self-Service Website (cf. section 17.6.1.2, page 163).

IMPORTANT: Please ensure that all required Token Policies are configured correctly and assigned to the right users, BEFORE starting assignment of tokens to users. If you change the **Token ID encoding** setting of a Token Policy afterwards, this will most likely invalidate all existing token assignments.

Token Policies are maintained on the **Token Policies** page. The first time you enter this page, it will look like this:



NOTE: If you do not see the **Token Policies** menu item in the navigation menu, then you have not allowed **Token authentication** on the **General Settings** page (cf. section 17.3.2 page 110).

Initially, the SMS PASSCODE database will only contain a single Token Policy called *Default Token Policy*. This policy cannot be deleted and will always be assigned to users that are not assigned to any other Token Policy. You can edit the *Default Token Policy*, and you can add any number of additional Token Policies. It is recommended to create additional Token Policies in the following two cases:

- Your organization is using several types of tokens with different characteristics. In this case, create a Token Policy per token type.
- Your organization is only using one type of tokens, but you need to import one or more token seed files for these tokens. In this case, you need to create an additional Token Policy, since the *Default Token Policy* does not support import of token seed files.

In all other cases, it is recommended not to create any additional Token Policies, but instead just edit the *Default Token Policy* and configure it according to your requirements.

To maintain Token Policies, proceed as follows:

- To add a new Token Policy, click the **Add new Token Policy...** button.
- To edit a Token Policy, click the **Edit...** button on the policy.
- To delete a Token Policy, click the **Delete** button on the policy.

Policies > Token Policies

Maintain Token Policies

Add new Token Policy... **a**

Select columns Set filter

Name	Description	Token mode	Token type	Passcode length	Edit...	Delete
Default Token Policy	Default Token Policy	USB Key	Hardware Token		Edit...	Delete
Google Authenticator (HOTP)	Policy for using Google Authenticator (event-based)	OATH / HOTP	Software Token	6	Edit...	Delete
Google Authenticator (TOTP)	Policy for using Google Authenticator (time-based)	OATH / TOTP	Software Token	6	Edit...	Delete
MS Authenticator	Policy for using MS Authenticator	OATH / TOTP	Software Token	6	Edit...	Delete

b **c**

NOTE: The built-in **Default Token Policy** is a special policy, which is assigned to User Group Policies and users by default. You can edit, but not delete this policy.

IMPORTANT: Please note when deleting a Token Policy that all User Group Policies and/or users referring to this Token Policy will be set to refer to the **Default Token Policy** instead.

17.9.1 Creating a new Token Policy

When creating a new Token Policy, you have to make an important decision, how to maintain the token IDs (also called “token seeds”) of the tokens that will be assigned to users referring to this Token Policy:

Create new Token Policy

How would you like to maintain the token IDs of the users assigned to the new Token Policy?

☒ **Manual entry**
Select this option to enable manual entry of token IDs. Typically used for software tokens.

☐ **Import from token seed file(s)**
Select this item to import token IDs from token seed files containing mappings from public token serial numbers to secret token IDs. Typically used for hardware tokens.

Create Cancel

The two options work as follows:

- **Manual entry:** This option means that token IDs have to be entered directly, when assigning a token to a user. This can be handled in two ways:
 - Administrator provisioning: An administrator can enter the token ID directly on the user maintenance page, when provisioning the token for the user.
 - Self-provisioning: The end-user can enter the token ID in the SMS PASSCODE Self-Service Website, if allowed to.

Manual entry is the most common choice for software tokens, where the token ID is not pre-loaded into the tokens by the token manufacturer but can be chosen as desired.

Token sharing is not supported with this option. I.e. even if you enter the same token ID for two users, this will be treated as two independent tokens.

- **Import from token seed file(s):** This option means that token IDs are determined indirectly. In this case, you will need to import so-called *token seed files*. Such a file defines the mappings from public token serial numbers to private token IDs. After having imported one or more relevant token seed files, token assignment can be handled in two ways:
 - Administrator provisioning: An administrator can enter the token serial number directly on the user maintenance page, when provisioning the token for the user.
 - Self-provisioning: The end-user can enter the token serial number in the SMS PASSCODE Self-Service Website, if allowed to.

In either case, the entered token serial number is used by the SMS PASSCODE system to determine the token ID via the imported token seed file mappings.

Token sharing is supported with this option. I.e. it is allowed to assign the same token serial number to several users, who can then share the corresponding token.

Import of token seed files is typically used for hardware tokens, where token IDs are pre-loaded into the tokens by the token manufacturer, and the manufacturer provides a corresponding token seed file, when delivering the tokens. The token serial numbers are typically printed directly on each token.

Requirements

Please note that the following token seed file formats are supported: CSV and PSKC. Any other proprietary file formats are not supported.

Additionally, only OATH tokens are supported, when importing token seed files. When using USB Keys ("YubiKeys"), please select the **Manual entry** option.

IMPORTANT: Permanent decision

The selected option for handling of token IDs is **permanent**. I.e. after creating a new Token Policy, you will not be able to switch the option for this Token Policy. However, you can always delete the Token Policy and create a new one.

The subsections below explain the different settings of a Token Policy in detail. First section 17.9.2 describes the settings available in **Manual entry** mode, whereas section 17.9.3 describes the settings available in **Import from token seed file(s)** mode.

17.9.2 Settings of a Token Policy in Manual Entry Mode

When maintaining a Token Policy in **Manual entry** mode, the following page is shown:

The different settings are described in detail below. When making changes to a Token Policy please remember to click the **Save** button to store the changes permanently.

	Setting	Explanation
(a)	Name	<p>The name used to identify the Token Policy. Giving the Token Policy a unique name is mandatory.</p> <p>Note: If you are planning to permit end-users to select Token Policies in the SMS PASSCODE Self-Service Website, then it is recommended to give the Token Policies descriptive names, since end-users will have to select the policies by name.</p>
(b)	Description	<p>Optional description of the Token Policy, for your own records. Here you can describe the purpose of the policy in more detail.</p>
(c)	Token Mode	<p>This setting is used to specify the general type of the token. The following types are supported:</p> <ul style="list-style-type: none"> <u>USB Key:</u> Proprietary “YubiKey” token. <p>Note: As mentioned in section 17.3.2 (page 110), you need to sign up for a 3rd party web service in order to validate logins using this type of token.</p> <ul style="list-style-type: none"> <u>OATH / HOTP:</u> Event-driven OATH compliant token. <u>OATH / TOTP:</u> Time-driven OATH compliant token.

When Token Mode **USB Key** is selected, no additional settings are required. For the OATH Token modes, more settings will be shown that allow configuration of the specific OATH tokens in question:

Policies > Token Policies

Create a new Token Policy

Settings Imported tokens

Name: MyManualEntryPolicy

Description:

Token mode: OATH / HOTP ▼

Token type: Hardware Token ▼ **d**

Passcode length: 6 ▼ **e**

Hash function: HMAC-SHA-1

Token ID encoding: HEX (Base16) ▼ **h**

Token Policy settings available with **Token Mode = OATH / HOTP**

Policies > Token Policies

Create a new Token Policy

Settings Imported tokens

Name: MyManualEntryPolicy

Description:

Token mode: OATH / TOTP ▼

Token type: Hardware Token ▼ **d**

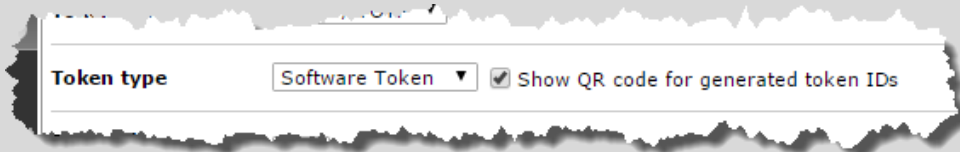
Passcode length: 6 ▼ **e**

Hash function: HMAC-SHA-1 ▼ **f**

Time step: 30 second(s) **g**

Token ID encoding: HEX (Base16) ▼ **h**

Token Policy settings available with **Token Mode = OATH / TOTP**

	Setting	Explanation
(d)	Token type	<p>Use this setting to specify the type of token, i.e. whether it is a hardware token or software token. The difference between these types of tokens is the way token IDs are assigned.</p> <p>For hardware tokens, the vendor has pre-loaded a unique token ID into each token. When assigning a specific token to a user, the administrator or user must ensure that the correct pre-loaded token ID is entered and assigned to the user.</p> <p>For software tokens, no token ID has been pre-loaded. The administrator or user may enter any token ID of own choice. In this case, SMS PASSCODE provides a Generate button, which can be used optionally for generating a random token ID.</p> <p>When setting the token type to "Software Token", an additional option Show QR code for generated token IDs appears:</p>  <p>Select this option, in case you would like generated token IDs to be presented as QR codes. This applies not only to the Web Administration Interface, but also to the SMS PASSCODE Self-Service Website. I.e. in case a user has been allowed to set a token ID in the Self-Service Website, then the user might generate a token ID himself and scan the resulting QR code. This provides a convenient way for self-enrollment of software tokens.</p> <p>QR codes are supported by many popular software tokens. The QR code will contain the generated token ID, and additionally other relevant parameters corresponding to the user's Token Policy. The following attributes are provided by the QR code:</p> <ul style="list-style-type: none"> • Token ID • Passcode length • Hash function • Time step <div style="border: 1px solid black; background-color: #ffcc00; padding: 10px; margin-top: 10px;"> <p>IMPORTANT (Software Tokens ignoring QR code attributes)</p> <p>Please note that software tokens of some vendors may ignore one or more of the attributes provided by the QR code, because specific behavior is hardcoded into the software token. For example, a specific passcode length or time step size might have been hardcoded. In such cases, it is important that the Token Policy is configured correctly according to the hardcoded attributes of the software token in question (please consult the specifications of the software token).</p> </div>
(e)	Passcode length	<p>Use this setting to specify the number of digits in the passcodes generated by the OATH token. A length of 6 digits is most common, but SMS PASSCODE also supports tokens with 7 or 8 digits.</p>

	Setting	Explanation
(f)	Hash function	<p>This setting is for time-based (TOTP) OATH tokens only.</p> <p>According to the OATH standard, TOTP tokens are allowed to use the HMAC-SHA-1, HMAC-SHA-256 or HMAC-SHA-512 function for passcode generation. Use this setting to specify the function used by your specific tokens, according to the token manufacturer's specification. If in doubt, please try the different settings by trial-and-error, until authentication succeeds.</p> <p>HMAC-SHA-1 is the most common choice.</p>
(g)	Time step	<p>This setting is for time-based (TOTP) OATH tokens only.</p> <p>Use this setting to specify the validity period of each generated passcode. Please refer to the specification of your tokens to select the correct duration.</p> <p>Most commonly, TOTP tokens generate a new passcode every 30 or 60 seconds.</p>
(h)	Token ID encoding	<p>Use this setting to specify the format of the token IDs, when they are entered either into the Web Administration Interface (by administrators or via user synchronization from a user store) or into the Self-Service Website (by end-users).</p> <p>If in doubt about the token ID format, here are some hints:</p> <ul style="list-style-type: none"> • HEX (Base16) IDs may contain digits 0-9 and letters A-F (case insensitive). • Base32 IDs may contain digits 2-7, letters A-Z (case insensitive) and the character "=" for padding. • Base64 IDs may contain digits 0-9, letters A-Z and a-z (case sensitive), characters "/" and "+", and the character "=" for padding. <p>If still in doubt, please try the different settings by trial-and-error, until authentication succeeds. For software tokens, Base32 is the most common setting.</p>

17.9.3 Settings of a Token Policy in Token Seed File Import Mode

When maintaining a Token Policy in **Import from token seed file(s)** mode, the following page is shown:

The screenshot shows the 'Edit Token Policy: MyTokenSeedFilePolicy' page in the 'Imported tokens' mode. The sidebar on the left contains navigation links for Users, Policies, Hosts, Transmission, Monitoring, and Settings. The main content area has a 'Settings' tab and an 'Imported tokens' tab. The settings include: Name (MyTokenSeedFilePolicy), Description (empty text area), Token mode (OATH / TOTP), Passcode length (6), Hash function (HMAC-SHA-1), and Time step (30 second(s)). On the right, there are 'Save' and 'Cancel' buttons, and a link to 'Import tokens from file...'.

The settings available are the same as in **Manual entry** mode (cf. section 17.9.2 above), except the following minor differences:

- **Token mode:**
 - Only OATH compliant tokens are supported in this mode. USB Keys (“YubiKeys”) are not supported.
- **Token type:**
 - This setting is not available in this mode, since it is not relevant.
- **Token ID encoding:**
 - This setting is not available in this mode, since the encoding is chosen during import of token seed files.

The following additional features are available in **Import from token seed file(s)** mode:

The screenshot shows the 'Edit Token Policy: MyTokenSeedFilePolicy' page in the 'Imported tokens' mode. The sidebar on the left contains navigation links for Users, Policies, Hosts, Transmission, Monitoring, and Settings. The main content area has a 'Settings' tab and an 'Imported tokens' tab. The settings include: Name (MyTokenSeedFilePolicy), Description (empty text area), Token mode (OATH / TOTP), Passcode length (6), Hash function (HMAC-SHA-1), and Time step (30 second(s)). On the right, there are 'Save' and 'Cancel' buttons, and a link to 'Import tokens from file...'. Red circles 'a' and 'b' highlight the 'Import tokens from file...' link and the 'Imported tokens' tab, respectively.

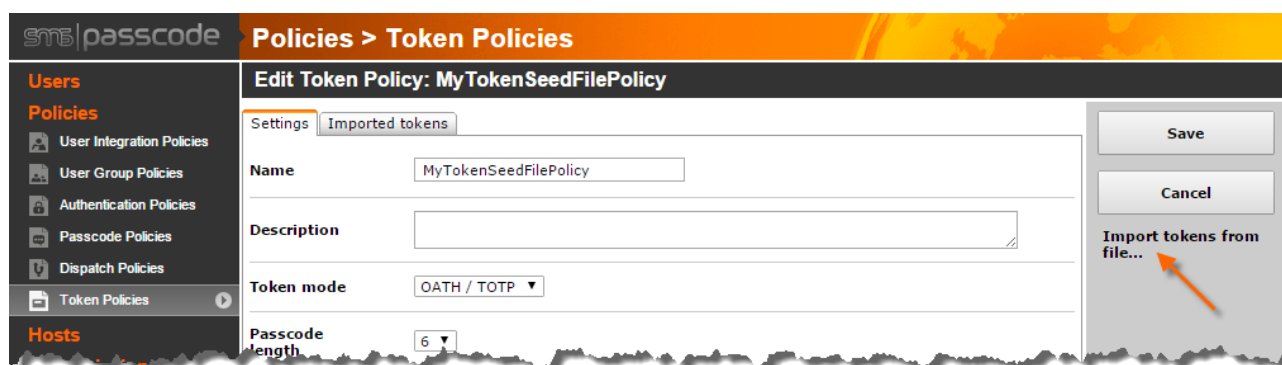
	Feature	Explanation
(a)	Import tokens from file...	Click this link to import a token seed file and store the imported mappings as part of this Token Policy.
(b)	Imported tokens	Click this tab to inspect and maintain previously imported token seed mappings. For example, you can inspect current token assignments or remove previously imported token mappings.

The following two subsections describe these features in more detail.

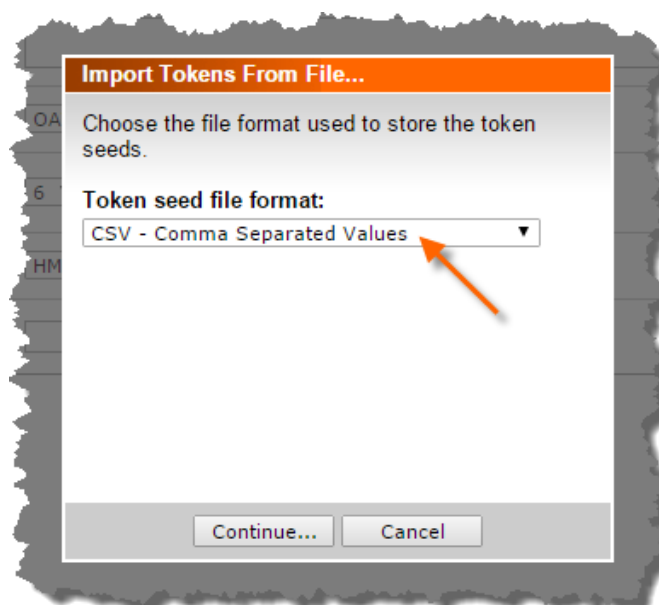
17.9.3.1 Importing Token Seed files

To import a new token seed file into a Token Policy, proceed as follows:

- BEFORE importing a token seed file, please ensure that all settings of the Token Policy comply with the tokens that you are going to import. If you are going to import several token seed files for tokens with different characteristics, then you must create several Token Policies, each one having settings matching the corresponding tokens.
- To start an import, click the **Import tokens from file...** link:



- A dialog appears. Select the appropriate format of the token seed file that you going to import, then click the **Continue...** button:



CSV file format:

When importing a token seed file in CSV format, please note the following requirements:

- Every line must describe the token seed mapping for exactly one token.
- Every line must contain exactly two fields containing "Token S/N" and "Token ID", in this order. Comma (",") or semi-colon (";") are allowed as field delimiters.
- No field headers are expected, i.e. the first line contains the mapping of the first token.

PSKC file Format:

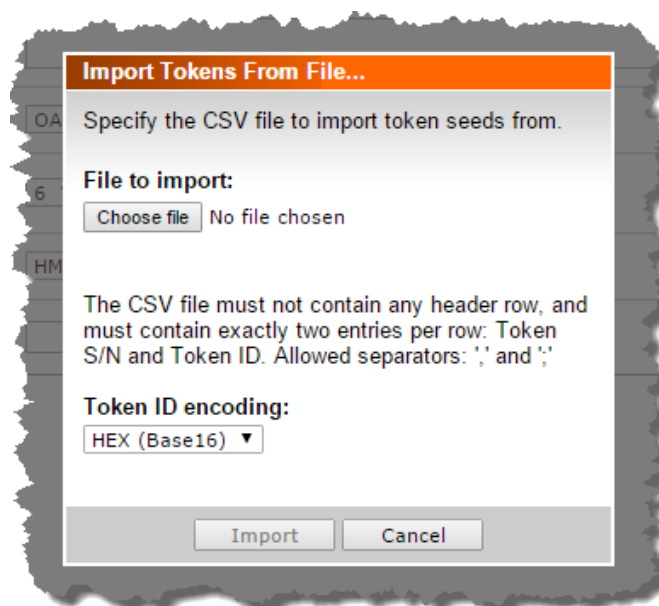
When importing a token seed file in PSKC format, please note the following requirements:

- Both encrypted and non-encrypted PSKC files are supported
- A PSKC file might in rare cases contain tokens with different characteristics, e.g. tokens with different time step sizes. The import routine will automatically detect the characteristics of the tokens in the PSKC file and only import the tokens with characteristics matching the settings of the Token Policy (the remaining ones are skipped). To import all tokens from a PSKC file containing tokens with different characteristics, create several, matching Token Policies, then import the same file into each such Token Policy. This will result in a correct distribution of the tokens into the matching Token Policies.

- A dialog appears for selecting the token seed file to import.

CSV file format:

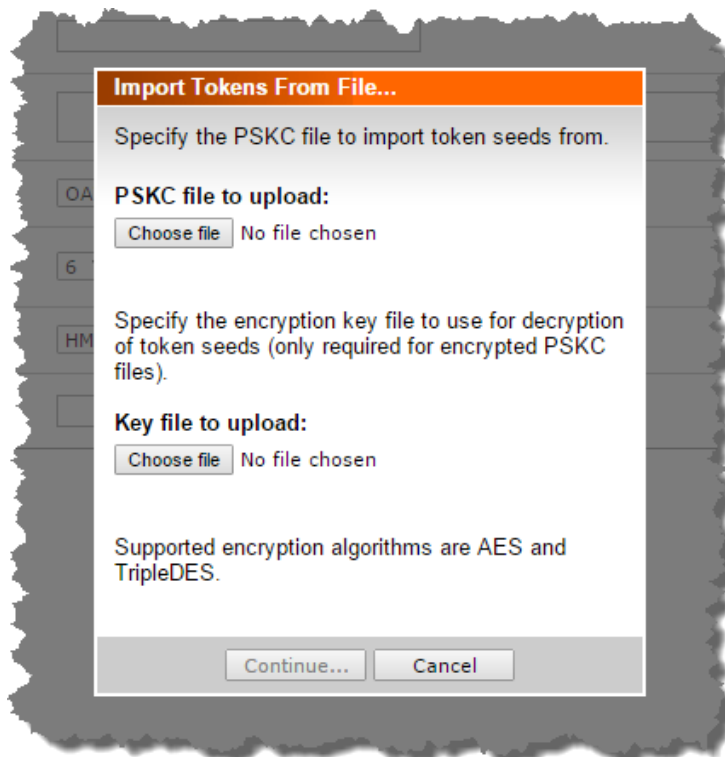
In case of a CSV file, you need to specify the path of the file, and select the correct encoding of the token IDs:



To import the file, click the **Import** button.

PSKC file Format:

In case of a PSKC file, you need to specify the path of the file. Additionally, you may specify the path of the file containing the encryption keys ("key file"). However, this is only required, when the token IDs in the PSKC file have been encrypted – otherwise, just leave the path of the key file empty:



When you are ready to import the file, click the **Continue...** button. A message will appear, informing about the number of tokens in the file, and informing about the number of tokens being imported (with characteristics matching the Token Policy) and being skipped (with characteristics not matching the Token Policy).

IMPORTANT

Any newly imported tokens are NOT persisted to the SMS PASSCODE database, until you click the **Save** button on the Token Policy. I.e. just after the import has been completed, you can inspect the import result on the **Imported tokens** tab and still cancel the import, if the result is not as expected.

The next section describes how to inspect or maintain the imported tokens.

17.9.3.2 Maintaining Imported Tokens

The **Imported tokens** tab on a Token Policy in **Import token seed file(s)** mode lists all information regarding the token seed files imported into this Token Policy so far:

Policies > Token Policies

Edit Token Policy: MyTokenSeedFilePolicy

Settings Imported tokens

	Total	In use	Available
Imported tokens	4000	0	4000

Select columns Set filter Clear filter Page size: 500

Delete selected

	Token serial number	Import date time	Import filename	Assigned user count	Assigned users
<input type="checkbox"/>	1234567890123	9/2/2015 3:00:36 PM	Tokens.csv	0	
<input type="checkbox"/>	1234567890124	9/2/2015 3:00:36 PM	Tokens.csv	0	
<input type="checkbox"/>	1234567890125	9/2/2015 3:00:36 PM	Tokens.csv	0	
<input type="checkbox"/>	1234567890126	9/2/2015 3:00:36 PM	Tokens.csv	0	
<input type="checkbox"/>	1234567890127	9/2/2015 3:00:36 PM	Tokens.csv	0	

Save Cancel

Import tokens from file...

The topmost table shows overall statistics for the imported tokens:

- **Total:** Total number of tokens imported
- **In use:** Number of imported tokens that have been assigned to at least one user (token sharing is supported, i.e. a token is allowed to be assigned to one or more users).
- **Available:** Number of imported tokens that have not been assigned to any user yet.

The table at the bottom lists the specific data for each imported token. By inspecting this data, you can for example get answers to the following questions:

- When was the token imported? ("Import date time")
- What was the name of the file from which the token was imported? ("Import filename")
- How many users have been assigned to this token? ("Assigned user count")
- Which users have been assigned to this token? ("Assigned users")

The **Set filter** button allows you to filter the list of tokens, e.g. to find a specific token S/N, to list all tokens imported from a specific file, or to display available tokens only.

If you want to delete any earlier imported tokens, e.g. because a token has been lost or damaged, please proceed as follows:

Policies > Token Policies

Edit Token Policy: MyTokenSeedFilePolicy

Settings Imported tokens

	Total	In use	Available
Imported tokens	4000	0	4000

Select columns Set filter Clear filter Page size: 500

Delete selected 2 tokens selected.

	Token serial number	Import date time	Import filename	Assigned user count	Assigned users
<input type="checkbox"/>	1234567890123	9/2/2015 3:00:36 PM	Tokens.csv	0	
<input checked="" type="checkbox"/>	1234567890124	9/2/2015 3:00:36 PM	Tokens.csv	0	
<input type="checkbox"/>	1234567890125	9/2/2015 3:00:36 PM	Tokens.csv	0	
<input type="checkbox"/>	1234567890126	9/2/2015 3:00:36 PM	Tokens.csv	0	
<input checked="" type="checkbox"/>	1234567890127	9/2/2015 3:00:36 PM	Tokens.csv	0	
<input type="checkbox"/>	1234567890128	9/2/2015 3:00:36 PM	Tokens.csv	0	
<input type="checkbox"/>	1234567890129	9/2/2015 3:00:36 PM	Tokens.csv	0	
<input type="checkbox"/>	1234567890130	9/2/2015 3:00:36 PM	Tokens.csv	0	

- Select the checkboxes to the left of the tokens to delete (select the checkbox in the header row to select all visible tokens at once).
- Then click the **Delete selected** button.

Please note, that deletions are not committed, until you click the **Save** button on the Token Policy.

17.10 Users

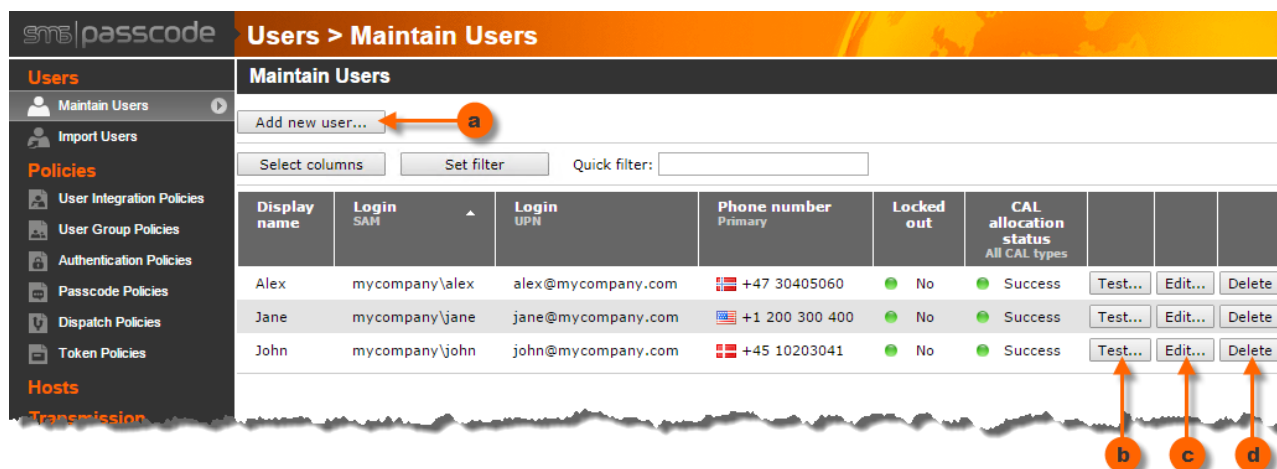
The **Maintain users** page is used for maintaining SMS PASSCODE users. Only users in the SMS PASSCODE database will be granted access by SMS PASSCODE.

Users can be maintained in two different ways – manually or using *User Integration Policies* (i.e. **User store integration**).

You can use both ways at the same time. I.e. you can decide to maintain some users manually, while other users are imported automatically using *User Integration Policies* (cf. section 17.5, page 126).

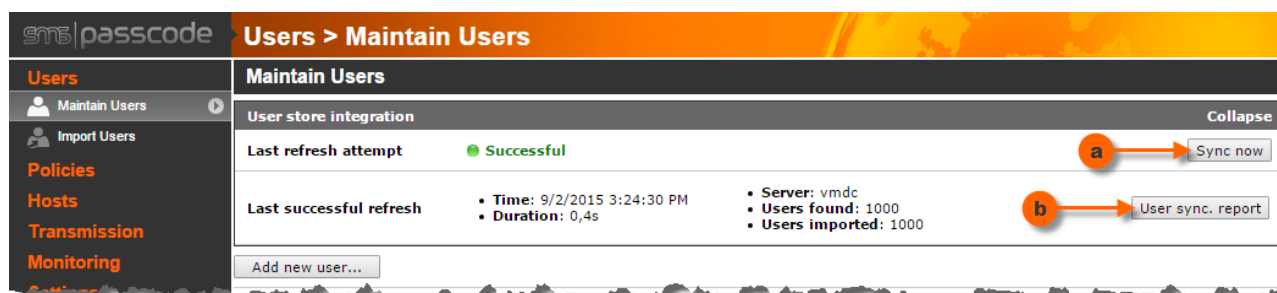
User store integration is disabled by default. You can enable it on the **General Settings** page (cf. section 17.3.1, page 109).

When entering the **Maintain users** page, the appearance will depend on whether **User store integration** is enabled or not. In case **User store integration** is disabled, the page will look similar to this:



- Click the **Add new user...** button to create a new user manually.
- Click the **Test...** button to send a test message to a specific user. This is useful for testing, whether the correct phone number or email address has been assigned to the user, or to test whether message transmission works in general.
- Click the **Edit...** button to edit an existing user.
- Click the **Delete** button to delete an existing user.
Note: The **Delete** button is disabled for users imported by a *User Integration Policy* because such users are maintained via the source user store of the UIP.

If **User store integration** is enabled, the **Maintain users** page will additionally show user synchronization information at the top of the page:



- Click the **Sync now** button to trigger a new user synchronization immediately
- Click the **User sync. report** button to get a detailed report about the last successful synchronization. For example, use this report to inspect which users were skipped and why they were skipped.

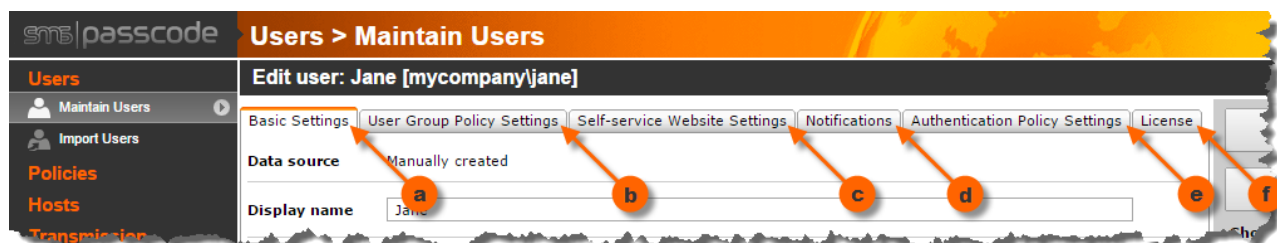
Please note, that you can also bulk import users from a comma-separated file (cf. section 17.11, page 253).

The following subsections describe in detail the settings that can be maintained while creating a new user or editing an existing user.

17.10.1 Settings of a User

When creating a new user or maintaining an existing user, a tab control is shown for configuring the different settings of the user. The settings are divided into 6 tabs:

- a. **Basic Settings**
The main settings of the user, for example username(s) and (mobile) phone number.
- b. **User Group Policy Settings**
The *User Group Policy* (UGP) assigned to the user, and all the settings inherited from this UGP. On this tab, you can inspect the inherited settings and override them if needed.
- c. **Self-service Website Settings**
The Self-service Website settings inherited from the assigned UGP, i.e. permissions for the Self-service Website. On this tab, you can inspect the inherited settings and override them if needed.
- d. **Notifications**
Information about when different types of notifications have been sent to the user.
- e. **Authentication Policy Settings**
Settings inherited from the *Authentication Policy* assigned to the user. On this tab, you can inspect and control the current state of *Learning Mode* for the user.
- f. **License**
Displays the license settings inherited from the assigned UGP, and the current license allocation status. Optionally, you may override the inherited license settings on this tab.



The different settings are described in detail in the following subsections. When making changes to a user please remember to click the **Save** button to store the changes permanently.

17.10.1.1 User: Basic Settings

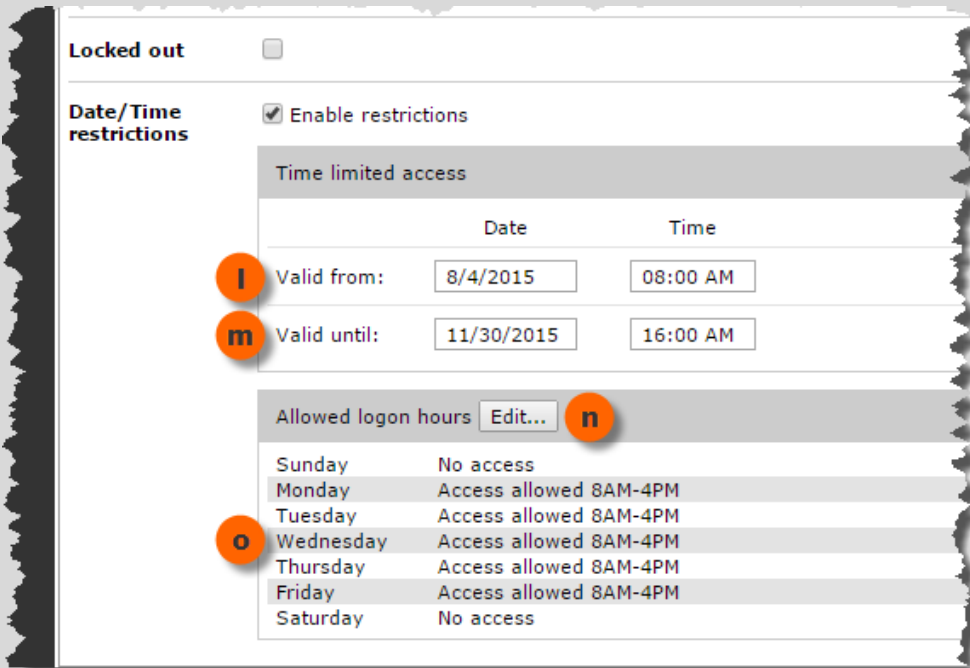
This section describes the settings available on the **Basic Settings** tab while maintaining a user. Please note, that most entries are optional. However, it is mandatory to enter at least one login name (in either SAM or UPN format) that uniquely identifies the user.

	Setting	Explanation
(a)	Data Source	Specifies from where the user originates, i.e. whether the user has been created manually, or imported by a <i>User Integration Policy</i> .
(b)	IntelliTrust	<div> Note: This row is only shown if IntelliTrust™ integration has been enabled on the General Settings page (cf. section 17.3.4, page 119). </div> <p>Shows the current state of synchronizing the user to IntelliTrust™. Possible states are:</p> <ul style="list-style-type: none"> • Pending: Means that no attempt has been made yet to synchronize the user. • Success: Means that the user data has been synchronized successfully. • Failure: Means that synchronizing the user failed. An error message will describe the reason for the failure.
(c)	Display Name	Optional, descriptive name of the user – to be used for searching and filtering.

	Setting	Explanation
(d)	Login (SAM)	<p>Login name of the user in SAM account format.</p> <p>When using a single domain for authentication, you can just enter the login name without any domain name prefix. However, if you are planning to create users from different domains, you should always enter the user name in the format <i>domain\username</i> to avoid name conflicts in case some users from different domains have identical user names.</p>
(e)	Login (UPN)	Login name of the user in UPN format (<i>user@domain</i>).
(f)	Phone number (primary)	<p>(Primary) phone number to be used for receiving passcode messages or notifications.</p> <p>You may explicitly enter an international phone number prefix (e.g. +44). If no prefix is entered, then the <i>default prefix</i> is assumed. The default prefix is configured on the General Settings page (cf. section 17.3.1, page 109).</p>
(g)	Phone number (secondary)	<p>Secondary phone number to be used for receiving passcode messages or notifications in failover scenarios. Used by <i>Dispatch Policies</i> (cf. section 17.18, page 271).</p> <p>You may explicitly enter an international phone number prefix (e.g. +44). If no prefix is entered, then the <i>default prefix</i> is assumed. The default prefix is configured on the General Settings page (cf. section 17.3.1, page 109).</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: This field is only available if secondary phone numbers have been enabled on the General Settings page (cf. section 17.3.1, page 109).</p> </div>
(h)	Email	Email address to be used for receiving passcode messages or notifications (by email).
(i)	Token ID	<p>The unique ID that identifies the token assigned to the user. Entering such an ID will allow the user to use the designated token for authentication, but only if token authentication has also been <u>allowed</u> (on the User Group Policy Settings tab).</p> <p>If the user should be assigned an OATH <u>software</u> token, then a token ID of own choice can be used. In this case, the Generate button can be clicked to generate a random token ID. Please enter such random token ID into the software token immediately, since it cannot be displayed later again. If the option Show QR code for generated token IDs has been enabled on the user's Token Policy, then the generated token ID will be shown as a QR code. This provides a very convenient way for the administrator to enter the token ID into the software token – simply by scanning the QR code (requires that the software token supports QR codes).</p>

	Setting	Explanation
		 <p>If the user should be assigned a token of type USB Key (YubiKey) and you have the USB Key at hand, then the easiest way to enter the ID is to place the cursor in the Token ID field, insert the USB Key into a USB port, and click the button on the USB Key.</p> <div data-bbox="414 1108 1433 1205" style="border: 1px solid black; background-color: #f4a460; padding: 5px;"> <p>Note: This field is only available if token authentication has been allowed on the General Settings page (cf. section 17.3.2, page 110), and the user is assigned to a Token Policy NOT using token seed file imports.</p> </div> <p>Token Resync: When using OATH tokens, you may need in some cases to perform a <i>Resync</i> of the token, if it gets out of sync for some reason. One possible reason is that an existing, already used token, is re-assigned from one user to another.</p> <p>When a token ID has been defined and the user is allowed to perform token authentication, a Resync button will appear beside the token ID field. Click the button to perform a resync. A dialog will pop up and ask you to enter two <u>consecutive</u> OTPs from the token. Using these two codes, the system will resynchronize the internal token state, and the token should work again.</p> <p>If allowed to, end-users can also perform a token resync by themselves using the SMS PASSCODE Self-Service Website. The resync permission is set on the Self-service Website Settings tab of the user's UGP (or overridden on the Self-service Website Settings tab of the user).</p>

	Setting	Explanation
(j)	Token S/N	<p>If the user has been assigned a Token Policy with token seed file imports, then you will not see the Token ID field, but instead a Token S/N field.</p> <p>Note: This field is only available if token authentication has been allowed on the General Settings page (cf. section 17.3.2, page 110), and the user is assigned to a Token Policy using token seed file imports.</p> <p>This field allows you to enter the public token S/N of a token to assign it to the user. The token S/N is typically printed directly on the physical token itself.</p>
(k)	PIN	<p>Optional code, typically consisting of 4 digits, that must be entered in front of each passcode during SMS PASSCODE authentication attempts.</p> <p>Note: This field is only available if the usage of PIN codes has been allowed on the General Settings page (cf. section 17.3.2, page 110).</p> <p>Note: PIN codes do not take effect, when IntelliTrust™ authentication is in use (Hybrid Setup).</p>
(l)	Locked Out	<p>Specifies whether the user account has been locked out. You can manually lock out or unlock a user account. Furthermore, an account might also become locked out automatically by the system due to different types of authentication attacks. If this happens, a note is displayed below the checkbox explaining the reason for the lockout. The note might as well inform about the duration of the lockout, in case it is a temporary lockout set by the system.</p>

	Setting	Explanation
(k)	Date/Time restrictions	<p>Select this option if you would like to define date and/or time restrictions for the user, i.e. to restrict when the user is allowed to log in to any of the SMS PASSCODE protected authentication clients.</p> <p>This option is deselected by default. When selecting the option, additional options become available at the bottom of the Basic Settings tab:</p>  <ul style="list-style-type: none"> • The section Time limited access contains settings that allow you to define, when the user account becomes active (l) and/or expires (m). You may set Valid from without setting Valid until, and vice versa. It is optional to enter anything into the Time fields. If nothing is entered into a Time field, then the whole day of the entered date is included. <ul style="list-style-type: none"> ○ If setting (l) is set, then a user is not allowed to log in to any SMS PASSCODE protected authentication client, until the specified date (and time). ○ If setting (m) is set, then a user is not allowed to log in to any SMS PASSCODE protected authentication client after the specified data (and time). <p>Among others, these settings are useful for defining a restricted period of remote access for an external consultant.</p> • The section Allowed logon hours allows you define a fixed schedule of allowed logon hours, i.e. define specific hours of each week day, where the user is allowed to log in to any SMS PASSCODE protected authentication client. To define the schedule, click on the button Edit... (n) and select the allowed logon hours in the week-hour-matrix that appears. Afterwards, a summary of the selected schedule is displayed at the bottom of the section (o).

17.10.1.2 User: User Group Policy Settings

This section describes the settings available on the **User Group Policy Settings** tab while maintaining a user.

The main purpose of the **User Group Policy Settings** tab is to provide the option to select the *User Group Policy* (UGP) to assign to the current user (a):

Users > Maintain Users

Edit user: Jane [mycompany/jane]

Basic Settings | **User Group Policy Settings** | Self-service Website Settings | Notifications | Audit

	Override	Policy
User Group Policy	<input type="checkbox"/>	Default User Group Policy ▼ (a)
Authentication Policy	<input type="checkbox"/>	Default Authentication Policy ▼ (b)
Passcode Policy	<input type="checkbox"/>	Default Passcode Policy ▼
Dispatch Policy	<input type="checkbox"/>	Default Dispatch Policy ▼
Token Policy	<input type="checkbox"/>	Default Token Policy ▼
Passcode type	<input type="checkbox"/>	<input checked="" type="radio"/> One-time passcode (OTP) <input type="radio"/> Personal passcode
SMS type	<input type="checkbox"/>	<input checked="" type="radio"/> Flash SMS <input type="radio"/> Standard SMS
Token authentication	<input type="checkbox"/>	<input type="radio"/> Allow <input checked="" type="radio"/> Deny
Personal passcode	<input type="checkbox"/>	No Personal passcode has been defined Note: A personal passcode can be used for two purposes: 1) For accessing the Password Reset Website (in case the user is allowed to) 2) For temporarily being able to authenticate without a one-time passcode, e.g. while passcode type is switched to Personal Passcode.

As soon as a UGP has been selected, region (b) will show the settings that the user inherits from this UGP. In case you need to define a user specific exception, you can override any of the inherited settings by selecting the *override checkbox* of the setting in question. The *override checkboxes* are located in the *override column*, region (c).

Please read section 17.6.1.1 (page 160) for a detailed description of the various UGP settings.

17.10.1.3 User: Self-service Website Settings

This section describes the settings available on the **Self-service Website Settings** tab while maintaining a user. You only need to maintain settings on this tab if you intend to make use of the SMS PASSCODE Self-service Website (cf. section 22, page 325), and you wish to override the Self-service Website permissions inherited from the UGP assigned to the user.

Users > Maintain Users

Edit user: Jane [mycompany]jane

Basic Settings | User Group Policy Settings | **Self-service Website Settings** | Notifications | Authentication Policy Settings

Permissions

Permission	Override	Allow	Deny
Access to Self-service	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Permission	Override	Read/Write	Read-only
Username	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Dispatch Policy	<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>
SMS type	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Primary phone number	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Secondary phone number	<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>
Email	<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>
Personal passcode	<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>
Passcode type	<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>
PIN	<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>
Token Policy	<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>
Token assignment	<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>
Permission	Override	Allow	Deny
Resync token	<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>

The **Self-service Website Settings** tab contains a *permission table* that shows the permissions of the user with respect to the SMS PASSCODE Self-service Website. Initially, region (a) shows the permissions inherited by the UGP assigned to the user. The *override checkboxes* in region (b) allow you to override individual permissions and define user specific exceptions.

Please read section 17.6.1.2, page 163, for a detailed description of the various Self-service Website permissions.

17.10.1.4 User: Notifications

This section describes the content of the **Notifications** tab while maintaining a user.

The **Notifications** tab lists the status of each type of SMS PASSCODE notification. This allows you to inspect:

- Which types of notifications are enabled or disabled for the user?
- When has a specific type of notification been sent to the user?

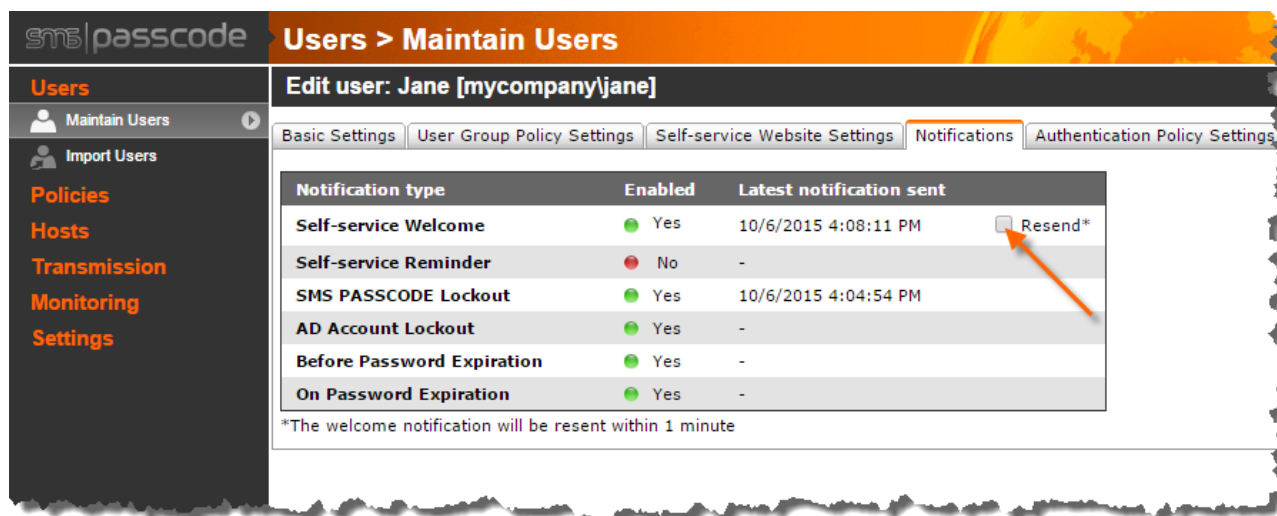
Notification type	Enabled	Latest notification sent	Resend*
Self-service Welcome	Yes	10/6/2015 4:08:11 PM	<input type="checkbox"/>
Self-service Reminder	No	-	
SMS PASSCODE Lockout	Yes	10/6/2015 4:04:54 PM	
AD Account Lockout	Yes	-	
Before Password Expiration	Yes	-	
On Password Expiration	Yes	-	

The welcome notification will be resent within 1 minute

Note: The notifications **AD Account Lockout**, **Before Password Expiration** and **On Password Expiration** are only shown on the tab, when the user has been imported from an Active Directory, and the user has been allocated a Password Reset CAL. Otherwise, these notifications are not relevant.

	Column	Explanation
(a)	Notification type	The name of the notification type
(b)	Enabled	Specifies, whether the corresponding type of notification in column (a) is currently enabled or disabled, according to the User Group Policy, to which the user is currently assigned.
(c)	Latest notification sent	Specifies the most recent date and time, when the corresponding type of notification in column (a) was sent to the user. A dash ("-") means that the corresponding type of notification has never been sent to the user.

Additionally, in case you would like to re-send the **Self-service welcome notification** to the user, you can select the checkbox **Resend**:



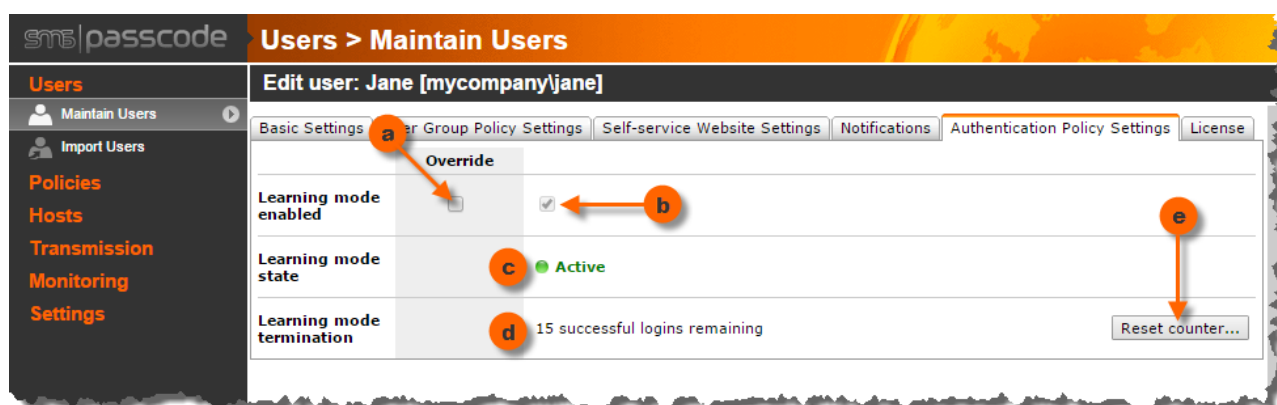
Afterwards, you must also click the **Save** button to actually trigger the resending of the notification.

17.10.1.5 User: Authentication Policy Settings

This section describes the content of the **Authentication Policy Settings** tab while maintaining a user.

Note: The **Authentication Policy Settings** tab is only available when the setting **Geo IP and IP history** is enabled on the **General Settings** page.

As explained in section 17.8.2.3 (page 201), the Authentication Policy assigned to a user might define settings for the user regarding *Learning Mode*. While maintaining a user, the **Authentication Policy Settings** tab is used to control and display current state information regarding the *Learning Mode*:

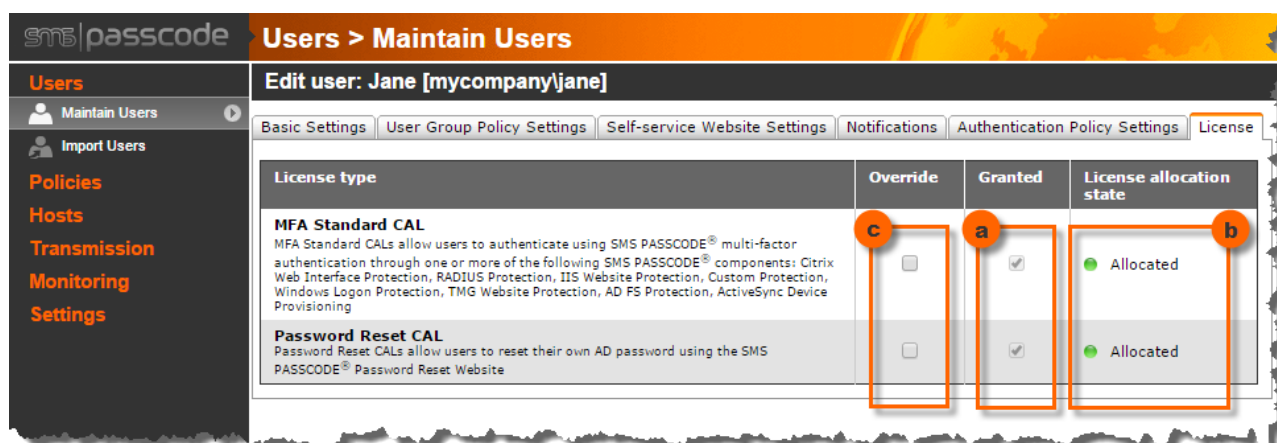


	Setting	Explanation
(a)	Learning Mode Enabled	By default, checkbox (b) displays whether <i>Learning Mode</i> is enabled according to the Authentication Policy assigned to the user (inherited setting). However, the inherited setting can be overridden by selecting checkbox (a) and hereafter selecting/clearing checkbox (b) as required.
(b)		

	Setting	Explanation
(c)	Learning Mode State	This row displays whether <i>Learning Mode</i> is currently active or not for the user. It might be deactivated because <i>Learning Mode</i> has not been enabled. If <i>Learning Mode</i> is enabled, it could be deactivated due to the fact, that the learning mode period has terminated (since the learning mode threshold has been exceeded)
(d)	Learning Mode Termination	If <i>Learning Mode</i> is currently active, then this row displays the number of remaining multi-factor authentications that the user must still complete successfully, before the learning mode terminates
(e)	Reset Counter...	Click the Reset Counter... button, if you would like the <i>Learning Mode</i> to start all over again for the user. The number of remaining successful authentications will be reset to the <i>Learning Mode Threshold</i> defined by the Authentication Policy currently assigned to the user.

17.10.1.6 User: License

This section describes the content of the **License** tab while maintaining a user. On this tab, you can inspect the license status of the user, and optionally also to override license grants:



For a description of *License Grants* vs. *License Allocations*, please read section 17.6.1.4 (page 181).

	Column	Explanation
(a)	Granted	By default, this column shows the CAL grants inherited from the User Group Policy assigned to the user. A selected checkbox indicates that the corresponding type of CAL has been granted to the user.
(b)	License allocation state	This column shows the actual license allocation state. Only if the column shows a green light and the text "Allocated", then the granted type of CAL was allocated successfully to the user. A CAL might lack allocation due to missing licenses or license limits (cf. section 17.6.1.4, page 181).

	Column	Explanation
(c)	Override	<p>This column allows you to override the inherited CAL grants. When selecting a checkbox in this column, the checkbox in the Granted column becomes enabled, allowing you to select or clear that checkbox to grant or remove the corresponding type of CAL, respectively.</p> <p>Overriding CAL grants is normally not recommended, but it might be useful in exceptional cases. For example, it could be useful for temporarily releasing a specific type of CAL from a user, because it is urgently missing for another user due to lack of licenses.</p>

In case you need to get an overview of CAL grants and allocations across users, you have several options for achieving this:

- Go to the **License** page to see the overall statistics for license allocations (cf. section 17.4, page 122).
- Use other license management options (cf. section 17.4.3, page 125).

17.10.2 User IP History

If the setting **Geo IP and IP history** has been enabled on the **General Settings** page, the SMS PASSCODE database will automatically record a history of the end-user IP addresses used by each individual user.

While maintaining a user, you gain access to the IP history of the user by clicking the **Show IP History...** link in the right pane:



NOTE: The **Show IP History...** link is only available if the **Geo IP and IP history** setting has been enabled on the **General Settings** page.

When clicking the link, a new window is opened, showing the end-user IP addresses from which the user has recently authenticated successfully. "Recently" means, that the user has authenticated from an IP address within the **IP expiration** period defined by the Authentication

Policy assigned to the user (cf. section 17.8.2.3, page 201). The IP history shows the following information:

IP History List of Jane [mycompany]jane

Trusted IP threshold: Required IP trust level is 3

Buttons: Add new entry..., Delete all, Refresh, Close

IP	Last usage	Trusted	Country Name	Organization	Trust Level
194.150.8.230	10-05-2012 17:41:30	No	France	DDB Paris	1
94.236.83.64	10-05-2012 17:40:42	Yes	United Kingdom	Rackspace.com	5

	Item	Explanation
(a)	Trusted IP threshold	Informative text showing the currently required <i>Trust Level</i> that an end-user IP address must reach before it becomes a <i>Trusted IP</i> according to the Authentication Policy currently assigned to the user
(b)	Refresh	If the User IP History window is kept open for a while, the IP history might become outdated, e.g. because the user has performed new authentications in the meantime. Please click the Refresh button to update the list and make it display the most recent data.
(c)	Add new entry...	This button lets you add a new end-user IP address manually to the user's IP history. This could for example be useful, if you have configured the SMS PASSCODE system NOT to identify <i>Trusted IP</i> addresses, but prefer to add <i>Trusted IPs</i> manually.
(d)	Delete all	This button lets your clear the whole IP history of the user. A confirmation dialog will ask you to confirm this action. If confirmed, the user's IP history is deleted permanently.
(e)	Edit...	You may edit any individual IP entry in the user's IP History by clicking the Edit... button in the corresponding row. This might be useful, e.g. if you would like to change the <i>Trust Level</i> of an entry manually.
(f)	Delete	You may delete any individual IP entry in the user's IP History by clicking the Delete button in the corresponding row.
(g)	Close	Click the Close button to close the window.

The user's IP History list displays valuable information about each entry:

IP	Last usage	Trusted	Country Name	Organization	Trust Level
194.150.8.230	10-05-2012 17:41:30	No	France	DDB Paris	1
94.236.83.64	10-05-2012 17:40:42	Yes	United Kingdom	Rackspace.com	5
65.55.58.201	10-05-2012 17:40:06	Yes	United States	Microsoft Hosting	5
64.4.11.37	10-05-2012 17:39:36	Yes	United States	MS Hotmail	25
217.150.151.9	10-05-2012 17:39:07	No	Germany	T-Systems International GmbH	2
91.224.210.130	10-05-2012 17:38:31	Yes	Denmark	TV2 Danmark A/S	10

	Column	Explanation
(a)	IP	Specifies an end-user IP address from which the user has authenticated successfully.
(b)	Last usage	Specifies the time and date of the last occurrence when the user authenticated successfully from the IP address.
(c)	Trusted	Specifies whether the IP address is currently treated as a <i>Trusted IP</i> . This depends on the fact whether the current <i>Trust Level</i> of the IP address has reached the current <i>Trusted IP threshold</i> , which is displayed at the top of the User IP History window.
(d)	Country Name	Displays the name of the country, where the IP address is located.
(e)	Organization	Displays the name of the organization owning the IP address.
(f)	Trust Level	Displays the current <i>Trust Level</i> of the IP address. The <i>Trust Level</i> is updated on every successful multi-factor authentication according to the Authentication Rules of the Authentication Policy currently assigned to the user (cf. section 17.8.2.5, page 204).

In case you would like to sort the entries in the list according to the values of a specific column, please click the header of that column.

17.10.3 User Login History

If **Authentication Monitoring** has been enabled on the **General Settings** page, the SMS PASSCODE database will automatically record every attempt of any user trying to log in to any SMS PASSCODE protected authentication client.

All recorded authentication attempts can be monitored on the **Authentications Monitoring** page (cf. section 17.19, page 296). However, while maintaining a user, there is a shortcut to gain immediate access to this specific user's login attempts ("Login History") by clicking the **Show Login History...** link in the right pane:



NOTE: The **Show Login History...** link is only available if **Authentication Monitoring** has been enabled on the **General Settings** page.

Clicking the link **Show Login History...** will redirect the WAI directly to the **Authentications Monitoring** page (described in section 17.19, page 296) and automatically configure a row filter that only displays the authentication attempts of the user in question.

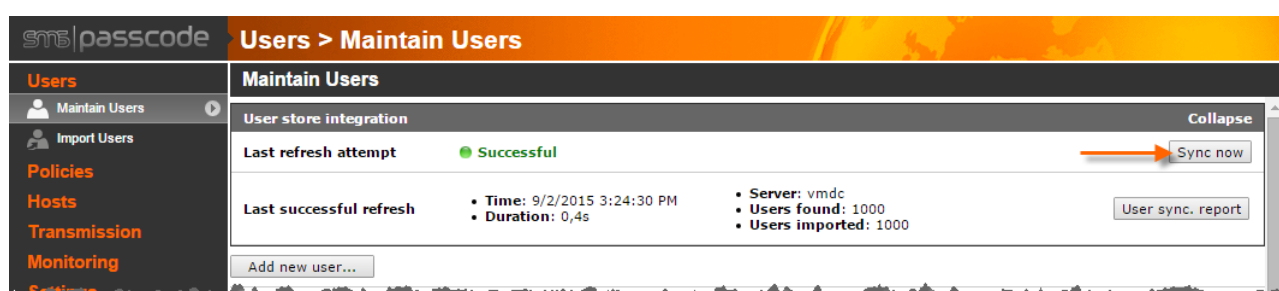
Immediate access to the user's current login history might for example be useful for an internal helpdesk, in case a user has problems with performing a successful login. The helpdesk can

immediately inspect the most recent login attempts and inspect the reasons for failed login attempts.

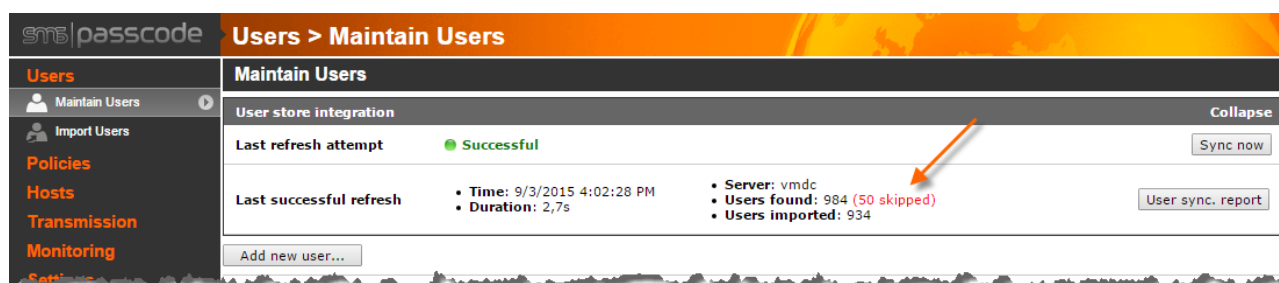
17.10.4 Adding and Deleting Users via User Store Integration

When **User store integration** has been enabled, you can also maintain users using one or more selected user groups in an Active Directory (or other type of LDAP directory). All users belonging to these user groups are automatically added to the SMS PASSCODE user grid on the **Maintain users** page. When a user is removed from one of the selected user groups, then the user is automatically removed from the SMS PASSCODE user grid as well.

Please note that when users are added or removed from a selected user group, then these changes will not occur immediately in the SMS PASSCODE user grid because SMS PASSCODE checks for changes in the user store periodically. If you wish to force a change in the user store to take effect in SMS PASSCODE immediately, you can manually force an instant refresh. To force a refresh, click the **Sync now** button on the **Maintain users** page:



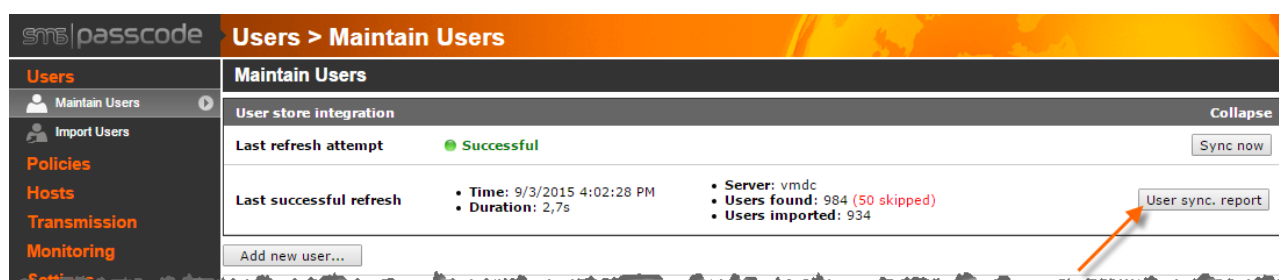
If some users are not imported into SMS PASSCODE from the user store, even though they are member of a selected user group, then these users will be displayed as “skipped”:



Users might be skipped due to the following reasons:

- A phone number is required according to the UIP, but it is missing or is incorrect. Please check the content of the field containing the phone number, in the user store.
- An email address is required according to the UIP, but it is missing or is incorrect. Please check the content of the field containing the email address, in the user store.
- The same user is being imported multiple times (only possible when several UIPs have been set up to import users from the same user store).

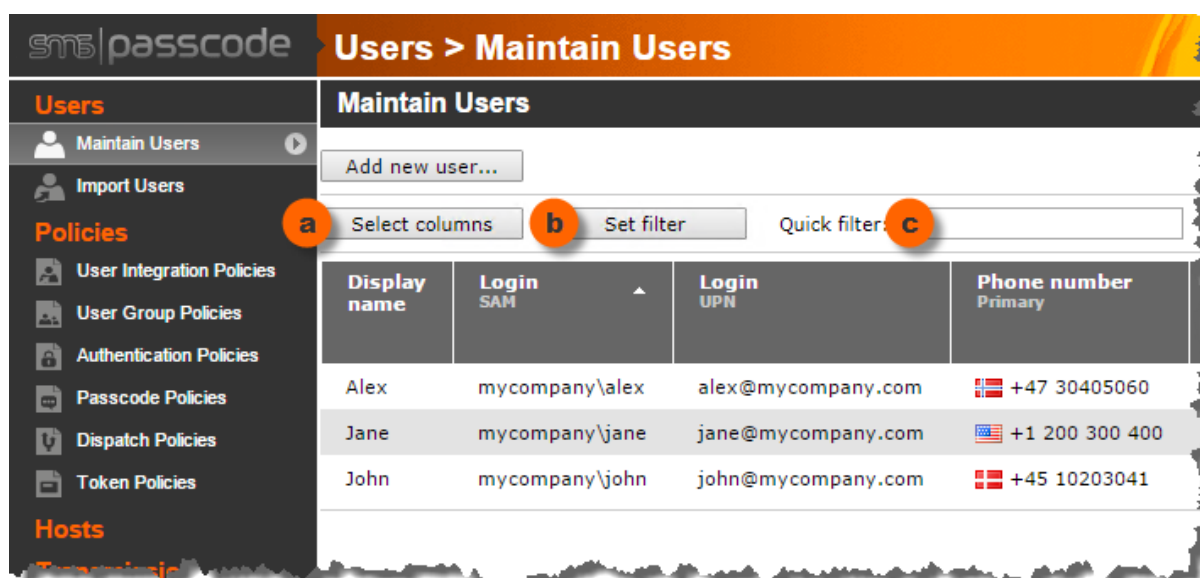
Please click the **User sync. report** button to get the exact details regarding any skipped users:



You can also inspect the Windows event viewer to get the exact details regarding any skipped users. The user synchronization event entry will contain the details.

17.10.5 User Data Filtering

When maintaining users, it is sometimes convenient to be able to filter the amount of information shown in the user grid. You can apply both **row filtering** and **column filtering** on the **Maintain Users** page to limit the amount of information shown:



- Column filter:** Click the **Select columns** button to define, which columns to display in the user grid. The selected columns are remembered for the current user, across browser sessions.
- Row filter:** Click the **Set filter** column to restrict the number of users shown in the user grid. The filter is defined by one or more conditions on the user attributes – only users fulfilling these conditions will be shown in the user grid. If you specify several conditions in the filter, then the conditions are combined into an “AND-filter”, meaning users are hidden from the user grid unless they fulfill all conditions of the filter. The defined row filter is remembered for the current user, but only for the current browser session.

- c. **Quick filter:** This feature allows you to define a more flexible filter in a very quick way. You simply enter the content into the quick filter that you want to search for, and the user grid will then only show users, that *contain* the entered value in any of the following attributes:
- Display name
 - Login (SAM)
 - Login (UPN)
 - Email
 - Phone number (primary or secondary)

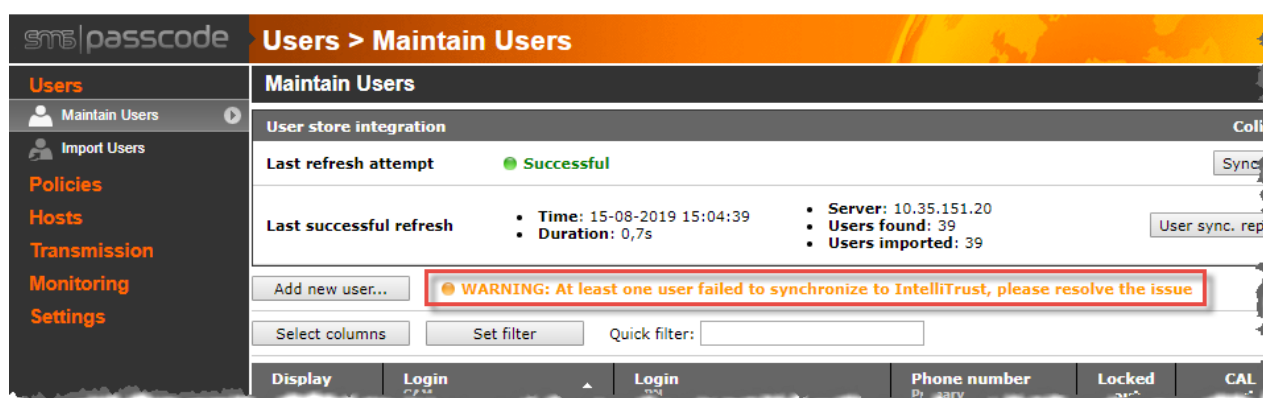
In other words, the **quick filter** allows you to search for users with a specific name, login name, email or phone number in a very quick way. The quick filter is automatically cleared, as soon as you leave the page.

NOTE: You can combine the **Row filter** and the **Quick filter**. This will restrict the user grid to only show users that fulfill both filters.

17.10.6 IntelliTrust User Sync Status

If you have enabled IntelliTrust™ integration (Hybrid Setup, cf. section 17.3.4, page 119), the SMS PASSCODE database will automatically start to synchronize SMS PASSCODE users to the IntelliTrust™ cloud service. For troubleshooting, the **Maintain Users** page allows you to inspect the current status of such synchronization.

In case synchronization has failed for any user, you will see the following message:



To find out, which user has not synchronized properly, you can apply column and row filtering on the user grid, as described in the previous section. For this purpose, you can enable the following columns in the user grid, or apply filtering on them:

- **IntelliTrust sync: Status**
Shows the status of the last sync attempt. Filter on “Failure” to find any users with a failed sync attempt.
- **IntelliTrust sync: Last successful sync**
Shows the date and time of the last successful sync of a user.
- **IntelliTrust sync: Error message**
In case of a failed sync, shows an error message describing the cause.

For more detailed troubleshooting of the IntelliTrust™ synchronization mechanism, you can also open and inspect the event log container **SMS PASSCODE IntelliTrust Connect**, located on the server, where the SMS PASSCODE Database service has been installed.

17.11 Importing Users

Instead of creating each user manually, you can also bulk import users into SMS PASSCODE. To perform an import, you need a comma-separated (CSV) file containing the user data.

To start the import process, select **Import users** in the navigation menu:

Users > Import Users

Import Users

Import users from a comma separated (CSV) file. The first row **MUST** contain headers describing which data is contained in the file, and the order of the data. The following headers are allowed:

Header	Description
LoginSAM:	Login name (SAM)
LoginUPN:	Login name (UPN)
DisplayName:	User display name
PhoneNumber:	Phone number
SecondaryPhoneNumber:	Secondary phone number
Email:	Email address
PIN:	PIN code
UserID:	Unique user identifier. When a unique identifier is attached to a user, the import will still recognize the user, even when the user login has been renamed.
TokenID:	ID of the user's token (for token authentication)
PersonalPasscode:	The user's personal passcode

Example:

```
"LoginSAM", "PhoneNumber", "DisplayName"
"user1", "20222223", "Jane Wellington"
"user2", "+49 012345 1234567", "Hans Schmidt"
```

File to import: No file chosen

Import destination: ▼

If the import file contains users already present in the database, how would you like to handle these users:

☒ Skip: Do not import these users

☐ Replace: Existing users are replaced with data from the import file

If the database contains users (within the destination), which are not present in the import file, how would you like to handle these users:

☒ Skip: Just leave these users in the database

☐ Remove: Remove these users from the database

© SMS PASSCODE A/S

The **Import users** page contains information regarding the expected syntax of the comma-separated file. You decide yourself which data is contained in the CSV file; the first row of the file is used to define the content, i.e. this row must contain header names of the columns in the file. The remaining rows must contain data in the exact order defined by the header row.

Please note, that it is also possible to initiate the import of users using a PowerShell cmdlet. This is especially useful if you would like to schedule an automated periodic import or synchronization of users from a comma-separated file. Please read section 17.11.1 below for more details regarding this.

17.11.1 Importing and Synchronizing Users from other Data Sources

If you need to import users into the SMS PASSCODE database from another source than a Microsoft Active Directory or an LDAP directory, then this is also possible. You can either decide to handle the import using your own logic, using SMS PASSCODE PowerShell cmdlets to

insert/update/delete users (cf. section 18, page 308) – or alternatively you can use comma-separated files. In the latter case, you should export all users from your data source to a comma-separated file, and afterwards import this file into the SMS PASSCODE database. If the user export/import is a one-time task, you can simply import the comma-separated file using the SMS PASSCODE Web Administration interface (cf. section 17.11 above).

However, if you wish to set up an automated periodic import or synchronization from a comma-separated file, you can make use of the `Import-SmsPcUser` PowerShell cmdlet.

The `Import-SmsPcUser` cmdlet is installed as part of the SMS PASSCODE PowerShell Support component – it is always present on the server hosting the SMS PASSCODE **Database Service** but can also optionally be installed on other machines.

To get more information about parameters and expected syntax, please type the following in a PowerShell console:

```
Get-Help Import-SmsPcUser -Detailed
```

To import users from a comma-separated file, use this syntax:

```
Import-SmsPcUser -Path 'csv-file-name'
```

Replace **'csv-file-name'** with the path to your comma-separated file. You can add additional arguments to obtain different behaviors. Different examples are listed below:

- **Add new users:** Import users from a comma-separated file. Any users already present in the database are not overwritten. No users are removed from the database:

```
Import-SmsPcUser -Path 'csv-file-name'
```

- **Add new users, overwriting existing users:** Import users from a comma-separated file. Any users already present in the database are overwritten with possibly new data. No users are removed from the database:

```
Import-SmsPcUser -Path 'csv-file-name' -ReplaceExistingUsers
```

- **Synchronize users:** Import users from a comma-separated file. Any users already present in the database are overwritten with possibly new data. Any users present in the database, but NOT present in the comma-separated file, are removed from the database:

```
Import-SmsPcUser -Path 'csv-file-name' -ReplaceExistingUsers -RemoveUnknownUsers
```

Using the `Import-SmsPcUser` cmdlet, you can set up a periodic custom synchronization of users from your specific data source to SMS PASSCODE. This custom synchronization will work exactly

as the built-in **User store integration**. To configure a custom synchronization, please proceed as follows:

- Schedule a periodic task, e.g. using the Windows Task Scheduler. This task should call a PowerShell script, that will:
 - a. Export the required users from the data source to a comma-separated file.
 - b. Call `Import-SmsPcUser` with the generated comma-separated file as input and with the arguments shown above at **Synchronize users**.

You can even set up multiple custom synchronizations that will work in parallel on their own subset of users, analogously to the built-in **User store integration**. Moreover, you can have several custom synchronizations and several UIPs run simultaneously.

17.12 Transmitter Hosts

If you plan to make use of several Transmitter services, you must **authorize** each such Transmitter service. Authorization is carried out by specifying the host name of each server allowed to run the Transmitter service. The procedure for this is described in the following subsection.

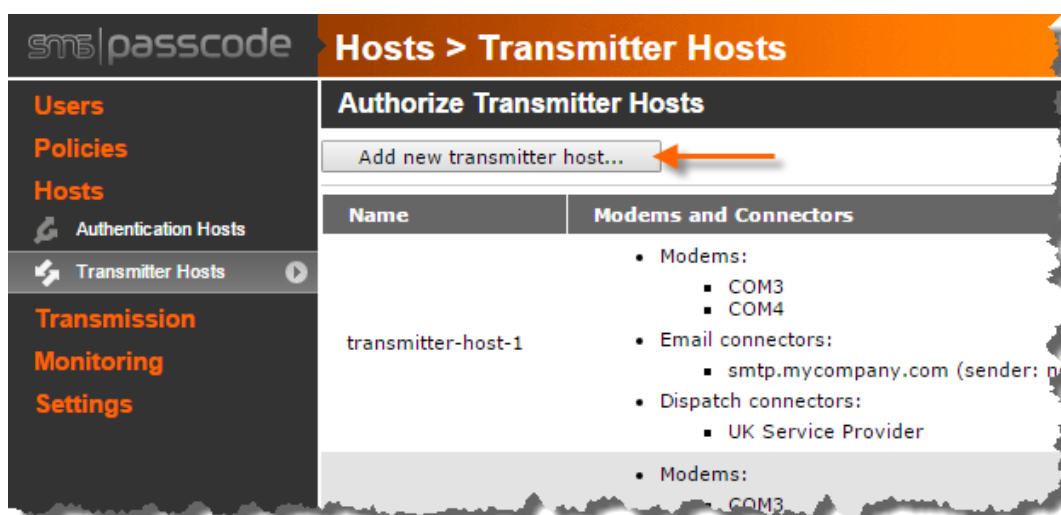
IMPORTANT – authorize before installation:

Remember to authorize each Transmitter service host **BEFORE** the Transmitter service is installed on it. If this is not observed, then the Transmitter service will shut down after installation because of missing authorization. You will then need to restart the Transmitter service manually after it has been authorized.

17.12.1 Maintaining Authorized Transmitter Hosts

To authorize a Transmitter host, please follow the instructions below:

1. Select the **Transmitter Hosts** page.
2. Click the **Add new transmitter host...** button



3. On the *Create a new Transmitter Host* page:
 - a. Enter the host name (or IP-address) of the server to be authorized.
 - b. Optionally, add one or more dispatchers (modems, Email Connectors or Dispatch Connectors) to the new transmitter (cf. section 17.12.2 below) – you can also postpone this action until later.
 - c. Click the **Save** button.

4. Now the host has been authorized and appears in the grid of authorized Transmitter servers:

Name	Modems and Connectors
transmitter-host-1	<ul style="list-style-type: none"> Modems: <ul style="list-style-type: none"> COM3 COM4 Email connectors: <ul style="list-style-type: none"> smtp.mycompany.com (sender: noreply@mycompany.com) Dispatch connectors: <ul style="list-style-type: none"> UK Service Provider
transmitter-host-2	<ul style="list-style-type: none"> Modems: <ul style="list-style-type: none"> COM3 COM4 Email connectors: <ul style="list-style-type: none"> smtp.mycompany.com (sender: noreply@mycompany.com) Dispatch connectors: <ul style="list-style-type: none"> UK Service Provider
transmitter-host-3	

If you need to correct the name of the server afterwards, then click the **Edit** button to the right of the authorized Transmitter host.

If you need to remove the authorization, then click the **Delete** button to the right of the authorized Transmitter host.



17.12.2 Assigning Dispatchers to a Transmitter

Each authorized Transmitter host is allowed to run a single instance of the SMS PASSCODE Transmitter Service, which is responsible for dispatching messages to users.

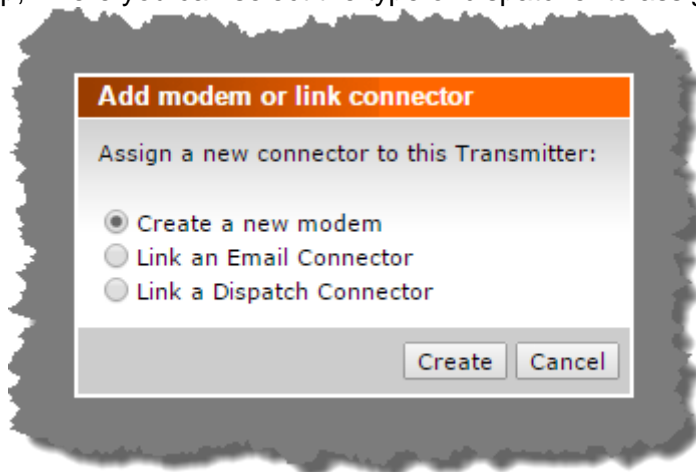
Each Transmitter Service needs to know, which dispatching methods it is allowed to use and how it can connect to required external services and devices. For example, it needs to know, on which COM ports modems are located, or where SMTP servers are located.

There are two ways to assign dispatchers to a Transmitter Service:

- 1) When maintaining a dispatcher, assign it to the Transmitters allowed to use it.
This is done on the respective pages for maintaining dispatchers, i.e. the pages **Modems**, **Email Connectors** and **Dispatch Connectors**.
- 2) When maintaining a Transmitter, assign the relevant dispatchers to it.
This is done by clicking the **Add...** button while maintaining the details of a Transmitter server:



A dialog will pop up, where you can select the type of dispatcher to assign:



A modem can only be connected to a single Transmitter Service (at a time), whereas an Email Connector or Dispatch Connector can be linked to any number of Transmitter Services.

17.13 Authentication Backend Service Hosts

When you install the Authentication Backend Service (ABS) on a server, you must **authorize** each such ABS. Authorization is carried out by specifying the host name of each server allowed to run the ABS. The procedure for this is described in the following subsection.

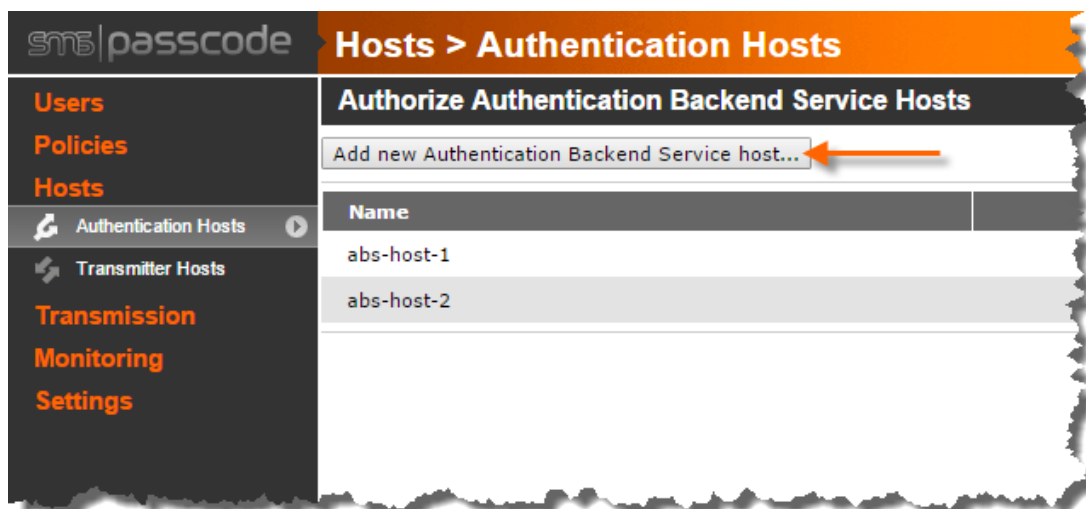
IMPORTANT – authorize before installation:

Remember to authorize each ABS host **BEFORE** the ABS is installed on it. If this is not observed, then the ABS will shut down after installation because of missing authorization. You will then need to restart the ABS manually after it has been authorized.

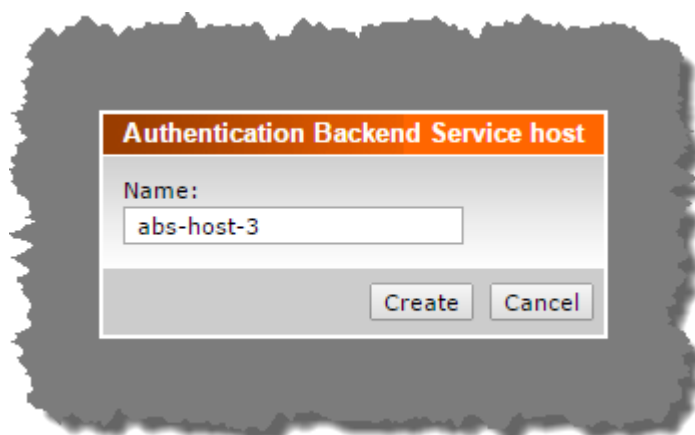
17.13.1 Maintaining Authorized Authentication Backend Service Hosts

To authorize an Authentication Backend Service (ABS) host, please follow the instructions below:

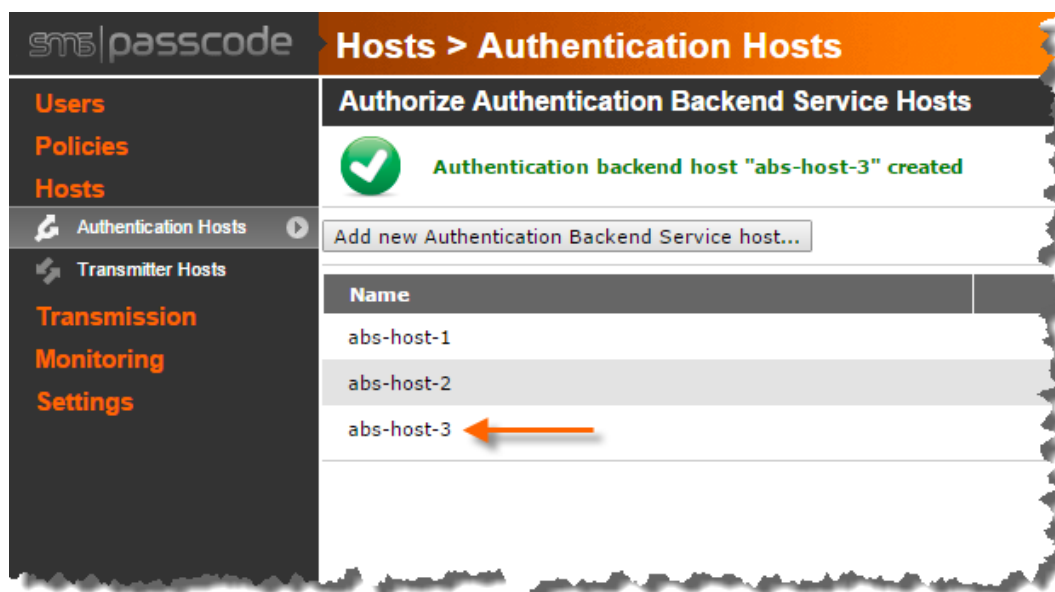
1. Select the **Authentication Hosts** page.
2. Click the **Add new Authentication Backend Service host...** button



3. A dialog appears where you can enter the host name (or IP-address) of the host to be authorized. Afterwards, click the **Create** button.

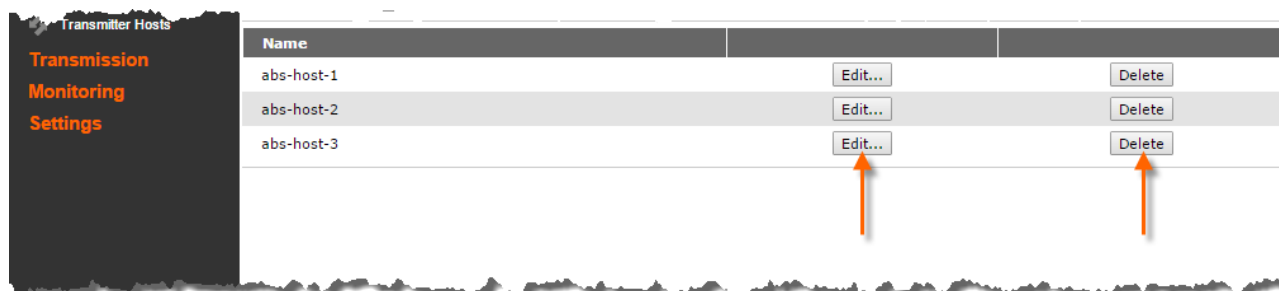


4. Now the host has been authorized and appears in the grid of authorized ABS hosts:



If you need to correct the name of the host afterwards, then click the **Edit...** button to the right of the authorized ABS host.

If you need to remove the authorization, then click the **Delete** button to the right of the authorized ABS host.



17.14 Modems

You can connect up to 32 modems to each Transmitter Service. To inform each Transmitter Service which modems to initialize and use, you must add each modem to the database.

Please note, that you can add and remove modems on the fly. For example, you can connect additional modems and create them in the database without restarting any Transmitter Service – which means zero downtime while reconfiguring modems.

To maintain modems, go to the **Modems** page.

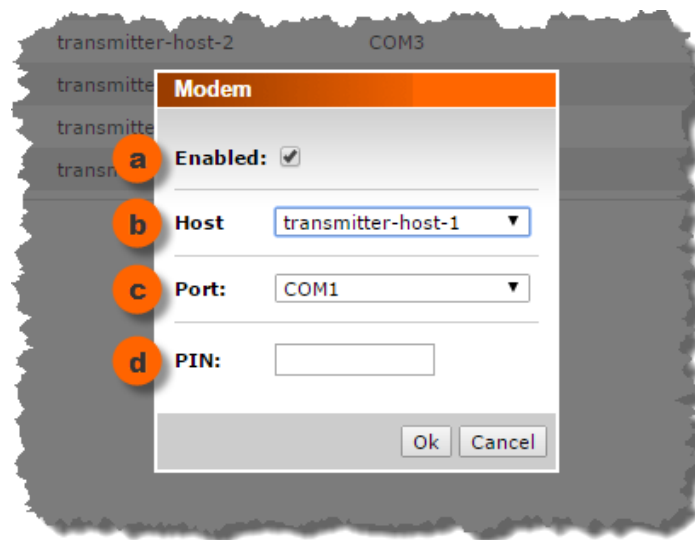
Enabled	Transmitter host	Com port	Has PIN			
<input checked="" type="checkbox"/>	transmitter-host-1	COM3		Test...	Edit...	Delete
<input checked="" type="checkbox"/>	transmitter-host-1	COM4		Test...	Edit...	Delete
<input checked="" type="checkbox"/>	transmitter-host-2	COM3		Test...	Edit...	Delete
<input checked="" type="checkbox"/>	transmitter-host-2	COM4		Test...	Edit...	Delete
<input checked="" type="checkbox"/>	transmitter-host-3	COM1		Test...	Edit...	Delete
<input checked="" type="checkbox"/>	transmitter-host-3	COM2		Test...	Edit...	Delete

- Click the **Add new modem...** button to create a new modem. A **Dispatch License** is required for every modem that you create in the SMS PASSCODE database.
- Click the **Test...** button to send a test message using a specific modem. In this way, you can test whether the selected modem is able to send an SMS successfully.
- Click the **Edit...** button to edit the settings of an existing modem.
- Click the **Delete** button to remove a modem.

The following subsection describes how to maintain the settings of a modem while creating a new one or editing an existing one.

17.14.1 Settings of a Modem

When creating a new modem or editing an existing modem in the SMS PASSCODE database, the following dialog will appear:



To maintain the settings of the modem, proceed as follows:

- Leave the **Enabled** checkbox selected if you want the modem to be active. Clear the checkbox to put the modem in a deactivated “standby” mode, where it will not be used for any transmissions, until it is enabled.
- Select the Transmitter host to which the modem has been connected.
- Select the serial port to which the modem has been connected.
- Enter the PIN code for the SIM card in the modem. Leave this field empty if the SIM card is not protected by a PIN code, or if the modem does not use a SIM card at all.

Finally click the **Ok** button to commit the changes.

When you create a new modem or move an existing modem to a new Transmitter host or serial port, the modem will automatically be initialized on the fly if the Transmitter Service is up and running on the specified host and the modem has been connected to the specified serial port. If you would like to verify the initialization, then inspect the **SMS PASSCODE Transmission** event log on the Transmitter host or inspect the **Modem monitoring** page (cf. section 17.20, page 307).

17.14.2 Removing Modems

Whenever you are planning to disconnect a modem from a Transmitter Service, you should remove such modem from the database beforehand. This allows the Transmitter Service to terminate the modem gracefully before it is disconnected.

To remove a modem, please follow the instructions below:

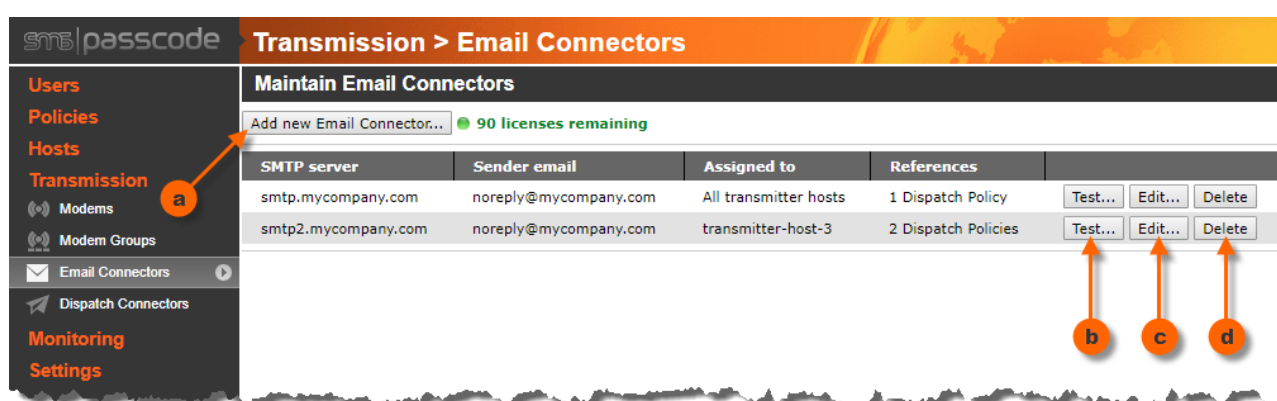
1. Select the **Modems** page.
2. Click the **Delete** button to the right of the modem to be deleted.
3. Confirm the deletion.
4. If the modem has not already been disconnected, then the modem is now automatically terminated on the fly (if the Transmitter Service is up and running on the specified server). The modem is terminated gracefully, i.e. any queued SMS messages will be sent before the modem is terminated. If you would like to verify the modem termination, then inspect

the **SMS PASSCODE Transmission** event log on the Transmitter host or inspect the **Modem monitoring** page (cf. section 17.20, page 307).

17.15 Email Connectors

If you are planning to send passcode messages or notifications by email, then you need to specify how email transmission can occur. To do this, you must create one or more *Email Connectors*. Each Email Connector indicates an SMTP server to use for transmission, and optionally also specifies any required credentials for authentication. You can define any number of Email Connectors, and each Email Connector can be assigned to any number of Transmitter Services. Assigning an Email Connector to a Transmitter Service simply means, that the Transmitter is allowed to send emails as defined by the Email Connector in question.

To maintain Email Connectors, go to the **Email Connectors** page:



- Click the **Add new Email Connector...** button to create a new Email Connector. A **Dispatch License** is required for every Email Connector that you create in the SMS PASSCODE database.
- Click the **Test...** button to send a test message using a specific Email Connector. In this way, you can test whether the selected Email Connector is able to send an email successfully.
- Click the **Edit...** button to edit the settings of an existing Email Connector.
- Click the **Delete** button to remove an Email Connector.

IMPORTANT: Please note when deleting an Email Connector, that all Dispatch Policy rules referring to this Email Connector will be deleted as well. Use the column **References** to get an overview of where an Email Connector is currently in use.

The following subsection describes how to maintain the settings of an Email Connector while creating a new one or editing an existing one.

17.15.1 Settings of an Email Connector

When creating a new or editing an existing Email Connector in the SMS PASSCODE database, the following page will appear:

Field Label	Field Value	Description
SMTP server (a)	smtp.mycompany.com	Enter a SMTP server address to be used for sending emails. Optionally: Port can be specified after a colon. E.g.: "mailserver01:3410".
Sender email (b)	noreply@mycompany.com	Email sender address to be used for sending emails.
Assigned to (c)	<input checked="" type="checkbox"/> All transmitter hosts <input checked="" type="checkbox"/> transmitter-host-1 <input checked="" type="checkbox"/> transmitter-host-2 <input checked="" type="checkbox"/> transmitter-host-3	Transmitter hosts allowed to use this email connector for sending messages.
Explicit credentials (d)	<input checked="" type="checkbox"/> Enabled	Enable explicit credentials for the SMTP server specified above.
Username (e)	smtpuser	Username of the user to be used.
Password (f)	*****	Password of the user to be used.
Plain text only (g)	<input type="checkbox"/> Enabled	Send email body as plain text.
References (h)	1 Dispatch Policy	Info regarding Dispatch Policies referencing this Email Connector (click on info for details)

To maintain the settings of the Email Connector, proceed as follows:

- Enter the IP address or host name of an SMTP server to use for sending emails.
- Enter the email address to be shown as the sender of all emails sent by SMS PASSCODE using this Email Connector.
- Select the Transmitter hosts that this Email Connector should be assigned to, i.e. the Transmitter hosts allowed to send emails using the specified SMTP server.

Typically, you will select "All transmitter hosts", unless you need to restrict the allowed Transmitter hosts to a specific subset. "All transmitter hosts" is a dynamic selection, that includes all currently created transmitter hosts, but also any transmitter hosts created in the future.

- Optional: Select the **Explicit credentials** checkbox if credentials for authentication are required to send emails using the specified SMTP server. Credentials are entered as e) **Username** and f) **Password**.
- Optional: Select the **Plain text only** checkbox to ensure that all emails sent via this Email Connector are sent as plain text only (meaning no HTML and no bitmaps are included in the emails).
- The **References** section informs, how many Dispatch Policies are currently referencing this Email Connector. The information is shown as a link that you can click to get more specific

details about the references. This is useful in case you have many Dispatch Policies and want to get an overview, where specific Email Connectors are in use.

Finally click the **Save** button to commit the changes.

When you create a new or edit an existing Email Connector, this Email Connector will be available for email dispatching immediately. Use the **Test...** button on the **Email Connectors** page to verify whether an Email Connector is functioning as expected.

17.16 Dispatch Connectors

SMS PASSCODE supports transmission of passcode messages and notifications by other means than using modems and Email Connectors. Using a **pluggable transmission infrastructure**, the SMS PASSCODE system allows transmission of messages using any transmission mechanism that is available using a server-based API. For example, this makes it possible to send messages by voice call, push notifications, chat or using 3rd party SMS gateways / web services.

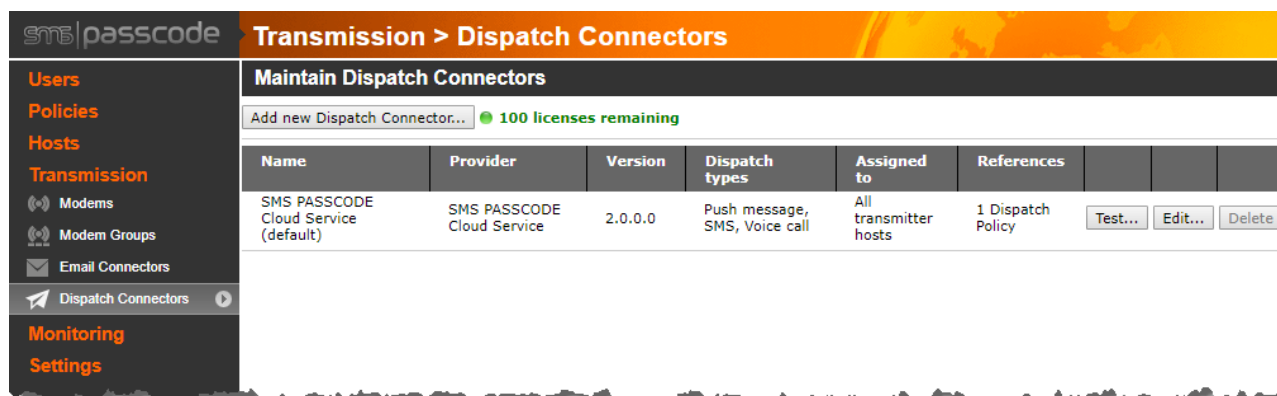
Every such transmission mechanism is made available to SMS PASSCODE using a **Dispatch plugin module**. The SMS PASSCODE installer includes plugin modules that support a long list of 3rd party message transmission providers. If you decide to use any of these providers for message transmission, this will work out-of-the-box. The only requirement is that you need to sign up for your own account at the chosen provider(s). If you have a specific requirement for using a transmission mechanism not supported out-of-the-box, then please read section 21 (page 318).

To make use of a specific plugin module for message transmissions, you need to create a **Dispatch Connector** in the SMS PASSCODE database. A Dispatch Connector defines which message transmission provider to use and lists the settings that you are required to enter for the chosen provider. Typically, you will need to enter account data that identifies your account at the chosen provider.

Please note, that you can create any number of Dispatch Connectors³² in the SMS PASSCODE database, which will allow you to configure failover, scaling (load balancing) and adaptive selection of message transmission providers between any such Dispatch Connectors, and/or between modems, and/or between Email Connectors (using **Dispatch Policies**, cf. section 17.18 page 271). As a result, you can configure any level of failover and scaling, according to your specific needs. Each Dispatch Connector can be assigned to any number of Transmitter hosts. Assigning a Dispatch Connector to a Transmitter host simply means, that such Transmitter Service is allowed to send messages as defined by the Dispatch Connector in question.

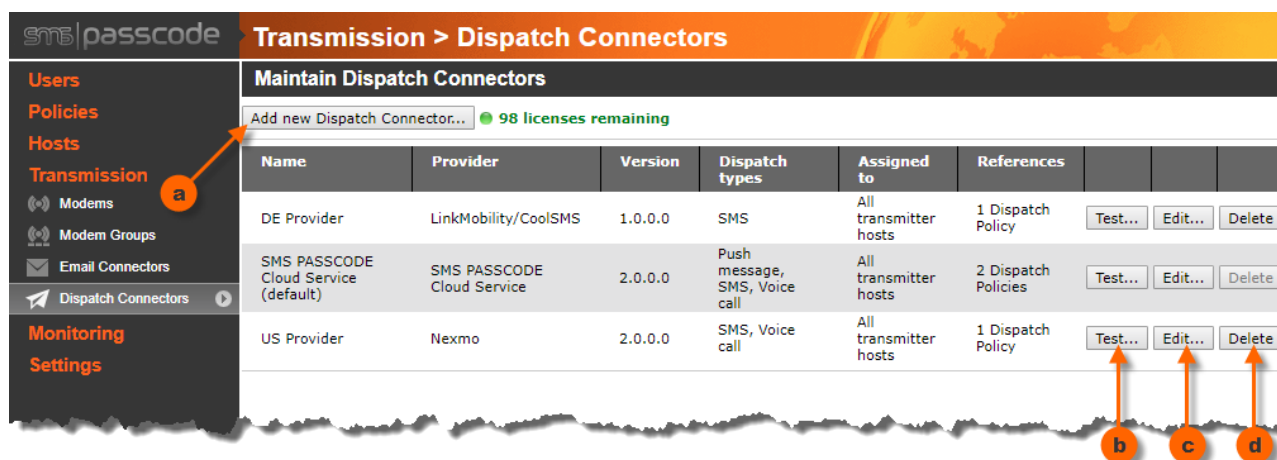
³² Assuming that you have the required number of available Dispatch Licenses

To maintain *Dispatch Connectors*, go to the **Dispatch Connectors** page. The first time you enter this page, it will look similar to this:



Initially, the overview page contains an automatically created default Dispatch Connector, called **SMS PASSCODE Cloud Service (default)**. This is a special Dispatch Connector that does not occupy any Dispatch License, and lets you connect to the SMS PASSCODE Cloud Service for convenient message dispatching. For more details on this default Dispatch Connector and on the SMS PASSCODE Cloud Service, please read section 17.16.2 (page 268). You cannot delete the default Dispatch Connector (but if you do not want to make use of it, you just need to make sure not to reference it in any of our Dispatch Policy rules).

To create, edit or delete Dispatch Connectors, proceed as follows:



- Click the **Add new Dispatch Connector...** button to create a new Dispatch Connector. A **Dispatch License** is required for every Dispatch Connector that you create in the SMS PASSCODE database.
- Click the **Test...** button to send a test message using a specific Dispatch Connector. In this way, you can test whether the selected Dispatch Connector is able to send messages as expected.
- Click the **Edit...** button to edit the settings of an existing Dispatch Connector.
- Click the **Delete** button to remove a Dispatch Connector.

IMPORTANT: Please note when deleting a Dispatch Connector, that all Dispatch Policy rules referring to this Dispatch Connector will be deleted as well. Use the column **References** to get an overview of where a Dispatch Connector is currently in use.

The following subsection describes how to maintain the settings of a Dispatch Connector while creating a new one or editing an existing one.

17.16.1 Settings of a Dispatch Connector

When creating a new or editing an existing Dispatch Connector in the SMS PASSCODE database, the following page will appear:

Transmission > Dispatch Connectors

Edit Dispatch Connector: US Provider

Name *Of own choice* **a** Enter a name of own choice for identifying this dispatch connector

Provider **b** Select the provider for dispatching messages
Version: 2.0.0.0

Assigned to **c** **d** ☒ All transmitter hosts
☒ transmitter-host-1
☒ transmitter-host-2
☒ transmitter-host-3 Transmitter hosts allowed to use this dispatch connector for sending messages.

References **e** 2 Dispatch Policies Info regarding Dispatch Policies referencing this Dispatch Connector (click on info for details)

Supported dispatch types **f**

SMS	Max message length: 912 Dispatch target: Phone number Supports differentiated behavior for "Flash SMS" setting on user: Yes
Voice call	Dispatch target: Phone number

Save **Cancel**

The settings are described in the table below.

	Setting	Explanation
(a)	Name	Enter a unique name identifying the Dispatch Connector.
(b)	Provider	<p>Select the message transmission provider that you would like to use.</p> <p>The drop-down control will list all the providers that are supported on your system, corresponding to the Dispatch plugin modules that have been installed.</p>
(c)	Provider-specific settings	This part of the page is dynamic. It will request you to enter the specific data that is needed by the provider that you selected in setting (b).
(d)	Transmitter hosts	<p>Select the Transmitter hosts that this Dispatch Connector should be assigned to, i.e. the Transmitter hosts allowed to send messages using the selected transmission provider.</p> <p>Typically, you will select "All transmitter hosts", unless you need to restrict the allowed Transmitter hosts to a specific subset. "All transmitter hosts" is a dynamic selection, that includes all currently created transmitter hosts, but also any transmitter hosts created in the future.</p>
(e)	References	Informs, how many Dispatch Policies are currently referencing this Dispatch Connector. The information is shown as a link that you can click to get more specific details about the references. This is useful in case you have many Dispatch Policies and want to get an overview, where specific Dispatch Connectors are in use.
(f)	Supported dispatch types	This section lists all the dispatch types supported by the chosen provider (b). Additionally, the capabilities of the provider are listed per dispatch type. The SMS PASSCODE system will automatically consider those capabilities and adjust accordingly, when needed.

Please remember to click the **Save** button to commit any changes.

When you create a new or edit an existing Dispatch Connector, the new or updated Dispatch Connector will be available immediately for sending messages. Use the **Test...** button on the **Dispatch Connectors** page to verify whether a Dispatch Connector is functioning as expected.

17.16.2 The Default Dispatch Connector

Starting from SMS PASSCODE version 2018, a default Dispatch Connector called **SMS PASSCODE Cloud Service (default)** is created automatically by the system after installation.

The default Dispatch Connector has the following special characteristics:

- It does not occupy a Dispatch License
- It cannot be deleted
- It always transmits messages using the **SMS PASSCODE Cloud Service**, a cloud service provided by Entrust Datacard.

The **SMS PASSCODE Cloud Service** supports 3 dispatch types: Push message, SMS and voice call. "Push message" refers to a special dispatch mechanism, where messages are sent end-to-end encrypted to the SMS PASSCODE Mobile app, which the end-user must have installed on his smart phone beforehand. SMS and voice call transmissions are provided for subscription customers at a flat-rate cost for convenient message dispatching.

Permission to use the different dispatch types is subject to specific prerequisites, summarized in the table below.

Dispatch Type	Prerequisite
Push message	Available to all customers on version 2018 or later, that are on an active Software Assurance agreement, or are on an active SPLP or subscription license. Each end-user must have downloaded, installed, and provisioned the SMS PASSCODE Mobile app beforehand (cf. section 21.1.1, page 321).
SMS / Voice call	Available to all customers on version 2018 or later, that have a valid trial or subscription license.

17.17 Modem Groups

All modems created in the database can be grouped into *modem groups*. The modem groups are maintained on the **Modem Groups** page. Modem groups are used by Dispatch Policies to restrict load balancing of message requests to subsets of all modems under certain circumstances. For example, you can group the modems according to country location or Telco operator.

To maintain modem groups, go to the **Modem Groups** page:

SMS PASSCODE Transmission > Modem Groups

Maintain Modem Groups

Add new modem group...

Name	Modems	References		
All modems	<ul style="list-style-type: none"> transmitter-host-1/COM3 transmitter-host-1/COM4 transmitter-host-2/COM3 transmitter-host-2/COM4 transmitter-host-3/COM1 transmitter-host-3/COM2 	2 Dispatch Policies	Edit...	Delete
UK Modems	<ul style="list-style-type: none"> transmitter-host-2/COM3 transmitter-host-2/COM4 	1 Dispatch Policy	Edit...	Delete
US Modems	<ul style="list-style-type: none"> transmitter-host-3/COM1 transmitter-host-3/COM2 	1 Dispatch Policy	Edit...	Delete

- Click the **Add new modem group...** button to create a new modem group.
- Click the **Edit...** button to edit a modem group.
- Click the **Delete** button to delete a modem group.

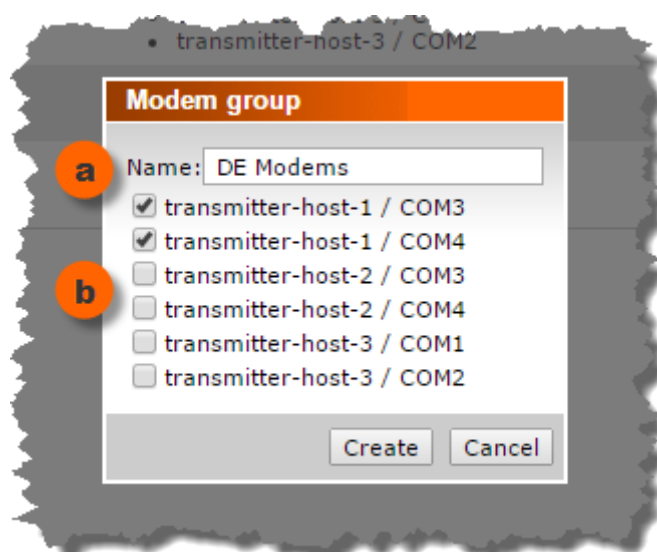
NOTE: The built-in modem group **All modems** is a dynamic group that will always contain all modems currently created in the database. You cannot edit or delete this modem group.

IMPORTANT: Please note when deleting a modem group, that all Dispatch Policy rules referring to this modem group will be deleted as well. Use the column **References** to get an overview of where a Modem Group is currently in use.

The following subsection describes how to maintain a modem group while creating a new one or editing an existing one.

17.17.1 Maintaining a Modem Group

When creating a new or editing an existing modem group in the SMS PASSCODE database, the following dialog appears:



To maintain the modem group, proceed as follows:

- Enter a unique name identifying the modem group.
- Select the checkboxes next to all the modems that should be members of the modem group.

Finally click the **Create** or **Save** button to commit the changes.

Any changes to an existing modem group will immediately be pushed to all Authentication Backend Services, thereby being taken into account on the fly.

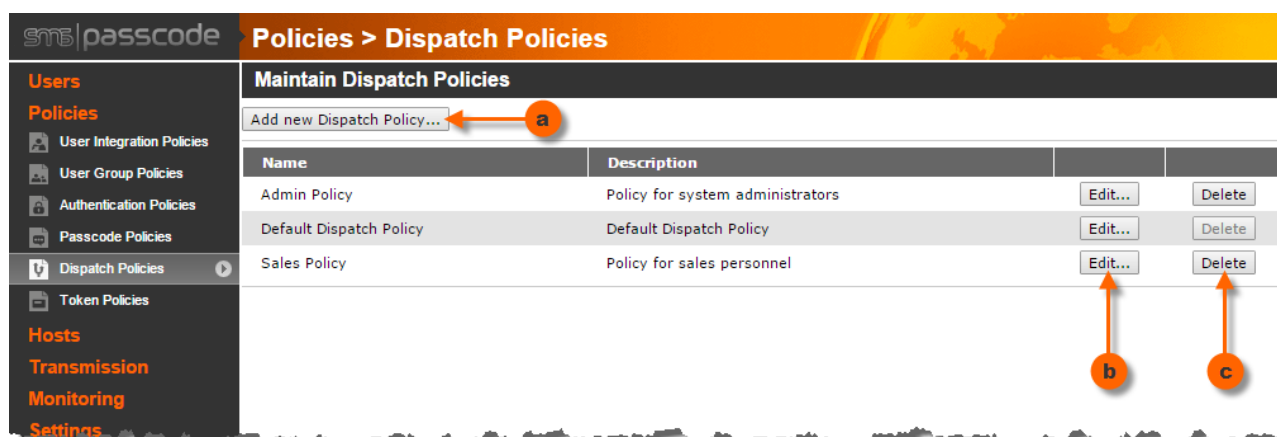
17.18 Dispatch Policies

Dispatch Policies (DPs) are used to define the rules for handling scaling (load balancing) and failover of message transmissions. The rules are very customizable, thereby giving you the flexibility to adjust the transmission behavior according to your specific requirements.

You can create any number of independent DPs, thereby assigning different rules to different users and/or different message types (passcode messages and notifications). Usually, DPs are statically assigned to users via User Group Policies (UGPs). On a UGP, it is possible to assign different DPs to use for passcodes messages and each type of notification (cf. sections 17.6.1.1 and 17.6.1.3), respectively. For passcode messages, it is even possible dynamically to allocate different DPs depending on the context of a specific user login – this is an advanced feature called *adaptive contextual message dispatching* (cf. section 17.8.2.5, page 204).

A DP rule specifies the type of dispatching to use for transferring a message to a user. For example, a DP could first send a passcode message by SMS to a user; but if the passcode is not entered within an expected time limit, then perform a voice call instead and read the passcode aloud. Another example could be to send passcode messages by email to users having a specific mobile number prefix.

DPs are maintained on the **Dispatch Policies** page:



- Click the **Add new Dispatch Policy...** button to create a new DP.
- Click the **Edit...** button to edit a DP.
- Click the **Delete** button to delete a DP.

NOTE: The built-in **Default Dispatch Policy** is a special policy, which is assigned to User Group Policies and users by default. You can edit, but not delete this policy.

IMPORTANT: Please note when deleting a DP that all User Group Policies, users and Authentication Policies referring to this DP will be set to refer to the **Default Dispatch Policy** instead.

The configuration of DPs is very flexible and allows for many different setups. The following subsections describe in detail, how DPs are configured and maintained.

First section 17.18.1 explains the overall idea of having a **sequence** of DP rules. Then section 17.18.2 explains how to maintain DPs, i.e. create new ones or edit existing ones. In particular, subsection 17.18.2.2 explains how to maintain the sequence of DP rules of a DP. Finally, section 17.18.3 lists some examples on the usage of DPs.

17.18.1 Dispatch Policy Rule Sequence

Each DP defines a **sequence** of prioritized DP rules, e.g. a specific sequence could consist of DP rules 1 to 5. Whenever an Authentication Backend Service receives a message request (passcode message or notification), it will evaluate the sequence of DP rules to determine the action to take. The sequence is always evaluated in strict order from the first to the last rule. I.e. if the sequence consists of n DP rules, then the rules are evaluated in this order:

- DP rule 1
- DP rule 2
- DP rule 3
- ...
- DP rule $n-1$
- DP rule n

The Authentication Backend Service will stop the evaluation of the sequence as soon as the first **matching** DP rule is found. I.e. the DP rule sequence can be seen as an “if-then-else” chain:

- **IF** DP rule 1 applies **THEN** use DP rule 1
- **ELSE IF** DP rule 2 applies **THEN** use DP rule 2
- **ELSE IF** DP rule 3 applies **THEN** use DP rule 3
- ...
- **ELSE IF** DP rule n applies **THEN** use DP rule n
- **ELSE** fail

Please note, that if all DP rules fail to match, then the message transmission will fail.

The possibilities using DP rules are very wide-ranging. You can create any number of DP rules and you can re-arrange the order of them as needed afterwards.

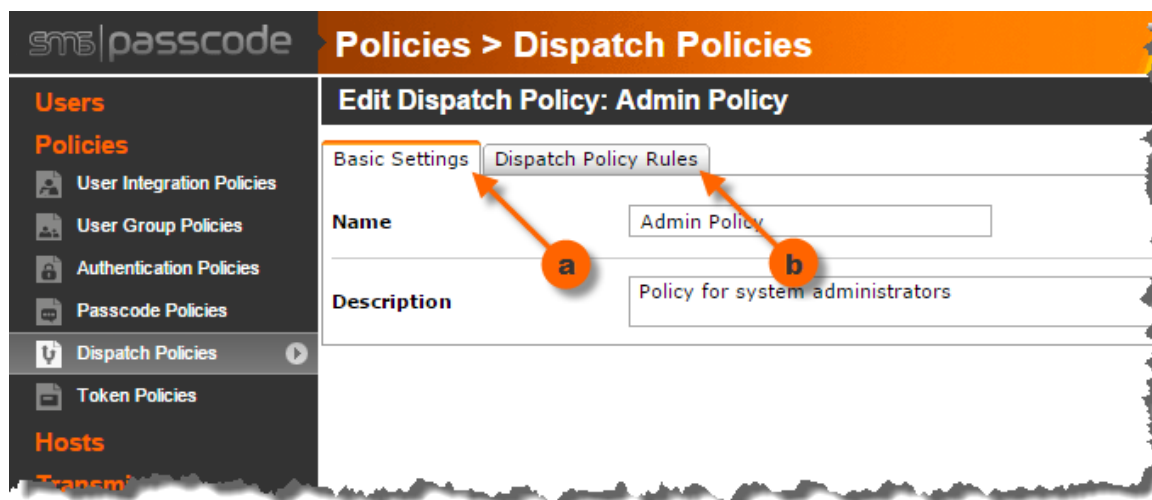
IMPORTANT:

Starting from version 2018, there is not a fixed default rule at the end of the sequence. This gives you greater flexibility, as you can now also control the configuration of the last rule.

17.18.2 Settings of a Dispatch Policy

When creating a new or editing an existing DP in the SMS PASSCODE database, a tab control is shown for configuring the different settings of the DP. The settings are divided into 2 tabs:

- a. **Basic Settings**
Settings for identifying the DP
- b. **Dispatch Policy Rules**
The sequence of DP rules specifying the message dispatching behavior



The different settings are described in detail in the following subsections. When making changes to a DP please remember to click the **Save** button at last to store the changes permanently. Otherwise, all changes will be lost.

17.18.2.1 Dispatch Policy: Basic Settings

This section describes the settings available on the **Basic Settings** tab while maintaining a DP. The Basic Settings are only used for identifying and describing the DP:

The screenshot shows the SMS Passcode interface. The top navigation bar includes the logo and the breadcrumb 'Policies > Dispatch Policies'. The left sidebar has a 'Users' section and a 'Policies' section. Under 'Policies', the following options are listed: User Integration Policies, User Group Policies, Authentication Policies, Passcode Policies, Dispatch Policies (which is highlighted with a play button icon), and Token Policies. The main content area is titled 'Edit Dispatch Policy: Admin Policy'. It features two tabs: 'Basic Settings' (which is active) and 'Dispatch Policy Rules'. Under the 'Basic Settings' tab, there are two labeled fields: (a) 'Name' with the value 'Admin Policy' and (b) 'Description' with the value 'Policy for system administrators'.

	Setting	Explanation
(a)	Name	A unique name identifying the DP. This entry is mandatory.
(b)	Description	Optional description of the DP, for your own records. Here you can describe the purpose of the DP.

17.18.2.2 Dispatch Policy: Dispatch Policy Rules

This section describes the **Dispatch Policy Rules** tab, where you can maintain the sequence of DP rules of a DP.

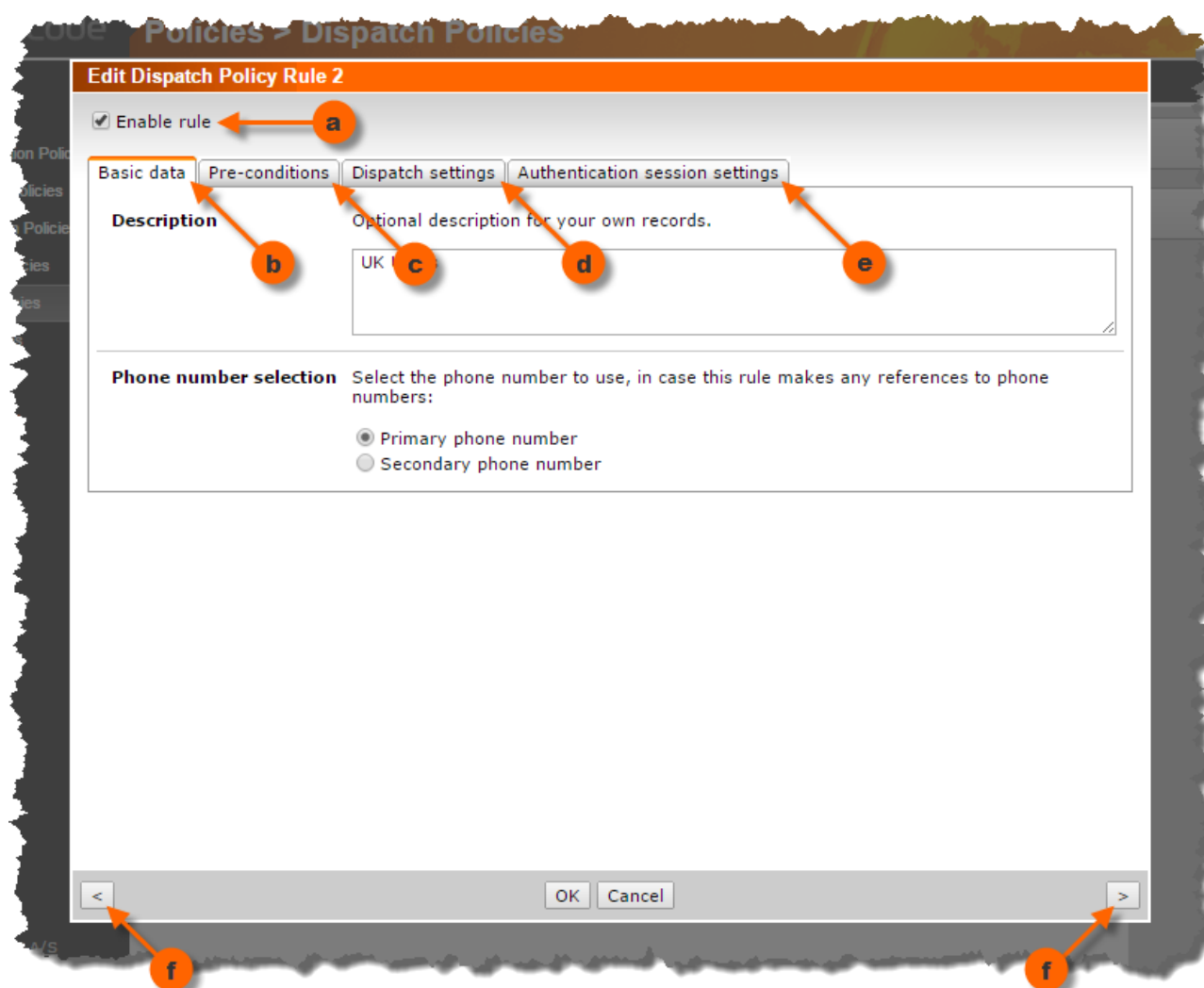


- a. Click the **Add new rule...** button to add a new DP rule to the sequence.
- b. Click the **Edit...** button to edit the settings of a DP rule.
- c. Click the **Delete** button to remove a DP rule from the sequence.
- d. To re-arrange the order of the DP rules: Click the title bar of a DP rule without releasing the mouse button and drag the DP rule to a new position in the sequence. Release the mouse button to drop the DP rule in the new position.

Please note, that you can make any number of changes to the DP rule sequence without affecting any current behavior. No changes will take effect until you click the **Save** button. I.e. as long as the **Save** button has not been clicked, you can undo all changes by leaving the page without clicking the **Save** button. However, when clicking the **Save** button, all changes are pushed to all Authentication Backend Services on the fly and will take effect immediately.

17.18.2.3 Settings of a Dispatch Policy Rule

This section describes how to maintain the settings of each individual DP rule in the DP rule sequence of a DP. When creating a new or editing an existing DP rule, the following dialog appears:



	Setting	Explanation
(a)	Enable rule	This checkbox specifies whether the DP rule is enabled (active). If you clear this setting, the DP rule will be skipped during evaluation. This might be useful for temporary de-activation of the DP rule.
(b)	Basic data	This tab contains the <i>basic data</i> of the DP rule. Please read section 17.18.2.3.1 below for details.
(c)	Pre-conditions	The settings on this tab allow you to define, whether the rule must only apply under certain circumstances. Please read section 17.18.2.3.2 (page 278) for details.
(d)	Dispatch settings	The settings on this tab allow you to define, which dispatch method to use for message transmission, and how to handle failover. Please read section 17.18.2.3.3 (page 280) for details.

	Setting	Explanation
(e)	Authentication session settings	The settings on this tab apply to passcode messages only. It is possible to define advanced failover for multi-factor authentication scenarios. Please read section 17.18.2.3.4 (page 284) for details.
(f)		Use the arrow buttons to step to the previous or next DP rule in the DP rule sequence (the arrow buttons are only available when editing an existing DP rule, not when creating a new one).

Click **Ok** to apply the changes to a DP rule, or **Cancel** to undo any changes. Please remember, that you still need to click the **Save** button to commit all changes to the database.

The settings on tabs (b)-(e) are described in the subsections below.

17.18.2.3.1 Settings of a Dispatch Policy Rule: Basic Data

The **Basic data** tab of a Dispatch Policy rule contains the following settings:

	Setting	Explanation
(a)	Description	Optional informative text for your own records. You can use it to describe the purpose of the DP rule.
(b)	Phone number selection	Select, whether a message should be sent to the user's primary or secondary phone number. This setting is only taken into account if the dispatch mechanism selected on the Dispatch settings tab is using phone numbers. Note: This option is only available if secondary phone numbers have been enabled on the General Settings page (cf. section 17.3.1, page 109).

17.18.2.3.2 Settings of a Dispatch Policy Rule: Pre-conditions

The **Pre-conditions** tab of a Dispatch Policy rule contains settings that allow you to specify, whether the rule should only apply under certain circumstances:

	Setting	Explanation
(a)	Apply	<p>This setting allows you to define, when this rule must apply:</p> <ul style="list-style-type: none"> Always apply this rule: Select this option, when dispatching according to this rule must always be attempted. Only apply this rule, when: Select this option, when dispatching according to this rule must only be attempted under certain circumstances – as specified by setting (b).

	Setting	Explanation
(b)	Conditions	<p>When setting (a) has been set to “Only apply this rule, when”, then you can use the three checkboxes in (b) to specify the condition(s) for applying dispatching according to this rule.</p> <p>If more than one checkbox is selected, then this is treated as a combined “AND condition” – meaning all selected conditions must be fulfilled for the DP rule to be applied.</p> <p>Phone number Select the phone number checkbox to enable a condition on the user's phone number. For example, you may only want to apply a specific dispatching mechanism, if the user's phone number starts with a specific international prefix.</p> <p>In case secondary phone numbers have been enabled on the General Settings page, then the phone number condition is always applied to the phone number selected on the Basic data tab (primary or secondary, respectively).</p> <p>Email Select the email checkbox to enable a condition on the user's email address. For example, you may only want to apply a specific dispatching mechanism, when the user's email address belongs to a specific domain.</p> <p>Token Select the token checkbox to enable a condition on the fact, whether the user has been assigned a token or not. This is useful, if you only want a specific rule to be applied, in case the user has a token assigned or not, respectively. For example, you might want to skip a specific dispatching mechanism for users with tokens, or you may want to delay the sending of OTP messages for users with tokens.</p> <div> Note: The token checkbox is only available if Token authentication has been allowed on the General Settings page (cf. section 17.3.2, page 110). </div>

17.18.2.3.3 Settings of a Dispatch Policy Rule: Dispatch Settings

The **Dispatch settings** tab of a Dispatch Policy rule contains settings that let you define the specific message dispatching behavior, when the rule is actually applied according to the conditions on the **Pre-conditions** tab.

CODE Policies > Dispatch Policies


Edit Dispatch Policy Rule 2

☒ Enable rule

Basic data Pre-conditions **Dispatch settings** Authentication session settings

a **Dispatch action** ☒ Send a message ☐ Do not send a message*

b **Dispatch type** Send the message by **SMS** using **b1**

b2  UK Modems
Modem group

The message will be sent as an SMS to the user's primary phone number.

c **Timeout** The message must be sent successfully within seconds, otherwise dispatching according to this rule is canceled.

Issue handling	Continue (to the next rule that applies)		Stop (no more rules applied)	
	Immediately	On timeout*	Immediately	On timeout*
d If dispatch not possible before timeout, then:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
e If the user's primary phone number has not been set, then:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	Setting	Explanation
(a)	Dispatch action	<p>This setting allows you to define, whether to send a message at all. Two options are available:</p> <ul style="list-style-type: none"> • Send a message: This is the default behavior, causing a message to be sent. • Do not send a message: This is a special purpose option for token users. This option will cause the rule NOT to send a message, but instead just introduce a pause of customizable duration. Selecting this option makes sense, if the rule has been restricted to apply to token users only, on the Pre-conditions tab. A typical usage is to introduce a pause for token users in the first rule of a DP. In this way, message transmission can be avoided, if the user makes use of his token, before the pause times out. <p>Note: This setting is only available if Token authentication has been allowed on the General Settings page (cf. section 17.3.2, page 110).</p> <p>Note: The “Do not send a message” option applies to passcode messages (authentication sessions) only. The rule will be skipped for notification transmissions, because introducing a pause does not make sense in this case.</p>
(b)	Dispatch type	<p>This setting allows you to define, how message transmission must occur. In the first drop-down list (b₁) you select, which type of message transmission you would like to use. The second drop-down list (b₂) will adapt according to this choice and provide a list of relevant dispatch mechanisms, from which you can choose.</p> <p>For example, when selecting “SMS” in drop-down list (b₁), then the drop-down list (b₂) will contain all modem groups that have been created, and all Dispatch Connectors that have been created and support SMS transmission.</p> <p>NOTE: The number of dispatch mechanisms shown in drop-down list (b₁) depend on your actual system configuration. For example, if you have not created any Email Connectors or any Dispatch Connectors supporting email, then Email will not be an option in the drop-down list. On the other hand, if you have installed a dispatch plugin module supporting a new dispatch mechanism, like for example Push-notification, then this dispatch mechanism will appear, if you have created a Dispatch Connector using such plugin module.</p>
(c)	Timeout	<p>This setting defines the maximum time allowed for transmission of the message. If transmission is not possible within this time, the rule will behave according to settings (d) and (e) in the Issue Handling section.</p>
(d)	Dispatch not possible within timeout	<p>Setting (d) is used to define, how the system must react, when a rule has been applied for message transmission, but transmission fails due to unexpected infrastructure problems. For example, because a Transmitter Service is down, a modem is down, or a modem is overloaded. You can choose between the following options:</p> <ul style="list-style-type: none"> • Continue / Immediately: Select this option to let the DP rule evaluation <u>progress immediately</u> to the next rule that applies, if transmission is not possible. “Immediately” means as soon as the system can <u>predict</u>, that transmission will most likely not occur within the specified timeout (c).

	Setting	Explanation
		<ul style="list-style-type: none"> Continue / On timeout: Select this option to let the DP rule evaluation progress to the next rule that applies, when transmission has not succeeded within the specified timeout (c). Stop / Immediately: Select this option to let the DP rule evaluation <u>stop immediately</u>, if transmission is not possible. "Immediately" means as soon as the system can <u>predict</u>, that transmission will most likely not occur within the specified timeout (c). "Stopping" means that no more DP rules will be applied for failover, and as a result, the message transmission fails. Stop / On timeout: Select this option to let the DP rule evaluation <u>stop</u>, when transmission has not succeeded within the specified timeout (c). "Stopping" means that no more DP rules will be applied for failover, and as a result, the message transmission fails. <p>The important difference between the Continue and Stop options is, that Continue allows the DP rule evaluation to continue, possibly applying subsequent DP rules, thereby providing the possibility to allow <u>failover</u> transmission mechanisms to kick in. In contrast, the Stop options will stop the DP rule evaluation and the message transmission attempt terminates with failure.</p> <p>The important difference between the Immediately and the On timeout options is:</p> <ul style="list-style-type: none"> "Immediately" means that the system should try to predict as soon as possible, whether it is likely to transmit the message successfully within the specified timeout (c). For example, if the rule is set to send a message using a modem group containing two modems, but both modems are unavailable, then the DP evaluation logic will progress immediately. On the other hand, if both modems are available, but messages have queued up due to a heavy load, then the system will automatically estimate the duration for sending all queued messages, and will immediately progress to the next DP rule, if the estimated queue time means that transmission will not be possible before the timeout. In contrast, "On timeout" means that the system will not make any predictions. No matter, which issue is observed, the system will keep on trying to send the message using the DP rule, until the timeout is actually exceeded. <p>The "Immediately" options are normally <u>recommended</u>, since they give a better user experience in case of errors, since failover rules can be applied as quickly as possible. On the other hand, the "On timeout" options could make sense for users with a token assigned, if they are likely to use the token in case of transmission errors. Note, that you can differentiate the behavior for token users and non-token users, by having dedicated rules with different token pre-conditions.</p>

	Setting	Explanation
(e)	Dispatch target not set	<p>Setting (e) is used to define, how the system must react, when the rule has been applied for message transmission, but the relevant Dispatch target is missing on the user. "Dispatch target" means, to where to send the message. Depending on the selected dispatch type (b), this is the user's phone number or email address.</p> <p>You can choose between the following behaviors, when a user's dispatch target is missing:</p> <ul style="list-style-type: none"> • Continue / Immediately: Select this option to let the DP rule evaluation <u>progress immediately</u> to the next rule that applies. • Continue / On timeout: Select this option to let the DP rule evaluation progress to the next rule that applies, when timeout (c) has expired. This effectively means that a pause is introduced. • Stop / Immediately: Select this option to let the DP rule evaluation <u>stop immediately</u>. "Stopping" means that no more DP rules will be applied for failover, and as a result, the message transmission fails. • Stop / On timeout: Select this option to let the DP rule evaluation <u>stop</u>, when timeout (c) has expired. This effectively means that a pause is introduced, and afterwards transmission fails. <p>The "Immediately" options are normally <u>recommended</u>, since they give a better user experience in case of a missing dispatch target, because failover rules can be applied as quickly as possible. On the other hand, the "On timeout" options could make sense for users with a token assigned. For example, it could be that users without a phone number are actually the users having a token assigned. In this case, it makes sense to introduce a pause for such users, enabling them to authenticate using a token.</p>

IMPORTANT – Issue handling for notifications

Please note, regarding settings (d) and (e) that the "**On timeout**" settings only apply to passcode message transmissions (authentication sessions). When sending notifications, "**On timeout**" options are always treated as their "**Immediately**" counterpart, since introducing a pause does not make sense in this case.

17.18.2.3.4 Settings of a Dispatch Policy Rule: Authentication Session Settings

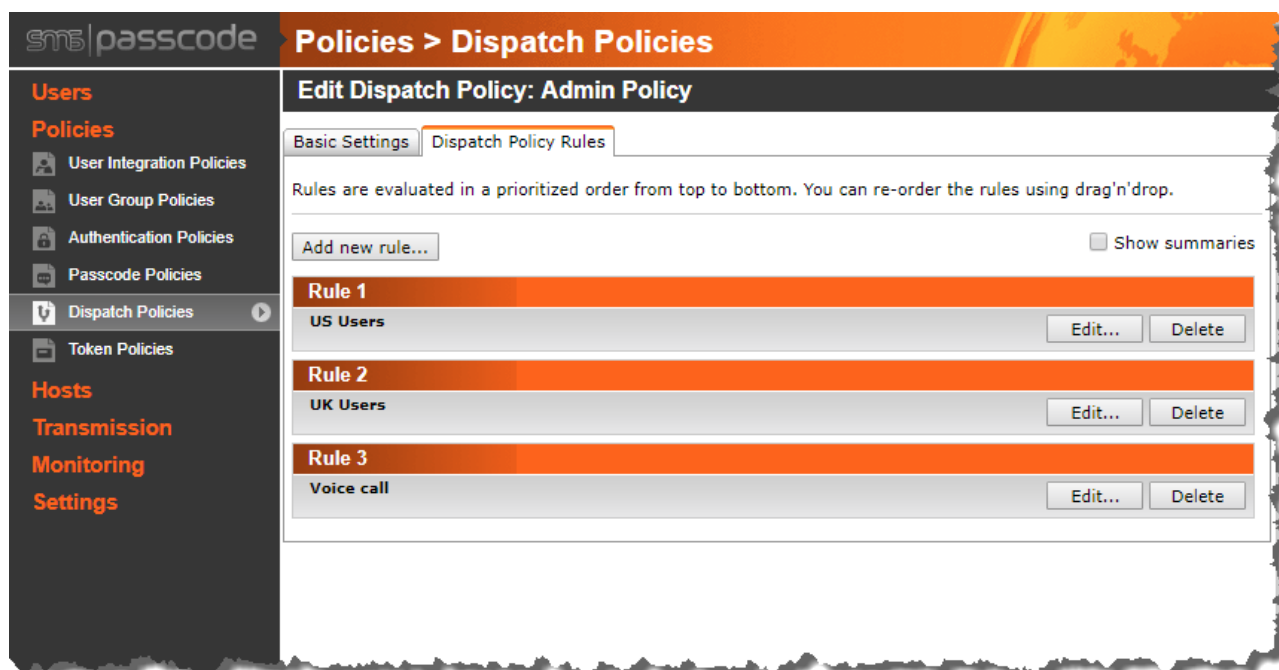
The **Authentication session settings** tab of a Dispatch Policy rule contains settings that let you define the behavior for authentication sessions. It is possible to configure the system for advanced failover, so that a passcode message is re-transmitted automatically using different dispatch settings, if the user does not enter the passcode within a specified timeout ("lifetime"). The settings on this tab are only relevant for passcode message transmissions, not for notifications:

	Setting	Explanation
(a)	Lifetime	<p>This setting specifies the lifetime of the DP rule. The following options are available:</p> <ul style="list-style-type: none"> • Determined by the passcode lifetime according to the passcode policy: Select this option to use the default passcode lifetime defined by the Passcode Policy assigned to the user. • Use custom duration: Select this option if you would like to override the default lifetime and enter a lifetime of own choice. For example, when configuring a second passcode message to be sent when the first one expires, it might be desirable to lower the lifetime of the first DP rule.

	Setting	Explanation
(b)	On expiration	<p>This setting specifies the behavior when a DP rule expires according to the lifetime of setting (a).</p> <ul style="list-style-type: none"> • Stop, authentication fails (default): Select this option if authentication must fail when the lifetime of the DP rule has expired. This is the default behavior. • Continue to the next rule that applies: When this option is selected, and the DP rule expires during an authentication session, the evaluation of the DP rule sequence will continue at the next rule that applies. <p>If another rule does apply, then the OTP³³ is re-transmitted according to this rule. This might be useful for automatic failover in the rare event of transmission problems or e.g. if the user uses two (mobile) phones for different purposes. E.g. if a DP rule expires, a new passcode message could automatically be sent using a different dispatch mechanism – or a new passcode message could be sent to the user's secondary phone number.</p> <p>If no other rule does apply, then authentication will fail.</p>

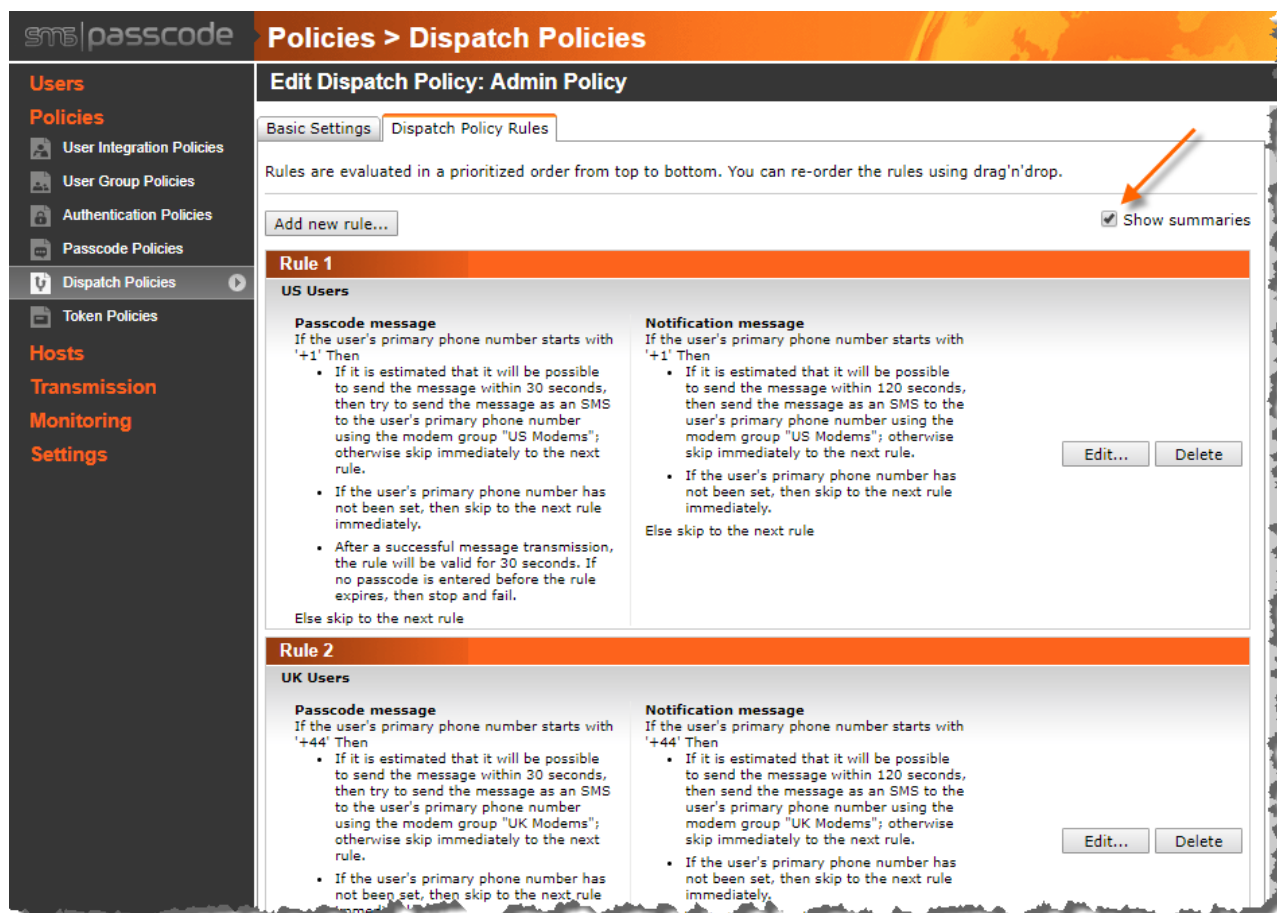
17.18.2.4 Dispatch Policy Rule Summaries

When maintaining a sequence of DP rules, by default, the **Dispatch Policy Rules** tab will only display the **Description** of each rule:



³³ Normally, the same OTP will be re-transmitted, to ensure the best user experience. However, the dispatch mechanism used for re-transmission might have limitations that do not allow re-transmission of the same OTP message. In such cases, a new OTP might be generated.

However, you may select the **Show summaries** checkbox to get a short summary of each DP rule. This is useful for getting a descriptive explanation of the settings of every rule:



17.18.3 Dispatch Policy Examples

This section shows different examples on how DPs can be applied for useful failover and scaling.

Example 1 (Prefix Load Balancing):

A large enterprise has acquired six modems, which are distributed between three different countries (2 modems at each location): United States, United Kingdom and Germany. A SIM card from a national operator has been inserted into each modem. Users from all three countries are logging into a Citrix Web Interface. To provide the most efficient SMS transmission and to lower the SMS transmission costs, it is desirable, that a modem is selected for each transmission that uses a SIM card with the same international mobile number prefix as the SIM card of the user requesting the SMS. This is also called **prefix load balancing**. To achieve this, you should proceed as follows:

1. Create three modems groups, one for each Country. For example, you could call the modem groups "US", "UK" and "DE". For each modem group, assign the two modems located in the corresponding country.
2. Create a DP containing a sequence of 4 DP rules:

Dispatch Policy Rule	Configuration															
#1	<div> <h3>Edit Dispatch Policy Rule 1</h3> <p><input checked="" type="checkbox"/> Enable rule</p> <p>Basic data Pre-conditions Dispatch settings Authentication session settings</p> <p>Specify, when this rule applies. When a rule does not apply, evaluation continues immediately at the next rule.</p> <p> <input type="radio"/> Always apply this rule <input checked="" type="radio"/> Only apply this rule, when: <div> <input checked="" type="checkbox"/> primary phone number starts with <input type="text" value="+1"/> <input type="checkbox"/> email starts with <input type="text"/> <input type="checkbox"/> token assigned and allowed <input type="text"/> </div> </p> </div> <div> <h3>Edit Dispatch Policy Rule 1</h3> <p><input checked="" type="checkbox"/> Enable rule</p> <p>Basic data Pre-conditions Dispatch settings Authentication session settings</p> <p>Dispatch action <input checked="" type="radio"/> Send a message <input type="radio"/> Do not send a message*</p> <p>Dispatch type Send the message by <input type="text" value="SMS"/> using <div> <div> US Modem group </div> </div> <p>The message will be sent as an SMS to the user's primary phone number.</p> <p>Timeout The message must be sent successfully within <input type="text" value="30"/> seconds, otherwise dispatch according to this rule is canceled.</p> <table border="1"> <thead> <tr> <th rowspan="2">Issue handling</th> <th colspan="2">Continue (to the next rule that applies)</th> <th>Stop (no more rules)</th> </tr> <tr> <th>Immediately</th> <th>On timeout*</th> <th>Immediately</th> </tr> </thead> <tbody> <tr> <td>If dispatch not possible before timeout, then:</td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td>If the user's primary phone number has not been set, then:</td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> <td><input type="radio"/></td> </tr> </tbody> </table> </p></div>	Issue handling	Continue (to the next rule that applies)		Stop (no more rules)	Immediately	On timeout*	Immediately	If dispatch not possible before timeout, then:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	If the user's primary phone number has not been set, then:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Issue handling	Continue (to the next rule that applies)		Stop (no more rules)													
	Immediately	On timeout*	Immediately													
If dispatch not possible before timeout, then:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>													
If the user's primary phone number has not been set, then:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>													

Dispatch
Policy Rule

Configuration

#2

Edit Dispatch Policy Rule 2

☒ Enable rule

Basic data

Pre-conditions

Dispatch settings

Authentication session settings

Specify, when this rule applies. When a rule does not apply, evaluation continues immediately at the

☐ Always apply this rule☒ Only apply this rule, when:☒ primary phone number starts with ☐ email starts with

Edit Dispatch Policy Rule 2

☒ Enable rule

Basic data

Pre-conditions

Dispatch settings

Authentication session settings

Dispatch action

☒ Send a message☐ Do not send a message*

Dispatch type

Send the message by using UK
Modem group

The message will be sent as an SMS to the user's primary phone number.

Timeout

The message must be sent successfully within seconds, otherwise dispatch according to this rule is canceled.

Issue handling

Continue (to the next rule that applies)		Stop (no more rules)
Immediately	On timeout*	Immediately

If dispatch not possible before timeout, then:

☒ ☐ ☐

If the user's primary phone number has not been set, then:

☒ ☐ ☐

Dispatch
Policy Rule

Configuration

#3

Edit Dispatch Policy Rule 3

☒ Enable rule

Basic data

Pre-conditions

Dispatch settings

Authentication session settings

Specify, when this rule applies. When a rule does not apply, evaluation continues immediately at the next rule.

☐ Always apply this rule☒ Only apply this rule, when:☒ primary phone number starts with ☐ email starts with

Edit Dispatch Policy Rule 3

☒ Enable rule

Basic data

Pre-conditions

Dispatch settings

Authentication session settings

Dispatch action

☒ Send a message☐ Do not send a message*

Dispatch type

Send the message by usingDE
Modem group

The message will be sent as an SMS to the user's primary phone number.

Timeout

The message must be sent successfully within seconds, otherwise dispatch according to this rule is canceled.

Issue handling

Continue

(to the next rule that applies)

(no more rules)

Immediately On timeout* Immediately

If dispatch not possible before timeout, then:

☒☐☐

If the user's primary phone number has not been set, then:

☒☐☐

Dispatch Policy Rule	Configuration																				
#4	<div> <div> Edit Dispatch Policy Rule 4 </div> <div> <input checked="" type="checkbox"/> Enable rule </div> <div> Basic data Pre-conditions Dispatch settings Authentication session settings </div> <div> Specify, when this rule applies. When a rule does not apply, evaluation continues immediately at the </div> <div> <input checked="" type="radio"/> Always apply this rule <input type="radio"/> Only apply this rule, when: <div> <input type="checkbox"/> primary phone number starts with <input type="text"/> </div> <div> <input type="checkbox"/> email starts with <input type="text"/> </div> <div> <input type="checkbox"/> token assigned and allowed <input type="text"/> </div> </div> </div> <div> <div> Edit Dispatch Policy Rule 4 </div> <div> <input checked="" type="checkbox"/> Enable rule </div> <div> Basic data Pre-conditions Dispatch settings Authentication session settings </div> <div> Dispatch action <input checked="" type="radio"/> Send a message <input type="radio"/> Do not send a message* </div> <div> Dispatch type Send the message by SMS using <div> All modems Modem group </div> The message will be sent as an SMS to the user's primary phone number. </div> <div> Timeout For passcodes, the message must be sent successfully within 30 seconds, otherwise dispatching according to this rule is canceled. For notifications, the message must be sent successfully within 120 seconds, otherwise dispatching according to this rule is canceled. </div> <div> Issue handling <table border="1"> <thead> <tr> <th></th> <th colspan="2">Continue (to the next rule that applies)</th> <th colspan="2">Stop (no more rules applied)</th> </tr> <tr> <th></th> <th>Immediately</th> <th>On timeout*</th> <th>Immediately</th> <th>On timeout*</th> </tr> </thead> <tbody> <tr> <td>If dispatch not possible before timeout, then:</td> <td><input type="radio"/></td> <td><input type="radio"/></td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td>If the user's primary phone number has not been set, then:</td> <td><input type="radio"/></td> <td><input type="radio"/></td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> </tbody> </table> </div> </div>		Continue (to the next rule that applies)		Stop (no more rules applied)			Immediately	On timeout*	Immediately	On timeout*	If dispatch not possible before timeout, then:	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	If the user's primary phone number has not been set, then:	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
	Continue (to the next rule that applies)		Stop (no more rules applied)																		
	Immediately	On timeout*	Immediately	On timeout*																	
If dispatch not possible before timeout, then:	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>																	
If the user's primary phone number has not been set, then:	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>																	

With these DP rules in place, each passcode message will be sent using a modem from the same country as the user, whenever at least one modem of the country is available and has a short queue (transmission possible within 30 seconds). Otherwise, the last rule will take over, i.e. the message will be load balanced between all available modems, including the modems located in the other countries.

Example 2 (SMS PASSCODE Mobile app failover):

A company prefers to transmit messages end-to-end encrypted via the SMS PASSCODE Mobile app, but would like to fail over to SMS transmission using the SMS PASSCODE Cloud Service, in

case an end-user has not installed the SMS PASSCODE Mobile app. To achieve this, create a sequence of 2 DP rules:

Dispatch Policy Rule

Configuration

#1

Edit Dispatch Policy Rule 1

☒ Enable rule

Basic data Pre-conditions Dispatch settings Authentication session settings

Dispatch action ☒ Send a message ☐ Do not send a message*

Dispatch type Send the message by **Push message** using
 SMS PASSCODE Cloud Service (default)
Dispatch connector
 The message will be sent as a push message to the user's primary phone number.

Timeout
 For passcodes, the message must be sent successfully within seconds, dispatching according to this rule is canceled.
 For notifications, the message must be sent successfully within seconds, dispatching according to this rule is canceled.

Issue handling	Continue (to the next rule that applies)		Immediately (no more)
	Immediately	On timeout*	
If dispatch not possible before timeout, then:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
If the user's primary phone number has not been set, then:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Edit Dispatch Policy Rule 1

☒ Enable rule

Basic data Pre-conditions Dispatch settings Authentication session settings

The settings below apply to **authentication sessions** only, not to notifications.

Lifetime Please select the lifetime of this rule:
☐ Determined by the passcode lifetime according to the passcode policy
☒ Use custom duration seconds

On expiration When the rule lifetime expires, then:
☐ Stop, authentication fails
☒ Continue to the next rule that applies
 Note: In case several passcode messages are sent, all OTPs sent during authentication session stay valid, until the **last** rule expires.

Dispatch
Policy
Rule

Configuration

#2

Edit Dispatch Policy Rule 2

☒ Enable rule

Basic data

Pre-conditions

Dispatch settings


Authentication session settings

Dispatch action

- ☒ Send a message
☐ Do not send a message*

Dispatch type

Send the message by SMS using

 SMS PASSCODE Cloud Service (default)
Dispatch connector

The message will be sent as an SMS to the user's primary phone number.

Timeout

For passcodes, the message must be sent successfully within 30 seconds, otherwise dispatching according to this rule is canceled.For notifications, the message must be sent successfully within 120 seconds, otherwise dispatching according to this rule is canceled.

Issue handling

Continue (to the next rule that applies)		Stop (no more rules applied)	
Immediately	On timeout*	Immediately	On timeout*

If dispatch not possible before timeout, then:

☐ ☐ ☒ ☐

If the user's primary phone number has not been set, then:

☐ ☐ ☒ ☐

Edit Dispatch Policy Rule 2

☒ Enable rule

Basic data

Pre-conditions

Dispatch settings

Authentication session settings

The settings below apply to **authentication sessions** only, not to notifications.

Lifetime

Please select the lifetime of this rule:

- ☒ Determined by the passcode lifetime according to the passcode
☐ Use custom duration 30 seconds

On expiration

When the rule lifetime expires, then:

- ☒ **Stop**, authentication fails
☐ **Continue** to the next rule that applies

Example 3 (operator failover):

A company has acquired four modems. Two of the modems are equipped with SIM cards from operator A, while the other two modems are equipped with SIM cards from operator B. Below, the modems are called Operator A and Operator B modems, respectively. By default, all passcodes

should be sent using the Operator A modems and all users have been assigned mobile phones with SIM cards from operator A. However, in case of any problems with operator A, the Operator B modems should be used instead. This means that if the Operator A modems are unavailable or cannot send any SMS, or if the users do not receive any SMS from operator A, then the system should failover to the Operator B modems. Selected important users have also been given SIM cards from operator B. The SMS passcodes should be sent to the operator B mobile number in the failover situation. In this way, operator network failover is realized at both the sending and receiving end. To achieve this, you should proceed as follows:

1. Create two modem groups, one called "Telco A" and one called "Telco B". For each modem group, allocate the two modems with SIM cards from the corresponding Telco operator.
2. Create a DP containing a sequence of 2 DP rules:

Dispatch Policy Rule	Configuration
#1	<div>Edit Dispatch Policy Rule 1 <input checked="" type="checkbox"/> Enable rule <div>Basic data Pre-conditions Dispatch settings Authentication session settings</div><div>Description Optional description for your own records. <div>Use Telco A modems</div></div><div>Phone number selection Select the phone number to use, in case this rule makes any numbers: <div><input checked="" type="radio"/> Primary phone number <input type="radio"/> Secondary phone number</div></div></div>

Dispatch
Policy
Rule

Configuration

Edit Dispatch Policy Rule 1

☒ Enable rule

Basic data

Pre-conditions

Dispatch settings

Authentication session settings

Dispatch action

- ☒ Send a message
☐ Do not send a message*

Dispatch type

Send the message by **SMS** usingTelco A
Modem group

The message will be sent as an SMS to the user's primary phone number.

Timeout

The message must be sent successfully within **30** seconds, otherwise the dispatch according to this rule is canceled.

Issue handling

Continue

(to the next rule that applies)

Immediately

On timeout*

Immediately

If dispatch not possible before timeout, then:

☐☐

If the user's primary phone number has not been set, then:

☒☐

Edit Dispatch Policy Rule 1

☒ Enable rule

Basic data

Pre-conditions

Dispatch settings

Authentication session settings

The settings below apply to **authentication sessions** only, not to notifications.

Lifetime

Please select the lifetime of this rule:

- ☐ Determined by the passcode lifetime according to the passcode policy
☒ Use custom duration **30** seconds

On expiration

When the rule lifetime expires, then:

- ☐ **Stop**, authentication fails
☒ **Continue** to the next rule that applies

Note: In case several passcode messages are sent, all OTPs sent during the authentication session are valid, until the session expires.

Dispatch
Policy
Rule

Configuration

#2

Edit Dispatch Policy Rule 2

☒ Enable rule

Basic data

Pre-conditions

Dispatch settings

Authentication session settings

Description

Optional description for your own records.

Use Telco B modems

Phone number selection

Select the phone number to use, in case this rule makes any ref numbers:

☐ Primary phone number☒ Secondary phone number

Edit Dispatch Policy Rule 2

☒ Enable rule

Basic data

Pre-conditions

Dispatch settings

Authentication session settings

Dispatch action

☒ Send a message☐ Do not send a message*

Dispatch type

Send the message by SMS using

Telco B
Modem group

The message will be sent as an SMS to the user's secondary phone number.

Timeout

The message must be sent successfully within 30 seconds, otherwise dispatching according to this rule is canceled.

Issue handling

Continue

(to the next rule that applies)

Stop

(no more rules apply)

Immediately

On timeout*

Immediately

On timeout

If dispatch not possible before timeout, then:

☐☐☒☐

If the user's secondary phone number has not been set, then:

☐☐☒☐

Dispatch Policy Rule	Configuration
	<div><h3>Edit Dispatch Policy Rule 2</h3><p><input checked="" type="checkbox"/> Enable rule</p><p>Basic data Pre-conditions Dispatch settings Authentication session settings</p><p>The settings below apply to authentication sessions only, not to notifications.</p><p>Lifetime Please select the lifetime of this rule:</p><p><input checked="" type="radio"/> Determined by the passcode lifetime according to the passcode lifetime</p><p><input type="radio"/> Use custom duration <input type="text" value="30"/> seconds</p><p>On expiration When the rule lifetime expires, then:</p><p><input checked="" type="radio"/> Stop, authentication fails</p><p><input type="radio"/> Continue to the next rule that applies</p></div>

17.19 Authentication Monitoring

The **Authentication Monitoring** page is used to monitor all authentication attempts, i.e. any attempts of any SMS PASSCODE user to authenticate against any SMS PASSCODE protected authentication client. The page can be used for several purposes:

- Retrospective inspection of past authentication attempts, e.g. for purposes of reporting, analysis or security review. Extensive filtering options provide many ways to inspect the registered attempts.
- Live inspection of current authentication attempts, e.g. in case of troubleshooting.
- Export of authentication attempts to CSV or XML files, e.g. for further analysis by 3rd party analysis systems. Again, the extensive filtering options let you export exactly the data needed.

NOTE: The **Authentication Monitoring** page is only available when **Authentication Monitoring** has been enabled on the **General Settings** page (cf. section 17.3.3, page 114).

Initially, when entering the **Authentication Monitoring** page, it will show all *Live Data* in a grid ordered descending by date and time, i.e. showing the most recent authentication attempts at the top:

Monitoring > Authentications

Authentications

Select columns Set filter Quick filter: Export...

Data Source: Live Data Refresh now Auto-Refresh 15 seconds Apply

Total number of live data records = 950 (95% of archive threshold). Oldest record from 7/12/2018 3:00:00 AM.
Last successful auto-archive operation: 8/24/2018 10:04:11 AM

1 2 3 4 5 6 7 8 9 10 ... >>

	Login successful	When	User (Display name)	Client type	End-user IP	Country	Organization
Show	Yes	8/21/2018 6:32:24 AM	peter wilson [secureshop\jane]	Citrix Web Interface	221.212.173.82	Iraq	Large Enterprise
Show	No	8/21/2018 5:28:48 AM	anna brown [othercompany\simon]	TMG Server	172.111.54.206	Jamaica	Large Enterprise
Show	No	8/21/2018 4:25:12 AM	janice johnson [othercompany\amanda]	IIS Website (ISAPI)	79.97.235.63	Palestinian territories	Large Enterprise
Show	Yes	8/21/2018 3:21:36 AM	simon roberts [othercompany\simon]	IIS Website (ISAPI)	182.58.247.36	Iraq	Large Enterprise
Show	Yes	8/21/2018 2:18:00 AM	janice jones [mycompany\simon]	Password Reset Website	38.1.35.98	Madagascar	Big Company
Show	No	8/21/2018 1:14:24 AM	simon roberts [secureshop\amanda]	Secure Device Provisioning	49.87.141.13	Christmas Island	Large Enterprise
Show	Yes	8/21/2018 12:10:48 AM	anna brown [secureshop\peter]	AD FS	147.183.219.11	South Sudan	Big Company
Show	Yes	8/20/2018 11:07:12 PM	simon roberts [bigcompany\bill]	Secure Device Provisioning	182.68.84.60	Madagascar	Large Enterprise

IMPORTANT:

Unfortunately, some authentication clients perform password validation before the corresponding SMS PASSCODE integration is allowed to kick in. This means that if an invalid password is entered in such cases, then the authentication client will deny access, before the SMS PASSCODE integration has the chance to detect the session. Consequently, "Invalid password" attempts will not show up in the SMS PASSCODE Authentication Monitor in such cases. This applies in the following cases:

- SMS PASSCODE IIS Website Protection: Always.
- SMS PASSCODE Windows Logon Protection: When RDP connections are validated using Network Level Authentication.
- SMS PASSCODE AD FS Protection.

Live Data means authentication attempts stored in the internal SMS PASSCODE database, i.e. not including any archived authentication attempts.

The monitoring page provides several useful features:

- Click the **Select columns** button to change the actual columns shown in the monitoring grid. For example, add the **Note** column, if you would like to see the reasons for failed authentication attempts.
- Click the **Set filter** button to define row-filtering conditions. For example, define a filter only showing rows of failed attempts, only rows for a specific user, only rows for a specific date interval, or only rows with attempts originating from a specific country (in case Geo-IP has been enabled). Alternatively, use the new **Quick filter** textbox to the right of the button, where you can simply enter some text to search for across most of the fields in the grid.
- Click the **Export...** button to export all data *currently shown* in the grid to a CSV or XML file, e.g. for purposes of reporting or further analysis.
- Click the **Data Source** drop-down to switch between displaying *Live Data* or *Archived Data* in the monitoring grid³⁴.
- Click the **Refresh now** button to update the monitoring grid, displaying any new data that might have appeared in the meantime.
- Select the **Auto-Refresh** checkbox to make the grid refresh its data automatically by a fixed time interval. This might be useful in case of troubleshooting.
- Click the **Show** link of any authentication attempt to display the full details of the entry.
- Click the **Show logins on map** button to plot all data *currently shown* in the grid on a world map ("geo mapping").

Some of these features are described in more detail in the following subsections.

³⁴ It is not possible to display or export *Live Data* and *Archived Data* at the same time. If you need to analyze both types of data combined, this is possible using the SMS PASSCODE PowerShell cmdlet `Get-SmsPcAuthenticationMonitorData` (cf. section 18.1, 309).

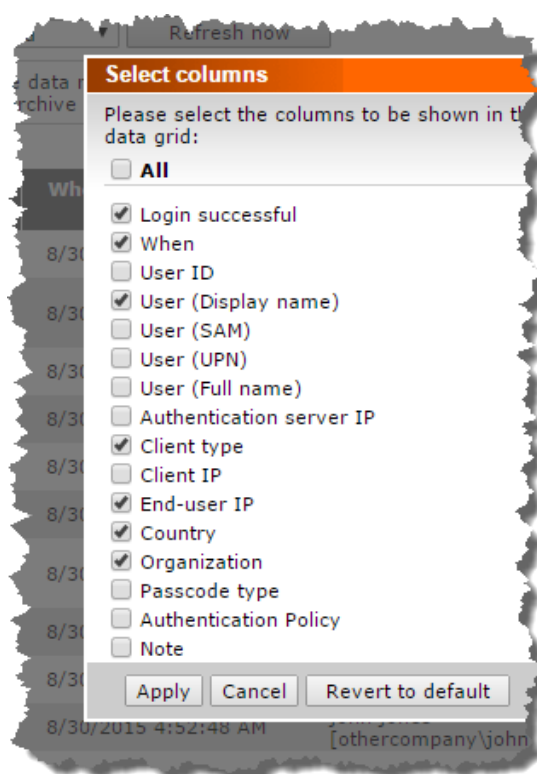
17.19.1 Column Filtering

Whenever a new authentication attempt is recorded in the SMS PASSCODE database, many useful details about the attempt are stored. The **Authentication Monitoring** grid only shows a small subset of these details. You can see all details of any authentication attempt by clicking on the **Show** link to the left of the row in question.

	Login successful	When
Show	Yes	8/21/2018 6:32:24 AM
Show	No	8/21/2018 5:28:48 AM
Show	No	8/21/2018 4:25:12 AM
Show	Yes	8/21/2018 3:21:36 AM
Show	Yes	8/21/2018 2:18:00 AM
Show	No	8/21/2018 1:14:24 AM
Show	Yes	8/21/2018 12:10:48 AM
Show	Yes	8/20/2018 11:07:12 PM
Show	No	8/20/2018 10:03:36 PM

Alternatively, you have the option of customizing which columns to show in the grid. To achieve this, click the **Select columns** button at the top of the page:

A dialog for selecting the columns to show in the grid will appear:



Select or clear the checkbox to the left of an attribute to make it appear or disappear in the grid, respectively. Select the checkbox **All** to make all columns appear in the grid. The individual attributes are described in the table below:

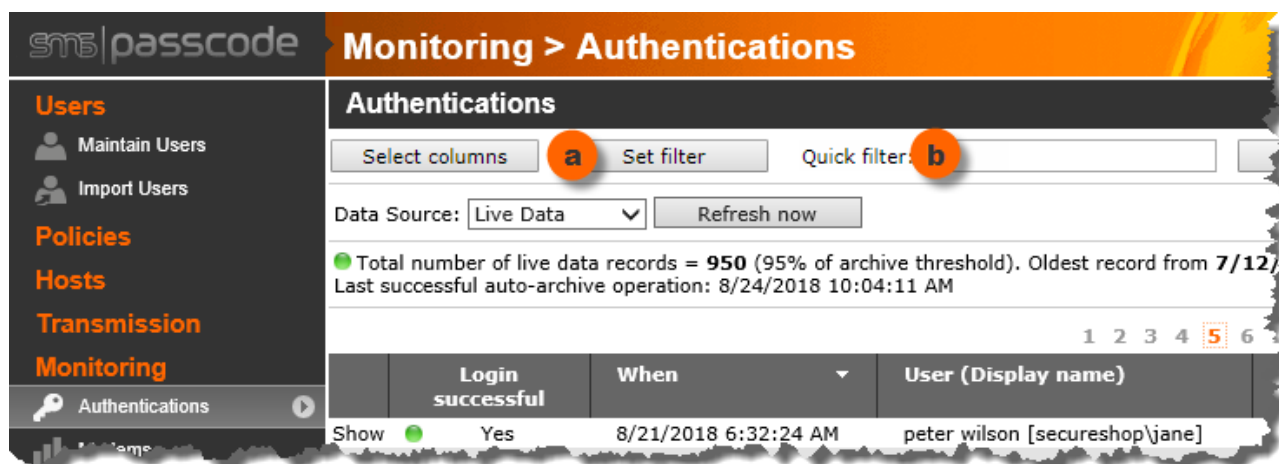
Attribute	Explanation
Login Successful	Specifies whether the authentication attempt succeeded or failed. In case of a failed authentication attempt, inspect the Note attribute to realize the exact reason of failure.
When	Specifies the date and time of the authentication attempt.
User ID	Specifies the unique ID of the end-user that attempted authentication. The unique ID is used internally by the SMS PASSCODE database. In case a user has been imported into the SMS PASSCODE database from an AD using a User Integration Policy, then the ID will be equal to the user's Security ID (SID) in the AD.
User (Display Name)	Shows the most exact name of the end-user that attempted authentication, depending on the fact which part of the user's name is known by the SMS PASSCODE database (full name, SAM, UPN).
User (SAM)	Shows the SAM account name of the end-user that attempted authentication. Empty, if the SAM account name of the user is not known.
User (UPN)	Shows the UPN of the end-user that attempted authentication. Empty, if the UPN of the user is not known.

Attribute	Explanation
User (Full name)	Shows the full name of the end-user that attempted authentication. Empty, if the full name of the user is not known.
Authentication server IP	Specifies the IP address of the SMS PASSCODE Authentication Backend Service host that actually determined, whether the authentication attempt was successful or not.
Client type	Specifies the type of client on which the end-user attempted to log in. E.g. Citrix Web Interface, RADIUS or Windows Logon.
Client IP	Specifies the IP address of the SMS PASSCODE protected authentication client to which the end-user attempted to log in. For example, the IP address of an SMS PASSCODE protected RADIUS server, or the IP address of an SMS PASSCODE protected OWA site.
End-user IP	Specifies the IP address of the end-user that attempted authentication.
Country	Specifies the country from which the end-user attempted to log in, determined from the end-user IP using Geo-IP. Note: This attribute is only available, if Geo-IP and IP history has been enabled on the General Settings page (cf. section 17.3.1, page 109).
Organization	Specifies the organization from which the end-user attempted to log in, determined from the end-user IP using Geo-IP. Note: This attribute is only available, if Geo-IP and IP history has been enabled on the General Settings page (cf. section 17.3.1, page 109).
Passcode type	Specifies the type of passcode that the end-user was using during the authentication attempt. Possibly values are: <ul style="list-style-type: none"> • Session-specific OTP • Token OTP • Personal Passcode • MFA bypassed³⁵
Authentication Policy	Specifies the name of the Authentication Policy and the rule number of this policy that was applied during the authentication attempt.
Note	Specifies the reason for a failed authentication attempt. Empty, if authentication succeeded.

³⁵ Multi-factor authentication can be bypassed only if bypassing has been allowed on the **General Settings** page. In this case, bypassing might occur due to two different reasons: Either because **PoC Mode** has been enabled, or because bypassing was determined by an Authentication Policy.

17.19.2 Row Filtering

Row filtering allows you to restrict the monitoring grid to show only a subset of all registered authentication attempts.



Filtering can be applied in two different ways:

- a. **Row filter:** Click the **Set filter** column to restrict the number of authentication attempts shown in the grid. If you specify several conditions in the row filter, then the conditions are combined into an “AND-filter”, meaning authentication attempts are hidden from the grid unless they fulfill all conditions of the filter.
- b. **Quick filter:** This feature allows you to define a more flexible filter in a very quick way. You simply enter the content into the quick filter that you want to search for, and the grid will then only show authentication attempts, that *contain* the entered value in any of the following attributes:
 - When
 - User (Display name)
 - User (SAM)
 - User (UPN)
 - User (Full name)
 - Authentication Server IP
 - Client type
 - Client IP
 - End-user IP
 - Country
 - Organization
 - Authentication Policy
 - Note
 - Dispatch History

NOTE: You can combine the **Row filter** and the **Quick filter**. This will restrict the grid to only show authentication attempts that fulfill both filters.

Row filters can be used for many purposes. Here are a couple of examples:

- Show only authentication attempts that failed
- Show only authentication attempts of a specific user

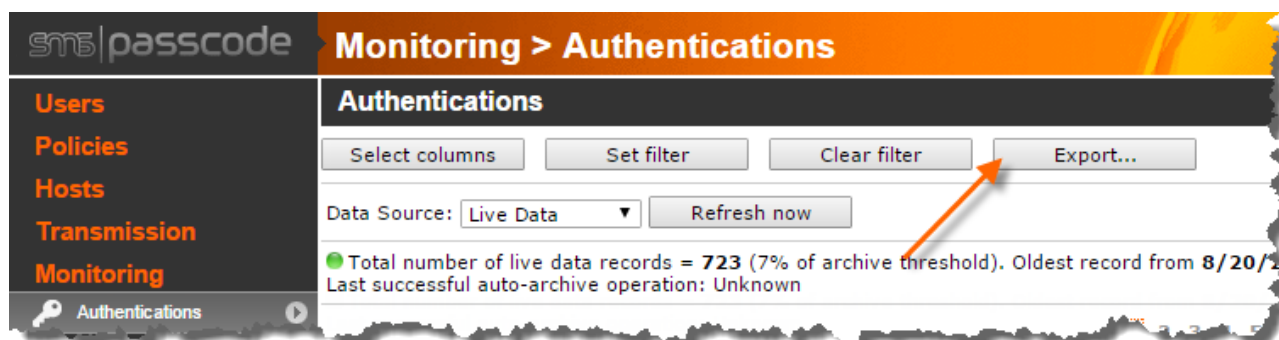
- Show only authentication attempts from a specific period
- Show only attempts to log in to a specific type of client
- Show only attempts to log in to an authentication client with a specific IP address
- Show only attempts to log in from a specific end-user IP address (or IP address scope)
- Show only attempts to log in from a specific country or organization
- Show only authentication attempts using a specific type of passcode

Moreover, since these filter examples can be combined in any way – you are given great flexibility for analyzing the authentication attempts in your organization.

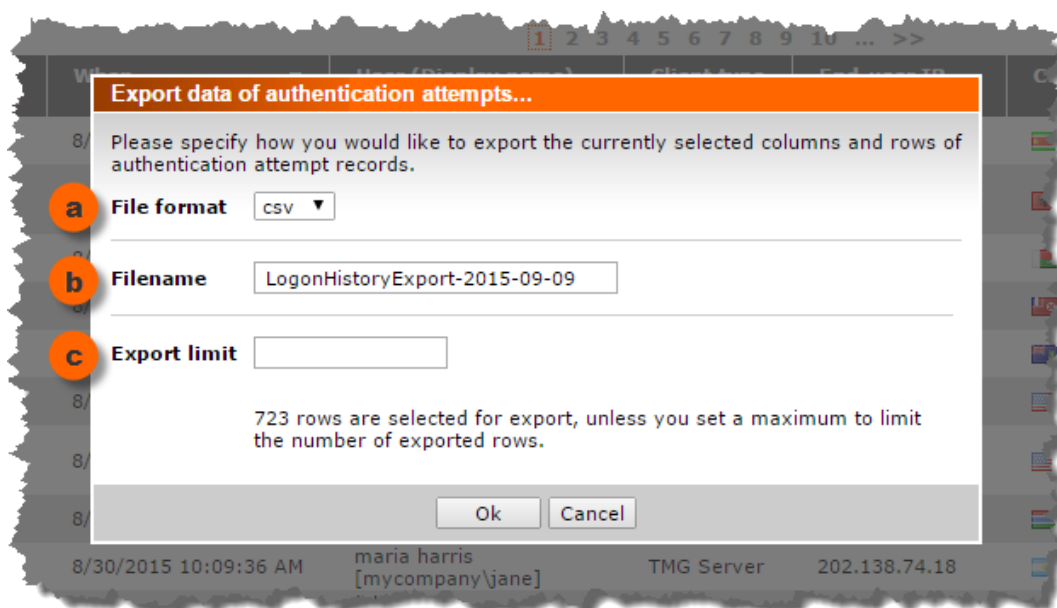
17.19.3 Exporting Data

As explained in the two previous sections about column and row filtering, you are able to customize the monitoring grid to show exactly the authentication attempts that you would like to inspect. When you have completed such filtering, you have the additional option to export the specific data shown in the grid, e.g. for further analysis in a 3rd party tool like Microsoft Excel, where you could create pivot tables or pivot charts from the data.

To initiate export of the current data of the grid, please click the **Export...** button.



The following dialog will appear:



Fill out the settings in the dialog and click the **Ok** button, to execute the export. Otherwise, click the **Cancel** button to abort the export.

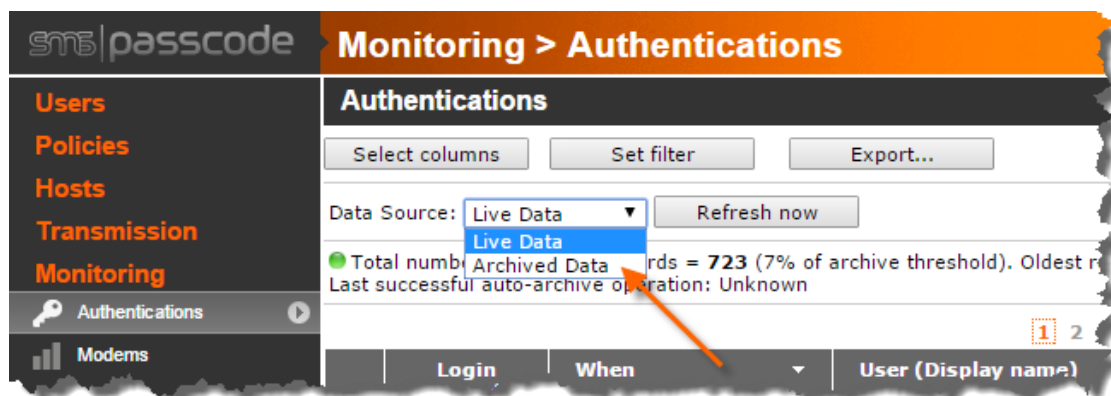
The settings in the dialog are described in the table below:

	Setting	Explanation
(a)	File format	Select whether to export data to a CSV or XML file.
(b)	Filename	Specify a name for the file that is going to contain the exported data.
(c)	Export limit	Optionally enter a record limit. If a number x is entered, then only the x topmost rows of the grid are exported. Otherwise, all rows of the grid are exported.

17.19.4 Switching Data Source

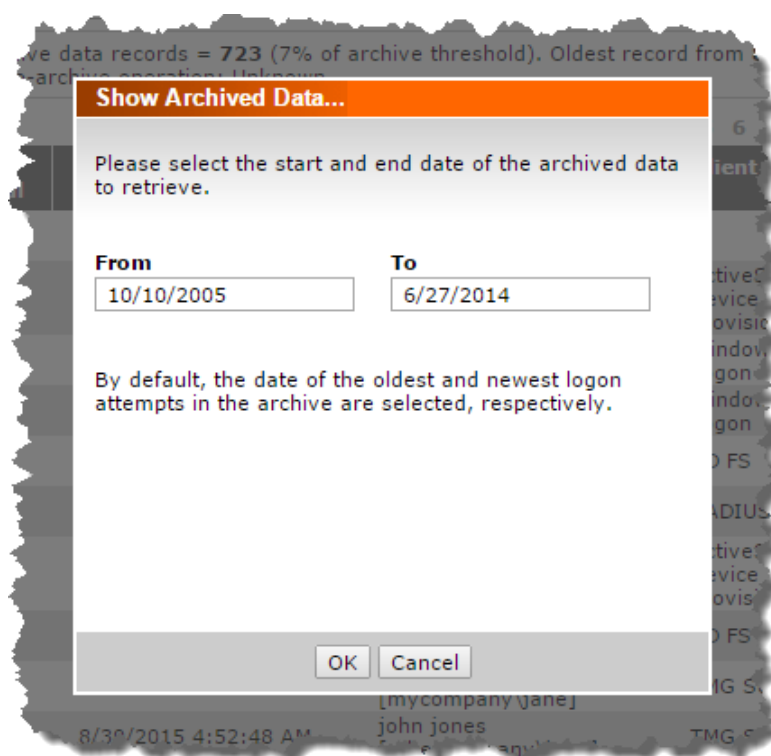
By default, the monitoring grid will display *Live Data*, i.e. authentication attempts stored internally in the SMS PASSCODE database, as opposed to archived data.

Use the **Data Source** drop-down to switch between *Live Data* and *Archived Data*:



When switching to *Archived Data*, the grid will instead display data from the current archive of authentication attempts, as defined by the current archiving settings on the **General Settings** page (cf. section 17.3.3, page 114).

First, a dialog will appear, asking you to select the period of archived data to display:



It is recommended not to import data of a longer period than needed, since importing a huge amount of archived authentication attempts can take a while. When you have selected the required period, the corresponding archived data is retrieved from the archive and displayed in the grid.

You have now exactly the same options for performing column and row filtering, plotting data on a world map or exporting data, similar to the situation of displaying *Live Data*.

17.19.5 Geo-mapping

The *Geo-mapping* feature allows you to visualize the authentication entries of the **Authentication Monitoring** page on a world map. When activating the feature, it will map the authentication entries currently shown on the **Authentication Monitoring** page. This means that you may apply row filtering and/or switch data source first, thereby allowing you to select the exact data to be visualized on the world map. For example, you could visualize login attempts for a specific period, a specific user and/or a specific type of authentication client. Furthermore, you may visualize all attempts, or only failing attempts.

Note: The *geo-mapping* feature only allows visualization of login attempts where the end-users' IP addresses were collected. Otherwise, required geo-IP information is not available for mapping the entries.

Once the desired login attempts for geo-mapping have been selected, click the **Show logins on map** button to perform the visualization of the entries on a world map:

Monitoring > Authentications

Authentications

Select columns Set filter Export...

Page size: 10

Data Source: Live Data Refresh now

☐ Auto-Refresh 15 seconds Apply

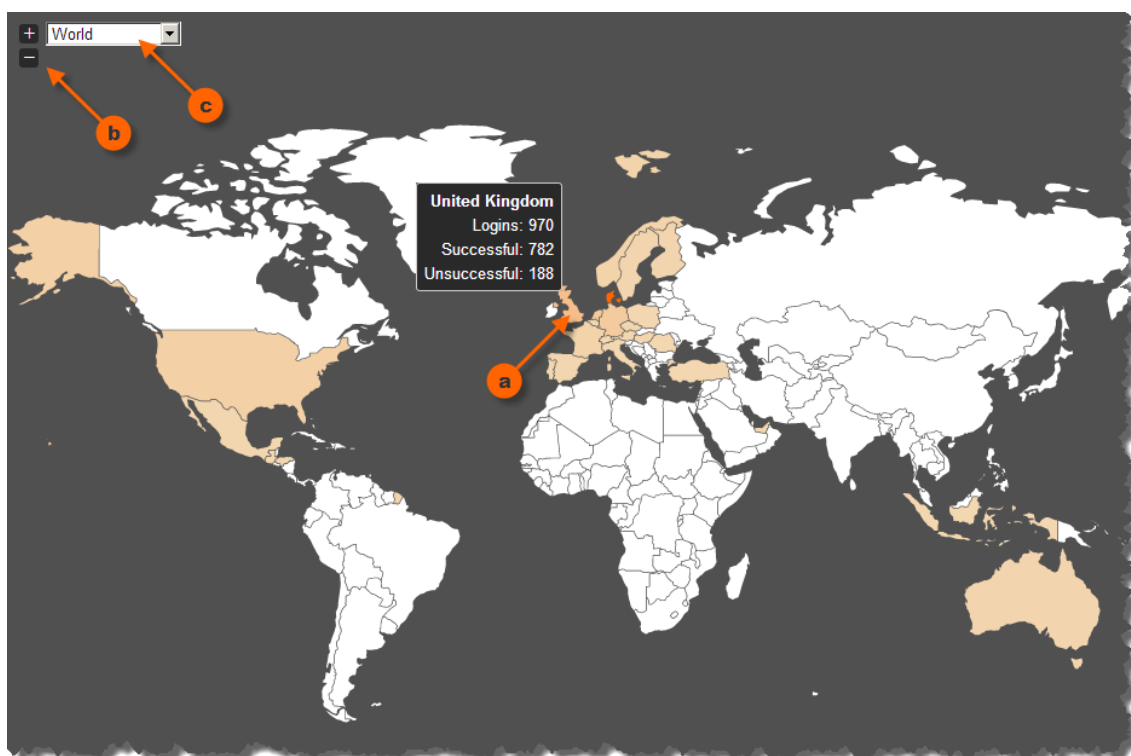
Total number of live data records = 950 (95% of archive threshold). Oldest record from 7/12/2018 3:00:00 AM.
Last successful auto-archive operation: 8/24/2018 10:04:11 AM

Show logins on map

	Login successful	When	User (Display name)	Client type	End-user IP	Country	Organization
Show	Yes	8/21/2018 6:32:24 AM	peter wilson [secureshop\jane]	Citrix Web Interface	221.212.173.82	Iraq	Large Enterprise
Show	No	8/21/2018 5:28:48 AM	anna brown [othercompany\simon]	TMG Server	172.111.54.206	Jamaica	Large Enterprise
Show	No	8/21/2018 4:28:16 AM	janice johnson	ITS Web Interface	172.111.54.206	Palestining territories	Large Enterprise

A world map will appear with each country colored according to the number of login attempts from the country (darker color means more login attempts). The following features are available on the world map:

- Click on any country to get the exact login statistics for this country.
- To navigate the map, you can click the +/- buttons at the upper left corner to zoom in and out, respectively. When zoomed in, you can drag the map by holding the mouse-button down.
- Alternatively, you can zoom into specific regions of the world map using the drop-down list in the upper left corner. The entry **Fit** will zoom in to the world map as much as possible, while still showing all countries with at least a single login attempt according to the currently selected data on the Authentication Monitoring page.



- **Avg. transmission time:** The average time per transmission measured since the modem thread was started.

Quarantined and Blacklisted Modems

If a modem has status **Quarantined** or **Blacklisted**, then the modem is unavailable for message transmissions. **Quarantined** means that the modem is temporarily unavailable, and will be re-initialized periodically, in an attempt to make it available again. **Blacklisted** means that the modem is permanently unavailable, and that you need to take action to make it available again. A typical example of blacklisting is that an incorrect PIN has been entered, making it impossible to initialize the modem.

In all cases, please inspect the event log of the relevant SMS PASSCODE Transmitter Service. The event log will contain details about, why the modem was quarantined or blacklisted.

You can always trigger an immediate attempt to re-initialize a modem, by disabling the modem on the **Modems** maintenance page, and then afterwards enable it again (or alternatively delete the modem, and then re-create it).

18 POWERSHELL SUPPORT

NOTE: This section only applies to SMS PASSCODE installations in the **On-premise** or **Hybrid Setup**.

As described in the previous section, the SMS PASSCODE Web Administration Interface provides a **graphical user interface** for administering SMS PASSCODE. This section describes an alternative way of performing many SMS PASSCODE administrator tasks, using PowerShell cmdlets. Please note that the current version of SMS PASSCODE does not include cmdlets for all possible SMS PASSCODE administrator tasks. In some cases, you will still need to make use of the SMS PASSCODE Web Administration Interface. More PowerShell cmdlets are likely to be added to future versions of SMS PASSCODE.

IMPORTANT: The SMS PASSCODE PowerShell cmdlets support PowerShell version 4.0 and later. Please ensure, that your PowerShell script execution policy is NOT limited to "Restricted" by a Group Policy— setting it to "RemoteSigned" is sufficient³⁶.

The table below summarizes, which SMS PASSCODE tasks can be performed using the Web Administration Interface (WAI) and PowerShell (PS), respectively.

Administrator task	WAI	PS
SMS PASSCODE general settings (read, update)	Yes	Yes
SMS PASSCODE license settings (read, update)	Yes	Yes
Users (read, create, update, delete, import from CSV file, lock, unlock)	Yes	Yes
User Integration Policies (read, create, update, delete)	Yes	Yes
User Group Policies (read, create, update, delete)	Yes	Yes

³⁶ <https://technet.microsoft.com/en-us/library/ee176961.aspx>

Administrator task	WAI	PS
Authentication Policies (read, create, update, delete)	Yes	No
Passcode Policies (read, create, update, delete)	Yes	No
Dispatch Policies (read, create, update, delete)	Yes	No
Token Policies (read, create, update, delete)	Yes	No
Authorized Transmitter Hosts (read, create, update, delete)	Yes	Yes
Authorized Authentication Backend Service Hosts (read, create, update, delete)	Yes	Yes
Modems (read, create, update, delete)	Yes	Yes
Modem Groups (read, create, update, delete)	Yes	No
Email Connectors (read, create, update, delete)	Yes	No
Dispatch Connectors (read, create, update, delete)	Yes	No
Modem Monitor (inspect)	Yes	No
Authentication Monitor (inspect live data and archived data)	Yes	Yes

The section below summarizes the PowerShell cmdlets available for performing SMS PASSCODE administrator tasks.

18.1 Cmdlet Overview

The following PowerShell cmdlets are available in the current version of SMS PASSCODE:

Cmdlet Name	Description
General Settings	
Get-SmspcSettings	Read general SMS PASSCODE settings
Set-SmspcSettings	Update general SMS PASSCODE settings
License Settings	
Get-SmspcLicense	Read SMS PASSCODE license settings
Set-SmspcLicense	Update SMS PASSCODE license settings (e.g. license code)

Cmdlet Name	Description
Users	
Get-SmspcUser	Read/list existing users in the SMS PASSCODE database
New-SmspcUser	Create a new (non-synchronized) user
Set-SmspcUser	Update an existing user
Remove-SmspcUser	Delete an existing (non-synchronized) user
Import-SmspcUser	Import users from a CSV file
Lock-SmspcUser	Lock out a user
Unlock-SmspcUser	Unlock a user
User Integration Policies	
Get-SmspcUserIntegrationPolicy	Read/list existing User Integration Policies in the SMS PASSCODE database
New-SmspcUserIntegrationPolicy	Create a new User Integration Policy (only possible, when User store integration has been enabled in multi-sync mode)
Set-SmspcUserIntegrationPolicy	Update an existing User Integration Policy
Remove-SmspcUserIntegrationPolicy	Delete an existing User Integration Policy (only possible, when User store integration has been enabled in multi-sync mode)
User Group Policies	
Get-SmspcUserGroupPolicy	Read/list existing User Group Policies in the SMS PASSCODE database
New-SmspcUserGroupPolicy	Create a new User Group Policy
Set-SmspcUserGroupPolicy	Update an existing User Group Policy
Remove-SmspcUserGroupPolicy	Delete an existing User Group Policy
Authorized Transmitter Hosts	
Get-SmspcTransmitterServiceHost	Read/List authorized Transmitter Service hosts
New-SmspcTransmitterServiceHost	Authorize a new Transmitter Service host
Remove-SmspcTransmitterServiceHost	Delete a previously authorized Transmitter Service host

Cmdlet Name	Description
Authorized Authentication Backend Service Hosts	
Get-SmspcAuthenticationBackendServiceHost	Read/List authorized Authentication Backend Service hosts
New-SmspcAuthenticationBackendServiceHost	Authorize a new Authentication Backend Service host
Remove-SmspcAuthenticationBackendServiceHost	Delete a previously authorized Authentication Backend Service host
Modems	
Get-SmspcModem	Read/list existing modems in the SMS PASSCODE database
New-SmspcModem	Create a new modem
Set-SmspcModem	Update an existing modem
Remove-SmspcModem	Delete an existing modem
Authentication Monitor	
Get-SmspcAuthenticationMonitorData	Retrieve data from the SMS PASSCODE Authentication Monitor. It is possible to retrieve both live data and archived data.
Get-SmspcAuthenticationMonitorStatistics	Retrieve statistics regarding "Live" and "Archived" entries of the SMS PASSCODE Authentication Monitor.

18.2 Permissions

To have permission to execute SMS PASSCODE PowerShell cmdlets, the following must be fulfilled:

- You must run the PowerShell console with administrator rights
- Your account must have write access to the SMS PASSCODE database file
- Ensure that the effective PowerShell script execution policy is set to "Unrestricted" or "RemoteSigned".

SMS PASSCODE PowerShell cmdlets are always installed on the SMS PASSCODE Database Service host. However, you can also optionally install the cmdlets on other machines, including workstations, to perform administrator tasks remotely. In such case, you must use the SMS PASSCODE Configuration Tool to set the host name or IP address of the SMS PASSCODE Database host, and to set the correct shared secret for the PowerShell cmdlets to connect properly to the SMS PASSCODE Database Service. An alternative for remote PowerShell administration is to use PowerShell Remoting.

18.3 Getting Started

The usage of each SMS PASSCODE PowerShell cmdlet is not described in this document, because PowerShell contains its own help system. In order to get help on any cmdlet, use the “Get-Help” command in PowerShell. For example, to get help on the Get-SmspcUser cmdlet, you can use any of the following commands:

- **Get-Help Get-SmspcUser**
This will show a short description of the Get-SmspcUser cmdlet.
- **Get-Help Get-SmspcUser -Examples**
This will show examples of the usage of the Get-SmspcUser cmdlet.
- **Get-Help Get-SmspcUser -Full**
This will show the full help description for the Get-SmspcUser cmdlet, including detailed help for all parameters, and including examples of usage.
- **Get-Help Get-SmspcUser -ShowWindow**
This will show the help text for the Get-SmspcUser cmdlet in a separate window.
- **Get-Help Get-SmspcUser -Parameter Identity**
This will show a description specifically for the requested parameter “Identity”.

18.4 Examples

This section shows examples of the usage of some of the SMS PASSCODE PowerShell cmdlets:

- Set a new SMS PASSCODE license code “S1234...”

```
Set-SmsPcLicense -LicenseKey S1234...
```

- Enable *User store integration*:

```
Set-SmsPcSettings -UserStoreIntegrationEnabled $True
```

- Allow *location and behavior aware authentication*:

```
Set-SmsPcSettings -GeoIpAndIpHistoryEnabled $True
```

- Create a new User Group Policy, called “My UGP”, which allows access to the Self-service Website.

```
New-SmsPcUserGroupPolicy -Name "My UGP" -SelfServiceAccessAllowed $True
```

- Create a new User Integration Policy, which imports users from the AD group “Remote Access”, from the domain “MyDomain”, and assign the User Group Policy “My UGP” to all imported users:

```
New-SmsPcUserIntegrationPolicy -ServerName MyDomain -GroupName "Remote Access" -UserGroupPolicyName "My UGP"
```

- Retrieve all SMS PASSCODE users that are currently locked out, and then unlock them:

```
Get-SmsPcUser -All | Where-Object {$_.LockedOut} | Unlock-SmsPcUser
```

- Check whether any users are lacking an MFA license:

```
if ((Get-SmsPcLicense).LicenseStatisticsMissingCount."MFA Standard" -gt 0)  
{ SomeRelevantAction }
```

- Retrieve all SMS PASSCODE authentication attempts performed between 2016-01-01 and 2016-05-31 from outside the US:

```
Get-SmsPcAuthenticationMonitorData -From 2016-01-01 -To 2016-05-31  
-IncludeArchiveData | Where-Object {$_.CountryName -ne "United States"}
```

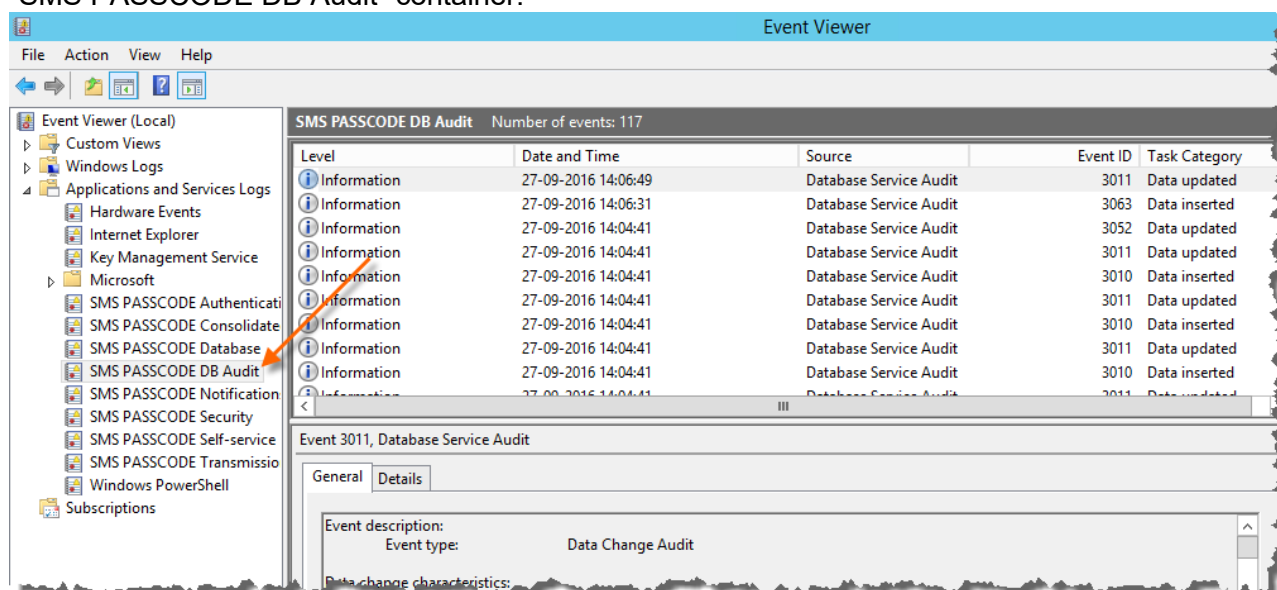
19 DATABASE AUDIT

NOTE: This section only applies to SMS PASSCODE installations in the **On-premise** or **Hybrid Setup**.

SMS PASSCODE includes an advanced database audit, that lets administrators inspect, exactly which data was changed in the SMS PASSCODE database, by whom and when. All data changes will be audited, no matter if they are applied via the Web Administration Interface, via PowerShell cmdlets, or by users using the SMS PASSCODE Self-service Website.

The audit is available as a dedicated Windows event log container on the server, where the SMS PASSCODE Database Service is installed. To access it, open the Event Viewer and select the

“SMS PASSCODE DB Audit” container:



Every event entry contains the following sections, documenting every data change in detail:

Section	Content
Data change characteristics	<ul style="list-style-type: none"> <u>Change performed by:</u> The name of the person that made the data change³⁷ <u>Type of object:</u> The type of object that was changed (for example “User” or “User Group Policy”) <u>Type of operation:</u> The type of data change (“Insert”, “Update” or “Delete”) <u>Identity of the object:</u> The identity of the actual object that was affected (for example the name of a user, or the name of a User Group Policy).
Properties of new object	In case of a newly inserted object, this section lists the values of each attribute of the new object.
Changed properties of object	In case of an update, this section documents exactly which attributes were changed, including the values of the attributes before and after the change.
Unchanged properties of object	In case of an update, this section lists the values of all the attributes that were not affected by the update.
Properties of deleted object	In case of a deleted object, this section lists the values of each attribute of the deleted object.

³⁷ Please note that when a change is made via the Self-service Website, the identity of the person performing the change will be reported as the identity of the Application Pool running the Self-service Website. Consider to assign a dedicated identity to the Application Pool in order to distinguish such audit entries. You can identify the actual user that performed an update, by inspecting the “Identity of the object”, since a user is only allowed to change attributes on his own user account.

Note: Sensitive data, like Personal Passcodes or PIN codes, will never be shown in the audit data. However, you will still be able to see, whether any of the sensitive data was changed, you just cannot see, what exact values have been set.

20 ROLE-BASED ADMINISTRATOR PERMISSIONS

NOTE: This section only applies to SMS PASSCODE installations in the **On-premise** or **Hybrid Setup**.

As described in previous sections, administrators can access and maintain data in the SMS PASSCODE database in two ways:

- Using the Web Administration Interface (WAI), a graphical user interface.
- Using SMS PASSCODE PowerShell cmdlets, a scripting interface.

By default, each administrator has either full permissions or no permissions via the WAI and PowerShell cmdlets, respectively. However, if you need more fine-grained control of permissions, **role-based administration** is a feature that allows you to define distinct permissions for different groups of administrators. For example, you might want to grant limited permissions to internal IT helpdesk personnel.

Overall, such distinct permissions can be assigned on two levels:

- **Database permissions:** As the name implies, database permissions are assigned on the database level. This means that such permissions apply, no matter how the database is accessed. More concrete, this means that such permissions apply both when requesting data changes via the WAI, or via SMS PASSCODE PowerShell cmdlets.

Database permissions are defined per entity in the database and allow to define, whether an administrator is allowed to insert, update or delete objects of such an entity. For example, whether an administrator can insert new users, update existing users, or delete existing users.

- **WAI page permissions:** Page permissions allow to define the pages (more specifically the URLs) within the WAI that an administrator is allowed to access. For example, whether an administrator is allowed to access the **Authentication Monitor** page.

Each set of database permissions and WAI page permissions are assigned according to defined administrator roles, which are in turn determined by the current administrator's Windows group memberships. This is explained in more detail in the section below.

20.1 Defining Role-based Permissions

To assign role-based permissions, you first need to plan the type of administrator roles needed. Each such role is defined by a unique name and a list of one or more Windows groups. For example, the name of a role could be "IT HelpDesk", and the related Windows Groups could be "IT West" and "IT East". In this case, any Windows users that are direct members of the Windows group "IT East" or "IT West" will be assigned the administrator role "IT HelpDesk", when logging in

to the WAI or using any SMS PASSCODE PowerShell cmdlets. This means that such users will be assigned the permissions defined by the "IT HelpDesk" role.

IMPORTANT: Direct group membership required

Please note that a user must be a direct member of one of the Windows groups assigned to an administrator role, for the role to be applied. Indirect group membership via sub-groups are not supported.

The administrator roles, and their related database permissions and WAI page permissions, are defined using an XML file with the name **AdminRoles.xml**, which you must manually create in the SMS PASSCODE installation folder on the server where the SMS PASSCODE Database service has been installed. If you have used the default installation path, then you must create an xml file with the following full path on the database host:

```
C:\Program Files\SMS PASSCODE\AdminRoles.xml
```

A convenient way to create this file is to make a copy of the file **AdminRolesExample.xml**, which is already present in the SMS PASSCODE installation folder.

Overall, the procedure for defining role-based permissions is:

1. Log in to the server, where the SMS PASSCODE Database service has been installed.
2. Locate the **AdminRolesExample.xml** file in the SMS PASSCODE installation folder, typically:

```
C:\Program Files\SMS PASSCODE\AdminRolesExample.xml
```

3. Make a copy of this file and rename the copy to **AdminRoles.xml**.
4. Remove the read-only flag from the **AdminRoles.xml** file.
5. Edit the **AdminRoles.xml** file, defining admin roles and related permissions according to your specific needs. Save the file, when done.
6. Restart the SMS PASSCODE Database service.

IMPORTANT: Whenever changes are made to the **AdminRoles.xml** file, such changes will not take effect, until the SMS PASSCODE Database service has been restarted. Also, any active WAI sessions must be closed, before changes apply there.

For exact details on defining administrator roles and related permissions, please inspect the **AdminRolesExample.xml** file.

A conflict might occur, if a user belongs to several administrator roles. For example, this can happen if the same Windows group is assigned to several administrator roles, or if a user belongs to several Windows groups, that are assigned to different administrator roles. In such cases the user is assigned to the first matching administrator role, using a top-down evaluation of the roles defined in the **AdminRoles.xml** file.

WARNING: Any administrator not matching any role defined in the **AdminRoles.xml** file will be granted full permissions by default. It is therefore a best practice when using role-based permissions to define a very broadly matching role as the final role and give such role very limited permissions.

20.2 Role-based Permissions in the Web Administration Interface

When role-based administration is active, any permission restrictions will automatically be reflected in the UI of the WAI. Examples:

- Page permissions:
Any menu items in the navigation menu that would redirect to a page with access denied, are automatically removed from the navigation menu. This ensures that the administrator sees a simplified navigation menu that corresponds to the permissions granted.
- Database permissions:
 - a. Any “Add” button that would cause a disallowed operation is automatically disabled. For example, the “Add User Group Policy” button is disabled if the administrator has not been granted the permission to create (insert) a new User Group Policy.
 - b. Any “Delete” button that would cause a disallowed operation is automatically disabled. For example, the “Delete User Group Policy” button is disabled if the administrator has not been granted the permission to delete a User Group Policy.
 - c. Any “Save” button that would cause a disallowed update operation is automatically disabled. For example, the “Save” button on the General Settings page is disabled if the administrator has not been granted the permission to update general settings.
- Active role:
In the left pane of the WAI, below the navigation menu, the currently assigned administrator role is displayed.

Below is a screen shot that gives an example of the impact that role-based permissions can have on the UI of the WAI:

Users > Maintain Users

Users

Maintain Users

Monitoring

Authentications

Modems

Settings

General

License

User store integration

Last refresh attempt **Successful**

Last successful refresh 10:05:22

- Server: DC2016-01.test1.local
- Users found: 19
- Users imported: 19

Add new user...

Select columns Set filter

1 2

Display name	Login SAM	Login UPN	Locked out	CAL
User Only On Test1	test1\useronlyontest1	useronlyontest1@test1.local	No	
User OnlySAMDiff	test1\useronlysam	useronlysamdiff@test1.local	No	
User OnlyUPNDiff	test1\useronlyupn	useronlyupndiff@test1.local	No	
User PassChange	test1\userpasschange	userpasschange@test1.local	No	
User Pass Expired	test1\userpassexpired	userpassexpired@test1.local	No	
User PIN	test1\userpin	userpin@test1.local	No	
User Diff SAM UPN	test1\usersam	userupn@test1.local	No	
User SAM Diff Domain	test1\usersamdiffdomain	userupndiffdomain@test1.com	No	
UserTEST1	test1\usertest1	usertest1@test1.local	No	

1 2

Role: Help Desk

Assigned role

Simplified navigation menu due to restricted permissions

Denied by DB permission

21 PLUGGABLE TRANSMISSION INFRASTRUCTURE

NOTE: This section only applies to SMS PASSCODE installations in the **On-premise** or **Hybrid Setup**.

The SMS PASSCODE transmission infrastructure is extendable using **dispatch plugin modules**. This means, that it is possible to implement/configure new transmission mechanisms and add such new mechanisms to your transmission infrastructure, should you have specific message transmission requirements.

The SMS PASSCODE installer includes plugin modules that support a long list of 3rd party message transmission providers. If you decide to use any of these providers for message transmission, this will work out-of-the-box. The only requirement is that you need to sign up for your own account at the chosen provider(s).

On the other hand, if you have very specific message transmission requirements, you can add your own, custom-made dispatch plugin modules. Dispatch plugin modules are added to your SMS PASSCODE transmission infrastructure in a very easy and convenient way:

1. Locate the “Plugins” folder on the host, where the SMS PASSCODE Database Service has been installed. The default path is:

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

Create a new subfolder for the new dispatch plugin module and copy your custom-made dispatch module to the new subfolder.

2. Restart the SMS PASSCODE Database Service. The new plugin module is loaded and automatically distributed to the SMS PASSCODE transmission infrastructure.
3. Create a **Dispatch Connector** in the SMS PASSCODE database that references the new dispatch plugin module as the provider.
4. Configure your **Dispatch Policies** to make use of the **Dispatch Connector** created in item 3.

IMPORTANT: The **Generic HTTP(s)** dispatcher allows you to add support for additional 3rd party message transmission web services that use a stateless HTTP(S) based API (such as RESTful APIs), without the need to implement a custom-made dispatch plugin module.

Before you decide to implement your own, custom-made dispatch plugin module, please note, that one of the dispatch plugin modules installed out-of-the-box is a **Generic HTTP(s)** dispatcher that can easily be customized to connect to most 3rd party message transmission web services that use a stateless HTTP(S) based API (such as RESTful APIs). If you would like to add support for such a web service provider that is not available out-of-the-box, please have a look at the configuration file for the **Generic HTTP(s)** dispatcher. The standard path for this configuration file is:

```
C:\Program Files\SMS PASSCODE\Plugins\GenericHttp\Custom.Config.xml
```

This file contains additional information, describing how to customize the **Generic HTTP(s)** dispatcher.

Any changes made to the `Custom.Config.xml` file do NOT take effect, until the SMS PASSCODE Database Service has been restarted (or the “Reload” button is clicked on the **General Settings** page in the Web Administration Interface).

Please contact SMS PASSCODE support, in case:

- You need additional information regarding customization of the **Generic HTTP(s)** dispatcher.
- You need additional information regarding the SMS PASSCODE Dispatch Plugin Module API.

21.1 SMS PASSCODE Cloud Service

A special plugin module is the one called **SMS PASSCODE Cloud Service**. This plugin module allows you to transmit messages via the SMS PASSCODE Cloud Service. This cloud service allows:

- Messages to be sent from your SMS PASSCODE infrastructure to smart phones of users that have installed the **SMS PASSCODE Mobile app**.
- Messages to be sent from your SMS PASSCODE infrastructure via SMS and voice calls at a flat-rate cost, in case you have a valid SMS PASSCODE trial or subscription license.

The SMS PASSCODE Mobile app has the following important features:

- It is free of charge, no extra costs for any subscription.
- The user is automatically notified using push notifications.
- Messages are transmitted **end-to-end encrypted**, meaning they are encrypted in your SMS PASSCODE infrastructure, and can only be decrypted by the actual instance of the SMS PASSCODE Mobile app on the user's smart phone.

IMPORTANT: Cloud Service Permissions

The SMS PASSCODE Cloud Service plugin supports 3 different dispatch types: Push message, SMS and voice call. If you configure any Dispatch Policy to use any of these dispatch types, and message transmission fails due to lack of permissions (listed in the Windows event log), then this can be due to the following reason:

Permissions to use the dispatch types SMS and voice call are only granted to trial customers and customers on a valid subscription license.

When installing SMS PASSCODE, a default Dispatch Connector is automatically created that utilizes the SMS PASSCODE Cloud Service plugin

Please note, that to send messages to the SMS PASSCODE Mobile app, you need to go through the following steps:

1. Configure a **Dispatch Policy** that makes use of the default **Dispatch Connector** and is set to use dispatch type "Push message".

For example, you can create a **Dispatch Policy**, that will first try to send push messages to the SMS PASSCODE Mobile app (rule 1), and then try to failover to SMS (rule 2). This policy will even work for users that have not installed the SMS PASSCODE Mobile app, since rule 1 will fail immediately in such cases and therefore failover to SMS transmission according to rule 2.

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

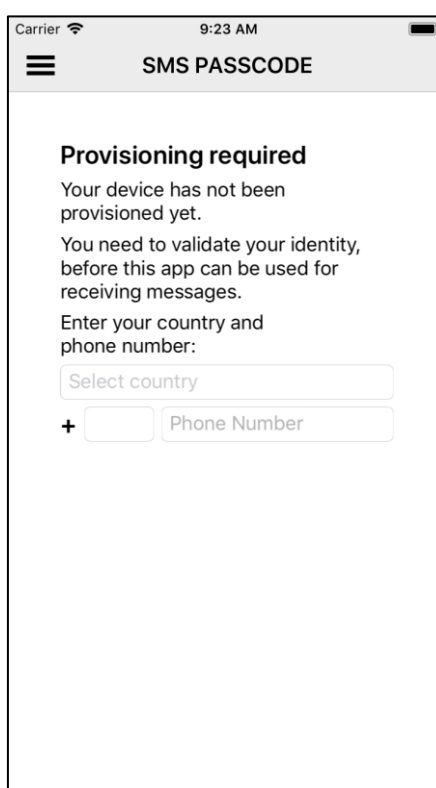
21.1.1 Provisioning the SMS PASSCODE Mobile App

The first time a user starts the SMS PASSCODE Mobile 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 SMS PASSCODE Mobile app.

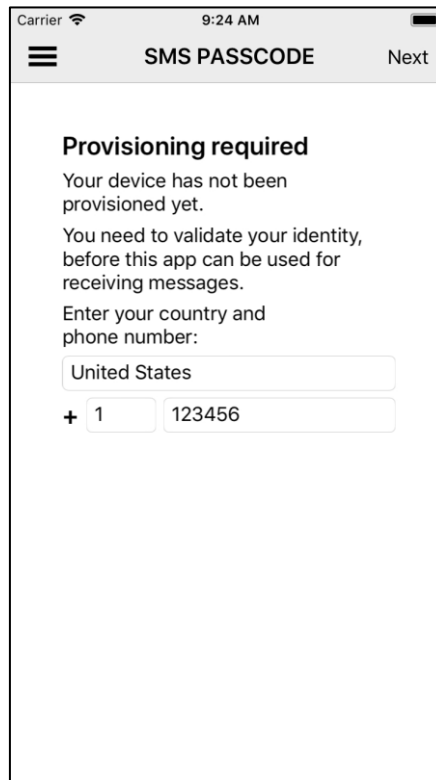
This means that whenever the same phone number is assigned to a new instance of the SMS PASSCODE Mobile app (on a new device), earlier provisioned devices will stop working immediately.

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



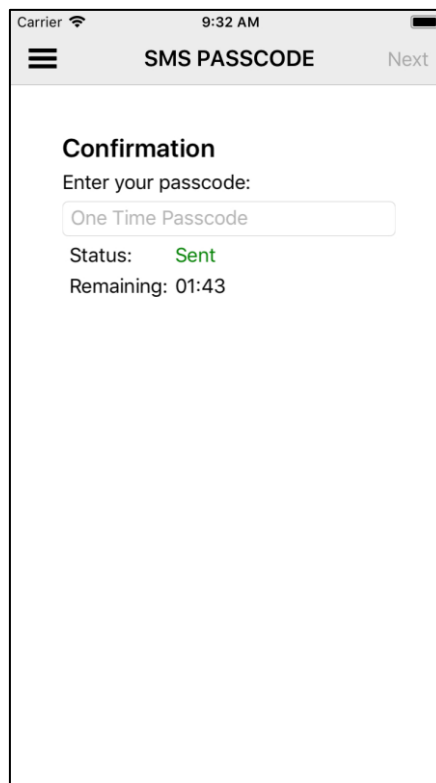
The screenshot shows the SMS PASSCODE Mobile App interface during the provisioning process. At the top, the status bar displays 'Carrier', signal strength, and the time '9:23 AM'. The app's header bar is grey with a hamburger menu icon on the left and the text 'SMS PASSCODE' in the center. The main content area has a white background and contains the following text: 'Provisioning required', 'Your device has not been provisioned yet.', 'You need to validate your identity, before this app can be used for receiving messages.', and 'Enter your country and phone number:'. Below this text are two input fields: 'Select country' and a field for the phone number, which is preceded by a '+' sign and a small square input box. The phone number field is labeled 'Phone Number'.

2. The user enters his phone number, including the international prefix (which can be filled by selecting the corresponding country). For example:



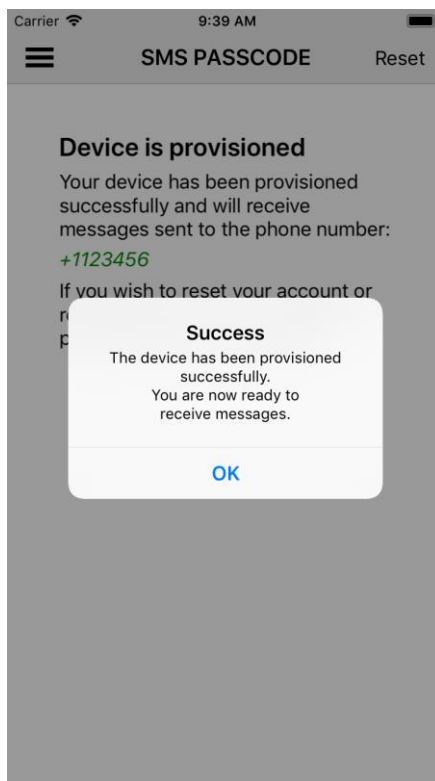
The screenshot shows a mobile app interface titled "SMS PASSCODE". At the top, there is a status bar with "Carrier", signal strength, "9:24 AM", and battery level. Below the status bar is a header with a hamburger menu icon, the title "SMS PASSCODE", and a "Next" button. The main content area has the heading "Provisioning required" followed by the text: "Your device has not been provisioned yet. You need to validate your identity, before this app can be used for receiving messages. Enter your country and phone number:". Below this text are two input fields. The first field is labeled "United States" and has a dropdown arrow. The second field is labeled "+ 1" and "123456".

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

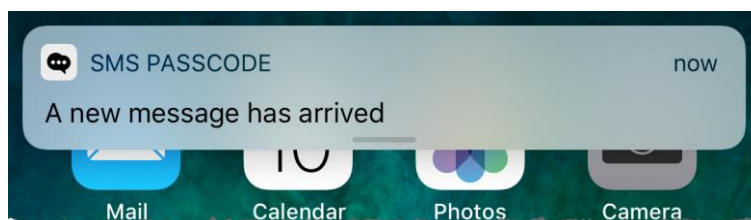


The screenshot shows a mobile application interface titled "SMS PASSCODE". At the top, there is a status bar with "Carrier", signal strength, and "9:32 AM". Below the status bar is a header with a hamburger menu icon, the title "SMS PASSCODE", and a "Next" button. The main content area is titled "Confirmation" and contains the text "Enter your passcode:". Below this is a text input field with the placeholder text "One Time Passcode". Under the input field, the status "Status: Sent" is displayed in green, and the remaining time "Remaining: 01:43" is shown.

4. If the correct OTP is entered, and the user clicks “Next”, the app provisioning completes successfully:



5. The user is now ready to receive encrypted messages using the SMS PASSCODE Mobile 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 SMS PASSCODE Mobile app will automatically open, decrypt the received message and show it to the user.

21.1.2 System Requirements for the SMS PASSCODE Mobile App

The plugin for the SMS PASSCODE Mobile app is automatically installed as part of an SMS PASSCODE installation.

System requirements for the SMS PASSCODE Mobile app itself:

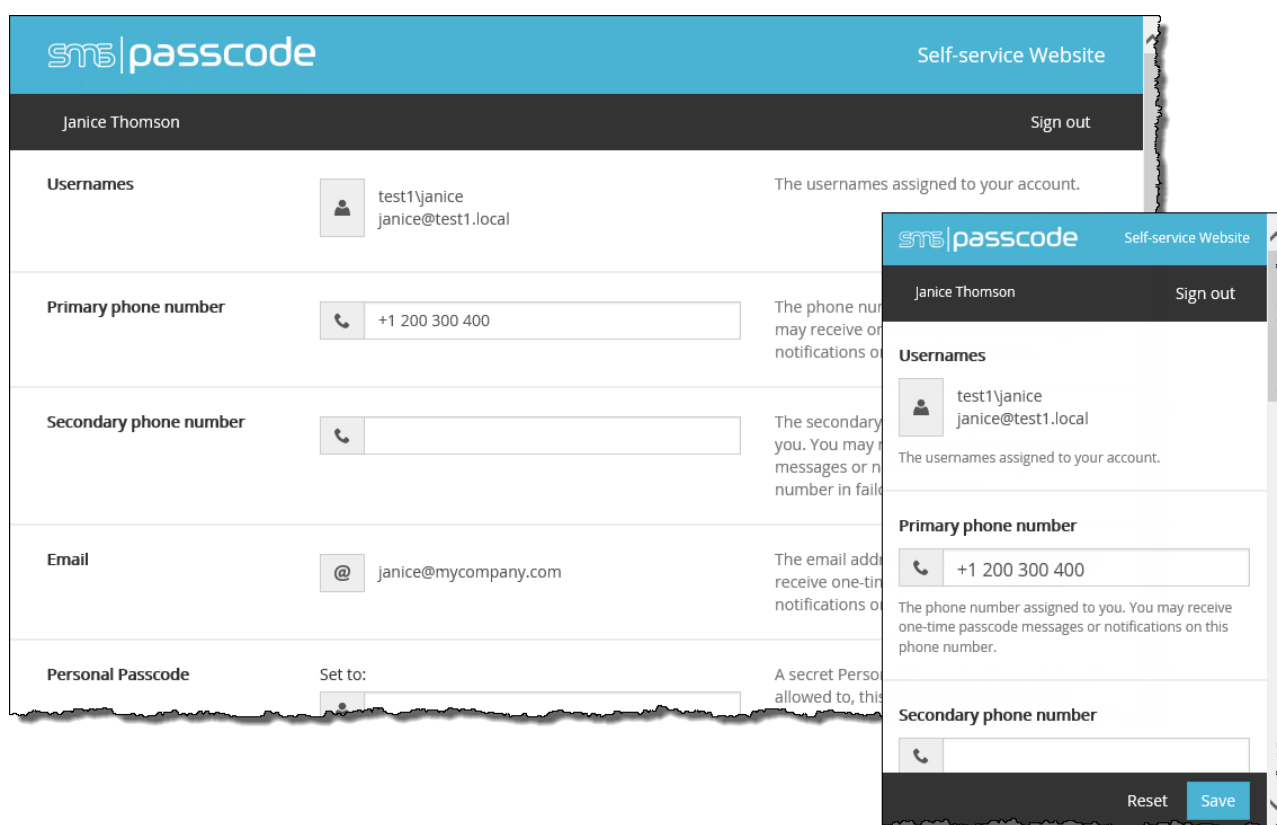
- Must be installed on a smartphone
- Supported on iOS, version 9.3 or later.
- Supported on Android, version 4.0.3 or later

22 SELF-SERVICE WEBSITE

NOTE: This section only applies to SMS PASSCODE installations in the **On-premise** or **Hybrid Setup**.

The SMS PASSCODE **Self-service Website** is an optional component. When installed, end-users can log in to this website to inspect or maintain settings regarding their own SMS PASSCODE user account. It is only recommended to install the Self-service Website if you are planning to let some or all of your end-users maintain SMS PASSCODE user account data themselves.

The Self-service Website uses a modern, responsive web design, which allows it to render nicely on both desktop browsers and smartphone screens.



IMPORTANT (AD accounts only)

Only AD user accounts can access the SMS PASSCODE Self-service Website (either created manually in the SMS PASSCODE database or imported using a User Integration Policy with **Directory type** set to **Active Directory**).

22.1 Examples of Usage

The SMS PASSCODE Self-service Website can be very useful in a number of different scenarios. For example:

- Initially, when installing SMS PASSCODE for the first time, you will need to have access to the (mobile) phone numbers of your end-users. If these phone numbers are already stored in your AD, or in a CSV file, you can simply make use of SMS PASSCODE **User Store Integration**, or import the data from the CSV file, respectively. However, if the phone numbers are not registered anywhere yet, you can decide to let the end-users enter their phone numbers by themselves using the SMS PASSCODE Self-service Website.
- Let new end-users register their phone numbers by themselves.
- Let end-users maintain their phone numbers in case they get a new phone number.
- Let end-users choose their **Dispatch Policy** by themselves. For example, you can let your users select by themselves, whether they want to receive passcodes by SMS, email or voice call.
- Let end-users enter their personal passcode. A personal passcode can be used for authentication in case of emergency or to reset the user's AD password using the SMS PASSCODE Password Reset Module.
- Let end-users enroll their tokens by themselves (in case you are making use of tokens, e.g. OATH software tokens or USB Keys).
- Let end-users maintain their private (secondary) mobile number or private email address, in case these are used for failover scenarios.

As can be seen, the Self-service Website allows for a lot of end-user flexibility. As an administrator, you can control in detail, whether you want to provide this flexibility to your end-users, and what permissions you want to grant them. You can control in detail:

- Who is allowed to access the Self-service Website
- What settings each user is allowed to change

This is controlled using **User Group Policy** settings (cf. section 17.6.1.2, page 163), but can also be set on each individual user by overriding the UGP settings (cf. section 17.10.1.3, page 243).

22.2 Self-service Notifications

To access the SMS PASSCODE Self-service Website, your end-users will need to know the URL to use. An easy way to provide this is to use SMS PASSCODE **Self-service notifications**. When enabled, SMS PASSCODE will automatically send welcome notifications including the URL of the Self-service Website to any new end-users. Additionally, reminder notifications can be enabled, which will automatically remind end-users, if they should forget to log in to the Self-service Website and enter any data defined as **mandatory** by the system administrator.

Self-service notifications are enabled on the **Notifications** tab on the **User Group Policy** maintenance page (cf. section 17.6.1.3.1, page 168). Among others, you may customize the content of welcome and reminder notifications to contain the information, which you would like to distribute automatically to your end-users.

22.3 Data Updates

When a user changes any personal settings in the Self-service Website, the changes are either written back to the SMS PASSCODE database or written directly back to the AD to which the user belongs. The following rules determine where an update will occur:

- If a user has been created manually in the SMS PASSCODE database, then any changes made by the user will be written to the SMS PASSCODE database, since the user is not part of any AD synchronization in this case.
- If a user has been imported from an AD by the SMS PASSCODE **User Store Integration** feature, using **User Integration Policies** (cf. section 17.5, page 126), then the following rules apply:
 - a. Any data NOT imported from the AD, will be updated in the SMS PASSCODE database, in case the user changes any such data. Examples of this are: Dispatch Policy, SMS type and user attributes set to “Do not import” in the user’s **User Integration Policy** (cf. section 17.5.4.3, page 140).
 - b. Any data imported from the AD, will be updated directly in the AD, in case the user changes any such data. The user attributes imported from AD, are the ones defined as “Import from attribute(s)” in the user’s **User Integration Policy** (cf. section 17.5.4.3, page 140).

22.4 Security Concerns

The SMS PASSCODE Self-service Website is configured to listen on TCP port 3000 by default, but you can also select any other TCP port during the installation. You should NOT make the Self-service Website available from outside your firewall. It is only recommended to make the site available on your internal network, since you could otherwise compromise³⁸ the multi-factor authentication security provided by SMS PASSCODE. If you insist to make the Self-service Website available from outside your firewall, then please ensure that it is well protected, e.g. by configuring it to use Integrated Windows Authentication and protecting it with SMS PASSCODE multi-factor authentication using the SMS PASSCODE IIS Website Protection component.

WARNING: It is NOT recommended to publish the SMS PASSCODE Self-service Website and make it publicly available.

In case you follow the recommendation above and do not publish the SMS PASSCODE Self-service Site to be publicly available, you might not need to be concerned about the network communication to and from the Self-service Website, depending on your trust in the internal

³⁸ The security could be compromised, in case a hacker would gain access to the Self-service Website and could change the phone number of a user. This would in fact eliminate the essential part of the multi-factor authentication of the user.

network. Nevertheless, in case you have any concerns regarding the network communication, you can take advantage of the following information:

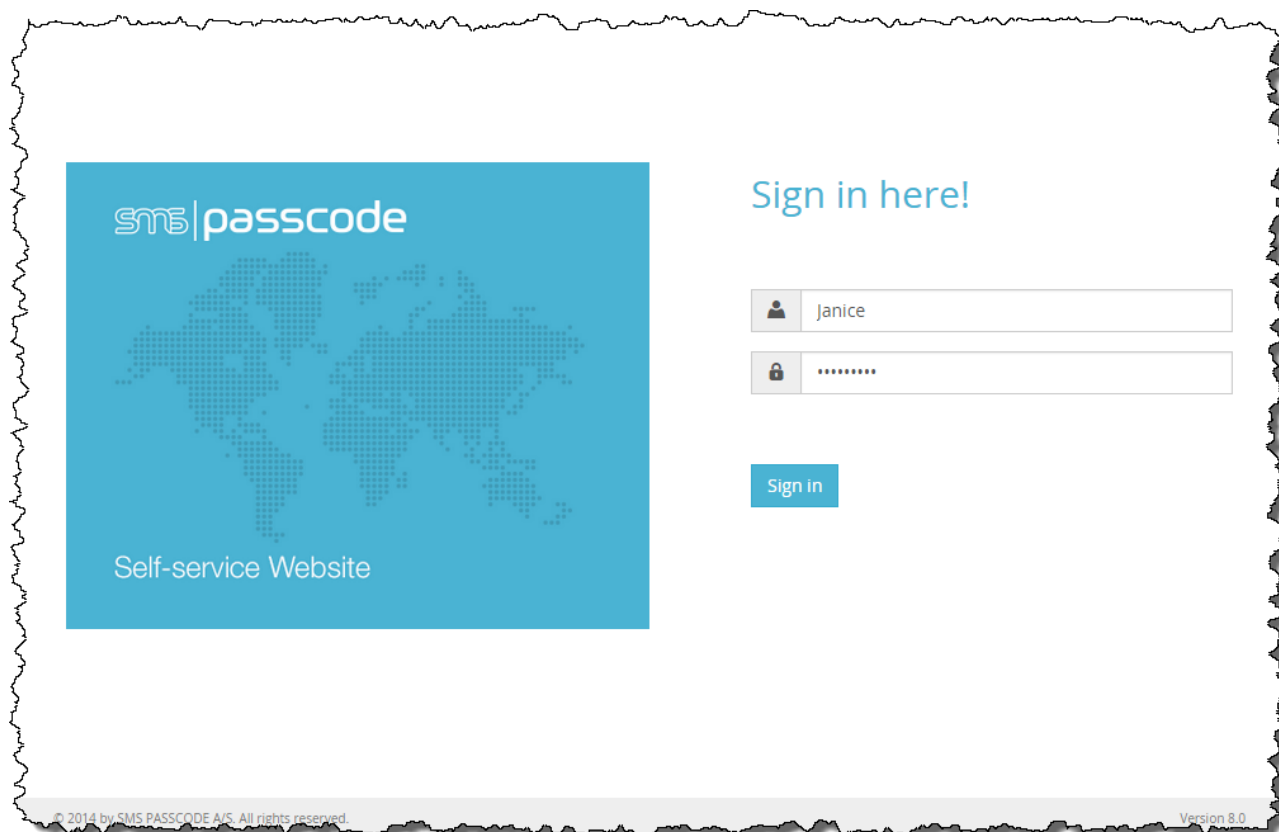
- Referring to section 22.3 above, the Self-service Website will write any data updates either directly to the SMS PASSCODE database and/or to the AD.
 - a. Network communication with the SMS PASSCODE database is always encrypted (using strong AES 256-bit encryption).
 - b. Network communication with the AD is encrypted using SSL/TLS, only if the corresponding user has been imported into the SMS PASSCODE database using a User Integration Policy with the setting “Encrypt communication using SSL” enabled (cf. section 17.5.4.2, page 133).
- Network communication between the end-user and the Self-service Website is only encrypted, in case you install an SSL certificate on the Self-service Website and enforce HTTPS for the site. It is definitely recommended to do so, in case you are planning to use form-based authentication (cf. next section).

22.5 Authentication

The SMS PASSCODE Self-service Website uses Integrated Windows Authentication (IWA) by default but can also be configured to use form-based authentication (FBA). IWA is required if you plan to protect the Self-service Website by SMS PASSCODE multi-factor authentication using the SMS PASSCODE IIS Website Protection component.

When using IWA, depending on the web browser type and configuration, the browser will either show a built-in logon dialog, or log in the user automatically using single sign-on.

When using FBA, a logon form is shown in the web browser for authentication:



You must edit the `web.config` file of the Self-service Website to configure, whether the Self-service Website should use IWA or FBA. The default location of this file is:

```
C:\Program Files\SMS PASSCODE\Web\SelfService\web.config
```

In this file, search for the tag `<system.web>`. Within this tag another tag of type `<authentication mode="...">` controls the type of authentication:

Activating IWA:

```
<authentication mode="Windows" />
```

Activating FBA:

```
<authentication mode="Forms">
    <forms loginUrl="Login.aspx"
           protection="All"
           timeout="30"
           name="SmsPasscodeProtectionAuth"
           enableCrossAppRedirects="false" />
</authentication>
```

You need to remove or comment out the part that should NOT be used. Commenting out is done by putting the characters `<!--` and `-->` around the part to be commented out.

IMPORTANT: When using IWA for the SMS PASSCODE Self-service Website, it is required to enable **delegation** from the server hosting the SMS PASSCODE Self-service Website to all domain controllers, with which the Self-service Website might communicate. Please read section 22.5.1 below for details, on how to set up delegation.

IMPORTANT: When using FBA for the SMS PASSCODE Self-service Website, it is recommended to protect the website using an SSL certificate and only allow access to the site using SSL (HTTPS). This is to ensure that user names and passwords are always sent encrypted across the network.

SMS PASSCODE IIS Website protection can be used together with FBA, however logout URL should be specified. (Please see section 25.4.4.3, page 413).

IMPORTANT (multi-domain infrastructure)

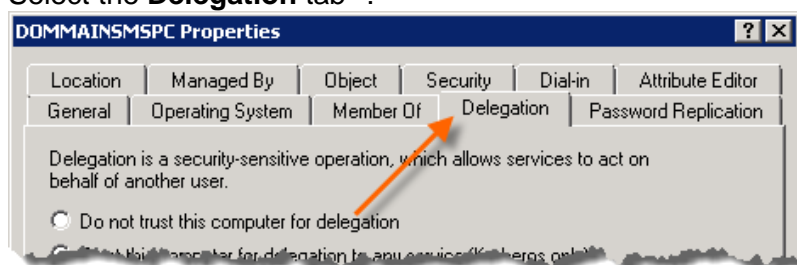
Please note the following for multi-domain scenarios (using child domains and/or trusted domains): When using FBA, an SMS PASSCODE Self-service Website supports authentication of users from multiple domains. When using IWA, an SMS PASSCODE Self-service Website only supports authentication of users from the domain, of which the website host is a member.

22.5.1 Configuring Authentication Delegation

When the Self-service Website is configured to use Integrated Windows Authentication (IWA), and users have been permitted to make changes that are written directly back to the AD, then the Self-service Website needs to be able to forward the authentication context of the user to any of the domain controllers in question. To be able to do so, the server hosting the SMS PASSCODE Self-service Website must be authorized to allow *delegation*.

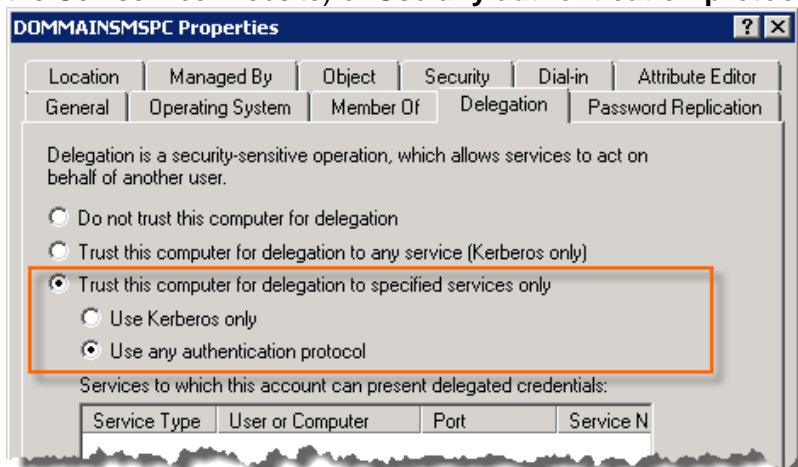
Delegation is allowed by editing the computer account of the Self-service Website server in the AD:

1. In the AD, locate the computer account of the server hosting the SMS PASSCODE Self-service Website.
2. Right-click the computer account and select **Properties**.
3. Select the **Delegation** tab³⁹:

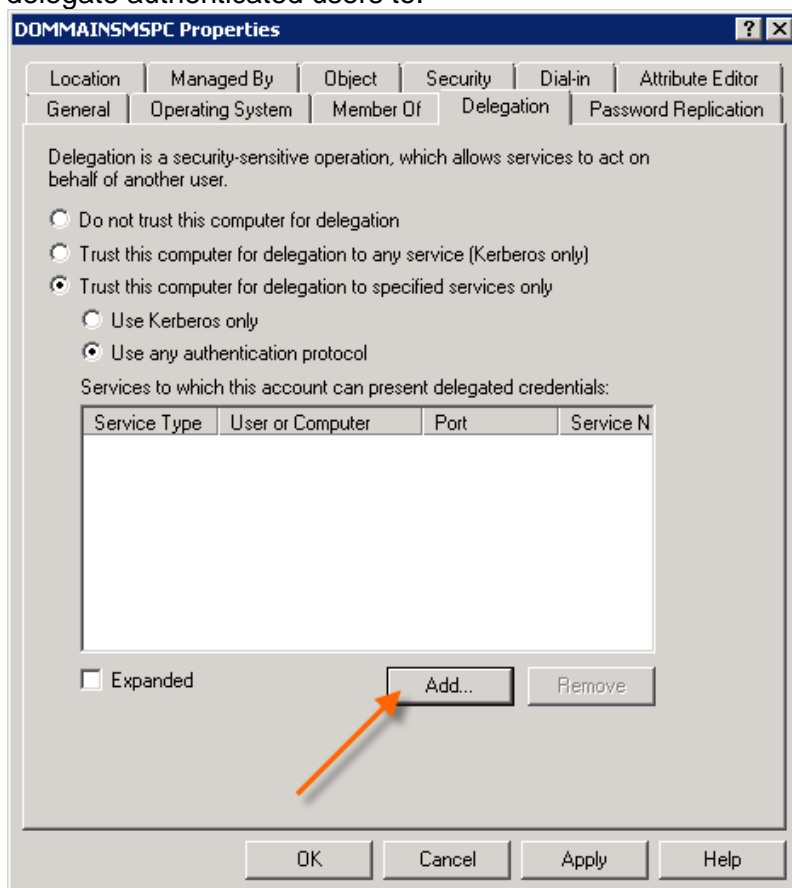


³⁹ If the **Delegation** tab is missing, then the domain functional level needs to be upgraded to at least level "Windows Server 2003" (please read <http://support.microsoft.com/kb/322692> for more details).

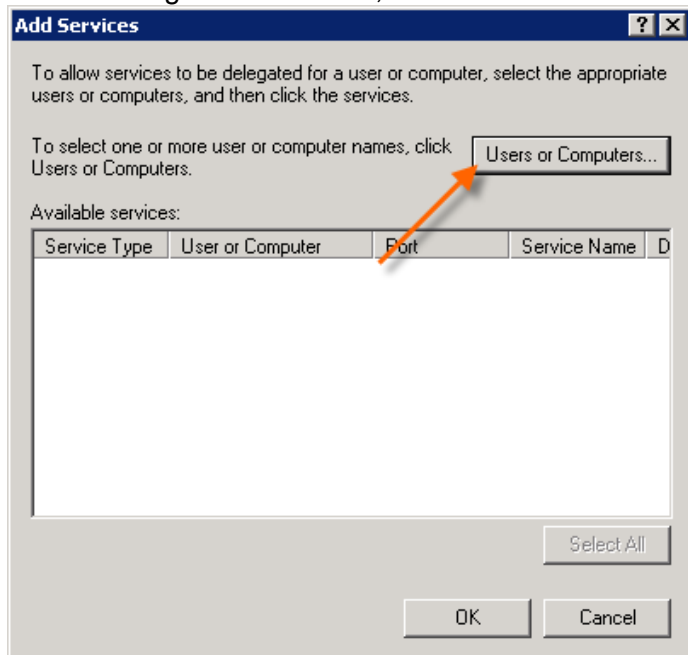
4. Select **Trust this computer for delegation to specified services only**, and select either **Use Kerberos only** (this will only allow domain members with Internet Explorer to access the Self-service Website) or **Use any authentication protocol**:



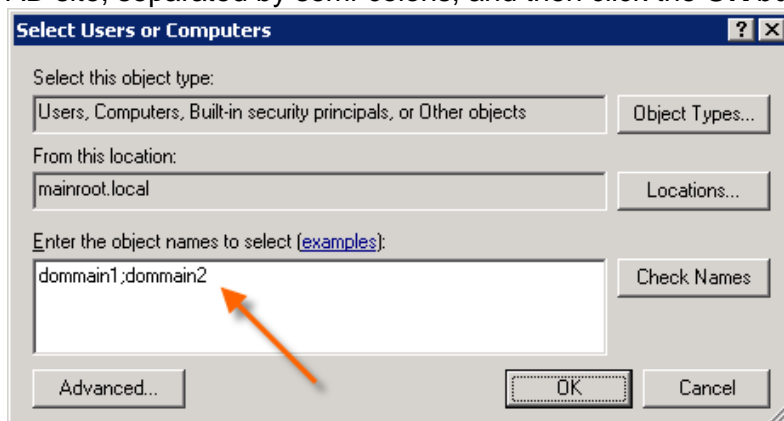
5. Now click the **Add** button to add all relevant domain controllers, that the server is allowed to delegate authenticated users to:



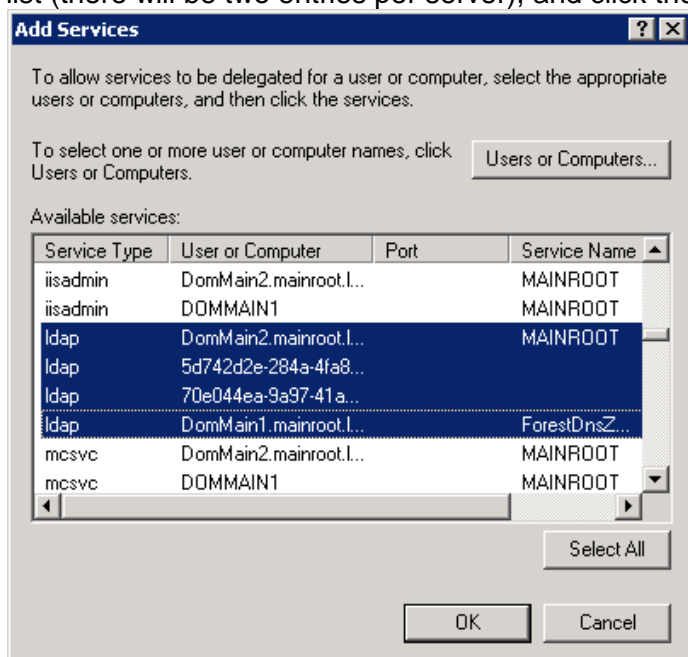
6. On the dialog **Add Services**, click the **Users or Computers...** button:



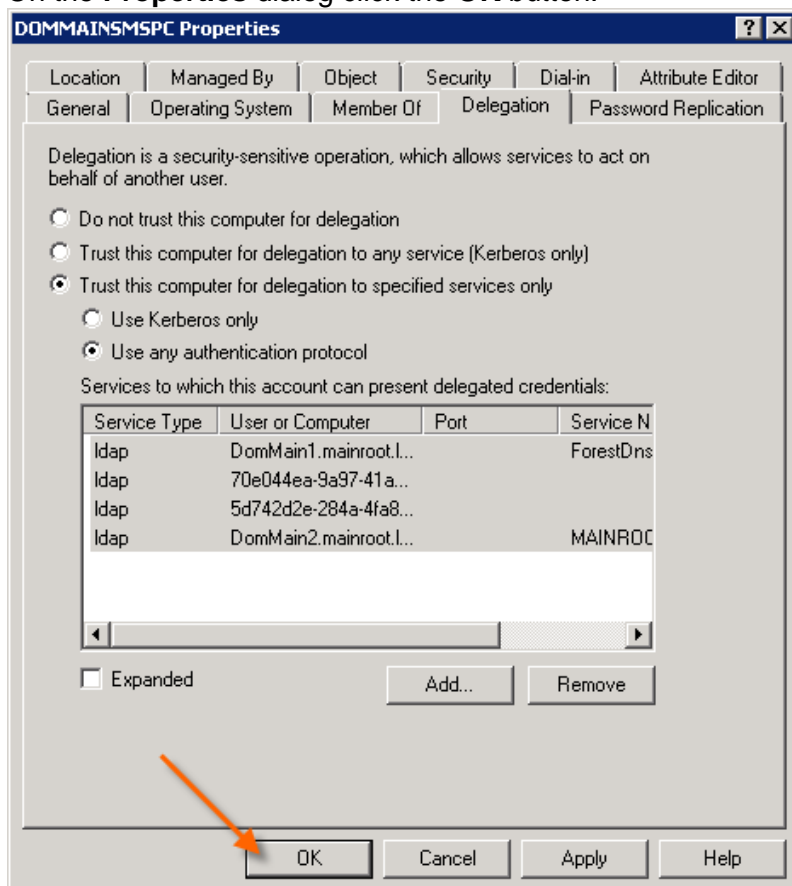
7. On the **Select Users and Computers** dialog, enter all relevant domain controllers of the AD site, separated by semi-colons, and then click the **OK** button:



8. When returning to the **Add Services** dialog, select all ldap protocols of the servers in the list (there will be two entries per server), and click the **OK** button.



9. On the **Properties** dialog click the **OK** button:



10. Delegation has now been configured.

NOTE: In order for the delegation changes to take effect on the Self-service Website server immediately, either reboot the Self-service Website server, or alternatively run the following command on the server:

```
gpupdate /force
```

22.6 Localization

When an end-user accesses the SMS PASSCODE Self-service Website, the site will be displayed in a localized language according to the current language settings of the end-user's web browser. Currently, the following localizations are supported:

- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German
- Hungarian
- Italian
- Korean
- Norwegian
- Polish
- Romanian
- Russian
- Spanish
- Swedish
- Turkish

English is used by default, if no matching localization is found.

23 PASSWORD RESET MODULE

NOTE: This section only applies to SMS PASSCODE installations in the **On-premise** or **Hybrid Setup**.

The SMS PASSCODE **Password Reset Module** allows end-users to log in to a Password Reset Website (PRWS) to reset their own AD Password in a convenient and secure way. This makes it possible for end-users to regain access to applications or network resources, whenever they have forgotten their AD password – without any need to involve internal IT personnel. In this way, the Password Reset Module can reduce the burden on the internal IT helpdesk.

One of the strengths of the SMS PASSCODE Password Reset Module is its ability to send out password reset related **notifications**. These notifications will both remind the user about the possibility to make use of the PRWS and inform how to access it -- two very important factors for getting the most out of a password reset solution. As an administrator, you can optionally enable any of the following types of notifications:

- **SMS PASSCODE lockout notification**
Notify users, when they are locked out from the SMS PASSCODE system, e.g. when they have entered a wrong password several times in a row during authentication in an SMS PASSCODE protected authentication client.
- **AD account lockout notification**
Notify users, when they are locked out in AD, e.g. when they have entered a wrong password several times in a row during authentication in any non-SMS PASSCODE protected application.
- **Password pre-expiration notification**
Notify users a few days before their current AD password will expire.
- **Password expiration notification**
Notify users when their AD password has just expired.

The two first types of notifications, the **lockout notifications**, are especially useful, since they will be triggered in the event that a user enters a series of wrong passwords, which is a typical scenario, when a user has forgotten his password. Additionally, they increase security, since the user is informed about any unexpected lockout, e.g. in case of a brute-force-attack by a hacker.

To preserve high security, access to the PRWS is protected by SMS PASSCODE multi-factor authentication by default. However, it is possible to customize the login flow of the PRWS in several ways, even allowing different login flows depending on the login context. For example, you can allow a more convenient login flow with lowered security, when the login occurs from a trusted context. Login flows are described in section 23.3 (page 337). The actual customization of login flows is accomplished on the Authentication Rules of an Authentication Policy (cf. section 17.8.2.5, page 204).

Recommended User Group Policy for users accessing the Password Reset Website

It is recommended that all users planned to make use of the SMS PASSCODE Password Reset Website are assigned to a UGP with the following settings:

- On the **Notifications** tab:
 - Specify the URL of the PRWS
 - Specify the URL of the SMS PASSCODE Self-service Website (SSWS)
 - Enable all types of notifications
- On the **Self-service Website Settings** tab of the UGP:
 - Allow access to the SSWS
 - Allow users to change their **Personal Passcode** in the SSWS, and set it as mandatory data (i.e. the user is forced to set it)
- On the **License** tab of the UGP:
 - Grant Password Reset CAL

Such a UGP will ensure that the users assigned to it will have a Personal Passcode ready for use, whenever they will need it to log in to the PRWS to reset their AD Password.

Additionally, the notifications will remind the users about the possibility to use the PRWS, and remind them how to access it, by providing a hyperlink directly within the notifications.

The SMS PASSCODE **Password Reset Module** consists of two components: The SMS PASSCODE **Password Reset Website** (PRWS) and the SMS PASSCODE **Password Reset Backend Service** (PRBS). These two components can be installed on the same server or on separate servers. The infrastructure of the Password Reset Module is described in more detail in section 23.4 (page 345).

23.1 Licensing

The SMS PASSCODE **Password Reset Module** requires separate client access licenses (CALs).

IMPORTANT: Password Reset CALs required

Please note, that a user must have been allocated a **Password Reset CAL** in order to:

- Access the PRWS
- Receive an AD account lockout notification, password pre-expiration notification or password expiration notification.

The table in section 9.2, page 30, shows the exact authentication behavior for Password Reset.

23.2 Best-Practice Setup of Password Reset

This section describes the best practice for setting up SMS PASSCODE when using the Password Reset module.

The recommended order of actions is:

1. Open the Web Administration Interface
2. For each User Group Policy (UGP) assigned to users that should have access to Password Reset, ensure the following configuration of the UGP:
 - a. On the **Notifications** tab of the UGP:
 - i. Specify the URL of the PRWS
 - ii. Enable relevant notifications. It is recommended to enable all of them.
 - b. On the **Self-service Website Settings** tab of the UGP⁴⁰:
 - i. Allow access to the Self-service Website (SSWS)
 - ii. Allow users to change their **Personal Passcode** in the SSWS, and set it as mandatory data (i.e. the user is forced to set it)
 - c. On the **License** tab of the UGP:
 - i. Grant Password Reset CAL

Each such UGP will ensure that the users assigned to it will have a Personal Passcode ready for use, whenever they will need it to log in to the PRWS to reset their AD password.

Additionally, the enabled notifications will remind the users about the possibility to use the PRWS and remind them how to access it.

3. In case you enabled **AD Account Lockout** notifications in step 2.a above, then consider lowering the lockout threshold in the password policy of your AD⁴¹. With **AD Account Lockout** notifications enabled it is useful that a user is locked out relatively quickly in AD, in order for the user to receive the notification with the PRWS URL.

23.3 Workflow for Performing a Password Reset

This section describes the possible login flows when accessing the SMS PASSCODE Password Reset Website (PRWS). Essentially, there are three different types of scenarios, when a user would like to access the PRWS:

- The user has forgotten his existing password (and has possibly received a lockout notification).
- The user has received a password pre-expiration notification or password expiration notification and would like to renew his existing password.
- The user has been locked out and would like to unlock his account

There is a fundamental difference between these scenarios. In the first scenario, the user has forgotten his existing password, whereas in the second and third scenario the user has most likely

⁴⁰ You may skip this step, if you are only planning to make use of the "Simple" password reset flow, since personal passcodes are not required in this case (cf. section 23.3.2, page 343).

⁴¹ However, do not lower the lockout threshold in AD below the lockout threshold defined on the users' Authentication Policies (cf. section 17.8.2.2, page 197), in case you are protecting authentication clients with SMS PASSCODE multi-factor authentication.

not forgotten his existing password. This is relevant, because when accessing the PRWS, we would like to secure access using SMS PASSCODE multi-factor authentication, which means asking the user to enter his username, existing password and a one-time-passcode. As can be seen, we have a conflict in the first scenario, since the user must enter his existing password, which he has forgotten. Consequently, the user needs another way of proving his identity. The PRWS requires that the user must enter his **personal passcode** instead. Therefore, to make efficient use of the PRWS, all users should register their own personal passcode beforehand⁴² using the SMS PASSCODE Self-service Website (cf. section 22, page 325). This can be ensured by following the *best-practice* setup described in section 23.2 above.

The default login flow of the PRWS, which is also called the *strict flow*, always requires the user to enter his personal passcode to access the PRWS. This means, even in the case of a renewal of the existing password, when the user remembers his existing password, the user must still use his personal passcode for accessing the PRWS. If you would prefer a different behavior, then read on. It is possible to customize the login flow in several ways, as described below.

To understand the difference between the different login flows, let us first go through the default login flow, i.e. the *strict flow*, and examine how a user will proceed to reset his password. Afterwards, the other login flows are described, and the differences are pointed out.

23.3.1 Strict Flow

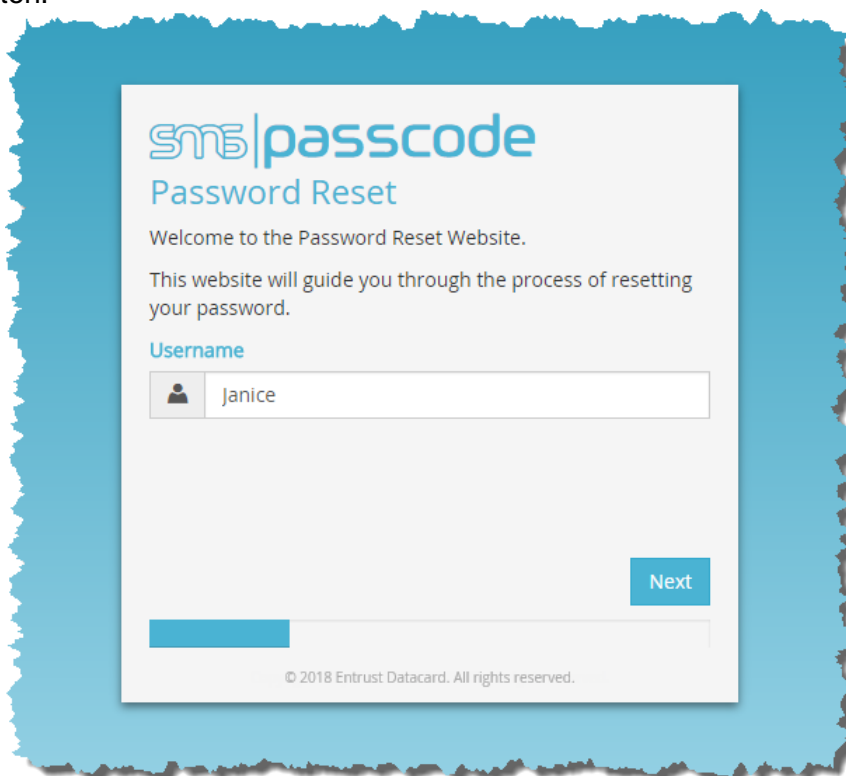
When accessing the PRWS using the *strict flow*, the procedure for performing a password reset is as follows:

1. First, the user opens a web browser and navigates to the PRWS. To do this, the user must know the URL of the site. One way to distribute this knowledge is to enter the PRWS URL into the User Group Policy and then use **Self-service notifications** to distribute it (cf. section 17.6.1.3.1, page 168). Additionally, the user is reminded about the PRWS URL, whenever she receives any of the other notifications enabled on the User Group Policy.

Note: If the user receives the notification containing the PRWS URL on a device with a browser, the easiest way to perform a password reset is just to click the URL and access the PRWS directly on the device. The PRWS has been designed with a modern, responsive web design, meaning that it will automatically adapt to the actual screen resolution, including small screen resolutions as seen on mobile devices.


⁴² An alternative is to import personal passcodes from AD for all users (via User Integration Policies), if any data suitable for personal passcodes is available, e.g. an employee number or social security number.

2. The PRWS opens and shows the welcome page. The user enters her user name and clicks the **Next** button:



The screenshot shows a web interface for 'sms|passcode Password Reset'. The header includes the logo and title. Below the title, a welcome message states: 'Welcome to the Password Reset Website. This website will guide you through the process of resetting your password.' A 'Username' label is followed by a text input field containing 'Janice'. A blue 'Next' button is positioned to the right of the input field. At the bottom, there is a progress bar and a copyright notice: '© 2018 Entrust Datacard. All rights reserved.'

3. Now the user must enter her personal passcode to prove her identity, and then click the **Next** button:



The screenshot shows the same web interface as the previous one, but with an additional 'Personal passcode' section. Below the 'Username' field, there is a 'Personal passcode' label and a text input field with a lock icon and masked characters '.....'. A 'Cancel' button and a blue 'Next' button are located to the right of the passcode field. The progress bar and copyright notice remain at the bottom.

4. A one-time passcode (OTP) is sent to the user according to the Dispatch Policy assigned (e.g. by SMS, voice call or secure email). The user receives the OTP and enters it to complete the multi-factor authentication, then clicks the **Next** button:

sms|passcode
Password Reset

Please authenticate using the one-time passcode sent to you.

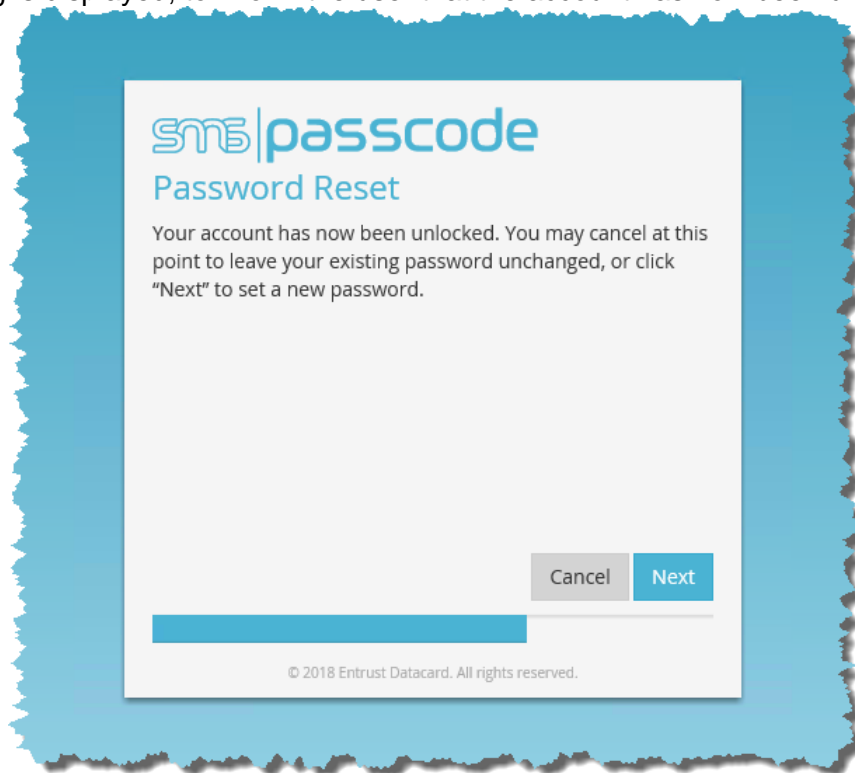
Username

Passcode

Status: **Sent**
Remaining: 00:00:43

© 2018 Entrust Datacard. All rights reserved.

5. Only in case the user's account was currently locked out in SMS PASSCODE or AD, then the following is displayed, to inform the user that the account has now been unlocked:



6. The user has now proven her identity and can reset her password, i.e. enter a new AD password. When the new password has been entered, the user clicks the **Next** button:



The screenshot shows a web interface for password resetting. At the top is the logo 'sms|passcode' and the title 'Password Reset'. Below this is a message: 'You have been granted access. Please choose a new password now.' The form contains three sections: 'Username' with a field containing 'Janice', 'New password' with a field containing seven dots, and 'Confirm password' with a field containing seven dots. At the bottom right are 'Cancel' and 'Next' buttons. A blue progress bar is at the bottom, and the footer reads '© 2018 Entrust Datacard. All rights reserved.'

7. If the new AD password fulfills all password policies, the user will get a success message:



The screenshot shows the same web interface as before, but with a success message: 'Your password has been changed successfully.' The 'Username' field still contains 'Janice'. The 'New password' and 'Confirm password' fields are now empty. At the bottom, there is a 'Completed' label above a full blue progress bar. The footer reads '© 2018 Entrust Datacard. All rights reserved.'

Note: In case the new password is rejected by the AD, e.g. due to password policy restrictions, the user will be given the chance to enter a new password again, until the password reset succeeds

8. The password has now been reset. The user can close the browser and use the new AD password.

23.3.2 Other Login Flows

The previous section described the default login flow of the PRWS, called the *strict flow*. As an administrator, you may configure the PRWS to use a different login flow. The possible flows are:

- *Strict flow*
- *Flexible flow*
- *Simple flow*

In addition to this, if *MFA bypassing* has been allowed on the **General Settings** page (cf. section 17.3.2, page 110), then you may also enable MFA bypassing on the PRWS. In total, this offers five different login flows, from which to choose:

Access	Strict Flow	Flexible Flow	Simple Flow
Allow access, use MFA	To authenticate, the user must enter: <ul style="list-style-type: none"> • Username • Personal passcode • OTP 	To authenticate, the user must enter: <ul style="list-style-type: none"> • Username • Existing password <u>or</u> personal passcode • OTP 	To authenticate, the user must enter: <ul style="list-style-type: none"> • Username • OTP
Allow access, bypass MFA	To authenticate, the user must enter: <ul style="list-style-type: none"> • Username • Personal passcode 	To authenticate, the user must enter: <ul style="list-style-type: none"> • Username • Existing password <u>or</u> personal passcode 	- (this combination is not allowed)
Deny access	Access is denied		

The **Access** and **Password reset flow** settings are set on the Authentication Rules of the user's Authentication Policy (cf. section 17.8.2.5, page 204). This means that you can define different login flows for different login contexts. As an example, you could use the *simple flow* when a user accesses the PRWS from a trusted location (e.g. internal LAN or trusted IP), and use the *Strict* or *Flexible* flow otherwise.

When *Flexible flow* is enabled, the user will see the following page, after having entered her username on the initial welcome page:



As shown, in this case the user can either enter her existing password, or alternatively click the **“I have forgotten my password”** link. If the link is clicked, then the user will jump to the page requesting the user to enter her personal passcode, similar to the *strict flow*.

Consequently, it only makes sense to use the *flexible flow*, if you are expecting your users to access the PRWS using their existing password in some cases. This will normally only be the case, if you have enabled password pre-expiration or password expiration notifications.

In case of the *simple flow*, the user can access the PRWS without entering any password or personal passcode at all, which is very convenient. However, please note that this comes at the cost of lowered security. If a user loses her device to a malicious person, this person then only needs to know the user's username to reset the password, thereby gaining access to all applications that the user has access to!

SECURITY WARNING!

Lowering the security for accessing the PRWS lowers the security for accessing all other applications protected by the user's AD password!

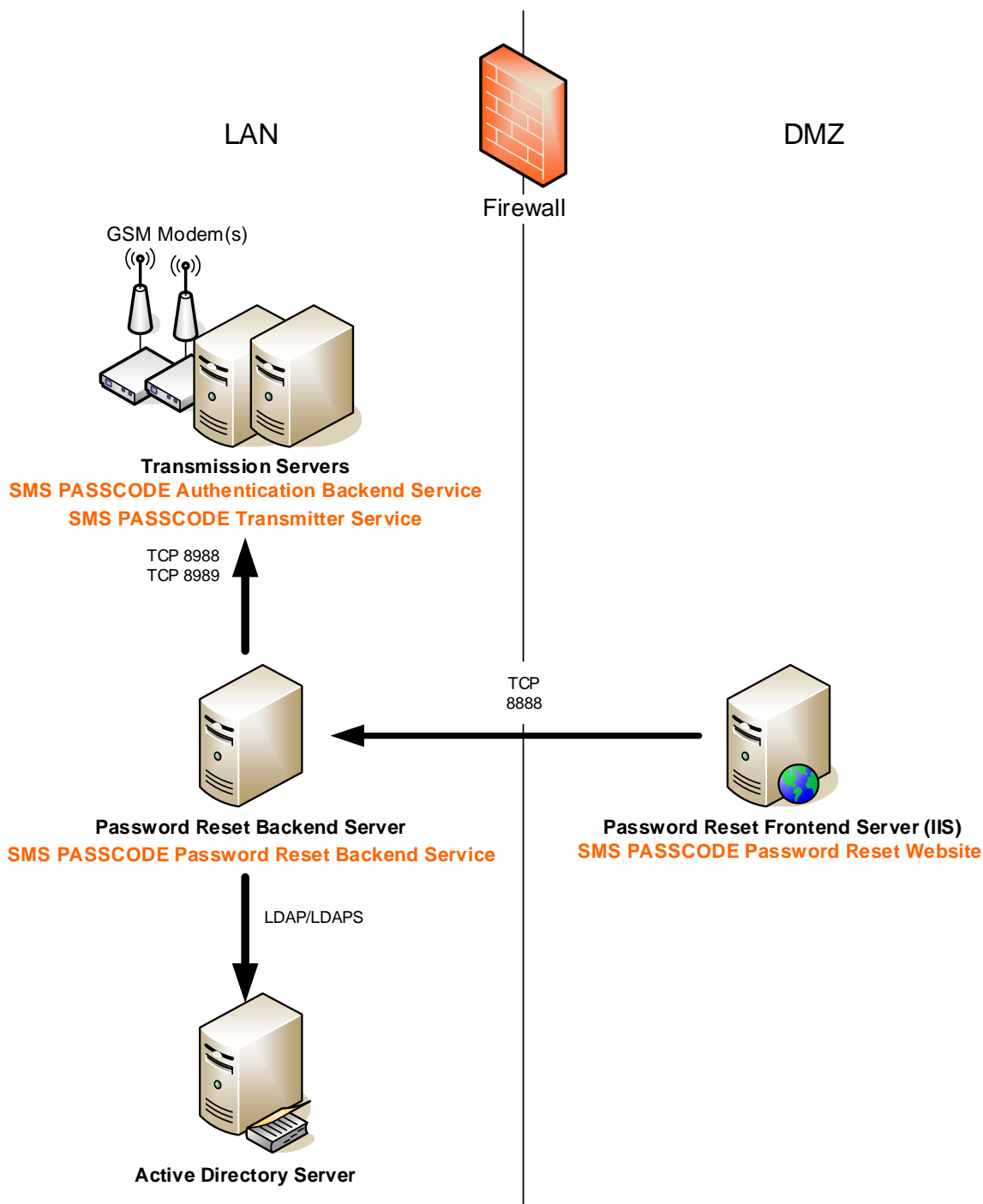
23.4 Password Reset Infrastructure

As mentioned previously, the SMS PASSCODE **Password Reset Module** consists of two components: The SMS PASSCODE **Password Reset Website** (PRWS) and the SMS PASSCODE **Password Reset Backend Service** (PRBS).

The PRWS is a website that provides the frontend of the Password Reset module; i.e. it provides a user interface that allows users to walk through the workflow of changing their own AD password.

Since the PRWS will typically be installed in a DMZ, at least if users are allowed to perform a password reset remotely, it makes sense to separate the website from the actual password reset logic, which should be as well-protected as possible. Therefore, the actual password reset logic is implemented by a separate service: The SMS PASSCODE **Password Reset Backend Service** (PRBS). This service is responsible for performing the actual password reset actions, including communication with the relevant domain controllers.

The separation of the PRWS and PRBS allows you to install the PRWS in a DMZ, while the PRBS can be installed behind the firewall (on the LAN side). An example of such a multi-server setup is shown in the following diagram:



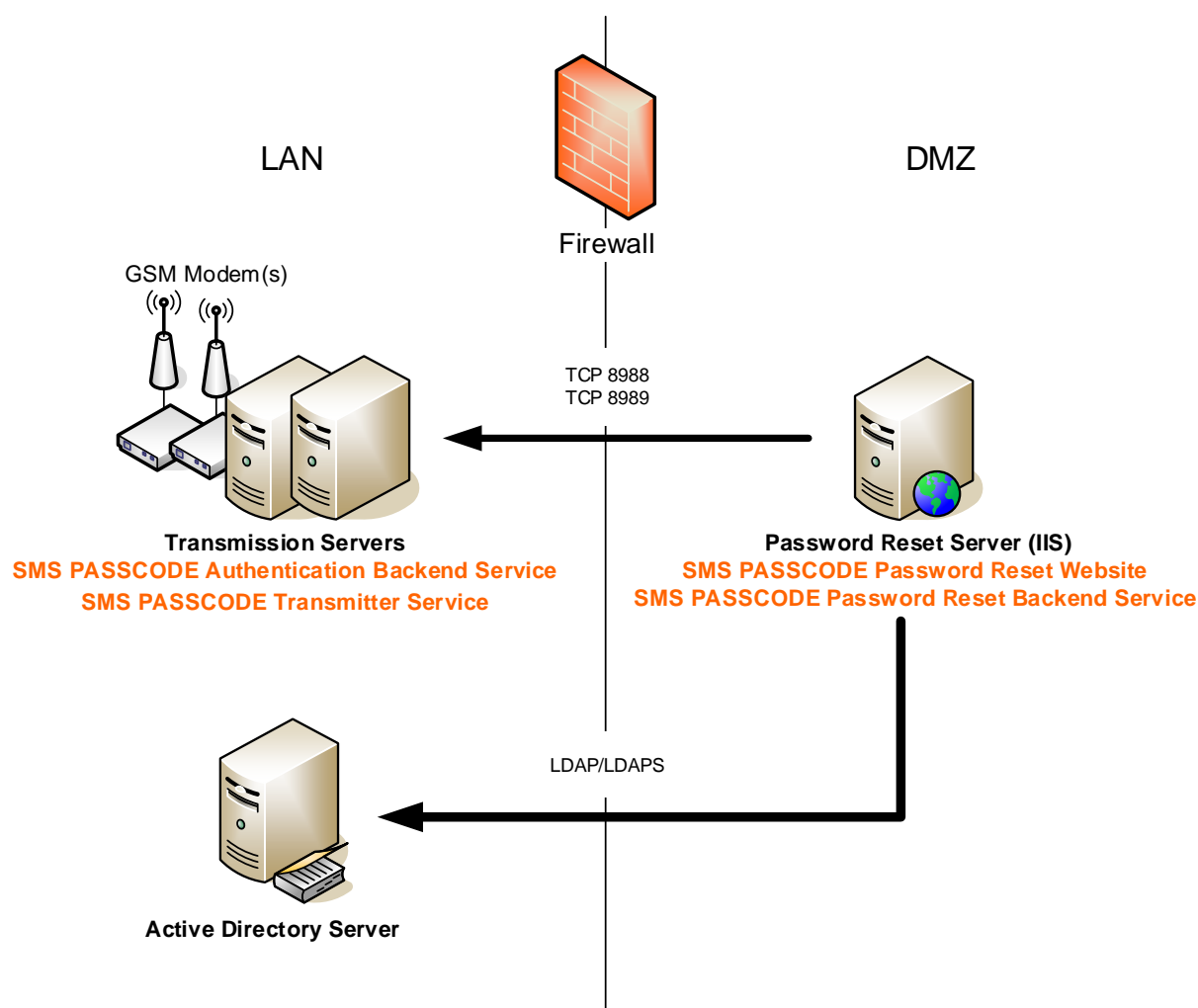
Password Reset multi-server setup (best practice)

As can be seen from this diagram, the PRWS communicates with the PRBS on a single TCP port (TCP port 8888 by default, but configurable), which must be opened from the DMZ to the LAN. The PRBS communicates with the SMS PASSCODE transmission infrastructure through SMS PASSCODE Authentication Backend Services (TCP port 8988 by default). Additionally, the PRBS is responsible for the communication with the relevant domain controllers, when performing the actual password resets, using either LDAP or secure LDAP (LDAPS), depending on the

configuration in the SMS PASSCODE Configuration Tool (cf. section 23.7.2.1, page 357). The remaining part of the SMS PASSCODE backend infrastructure, e.g. the SMS PASSCODE Database Service and SMS PASSCODE Web Administration Interface, is not shown in the diagram, since the PRBS does not depend directly on these components (please read section 11, page 43, for an overview regarding the complete SMS PASSCODE backend infrastructure).

The diagram above illustrates the recommended setup of the SMS PASSCODE Password Reset Module. It is not required to install the PRBS on a dedicated server, i.e. you can just as well install it on one of the servers hosting any SMS PASSCODE core components.

The SMS PASSCODE Password Reset Module provides full flexibility regarding the infrastructure needed, i.e. you can install it in many ways. For example, if you wish, you can install the PRWS and PRBS components on the same server. You may also install the PRWS and PRBS components multiple times on several servers. Each PRBS can handle requests from several Password Reset Websites, but each PRWS can point to one dedicated PRBS only. The diagram below illustrates a single-server setup of the Password Reset Module:



Password Reset single-server setup (not recommended)

The single-server setup is not recommended, except if you place the Password Reset Server on the LAN side, in case you only want internal users to have access to the Password Reset functionality.

Configuration of the Password Reset components, PRWS and PRBS, is performed using the SMS PASSCODE Configuration Tool. This is described in more detail in sections 23.6 (page 349) and 23.7 (page 350).

23.5 Security Concerns

The subsections below address several security concerns regarding the Password Reset Module. Please read these sections carefully.

23.5.1 Publishing the Password Reset Website

Since the PRWS is protected by SMS PASSCODE multi-factor authentication, it is safe to publish the site for external access. The advantage of doing so is that users will be able to reset their password even in remote access scenarios. An important pre-requisite is of course that all users' Personal Passcodes are well-protected and kept private.

Note:

- Unlike the PRWS, it is not recommended to publish the Self-service Website for public access, cf. section 22.4, page 327.
- It is recommended to install the PRWS in a DMZ, and to install the PRBS behind the firewall (on the LAN side), cf. section 23.4 (page 345).

23.5.2 Protecting the Password Reset Website with SSL/TLS

Since the PRWS uses form-based authentication, it is very important that the site is protected using SSL/TLS to ensure, that all credentials are transferred encrypted. Always remember to install an SSL certificate for the PRWS before making use of the site.

IMPORTANT

For security reasons the PRWS has been designed to require SSL/TLS encryption. Therefore, the PRWS will NOT work before an SSL certificate has been installed for the site and HTTPS has been enabled successfully.

23.5.3 Encryption of the Network Communication with the AD Controller

Whenever a user requests a password reset, the actual action of resetting the password is performed by sending an LDAP request from the PRBS to an AD Controller. It is recommended to protect this network communication using SSL/TLS. SSL/TLS encryption is enabled using the SMS PASSCODE Configuration Tool as described in section 23.7.2.1 below.

23.5.4 Protecting the Password Reset Module against Attacks

The PRWS might be a target for *Brute-force* or *Denial-of-Service attacks*. To protect against such attacks, both the PRWS and PRBS will continuously monitor all attempts to access the site and will take appropriate actions, whenever any unusual behavior is observed. These defensive actions are either to restrict the access to the PRWS and/or to send alerts to selected administrators. The configuration of these actions is performed using the SMS PASSCODE Configuration Tool as described in section 23.7.2.2 below.

23.6 Configuring the Password Reset Website

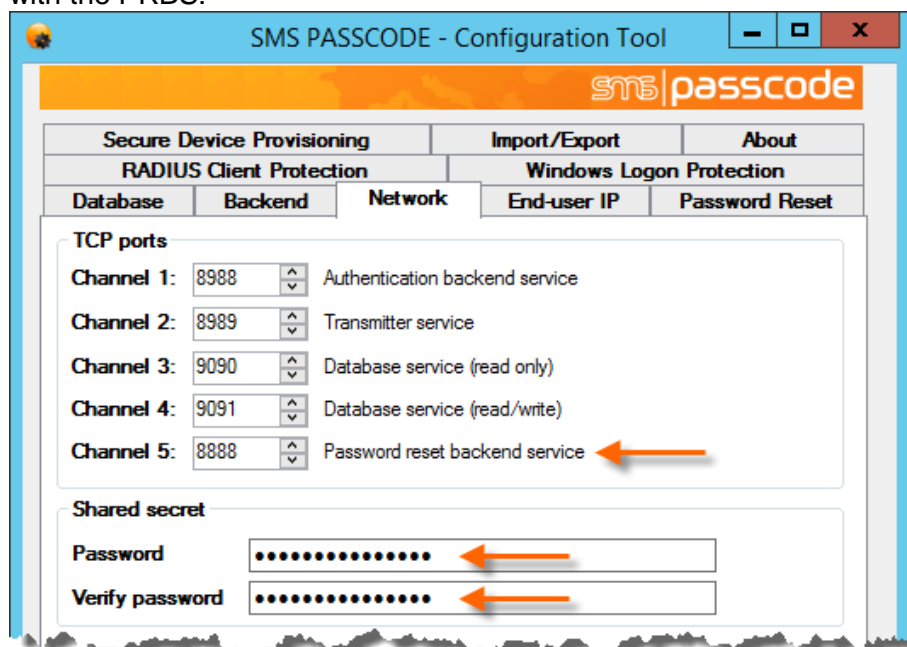
Before taking the PRWS into use, please complete the following actions in the specified order:

1. Configure communication with the PRBS in the SMS PASSCODE Configuration Tool.
This is described in section 23.6.1 below.
2. Protect the PRWS using an SSL certificate.
This is described in section 23.6.2, page 350.

23.6.1 Configure Communication with the Password Reset Backend Service

For the PRWS to work, communication with a PRBS must be configured. This is configured using the SMS PASSCODE Configuration Tool; either when it pops up during installation of the PRWS, or alternatively by starting it manually afterwards (cf. section 25.5.5, page 420). The Configuration Tool contains two tabs that are relevant for setting up the PRBS communication:

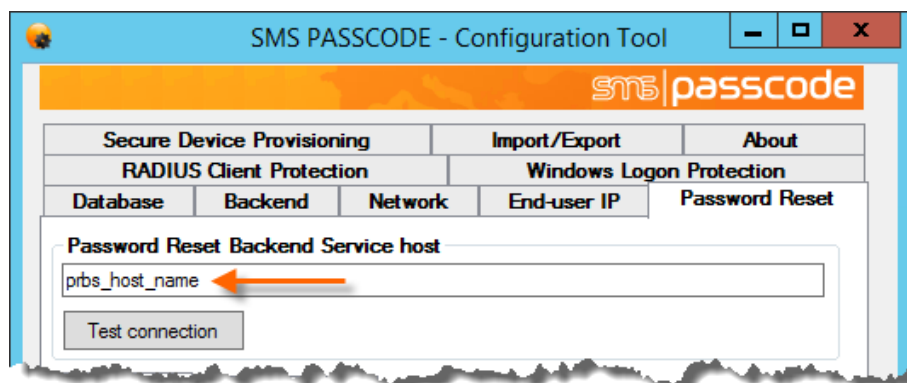
1. On the **Network** tab, specify the TCP port and Shared Secret to use for communication with the PRBS:



IMPORTANT:

The **TCP port** and **Shared Secret** must match the entries entered in the Configuration Tool on the PRBS host; otherwise, communication with the PRBS will fail (cf. section 23.7.2.3, page 361).

2. On the **Password Reset** tab, specify the name or IP address of the server hosting the PRBS:



In case the PRBS is already installed and configured on the target host, you can click the **Test connection** button to verify whether the PRWS is able to communicate with the PRBS⁴³.

23.6.2 Protect the Password Reset Website using SSL/TLS

To protect the PRWS using SSL/TLS, you must install an SSL certificate on the SMS PASSCODE Password Reset Website in the IIS Manager. This is a standard IIS management task. Several guides for this exist on the internet, e.g. <http://support.microsoft.com/kb/299875> or <http://learn.iis.net/page.aspx/144/how-to-set-up-ssl-on-iis-7-and-above>.

After having installed the SSL certificate successfully, please check that you can access the home page of the PRWS using HTTPS. It might only be the home page itself that will work at this stage. To make the PRWS fully functional, you must also ensure that the PRBS has been installed and configured as described in the next section.

23.7 Configuring the Password Reset Backend Service

Before taking the PRBS into use, please complete the following actions in the specified order:

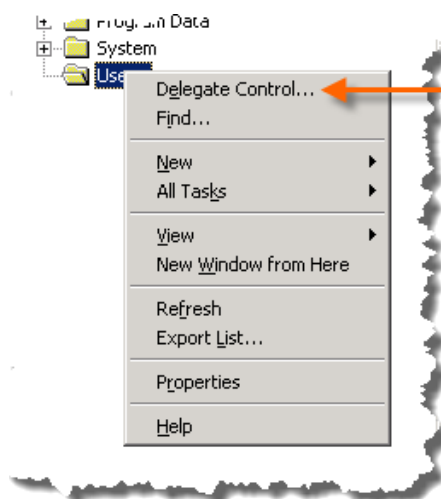
1. Set up a dedicated user account in your AD to be used for performing password resets. This is described in section 23.7.1 below.
2. Configure Password Reset settings in the SMS PASSCODE Configuration Tool. This is described in section 23.7.2, page 357.

⁴³ The **Test connection** button is not available, if the Configuration Tool was started automatically during installation of the PRWS, and the PRBS is installed on the same host; this is because the Configuration Tool knows in this case, that the PRBS has not been started yet, i.e. the connection test is known to fail.

23.7.1 Setting Up a Dedicated User Account for Password Reset

To be able to perform password resets on your behalf, the SMS PASSCODE Password Reset Module must be given the credentials of a user who has been delegated password reset rights. It is recommended that you create a dedicated user account for this. Please proceed as follows:

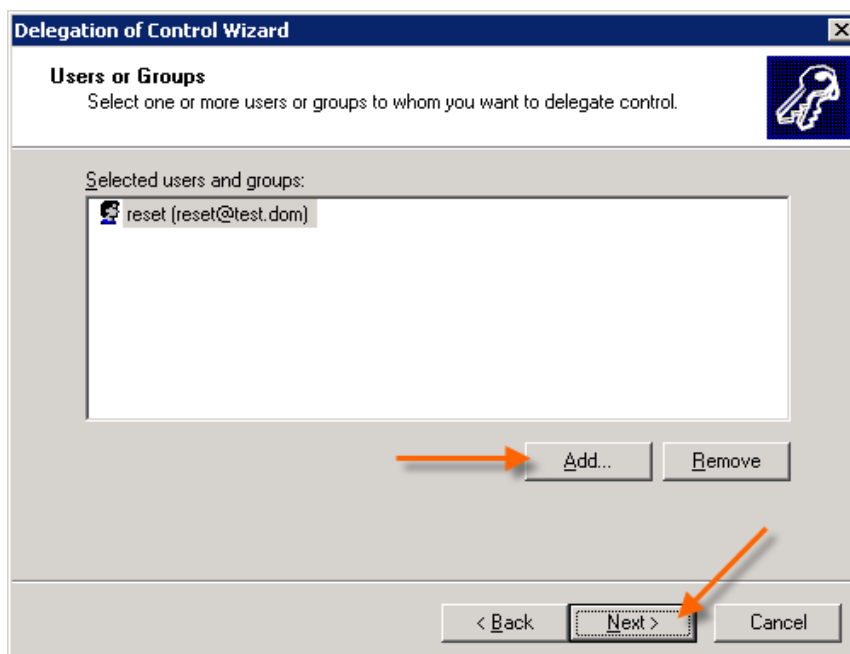
1. Create a new user account in your AD. For example, call it “SMSPC Password Reset User”. This user is called the *Password Reset Account* below.
2. Configure the *Password Reset Account* to have permission to reset the password of all users that are granted access to any PRWS connected to the PRBS. To do so, you must open the **Active Directory Users and Computers** management console for your AD and then locate the nodes (OUs) that contain the relevant users. For each such node, the *Password Reset Account* must be assigned the permission to reset passwords of the users contained in the node. Due to inheritance, you do not need to assign this permission explicitly to each node. You can either assign the permission to the top-level node of the domain, or for better control assign the permission to the topmost OUs containing the relevant users directly or indirectly. Either way, to assign the permission to the relevant node(s), repeat the following actions for each such node:
 - a. Right click the node and select “Delegate Control...”



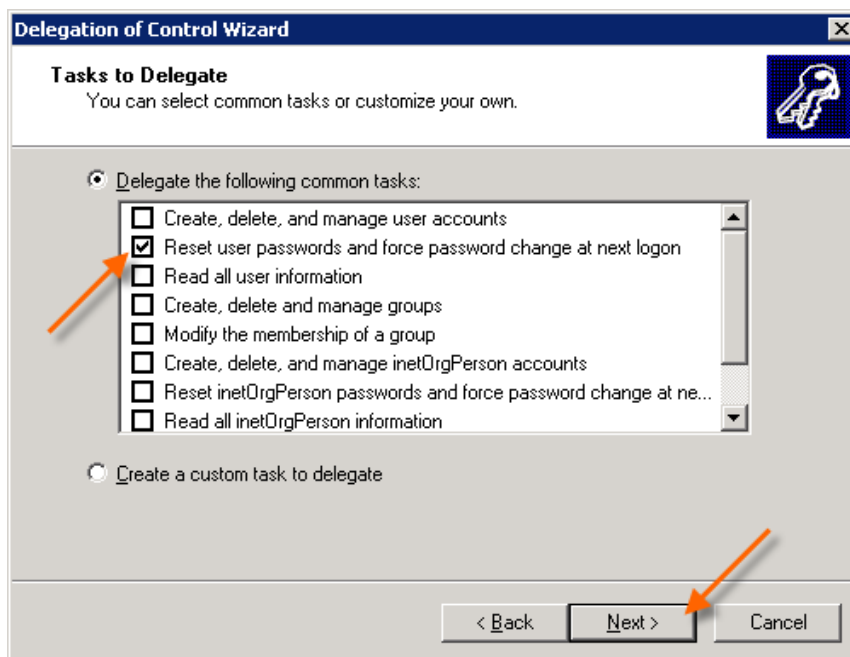
- b. The **Delegation of Control Wizard** dialog appears. Click **Next**.



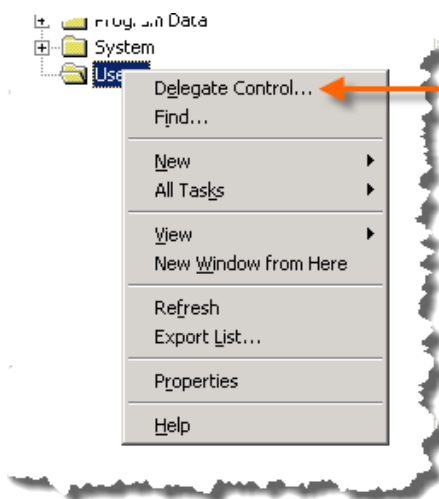
- c. A list appears where you must add the user that was created in step 1. Click the **Add...** button, add the user, and then click **Next**.



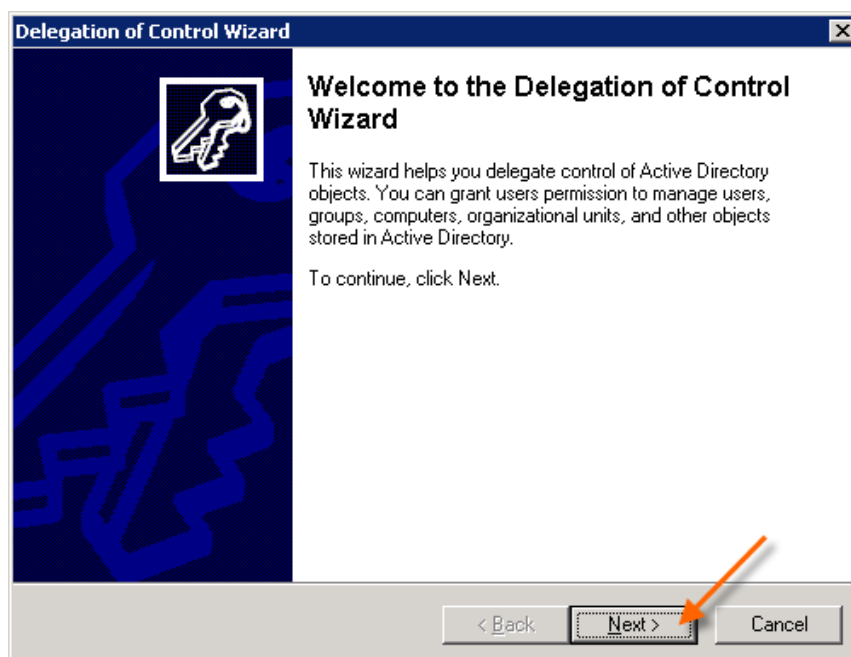
- d. Now select the option **Reset user passwords and force password change at next logon** and click **Next**.



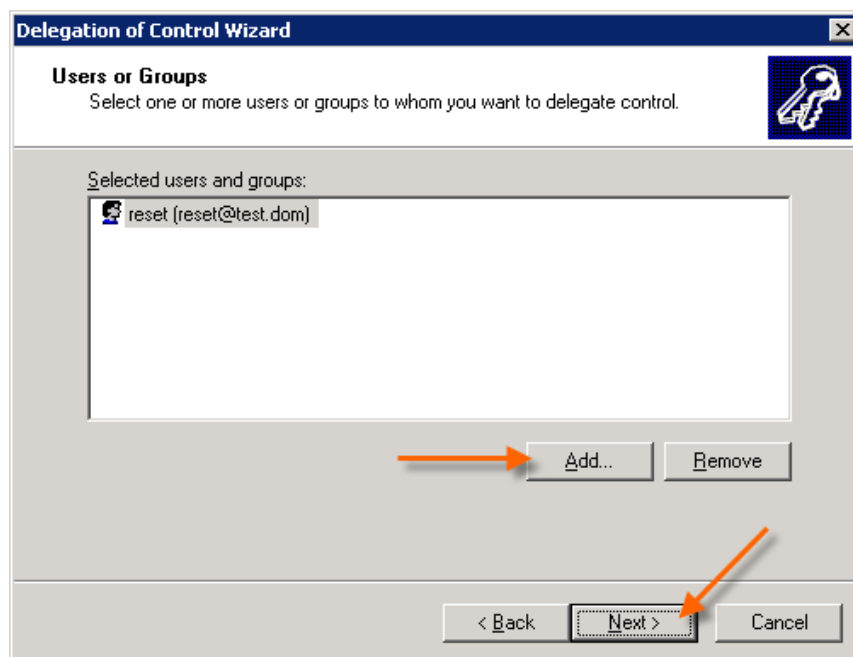
- e. On the final dialog, click **Finish**.
- f. The *Password Reset Account* has now been assigned the right to reset passwords of all users in the selected node. By default, the user will have this right for the node itself and the complete sub tree (all child OUs) as well, except branches where inheritance has been disabled.
- g. Right click the same AD node and select "Delegate Control..." again:



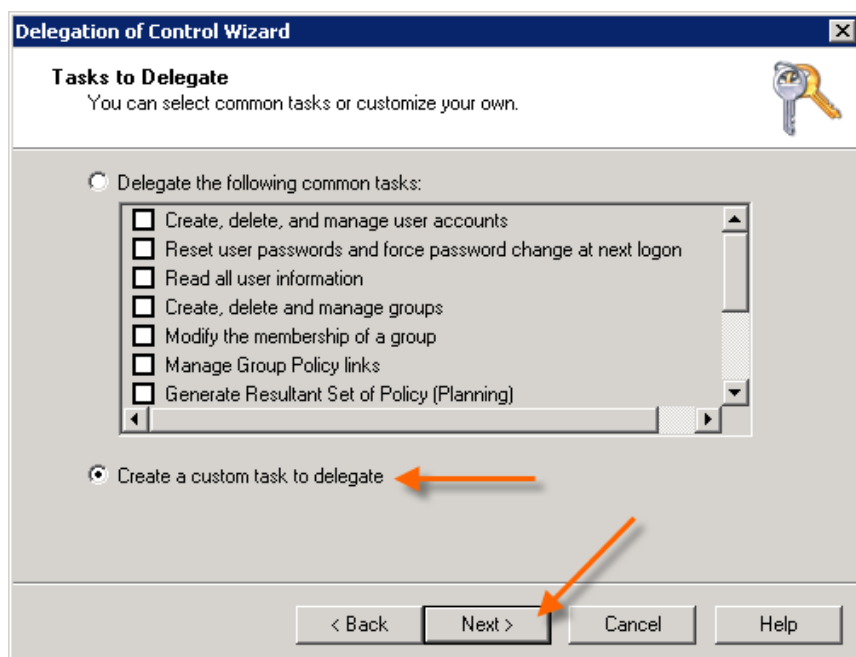
- h. The **Delegation of Control Wizard** dialog appears. Click **Next**.



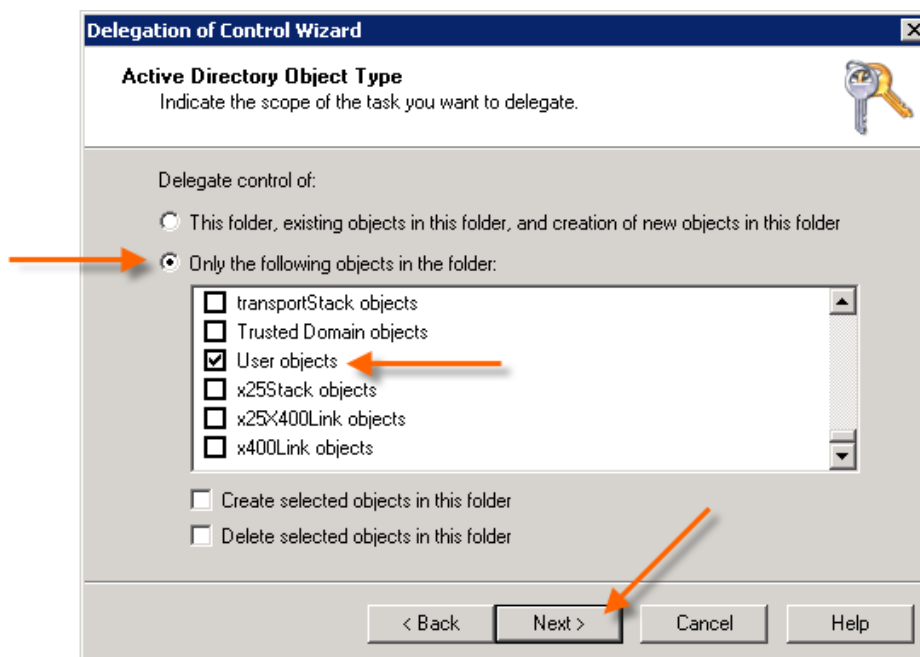
- i. A list appears where you must add the user that was created in step 1. Click the **Add...** button, add the user, and then click **Next**.



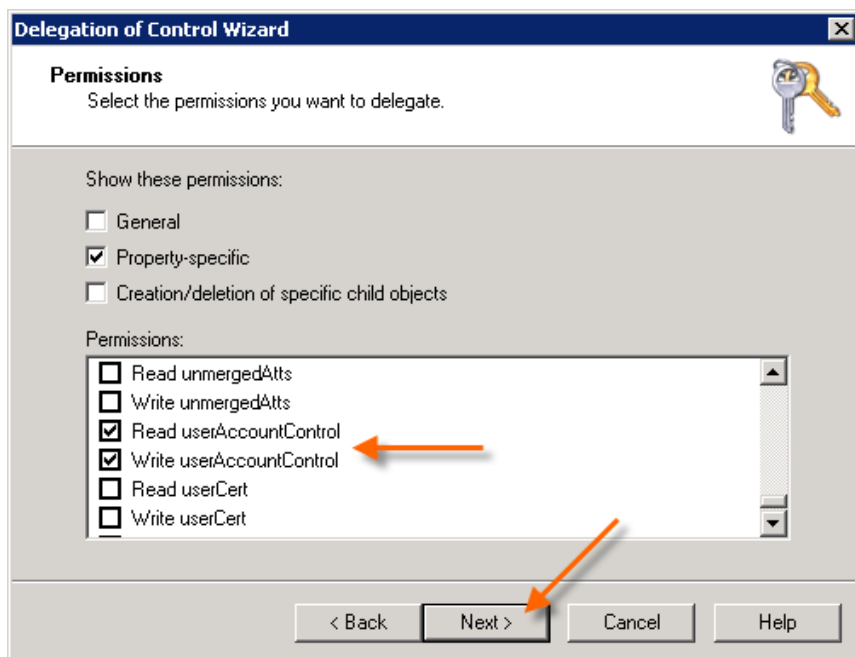
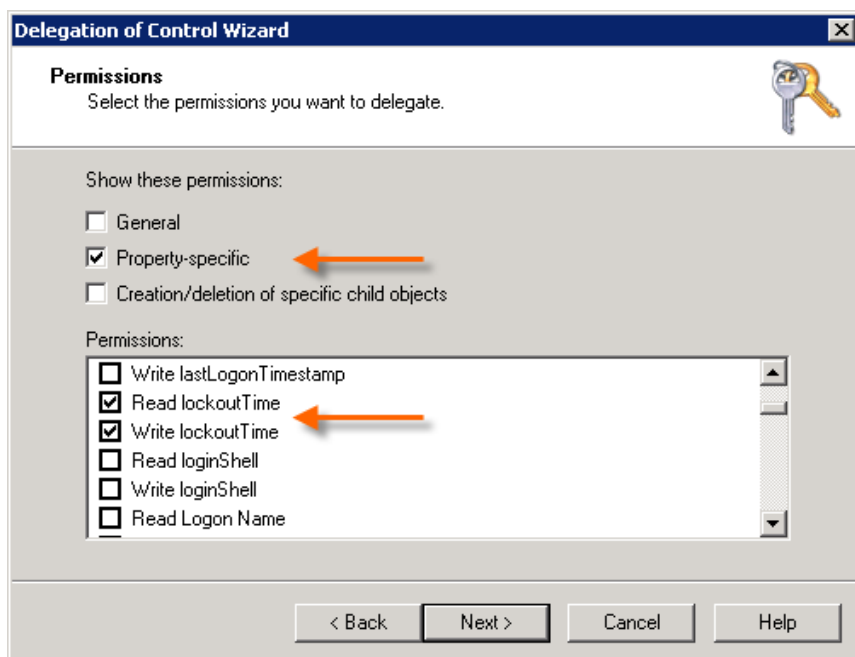
- j. Now select the option **Create a custom task to delegate** and click **Next**.



- k. Select the **Only the following objects in the folder** option, then select the **User objects** checkbox only, and finally click **Next**.



- l. Clear the **General** checkbox and select the **Property-specific** checkbox instead. In the **Permissions** section, select the **Read lockoutTime** and **Write lockoutTime** permissions, and the **Read userAccountControl** and **Write userAccountControl** permissions. Then click **Next**.



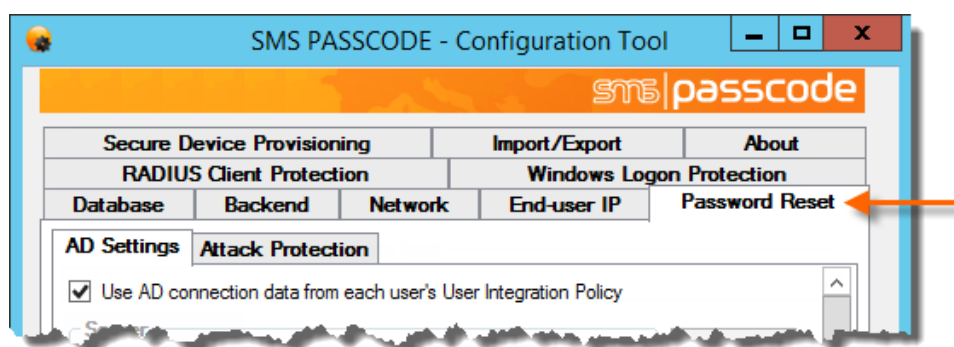
- m. On the final dialog, click **Finish**.
- n. The *Password Reset Account* has now been assigned the right to unlock users in the selected node. By default, the user will have this right for the node itself and the complete sub tree (all child OUs) as well, except branches where inheritance has been disabled.

If you are planning to allow end-users from multiple ADs to perform password reset operations, then you must repeat the above procedure for every involved domain.

23.7.2 Configure Settings of the Password Reset Backend Service

Before using the PRBS, some settings must be set in the SMS PASSCODE Configuration Tool. You can either specify these settings when the Configuration Tool pops up during installation of the PRBS, or alternatively start the Configuration Tool manually afterwards on the server where the PRBS has been installed. Please read section 25.5.5 (page 420) for instructions about starting the Configuration Tool manually.

When the SMS PASSCODE Configuration Tool has been started on the PRBS server, please select the **Password Reset** tab:



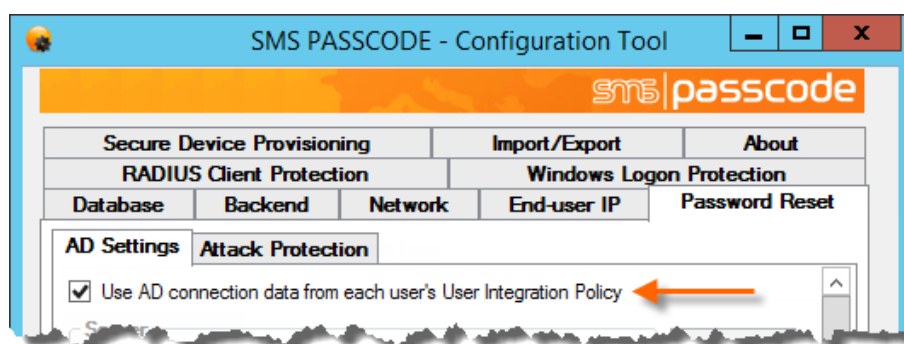
The Password Reset tab contains the two sub-tabs **AD Settings** and **Attack Protection**, which are described in the following two subsections.

23.7.2.1 Configuring AD Settings

On the **AD Settings** tab, you can specify the settings that instruct the PRBS about, which AD Controller it must contact to perform a Password Reset, and how to contact this AD Controller.

There are two ways to define such **AD Settings**:

1. If all your SMS PASSCODE users have been imported from an Active Directory, using one or more User Integration Policies (cf. section 17.5), then the most convenient way to set up **AD Settings** is simply to reuse the AD connection data from such User Integration Policies (UIPs). To do so, simply select the **Use AD connection data from each user's User Integration Policy** option:



IMPORTANT: Ensure password reset permissions

Please note, when reusing AD connection data from UIPs, that the AD credentials entered on such UIPs must not only have permissions for reading data from the relevant AD, but also proper permissions for resetting passwords on the users' behalf. To ensure this, on the UIPs, enter AD credentials of accounts that have been configured as dedicated password reset accounts (cf. section 23.7.1).

If an UIP is configured to use SSL/TLS (LDAPS) for user synchronization, then SSL/TLS (LDAPS) will also be used for password reset operations. This is recommended.

Multi-AD Support:

Reusing AD connection data from UIPs has an important additional benefit: As the UIP is determined from each individual user logging in to the SMS PASSCODE Password Reset Website, AD connection data can be reused from distinct UIPs. This means that a single PRBS can handle password reset operations across many different ADs.

- Alternatively, you can specify the AD connection data for password reset operations directly on the Password Reset tab. To do so, clear the **Use AD connection data from each user's User Integration Policy** option, then configure the remaining options as described below.

SMS PASSCODE - Configuration Tool

AD Settings **Attack Protection**

☐ Use AD connection data from each user's User Integration Policy

Server
Server to forward password requests to. Specify either the host name or IP address of a Domain Controller, or a Domain name.

Server name **Test**

SSL/TLS ☒ Encrypt communication using SSL/TLS

Password reset account
Specify credentials for a user with password reset privileges

Login

Password

Save **Cancel** **Close**

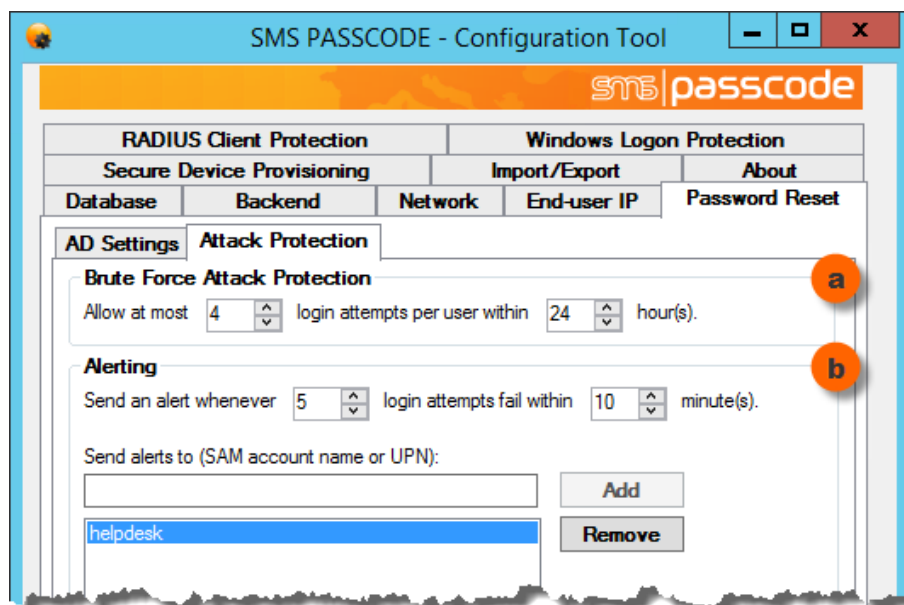
	Setting	Explanation
(a)	Server name	Please enter here the name or IP address of the AD Controller that the PRBS must contact whenever a user requests a password reset. You can also specify the DNS name of a domain to let the PRBS contact any AD Controller of such domain. If you leave the field empty, the PRBS will try to reach any AD Controller, of which the PRBS server itself is a member.
(b)	SSL/TLS	Check this option to enable SSL/TLS encryption of all communication (LDAP requests) between the PRBS and the specified AD Controller(s). It is strongly recommended to enable this option ⁴⁴ . To make SSL/TLS encryption work, you must install an SSL certificate on every relevant AD Controller. I.e. if the Server name option (a) has been set to a specific server name or IP address, then you must install a certificate on this specific server, and the certificate must have been issued to the exact same server name or IP address, respectively. Alternatively, if you have entered a domain name into the Server name option (a), then you must install a certificate on every AD Controller that the PRBS might contact, and the certificate must have been issued to the domain name.
(c)	Password reset account	Please enter here the credentials of the dedicated password reset user account used for contacting the AD Controller(s). If you have not yet created a dedicated password reset user account, then please read section 23.7.1 (page 351).
(d)	Test button	When all the settings above have been specified, please click the Test button. This will execute a test that checks the settings and reports whether everything works as expected. E.g. whether the AD Controller can be reached, whether SSL encryption works and whether the credentials for the password reset account are valid. In case any problems are reported, please correct the settings and retry the test, until it succeeds.

Remember to click the **Save** button to commit any changes.

⁴⁴ If you do not enable this option, PRBS might fail to reset passwords with the error message "A device attached to the system is not functioning" in the Password Reset event log. In case this happens, please enable the SSL/TLS option to solve the problem.

23.7.2.2 Configuring Attack Protection

On the **Attack Protection** tab, you can specify settings that instruct how the PRBS must react to *brute-force* and *Denial-of-Service* attacks:

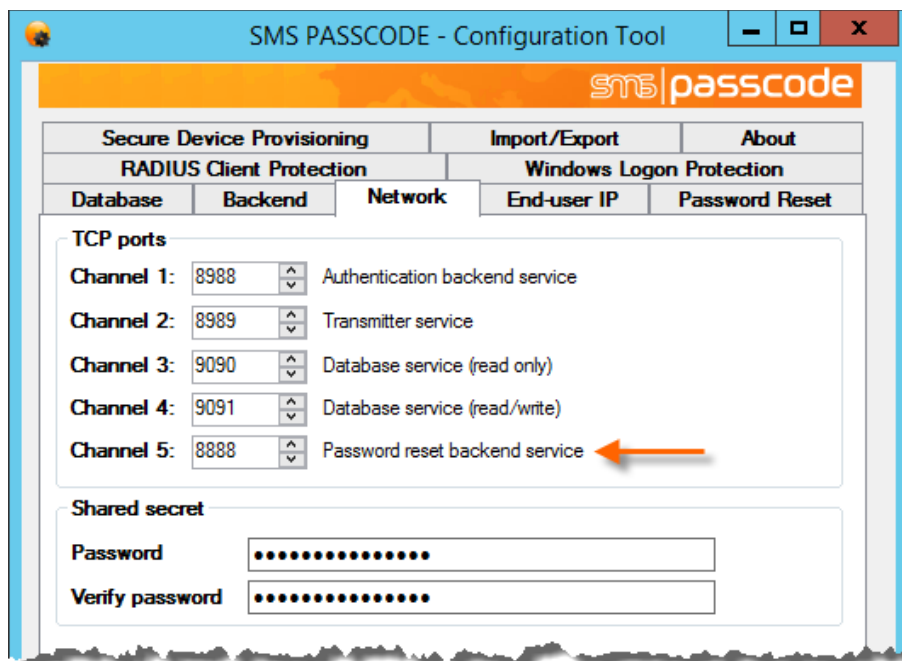


	Section	Explanation
(a)	Brute Force Attack Protection	Here you can specify how many login attempts are allowed per user within a specific period. If the number of allowed attempts is exceeded within the specified monitoring period, then the user will be denied access for a period (until the monitoring period again contains less attempts than allowed).
(b)	Alerting	You can set up the PRBS to send an alert whenever a specified number of login attempts have failed within a specified monitoring period. You can define any number of alert receivers. Each receiver name must match the SAM account name or UPN of a user in the SMS PASSCODE database. The Dispatch Policy of each matching user in the database determines how alerts will be sent, e.g. whether the alerts are sent by SMS or email. If you would like to have specific transmission rules for alerts (e.g. sending alerts to a specific public folder email address), then it is recommended to create one or more dedicated “alert users” manually in the SMS PASSCODE database, and specify mobile number, email address and Dispatch Policy as required on each such user.

Remember to click the **Save** button to commit any changes.

23.7.2.3 Network Communication

By default, the PRBS listens to incoming requests from SMS PASSCODE Password Reset Website(s) on TCP port 8888. It is recommended to use this default port, unless it conflicts with another application in your network. If needed, you may change the TCP port on the **Network** tab of the SMS PASSCODE Configuration Tool:

**IMPORTANT:**

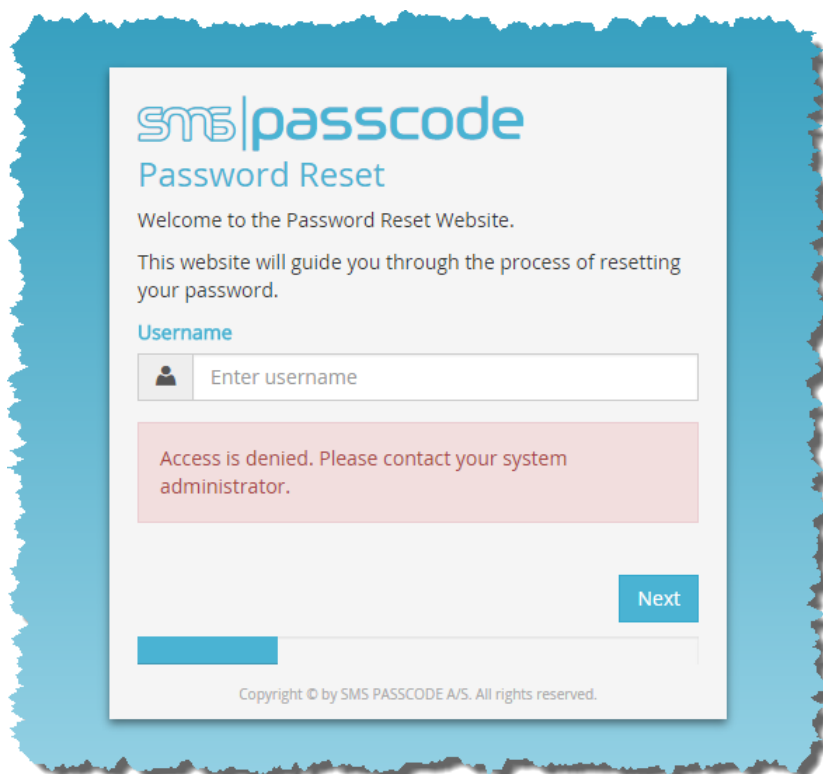
The **TCP port** and **Shared Secret** must match the entries entered in the Configuration Tool on each PRWS host; otherwise, communication from a PRWS to the PRBS will fail.

When the PRBS has been installed and configured, it is recommended to verify on the/each PRWS host, whether communication with the PRBS works as expected (cf. section 23.6.1, page 349).

23.8 Password Reset Event Log

When installing the PRBS on a server, a new Windows Event Log called **SMS PASSCODE Password Reset** is created automatically. Please open the Event Viewer management console and inspect the Password Reset event log, whenever you would like to get an overview, which users have reset or attempted to reset their password, and when.

Please also inspect the Password Reset event log on the PRBS server, in case a user is denied access to any PRWS connected to the PRBS in question:



The event log will contain an entry with the exact reason, why the user was denied access.

23.9 Localization

When an end-user accesses the SMS PASSCODE Password Reset Website, the site will be displayed in a localized language according to the current language settings of the end-user's web browser. Currently, the following localizations are supported:

- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German
- Hungarian
- Italian
- Korean
- Norwegian
- Polish
- Romanian
- Russian
- Spanish
- Swedish
- Turkish

English is used by default, if no matching localization is found.

24 SECURE DEVICE PROVISIONING

NOTE: This section only applies to SMS PASSCODE installations in the **On-premise** or **Hybrid Setup**.

SMS PASSCODE **Secure Device Provisioning** (SDP) is a component that integrates with Microsoft Exchange Server in order to let end-users perform secure, multi-factor authentication based provisioning of their own ActiveSync devices.

24.1 Background

Microsoft Exchange Server can be configured to automatically put any new ActiveSync device that is requesting access to a user's mailbox into **quarantine** mode. Whenever a device is put into quarantine mode, the end-user will receive a **quarantine email** at the same time. Additionally, the Exchange Server can be configured to send a copy of each such quarantine email to other internal personnel (e.g. internal IT helpdesk), to allow inspection of the ActiveSync request. From the content of the quarantine email someone must decide, whether the device should be granted access or not, and finally manually update the state of the device to "Access Granted" or "Access Blocked" in the Exchange Server's database.

The problem with this approach, especially in bigger companies, is: How does the system administrator (or other selected personnel) know, whether to approve a quarantined device or not? How to distinguish between a valid user device and a hacker attempting to get access to a user's email using the ActiveSync protocol?

A traditional approach is to implement a manual approval procedure, that takes up extra time for internal IT, and blocks users from accessing their emails until their devices have been approved. This causes unnecessary delays and loss of worker productivity. The best approach for solving the above problem is to enable the end-users to approve any new, quarantined ActiveSync device by themselves.

This is exactly, what the **SMS PASSCODE Secure Device Provisioning (SDP)** component allows; building on top of Microsoft Exchange Server's built-in quarantine functionality, it extends the standard workflow in a convenient and intuitive way, letting end-users provision their new ActiveSync devices by themselves, using a secure, multi-factor authentication based approach.

The procedure for self-provisioning is very easy:

1. The end-user sets up a new ActiveSync device and connects to the Exchange Server.
2. The Exchange Server sets the new device in quarantine mode and sends a quarantine email to the user. The quarantine email contains instructions and a URL to the SMS PASSCODE Secure Provisioning Website (SDP Website).
3. The user clicks the URL in the quarantine email and is redirected to the SDP Website.
4. The user is asked to validate his identity on the SDP Website, by performing an SMS PASSCODE multi-factor authentication.
5. On successful authentication, the SDP Website shows an overview of any known ActiveSync devices of the user, including the new, quarantined device.
6. The user clicks a button to grant the quarantined device access to the mailbox.

24.2 Deploying Secure Device Provisioning

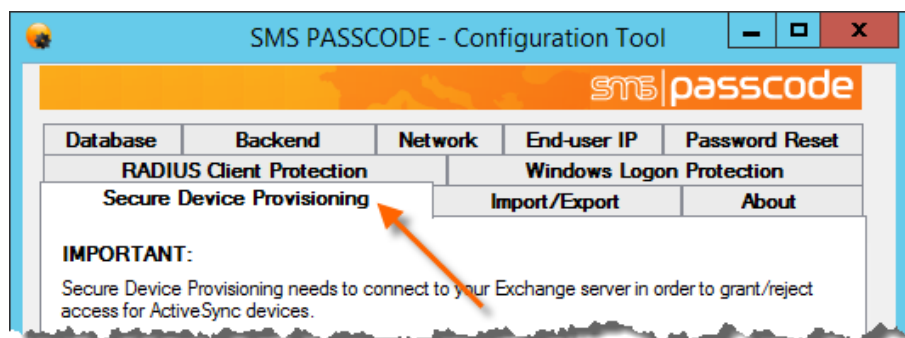
This section describes the procedure for installing and configuring the SMS PASSCODE Secure Device Provisioning (SDP) feature, including required configuration changes of your Exchange Server system.

To deploy SDP, please follow the procedure below:

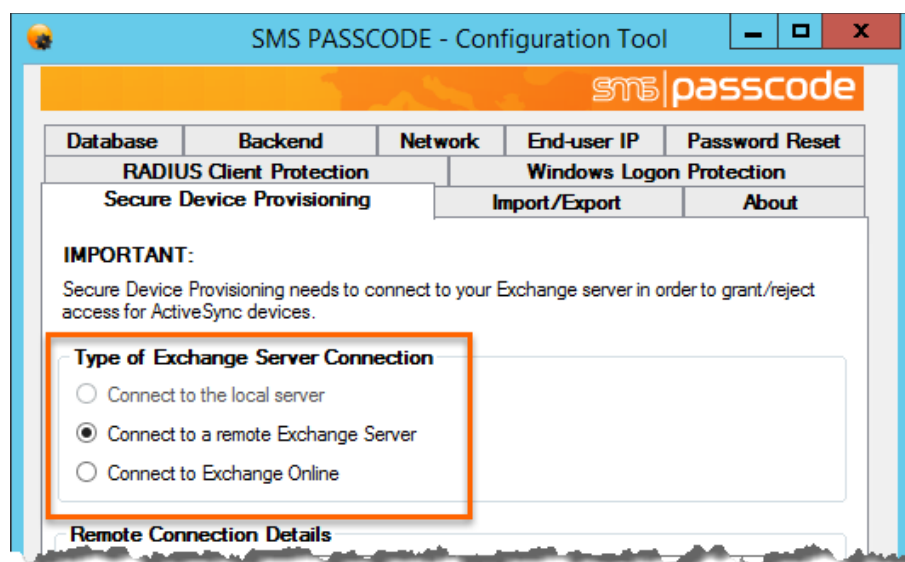
1. First install the SDP component on a Windows Server, preferable a server, from which the SDP Website can be published for external access. The Microsoft Internet Information Server (IIS) will be installed automatically, if not already present on the server.

Note: In previous SMS PASSCODE versions, the SDP component was required to be installed on every Exchange CAS role server. This is not the case anymore. You now only need to install the SDP component on a single Windows server. The server does NOT need to be the Exchange Server anymore, as the SDP component can make a remote connection to the Exchange Server. By default, connection to the Exchange server occurs on port 443 (https) but can be changed to port 80 (http).

- During installation of the SDP component, the SMS PASSCODE Configuration Tool will pop up. At this point, select the **Secure Device Provisioning** tab:

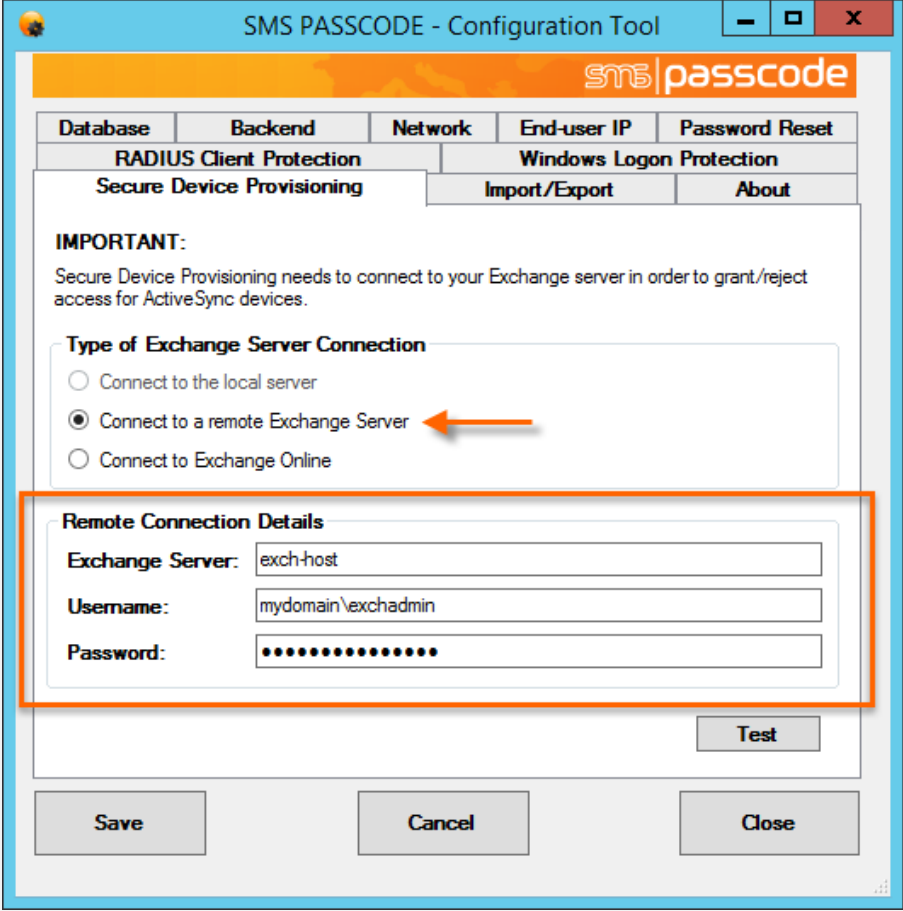


- On the **Secure Device Provisioning** tab, please select the planned type of Exchange Server connection:



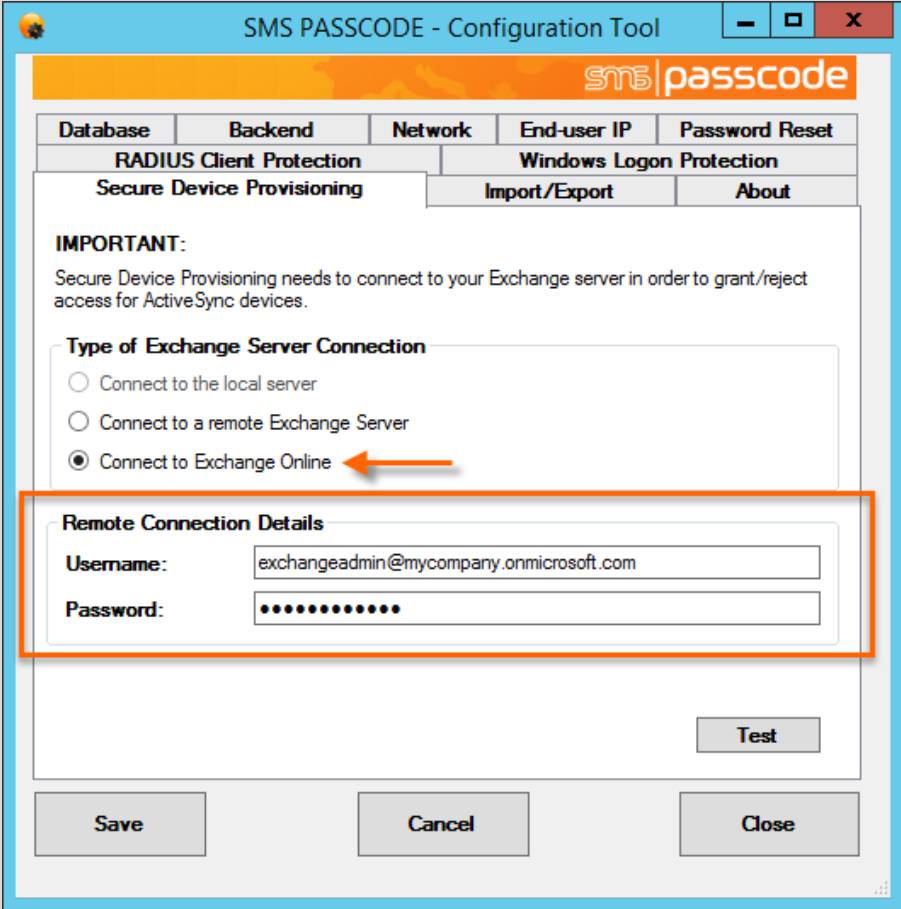
The possible options are:

Option	Description
Connect to local server	Select this option if you have installed the SDP component directly on a machine with an on-premise Exchange Server role, and you want to protect provisioning of ActiveSync devices on this local Exchange Server system. Note: This option is disabled, if no (supported) local Exchange Server system was detected.

Option	Description
Connect to remote Exchange Server	<p>Select this option if you want the SDP component to protect provisioning of ActiveSync devices on an on-premise Exchange Server system.</p> <p>In this case, specify the host name of the Exchange Server⁴⁵, and enter credentials of an Exchange administrator, that has permissions⁴⁶ to change the device state of all relevant users' ActiveSync devices:</p>  <p>Click the Test button to verify the connection to the Exchange Server and validate the credentials.</p>

⁴⁵ When just entering a host name, network traffic will default to https. If you require non-encrypted http, you must enter that explicitly using the following syntax: `http://hostname/powershell`

⁴⁶ The exchange administrator as a minimum is required to be a member of the following exchange role group - "Organization Management". In order to add a user to this group the following PowerShell command can be used `Add-RoleGroupMember "Organization Management" -Member "<name of the user>"`

Option	Description
Connect to Exchange Online (Office 365)	<p>Select this option if you want the SDP component to protect provisioning of ActiveSync devices on an Exchange Online system.</p> <p>In this case, enter credentials of an Exchange Online administrator, that has permissions⁴⁶ to change the device state of all relevant users' ActiveSync devices:</p>  <p>Click the Test button to verify the connection to the Exchange Online system and validate the credentials.</p>

Remember to click the **Save** button, when the appropriate configurations have been made.

You can always start the SMS PASSCODE Configuration Tool later again from the Windows start menu, if you need to change any of the settings. For example, if you need to enter new credentials, or wish to connect to a different Exchange Server system.

- Since the SDP Website uses form-based authentication, it is very important that the site is protected using SSL/TLS to ensure, that all credentials are transferred encrypted. Therefore, after successful installation of the website, you need to install an SSL certificate for it, before users can access it.

IMPORTANT

For security reasons the SDP Website has been designed to require SSL/TLS encryption. Therefore, the website will NOT work before an SSL certificate has been installed for the site and HTTPS has been enabled successfully.

5. Finally, you need to ensure that your Exchange Server system has been configured correctly. As the SDP component relies on built-in quarantine logic of the Exchange Server system, it is important that such quarantine logic is enabled. However, if such quarantine logic was not enabled beforehand in your system, then you need to plan this configuration change of your Exchange Server carefully, as it can otherwise disrupt all the existing ActiveSync devices of all your users. The next section describes the required steps to configure your Exchange Server system correctly.

24.2.1 Configuring Microsoft Exchange Server

For SMS PASSCODE Secure Device Provisioning (SDP) to operate correctly, your Microsoft Exchange Server must be configured appropriately:

- **Quarantine mode:** Quarantine mode must have been enabled for new ActiveSync devices.
- **Quarantine email content:** For improved user convenience, it is recommended to adapt the message content of the quarantine emails to provide instructions on the usage of the SDP Website, including the URL to the SDP Website.

By default, your Microsoft Exchange Server will allow any new ActiveSync device to connect. This section describes how to configure your Exchange Server to set any new ActiveSync device into **quarantine mode** and send a **quarantine email** to the device, when it attempts to connect. This configuration is required, because the SDP component builds on top of the built-in quarantine functionality of the Microsoft Exchange Server.

WARNING:

If you did not make use of the Exchange Server quarantine mode beforehand, then enabling this functionality will put all your already existing ActiveSync devices in quarantine mode, and your end-users will have to re-approve their existing devices in the SDP Website!

You should plan this carefully to minimize the impact on end-users.

As an alternative, it is possible to auto-approve all existing devices using a PowerShell script, just after enabling the quarantine functionality in Exchange Server.

RECOMMENDATION:

When configuring quarantine emails in your Exchange Server, it is recommended to set up administrators to receive copies of all quarantine emails, too. Such administrators will receive copies of the Exchange Server quarantine emails, whenever a user receives a quarantine email. Normally administrators will not need to take any actions on those copies of quarantine emails, but it is still a **best-practice** to receive them, to ensure administrators have the possibility of performing a manual device approval, in case self-provisioning by an end-user does not work for any reason.

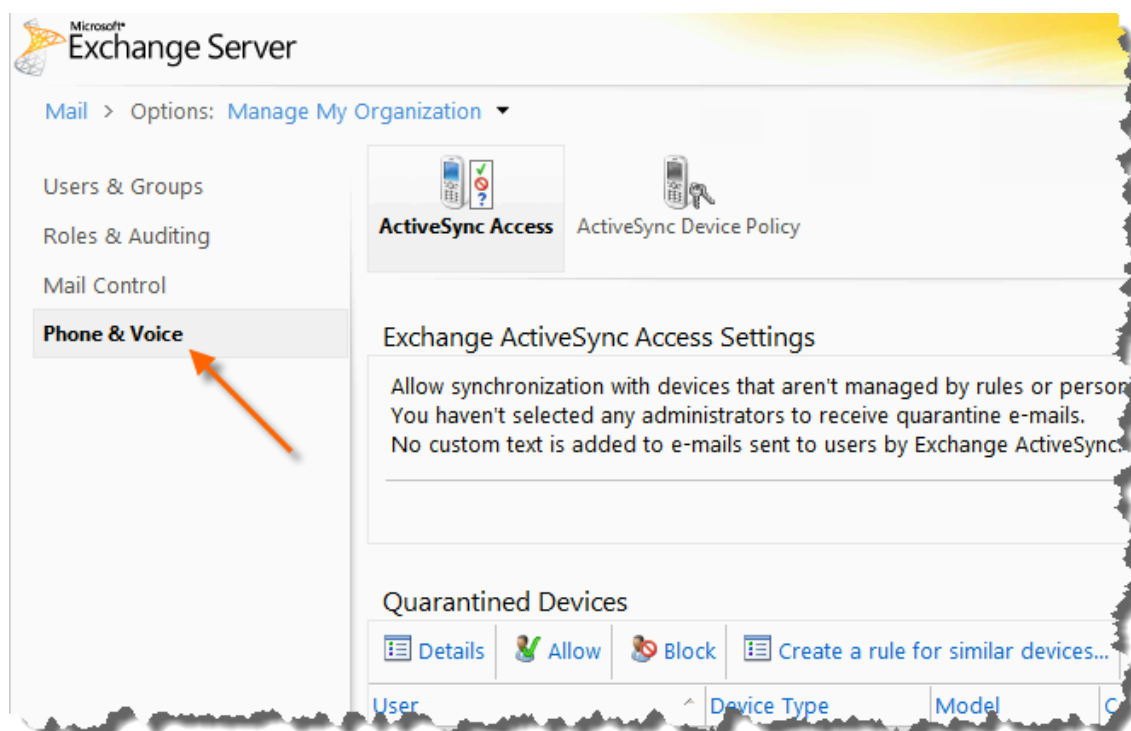
If you had already beforehand enabled quarantine logic in your Exchange Server system, then you should still follow the procedure described below, but only follow the step to adapt the content of the quarantine emails, to guide your users regarding the new SDP Website.

The procedure for enabling quarantine emails depends on the version of your Exchange Server. The next two subsections describe the required steps on an Exchange Server 2010 and 2013/2016/2019/Online, respectively.

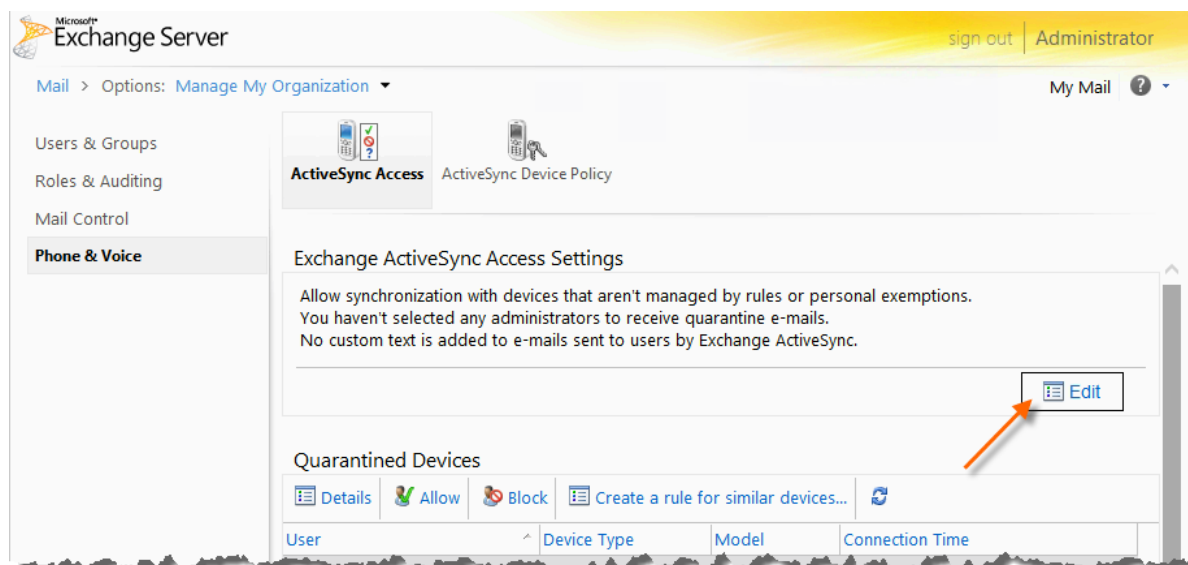
24.2.1.1 Enabling Quarantine Mode on Exchange Server 2010

To enable quarantine mode on an Exchange Server 2010, follow the steps below:

1. Log in to the Exchange Control Panel (ECP) and select the **Phone & Voice** tab on the left side:



2. On the **Phone & Voice** tab, click the **Edit** button on the right side:



3. On the **Exchange ActiveSync Settings** dialog that pops up:
 - a. Select the **Quarantine** radio button
 - b. Click the **Add...** button to add administrators to receive copies of quarantine emails.
 - c. Enter instructions for your end-users regarding how they must proceed to approve a quarantined device. It is recommended to add the public URL of your SDP website.

Example:

You can approve the quarantined device yourself by logging in to the Secure Device Provisioning Website at <https://sdp.mycompany.com> with your Windows credentials.

- d. Finally, click the **Save** button.

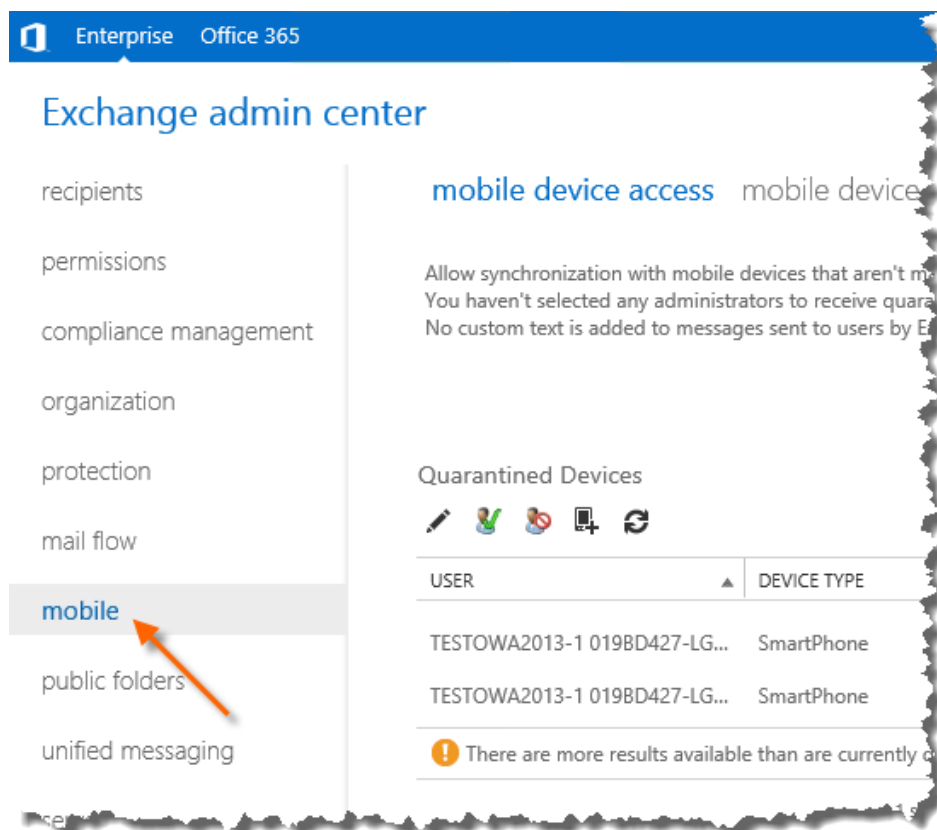
The screenshot shows the 'Exchange ActiveSync Settings' dialog box. It has a title bar and a main content area. The content area is divided into sections. The first section is 'Connection settings' with the text 'When a device that isn't managed by a rule or personal exemption connects to Exchange:'. Below this are three radio buttons: 'Allow access', 'Block access', and 'Quarantine - Let me decide to block or allow later'. The third radio button is selected and is marked with an orange circle 'a'. The second section is 'Quarantine notification e-mails' with the text 'Select administrators to receive e-mail when a device is quarantined.'. Below this is a table with two columns: 'Display Name' and 'SMTP Address'. Above the table are two buttons: '+ Add...' and '- Remove'. The '+ Add...' button is marked with an orange circle 'b'. The table is empty. Below the table is a text box with the text 'Enter text to include in e-mails sent to users who have a device in quarantine, blocked, or in the process of being identified:'. This text box is marked with an orange circle 'c'. At the bottom right of the dialog box are two buttons: a green checkmark icon followed by the text 'Save' (marked with an orange circle 'd') and a red 'X' icon followed by the text 'Cancel'.

4. This completes configuration of quarantine mode.

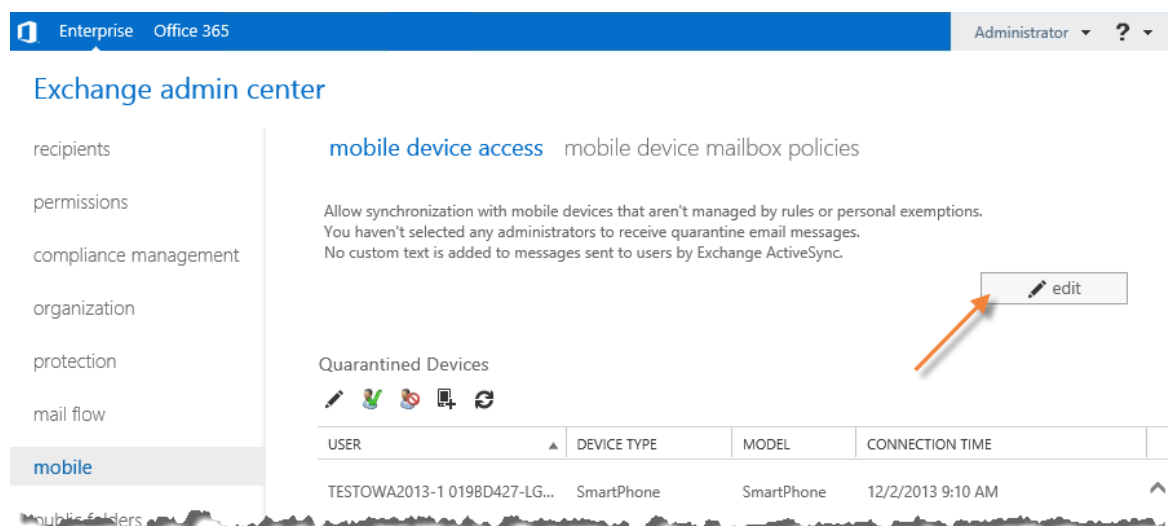
24.2.1.2 Enabling Quarantine Mode on Exchange Server 2013/2016/2019/Online

To enable quarantine mode on an Exchange Server 2013/2016/2019 or on Exchange Online, follow the steps below:

1. Log in to the Exchange Admin Center (EAC) and select the **mobile** tab on the left side:



2. On the **mobile** tab, click the **edit** button on the right side:



3. On the **Exchange ActiveSync access settings** dialog that pops up:
 - a. Select the **Quarantine** radio button
 - b. Click the **+** icon to add administrators to receive copies of quarantine emails.
 - c. Enter instructions for your end-users regarding how they must proceed to approve a quarantined device. It is recommended to add the public URL of your SDP website.

Example:

You can approve the quarantined device yourself by logging in to the Secure Device Provisioning Website at <https://sdp.mycompany.com> with your Windows credentials.

- d. Finally, click the **save** button.

The screenshot shows the 'Exchange ActiveSync access settings' dialog box. It has a title bar and a main content area. The content area is divided into sections. The first section is 'Connection Settings' with the text 'When a mobile device that isn't managed by a rule or personal exemption connects to Exchange:'. Below this are three radio buttons: 'Allow access', 'Block access', and 'Quarantine - Let me decide to block or allow later'. The 'Quarantine' option is selected. The second section is 'Quarantine Notification Email Messages' with the text 'Select administrators to receive email messages when a mobile device is quarantined.'. Below this is a table with two columns: 'DISPLAY NAME' and 'SMTP ADDRESS'. The table is empty. Below the table is a text box with the text 'Text to include in messages sent to users whose mobile device is in quarantine, blocked, or in the process of being identified:'. At the bottom right of the dialog are two buttons: 'save' and 'Cancel'. Annotations are placed on the dialog: 'a' is next to the 'Quarantine' radio button, 'b' is next to the '+' icon in the table, 'c' is next to the text box, and 'd' is next to the 'save' button.

Exchange ActiveSync access settings

Connection Settings
When a mobile device that isn't managed by a rule or personal exemption connects to Exchange:

☐ Allow access
☐ Block access
☒ Quarantine - Let me decide to block or allow later

Quarantine Notification Email Messages
Select administrators to receive email messages when a mobile device is quarantined.

DISPLAY NAME	SMTP ADDRESS
--------------	--------------

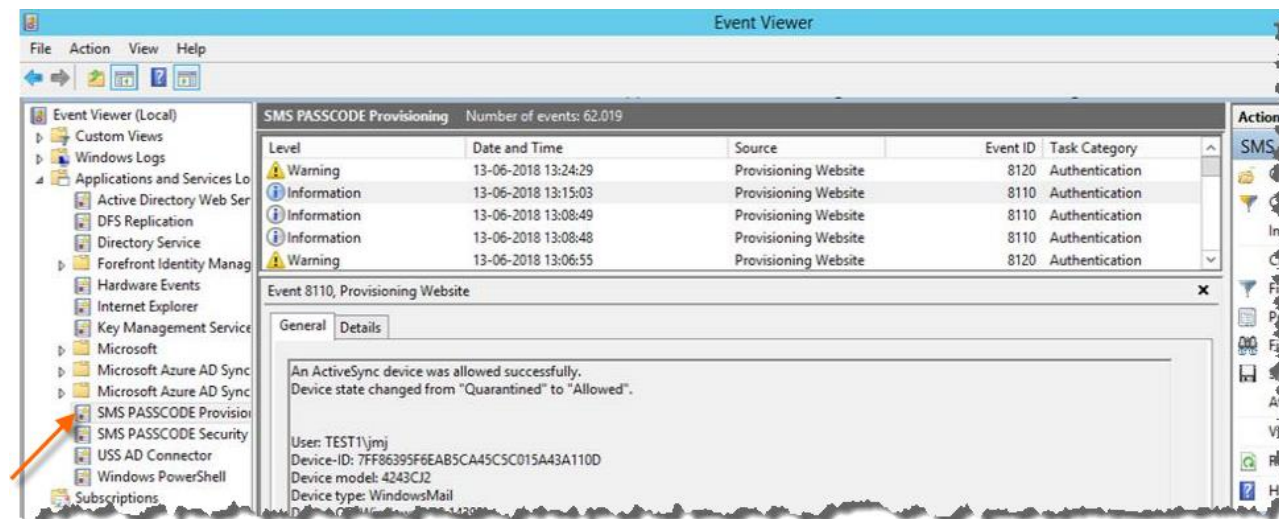
Text to include in messages sent to users whose mobile device is in quarantine, blocked, or in the process of being identified:

save Cancel

4. This completes configuration of quarantine mode.

24.3 Event Logging

On the server with SMS PASSCODE Secure Device Provisioning (SDP) installed, a separate Windows event log with the name **SMS PASSCODE Provisioning** is created. This event log contains among others an audit about all login attempts to the SDP website.



The event log also contains error entries in case any issues regarding the SMS PASSCODE Secure Device Provisioning component occur. Hence, the event log is a good starting point for troubleshooting the SDP component.

24.4 Localization

SMS PASSCODE Secure Device Provisioning supports localization for end-user related content. When an end-user accesses the SMS PASSCODE Secure Device Provisioning website, the site will be displayed in a localized language according to the current language settings of the end-user's web browser.

The following localizations are currently supported:

- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German
- Hungarian
- Italian
- Korean
- Norwegian
- Polish
- Romanian
- Russian
- Spanish
- Swedish
- Turkish

English is used by default, if no matching localization is found.

25 CONFIGURING AUTHENTICATION CLIENTS

25.1 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 scenario 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:
 - Citrix Web Interface 5.x:
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.

IMPORTANT

If you have enabled User Store Integration, and you are receiving the error message **“Unknown user, please contact your administrator”** during Citrix Web Interface logon, please read section 28.2 (page 435) for solving this problem.

25.2 Configuring RADIUS Protection

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

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

The required configuration steps are:

1. You must ensure that your RADIUS clients have been created and configured within the NPS server. This is described in section 25.2.1 below.

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

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

Configuring RADIUS settings in the SMS PASSCODE Configuration tool is described in section 25.2.2, page 380.

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 25.2.2.1, page 385).

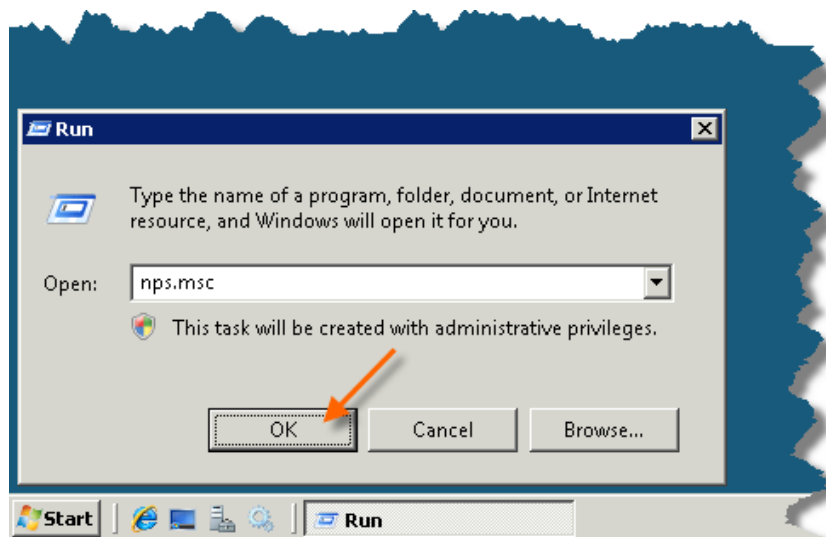
25.2.1 Configuring RADIUS Protection on a Windows Server

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:

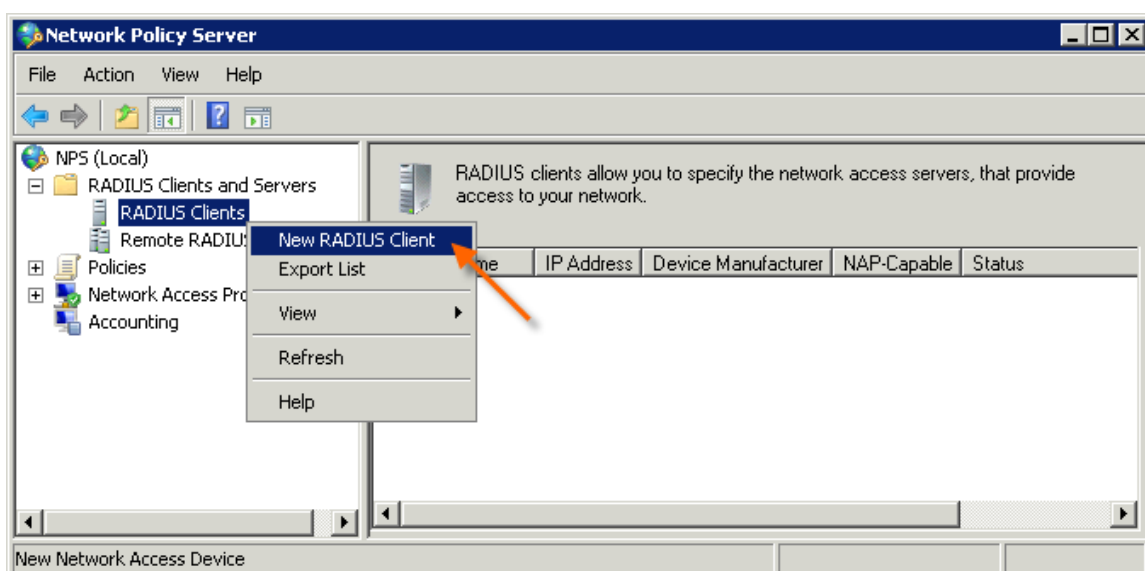
1. Configure all RADIUS clients in the usual way by specifying the **NPS server** as the RADIUS server. If you are in doubt how to perform the configuration, please refer to the configuration guide of the specific RADIUS client in question.

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**.

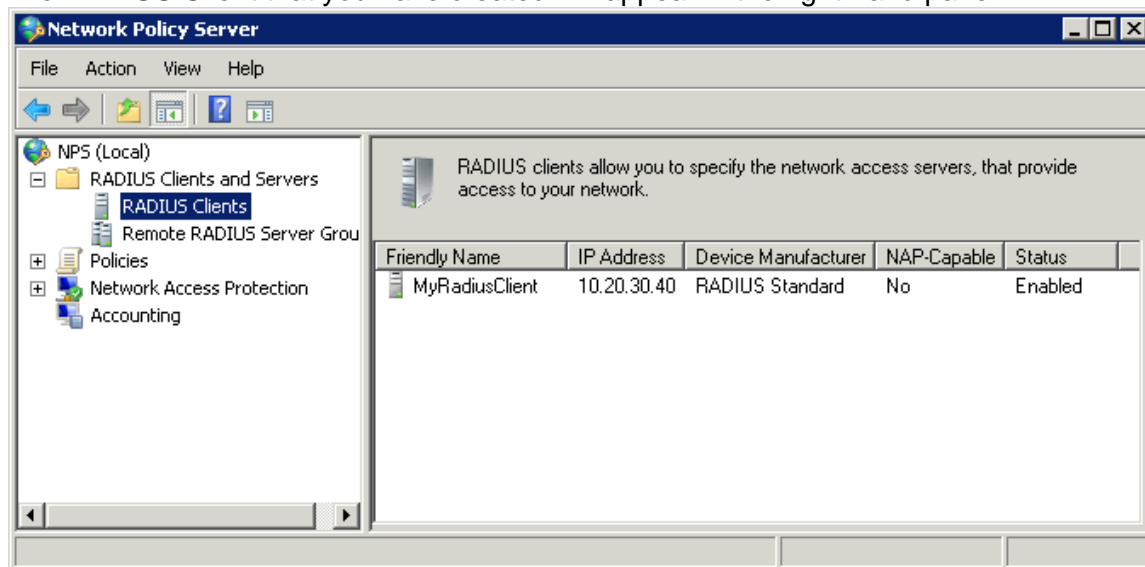


6. The **New RADIUS Client** dialog appears.
- Enter a “friendly name” of the RADIUS Client.
 - Enter the IP address of the RADIUS Client.
 - Enter and confirm the **Shared Secret**. It must match the shared secret configured on the RADIUS Client.
 - Click **OK**.

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

- Enable this RADIUS client:** A checked checkbox.
- Name and Address:**
 - Friendly name:** A text box containing 'MyRadiusClient'. An orange arrow labeled 'a' points to this box.
 - Address (IP or DNS):** A text box containing '10.20.30.40'. An orange arrow labeled 'b' points to this box. To the right of this box is a 'Verify...' button.
- Vendor:**
 - Text: 'Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.'
 - Vendor name:** A dropdown menu showing 'RADIUS Standard'.
- Shared Secret:**
 - Text: 'To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.'
 - Two radio buttons: 'Manual' (selected) and 'Generate'.
 - Shared secret:** A text box with masked characters (dots). An orange arrow labeled 'c' points to this box.
 - Confirm shared secret:** A text box with masked characters (dots). An orange arrow labeled 'c' points to this box.
- Additional Options:**
 - ☐ Access-Request messages must contain the Message-Authenticator attribute
 - ☐ RADIUS client is NAP-capable
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right. An orange arrow labeled 'd' points to the 'OK' button.

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



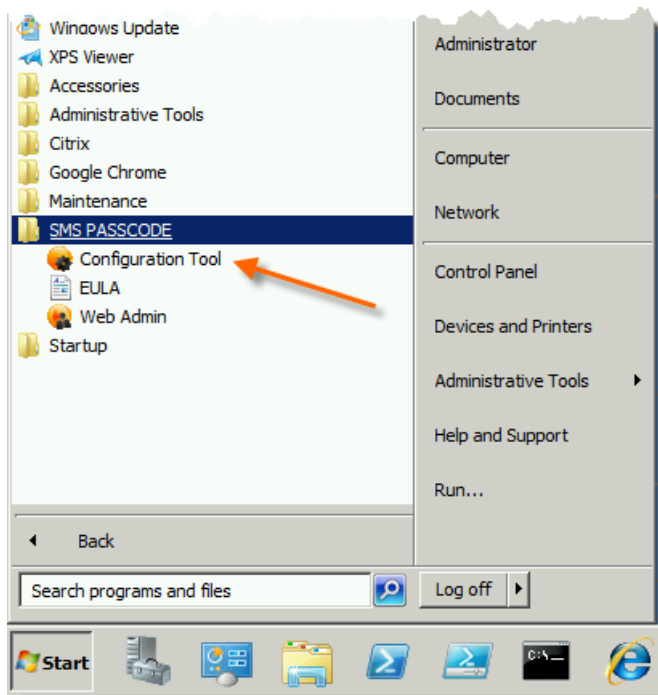
8. Repeat steps 5-7 if you need to create more RADIUS Clients.
9. This completes the standard configuration of RADIUS authentication using SMS PASSCODE. Please test each RADIUS client to make sure that RADIUS authentication works as expected.

25.2.2 Advanced Configuration of the RADIUS Protection Component

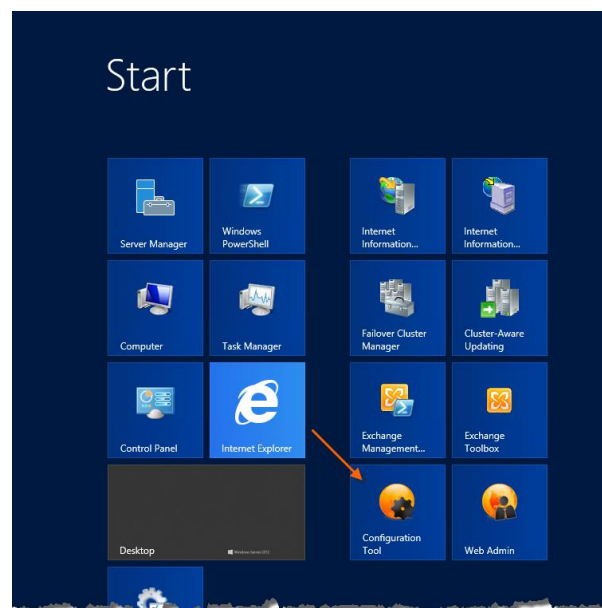
This section describes, how you can maintain advanced settings of the SMS PASSCODE RADIUS Protection component.

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...

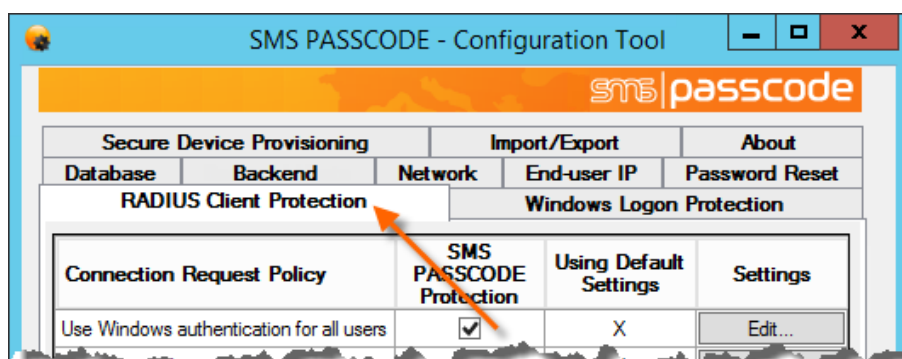


Windows Server 2008 R2

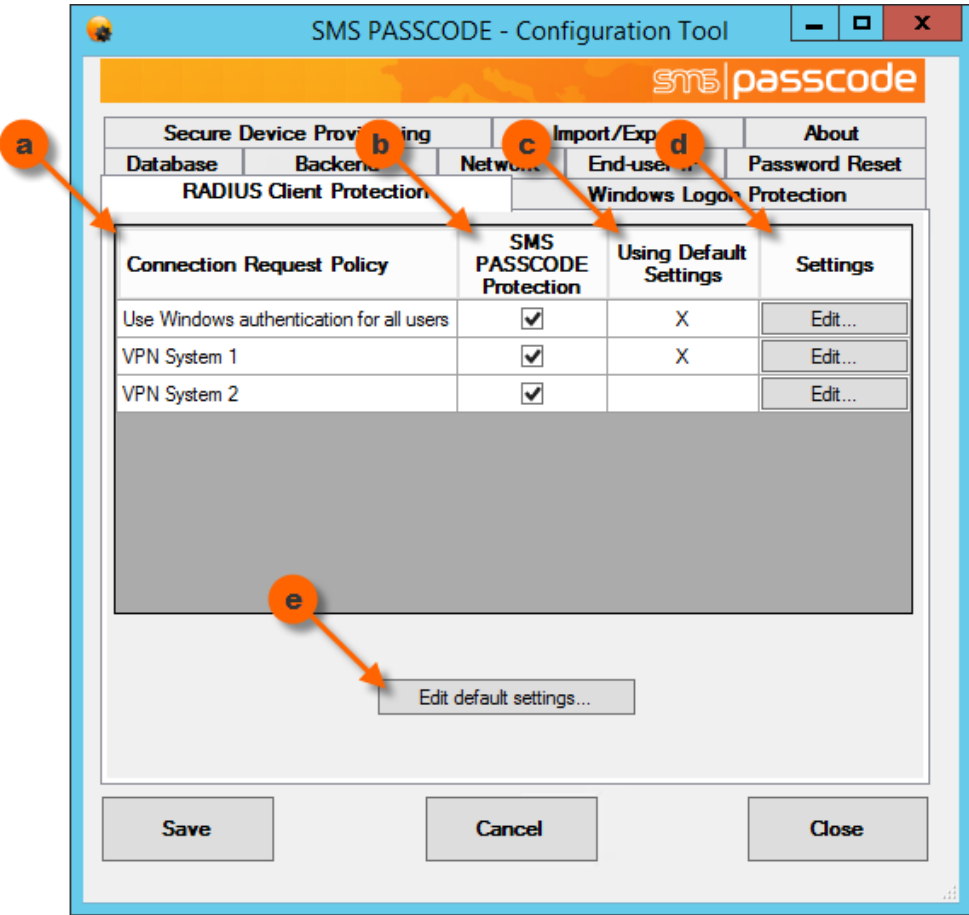


Windows Server 2012 / 2016 / 2019

...you will see a number of tabs. Select the **RADIUS Client Protection** tab to configure the advanced RADIUS settings:



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

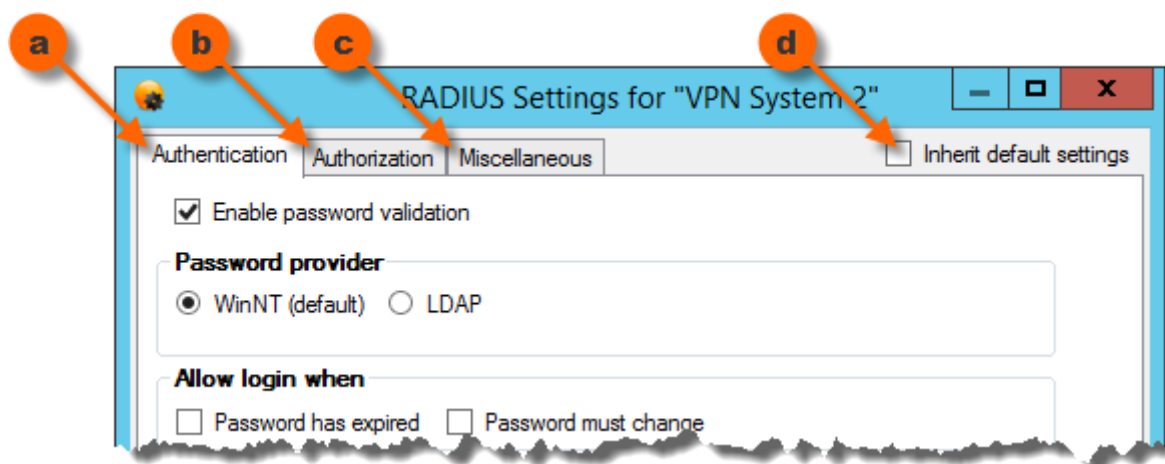


The columns of the table are explained below:

	Explanation
(a)	<p>Column (a) lists the names of all the CRPs that currently exist in the NPS. Whenever you create or delete CRPs in NPS, such changes are automatically reflected in the Configuration Tool (when you restart it).</p> <p>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.</p>

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

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



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

	Explanation
(a)	<u>Authentication:</u> This tab contains settings that affect the authentication behavior of the RADIUS Protection component. Please read section 25.2.2.1 (page 385) for further details.
(b)	<u>Authorization:</u> This tab allows to enable/disable the inclusion of a RADIUS authorization attribute in each RADIUS accept packet being sent to the RADIUS client on successful authentication, and to configure the authorization attribute. Please read section 25.2.2.2 (page 394) for further details.
(c)	<u>Miscellaneous:</u> This tab contains miscellaneous settings of the RADIUS Protection component regarding text encoding, end-user IP address collection, challenge/response behavior and more. Please read section 25.2.2.3 (page 398) for further details.
(d)	<u>Inherit default settings</u> This checkbox is only visible, when editing CRP-specific settings. Clear the checkbox to override the default settings and set CRP-specific settings. Select the checkbox 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.

25.2.2.1 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

1. An **Access Request** packet containing a username and a password is received from a RADIUS client.
2. The NPS extension resolves the user, i.e. checks whether the user can be found in the **SMS PASSCODE** database. 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 in the SMS PASSCODE database. If the user is not allowed to log in, then access is denied.
4. The password is verified using the configured password provider. By default, this means using Windows Authentication (either a local Windows user or an AD user). In this case, access is denied, if any of the following conditions are true:
 - a. The user password is incorrect.
 - b. The user is locked out or denied access.
 - c. The user password has expired.
 - d. The user password has been flagged "Must change at next logon".
5. Internal NPS logic is skipped.
(I.e. all authentication and authorization settings of the active Connection Request Policy and all settings of the Network Policy are ignored)
6. Now multi-factor authentication is performed according to the user's settings in the SMS PASSCODE database. 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.
8. 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*.

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

RADIUS Settings for "VPN System 2"

Authentication | Authorization | Miscellaneous ☐ Inherit default settings

a ☒ Enable password validation

b **Password provider**
☒ WinNT (default) ☐ LDAP

c **Allow login when**
☐ Password has expired ☐ Password must change

d **Push Authentication**
 Timeout: 120 seconds
☒ Fallback on timeout

e **Side-by-side**
 Enable NPS internal Connection
 Request Policies execution:
 Never

f **Default domains**
 Add Remove Up Down

☐ Allow logins from any domain (using fully qualified usernames only)

Reset to default settings... Ok Cancel

The settings have the following purposes:

a. Enable password validation

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

WARNING:

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

b. Password provider

NOTE: This setting is only available, when SMS PASSCODE is installed as an **On-premise** or **Hybrid Setup**. In a **Cloud Setup**, the **Password provider** setting is hidden and is always set to **WinNT**.

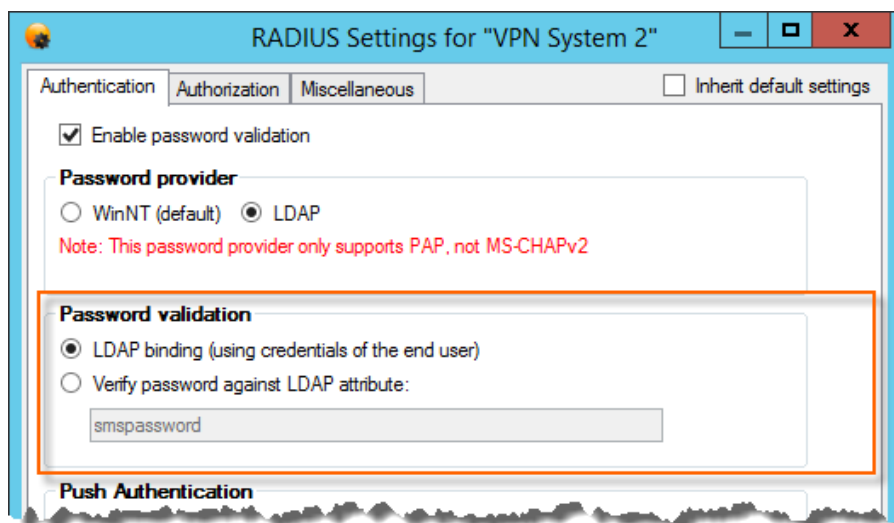
In step 4 of the *Standard Authentication Flow*, SMS PASSCODE will validate user passwords using the **WinNT** provider (i.e. validating the user's Windows password) by default. This will work in the following cases:

- **When the RADIUS server is not member of any AD domain:**
Authentication is only possible for local Windows users that have been created on the RADIUS server.
- **When the RADIUS server is member of an AD domain:**
Authentication is possible for local Windows users that have been created on the RADIUS server. Additionally, users in the domain of the RADIUS server can be authenticated. Finally, users in another AD domain ("domain X") can be authenticated, if a trust relationship has been created between the domain of the RADIUS server and the user's "domain X".

If you would like to authenticate users in "domain X" without creating a trust relationship, then consider using the **LDAP password provider**, instead of **WinNT** (described below).

You can select **LDAP** if you wish to validate user passwords against an LDAP directory using the LDAP protocol, for example in order to authenticate AD users outside the domain of the RADIUS server, or to authenticate non-AD users residing in a non-AD LDAP directory.

When selecting **LDAP**, a new **Password validation** section appears on the **Authentication** tab:



Here, you can specify, how LDAP authentication must occur:

- **LDAP binding:** The password entered by the user is validated by sending an LDAP authentication request to the LDAP directory. If the user has been imported from an AD, then NTLM is used for authentication. Otherwise, basic authentication is used.

WARNING: As noted above, LDAP binding will use **basic authentication** for users imported from a non-AD LDAP directory, i.e. for users imported via a User Integration Policy set to import from a "General LDAP" directory. In such cases, it is **strongly recommended** to enable SSL encryption on the User Integration Policy in order to ensure encryption of the LDAP traffic. Otherwise, users' credentials will be sent in clear text over the network.

- b. **Verify password against LDAP attribute:** The password entered by the user is validated, by checking whether it matches the content of a specific LDAP attribute on the user object in the LDAP directory. The name of the LDAP attribute to use is specified in the textbox.

Regardless of the type of LDAP authentication chosen, the NPS extension automatically knows which LDAP server to contact and knows how to communicate with it. This is determined by re-using the configuration data of the **User Integration Policy** that imported the user to the SMS PASSCODE database. Among others, the UIP settings also determine, whether SSL/TLS encryption must be used, when communicating with the LDAP server.

When using **Password provider = LDAP**, the **NPS IL setting** must be set to **Never** (see item e below).

NOTE (User import required for LDAP authentication)

LDAP password validation only works for users that have been imported to the SMS PASSCODE database using a User Integration Policy (UIP). This is because the UIP settings are reused in order to locate the right LDAP directory and perform LDAP authentication.

NOTE (PAP required for LDAP authentication)

LDAP password validation requires the RADIUS client to use the PAP protocol. MS-CHAP v2 is NOT supported.

c. **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".

NOTE:

The **Allow login when** section is only available, when **Password provider** (item b) has been set to WinNT. The settings of the section are not available for LDAP authentication.

d. Push Authentication

NOTE: This setting is only relevant, when SMS PASSCODE is installed as a **Hybrid** or **Cloud Setup**. In an **On-premise Setup**, the setting has not effect.

This setting controls the authentication behavior, when IntelliTrust™ risk-based authentication is active, and the outcome of the risk engine is to use *Push Authentication* as the first priority. In this case, the default behavior of the RADIUS server is the following:

- When an Access Request package is received from the RADIUS client, the RADIUS server will immediately forward a Push Authentication request to the end-user's mobile app (via the IntelliTrust™ cloud service).
- The RADIUS server will not send any package back to the RADIUS client, until either a) The user has reacted and either confirmed or rejected the push authentication, or b) a timeout of 120 seconds occurs. In case the user reacted before the timeout with a push authentication confirmation or rejection, an Access Accept or Access Reject package is returned to the RADIUS client, respectively.
- In case the 120 second timeout occurred, the RADIUS server will fail over and send an Access Challenge back to the RADIUS client, asking the user to authenticate using the next authentication mechanism in the prioritized list of authenticators that resulted from the evaluation of the risk engine. If no such failover authentication mechanism was configured in the IntelliTrust™ risk engine, then an Access Reject is returned instead.

A potential issue with the default Push Authentication behavior is that the RADIUS client might not want to wait for up to 120 seconds to receive a package back from the RADIUS server. It might have been configured to abort the authentication session before 120 seconds have elapsed. If possible, it is recommended to re-configure the RADIUS client to wait up to 120 seconds, before aborting the authentication session. Otherwise, it is recommended to change the **Timeout** setting to align it with the RADIUS client behavior. However, please take into consideration that the end-user should be given enough time to actually open the Push Authentication app and confirm/reject the Push Authentication request.

If you do not want the RADIUS server to fail over to a secondary authentication mechanism on Push Authentication timeout, then please clear the checkbox **Fallback on timeout**.

e. Side-by-side

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

The following abbreviations are used below:

- **CRP:** Connection Request Policy
- **NP:** Network Policy
- **NPS IL setting:** The setting called "Enable NPS internal Connection Request Policies execution" in the Side-by-Side section. "IL" is an abbreviation for "Internal Logic".

- **SVF setting:** The setting called “**Skip SMS PASSCODE validation and fail immediately** for passwords matching the regular expression” in the Side-by-Side section. “SVF” is an abbreviation for “**Skip Validation and Fail**”.

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

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

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

i. Empty (default):

This setting has no effect.

ii. Non-empty (password filtering):

If you enter a regular expression into this field, SMS PASSCODE will check, on each authentication attempt, whether the regular expression matches the password entered⁴⁷. If it does not match, then the authentication continues normally. On the other hand, if there is a match, then steps 2-4 of the *Standard Authentication Flow* are skipped altogether, meaning no user resolve or password validation is performed. Instead, the steps 2-4 are immediately treated as failed. As a result, the following behavior is achieved with a matching password:

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

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

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

⁴⁷ This is only supported, when the RADIUS client uses the PAP protocol. MS-CHAP v2 is not supported, since the password is not available in clear text for comparison in this case.

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

Use case	Required settings
<ul style="list-style-type: none"> Standard SMS PASSCODE multi-factor authentication must be performed for all users. No need for Network Policy support. 	<ul style="list-style-type: none"> Set the NPS IL setting to Never.
<ul style="list-style-type: none"> Standard SMS PASSCODE multi-factor authentication must be performed for all users. Support for Remote Access Policies is needed. 	<ul style="list-style-type: none"> Set the NPS IL setting to Always. Set the CRP authentication setting to Authenticate on this server.
<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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 <u>other</u> authentication system is NOT the user's AD password, and this authentication system is used often by users, which are <u>also</u> created in the SMS PASSCODE database, 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 <u>other</u> authentication system. On the other hand, if the users using the other authentication system are NOT created in the SMS PASSCODE database, then there is no problem, since SMS PASSCODE will not perform any AD password validations for non-SMS PASSCODE users.
<ul style="list-style-type: none"> 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. This is useful, if you would like to use SMS PASSCODE for authentication of non-AD users. 	<ul style="list-style-type: none"> 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.

f. Default domains

NOTE: This setting is only available, when SMS PASSCODE is installed as an **On-premise** or **Hybrid Setup**. In a **Cloud Setup**, the **Default Domains** setting is hidden, because in this case, users are always required to log in with a user name that exactly matches a user name or user alias that has been defined in the IntelliTrust™ tenant.

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 have two options:

Option 1: Explicit list of approved domains (most secure)

You can explicitly add the domains to the list, from which users are allowed to log in. The list of domains has two purposes:

1. **Restriction:** 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. **Prioritization:** 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.

If the NPS server has not joined any domain, then an empty list is treated as if it only contained the hostname of the NPS server. This will allow local Windows users on the NPS server to log in.

If the list is NOT empty, and you want to allow local Windows users on the NPS server to be able to log in, then you must manually add the hostname of the NPS server to the domain list.

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.

Option 2: Allow any domain (most flexible)

Alternatively, you can decide to allow logins from any domain, without defining the list of domains upfront. To choose this, select the **Allow logins from any domain (using fully qualified usernames only)** option. This is a flexible solution, in case your list of domains changes often, for example if you are a hosting partner.

Please note that in this case all users must log in using a fully qualified username, as there is no list to use for a prioritized search through the domains.

25.2.2.2 RADIUS Authorization Settings

NOTE: This section only applies, when SMS PASSCODE is installed as an **On-premise** or **Hybrid Setup**. In a **Cloud Setup**, the **Authorization** settings are not available.

When a user has been authenticated successfully by SMS PASSCODE RADIUS Protection, a RADIUS Access-Accept packet is returned to the RADIUS client. This packet does NOT contain any authorization information by default.

However, if your RADIUS client supports authorization, then you have two options for adding authorization information to the RADIUS Access-Accept packet:

- Enable the authorization feature of the SMS PASSCODE RADIUS Protection component
- Enable the internal NPS logic during authentication and set the Network Policy used to add authorization data.

It is possible to use both features together, in which case both features will add authorization information as defined.

This section describes how to configure the authorization feature of the SMS PASSCODE RADIUS Protection component. When this authorization feature is enabled, SMS PASSCODE RADIUS Protection will automatically determine the names of all AD groups, of which the authenticated user is a member. All or some of these group names are then added to the RADIUS authorization attribute and sent along with the RADIUS Access-Accept packet to the RADIUS client. The RADIUS client can subsequently retrieve all these group names from the attribute and allocate permissions depending on the AD group memberships of the user. It is even possible to apply transformations to the AD group names if the RADIUS client expects specific group names that you do not wish to create in your AD.

NOTE (User import required for authorization)

Collection of authorization data only works for users that have been imported to the SMS PASSCODE database using a User Integration Policy (UIP). This is because the UIP settings are reused in order to locate the right AD/LDAP directory in order to look up group memberships.

Authorization is configured on the **Authorization** tab:

RADIUS Settings for "VPN System 2"

Authentication | **Authorization** | Miscellaneous ☐ Inherit default settings

a ☒ Authorization enabled

Authorization attribute properties

Max size of attributes:
2048

Vendor code:
0

Attribute number:
0

Prefix: CTXSUserGroups= Separator: :

Restrict groups collected into the authorization attribute

Restrict to groups:

Add Remove Up Down

☐ Only collect first matching group

Reset to default settings... Ok Cancel

The settings have the following purposes:

a. Authorization enabled

This is the main setting to enable or disable authorization.

i. Cleared (default):

Authorization is disabled, i.e. no authorization attribute is included in any RADIUS Access-Accept packet.

ii. Selected:

Authorization is enabled, i.e. each RADIUS Access-Accept packet will contain an authorization attribute. The properties and content of the authorization attribute are defined

using the settings below.

b. Authorization attribute properties

This group of settings defines the main characteristics of the authorization attribute. The default settings are the settings expected by a Citrix Access Gateway with default settings.

Max size of attribute: Defines the maximum number of bytes to be used for adding authorization data to the RADIUS Access-Accept packet. The content of the authorization attribute will be cut off if it exceeds the specified maximum size. This is relevant, because a huge number of group memberships could potentially cause the complete RADIUS packet to exceed the maximum size allowed by the RADIUS protocol.

Vendor code: Use this setting to specify a vendor code in case your RADIUS client expects a specific vendor code in the authorization attribute.

Attribute number: Use this setting to specify an attribute number in case your RADIUS client expects a specific attribute number in the authorization attribute.

Prefix/Separator: The content of the authorization attribute will have a format like this:

[Prefix][Group1][Separator][Group2][Separator]....[GroupN][Separator]

Where [Group1], [Group2],..., [GroupN] are the names of the AD groups, of which the authenticated user is a member, and [Prefix] and [Separator] contain customizable content to be configured using the settings **Prefix** and **Separator**, respectively. E.g. if you set **Prefix** to "CTXSUserGroups=" and **Separator** to ";", and the user is a member of 3 groups called "OwaAccess", "CitrixAccess" and "SharePointAccess", then the content of the authorization attribute will be like this:

CTXSUserGroups=OwaAccess;CitrixAccess;SharePointAccess;

c. **Restrict groups collected into the authorization attribute**

SMS PASSCODE RADIUS Protection will collect all direct and indirect group memberships by default and put the names of such groups into the authorization attribute. If your users have many group memberships, the total length of the group names might exceed the maximum size allowed according to the **Max size of attribute** setting (item b, above), which will cause some of the group names to be cut off. Since you cannot predict which groups will be cut off, it might be better to select a restricted number of group names that you will actually need in your authorization attribute. This is just what the setting **Restrict groups collected into the authorization attribute** allows you to define.

You can add a number of group names to the list, which will restrict SMS PASSCODE RADIUS Protection to collect group names only from this list into the authorization attribute.

Group name transformation: When entering group names into the restriction list, you may enter the group names in a special format to perform transformation of the group names. The entry is case sensitive, and the syntax is:

[AD Group Name];[RADIUS Client Group Name]

For example, if you have an AD group called “Sales People” and you would like to report the group “OwaAccess” to the RADIUS client in this case, then you should add the following entry to the restriction list:

Sales People;OwaAccess

Only collect first matching group: If you select this setting, then SMS PASSCODE RADIUS Protection will at most put a single group name into the authorization attribute. This will be the first group in the restriction list, of which the authenticated user is a member. Restricting to a single group is useful if your RADIUS client will only accept a single value in the authorization attribute.

Since you can customize different settings per CRP of the NPS, this allows you to define different authorization behaviors for different CRPs – for example for different RADIUS clients.

25.2.2.3 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:

NOTE: This setting is only available, when SMS PASSCODE is installed as an **On-premise** or **Hybrid Setup**. In a **Cloud Setup**, the challenge message content is controlled by the IntelliTrust™ cloud service.

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. 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. Besides being useful for authentication monitoring, collecting end-user IP addresses is also useful in order to enable *location and behavior aware authentication* for even stronger security. Please read section 16.1 (page 96) to get a short overview about this topic.

IntelliTrust™ Integration

In case of a **Cloud Setup** or a **Hybrid Setup**, if collection of end-user IP addresses is enabled, such collected IP addresses will be forwarded to IntelliTrust™ as well, where they can be taken into account during evaluation of risk-based authentication. However, this only works, if the **Authentication API** application being used in IntelliTrust™ has been configured correctly to receive such IP addresses (cf. section 16.2, page 99).

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.

25.3 Configuring AD FS Protection

The SMS PASSCODE **AD FS Protection** component adds multi-factor authentication to applications that are accessible via AD FS. This section describes how to configure SMS PASSCODE **AD FS Protection** for such scenarios.

SMS PASSCODE **AD FS Protection** allows you to apply SMS PASSCODE multi-factor authentication to all authentication scenarios supported by the AD FS 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.

25.3.1 Background

AD FS is an optional Windows Server role in Windows Server 2012 R2 / 2016 / 2019. 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.

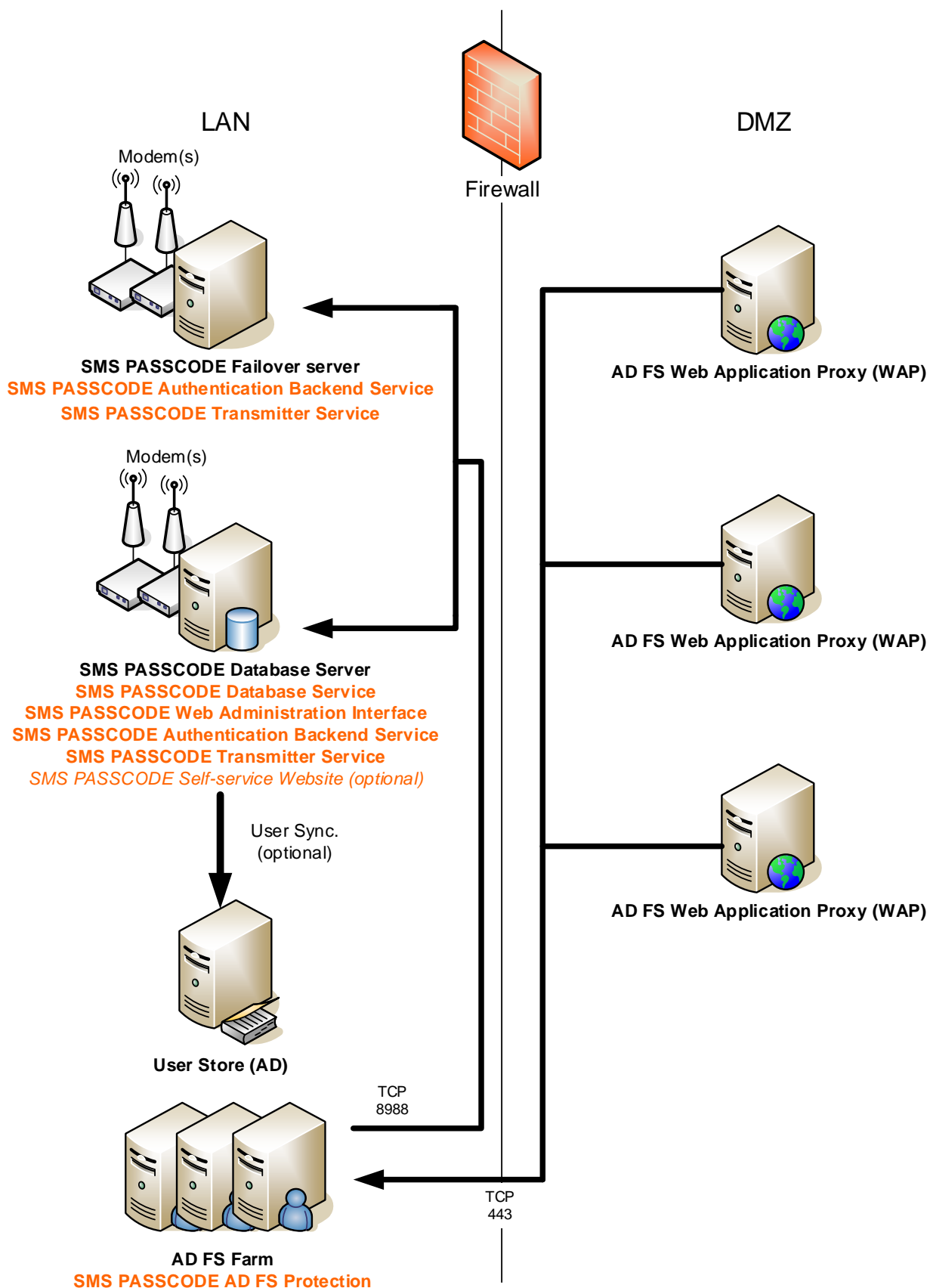
Any such authentication scenarios supported by the AD FS infrastructure can be extended with SMS PASSCODE multi-factor authentication (MFA), by installing SMS PASSCODE AD FS Protection on your AD FS server(s) and enabling MFA for the applications of your choice, in the AD FS management console.

25.3.2 AD FS Infrastructure

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

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

An example of an installation setup is shown below:



Note: In a **Cloud Setup**, the servers **SMS PASSCODE Database Server** and **SMS PASSCODE Failover server** will not be present. Instead, the **SMS PASSCODE AD FS Protection** component will communicate directly with the IntelliTrust™ cloud service.

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

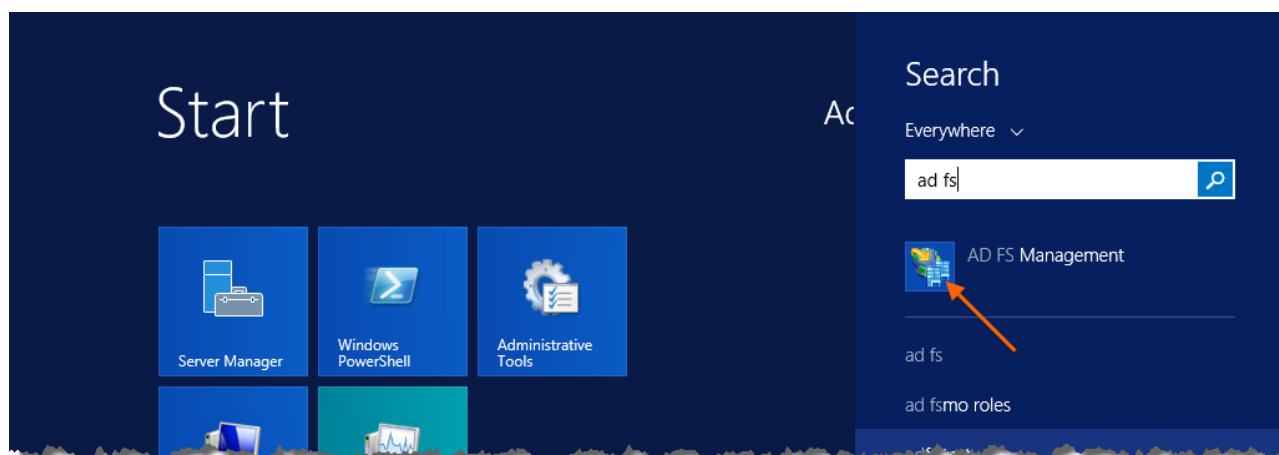
The installation of the AD FS Protection component on each AD FS server will install a so-called SMS PASSCODE AD FS **MFA Adapter** on every such server. You need to configure this MFA Adapter, to activate SMS PASSCODE multi-factor authentication. This is described below in sections 25.3.3 and 25.3.4 for AD FS 2012 R2 and 2016/2019, respectively.

25.3.3 Configuring the MFA Adapter for AD FS 2012 R2

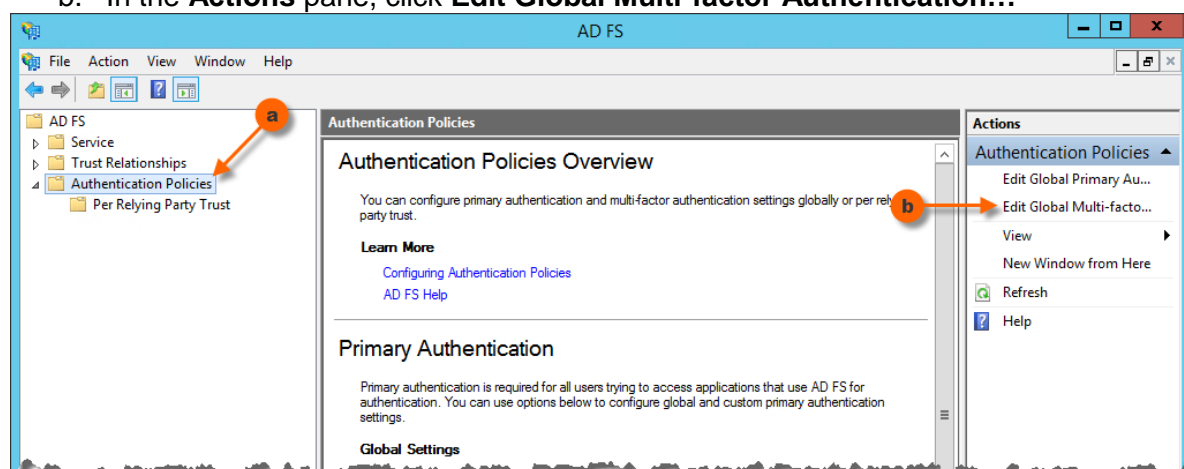
This section applies to Windows Server 2012 R2. It is described below, how you enable the SMS PASSCODE MFA Adapter, after you have installed it on your AD FS server (or on every AD FS server, in case of an AD FS farm).

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

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



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

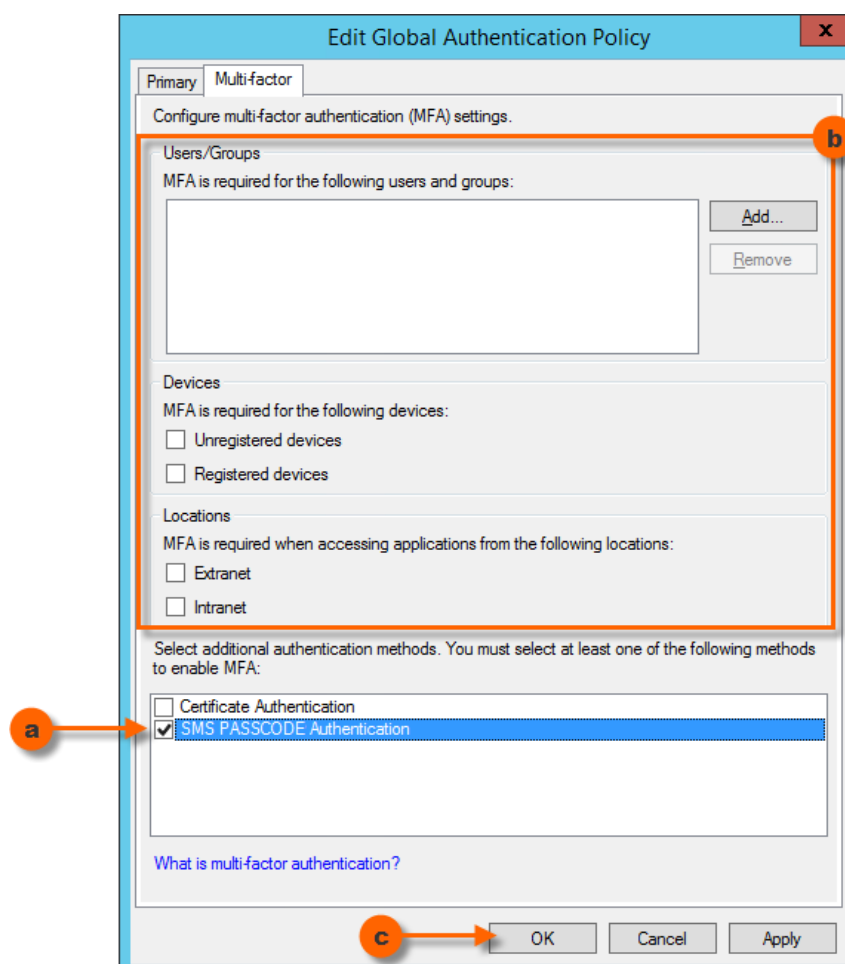


3. The dialog **Edit Global Authentication Policy** opens, with the tab **Multi-factor** selected.
 - a. In the bottom listbox, select the checkbox **SMS PASSCODE Authentication** in order to enable the SMS PASSCODE MFA Adapter.
 - b. Additionally, in order for multi-factor authentications to be triggered, you need to specify the conditions for multi-factor authentication to occur. Either you can specify conditions directly here, on the **Global Authentication Policy**, which will affect all applications ("Relying Parties") – or you may leave the conditions empty here, if you prefer to set individual MFA conditions per application afterwards⁴⁸.

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.



⁴⁸ 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.

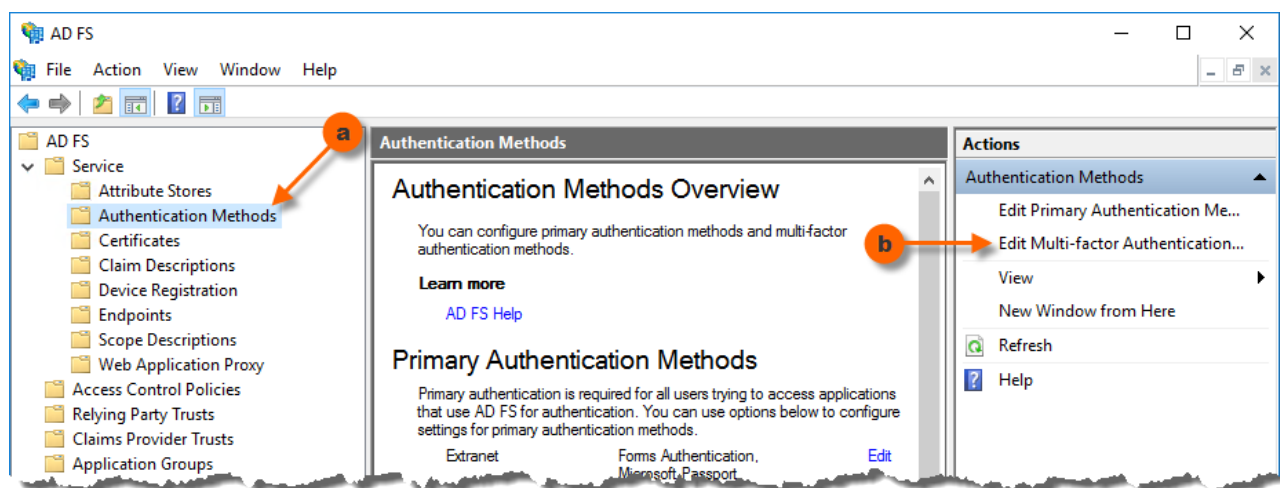
After having enabled and configured the SMS PASSCODE MFA adapter, please make sure to test the authentication behavior of the affected applications, in order to ensure the expected authentication behavior.

25.3.4 Configuring the MFA Adapter for AD FS 2016/2019

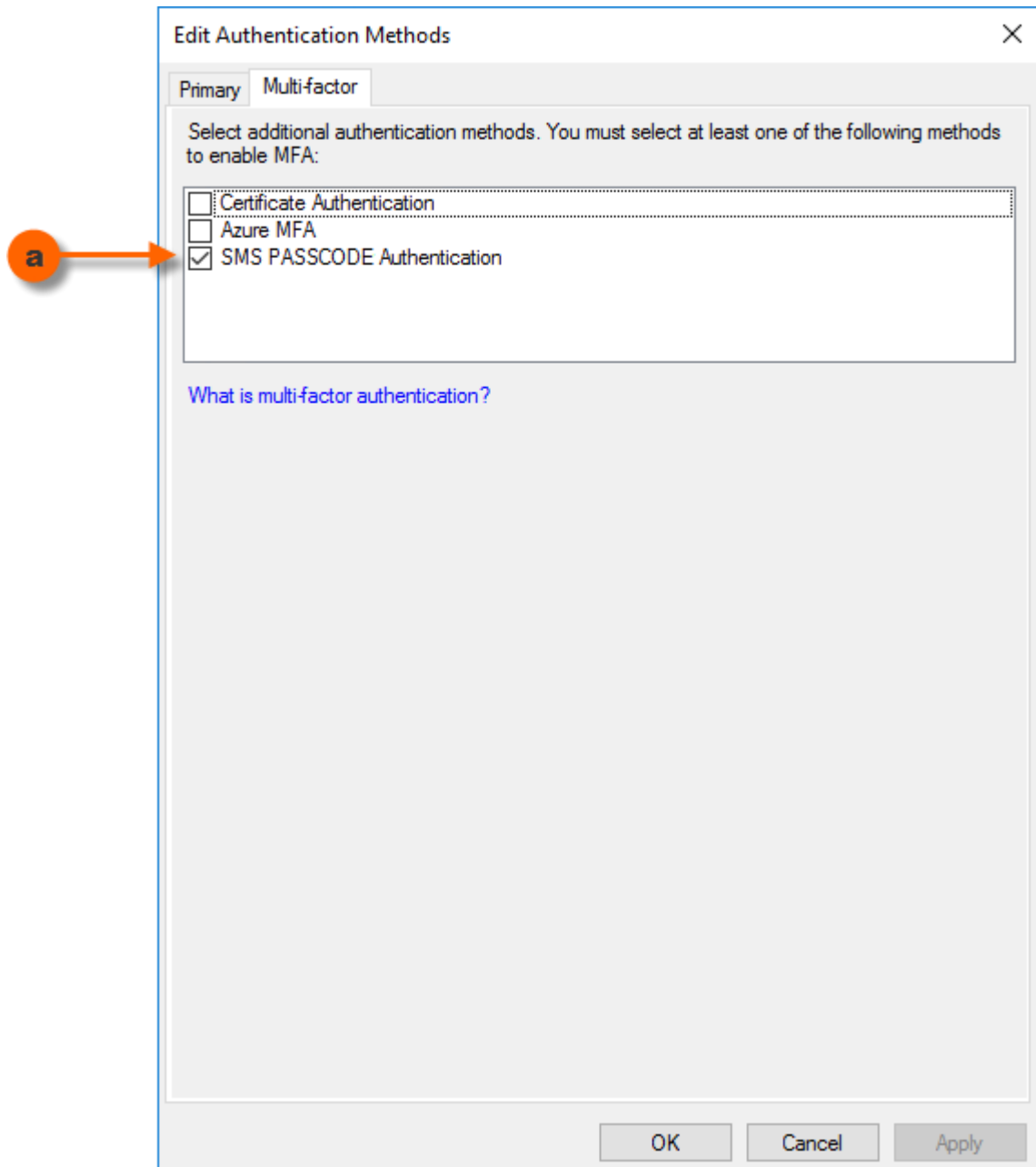
This section applies to Windows Server 2016 / 2019. It is described below, how you enable the SMS PASSCODE MFA Adapter, after you have installed it on your AD FS server (or on every AD FS server, in case of an AD FS farm).

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

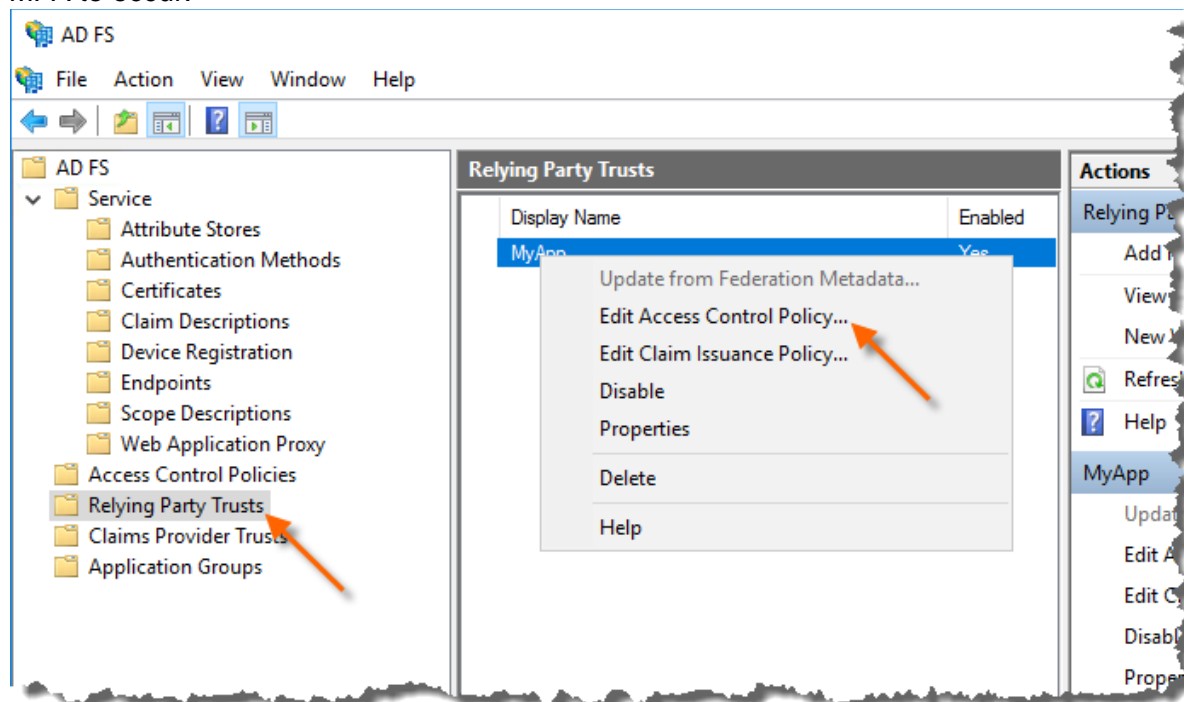
1. Open the AD FS Management console (`Microsoft.IdentityServer.msc`) on your primary AD FS server.
2. In the AD FS Management console:
 - a. Select the **Authentication Methods** node in the tree to the left.
 - b. In the **Actions** pane, click **Edit Multi-factor Authentication Methods...**



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, 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.

25.3.5 Uninstalling the MFA Adapter

In case you uninstall the SMS PASSCODE AD FS Protection component from an AD FS 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.

25.4 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 allowed by the SMS PASSCODE **IIS Website Protection** component, without SMS PASSCODE protection. You must manually enable SMS PASSCODE authentication if required.
- b. If you wish to protect other websites than OWA or RD Web Access by SMS PASSCODE authentication, then you must 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 / 2016 / 2019 only) and websites using Basic, Integrated Windows Authentication or ASP.Net Form Based 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.

25.4.1 Native HTTP Module

The SMS PASSCODE **IIS Website Protection** component is implemented using a native HTTP module. This module is added to the IIS running on the server and extends the behavior of the IIS.

The default path of the 64 bit module is:

```
C:\Program Files\SMS PASSCODE\ISAPI\SMSPASSCODE.IIS.HttpModule.dll
```

25.4.2 IIS Website Protection Configuration File

The behavior of the HTTP module is controlled by an 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 HTTP module by making changes to this configuration file. The most common configuration changes are made easiest using the **IIsAdministration** PowerShell module. This module is installed together with the IIS Website protection and immediately available through the PowerShell console. The PowerShell default location is over here:

```
C:\Program Files\SMS PASSCODE\PS\Modules\SMSPASSCODE.PS.IIsAdministration
```

The syntax and usage of the **IIsAdministration** PowerShell module is described in section 25.4.3 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 25.4.4.

IMPORTANT:

Whenever changes are made to the IIS Website protection configuration file using the **IlsAdministration** PowerShell module, these changes take effect immediately (Unless an explicit switch is provided to skip this step).

Whenever changes are made to the configuration file manually, these changes do not take effect until the **Repair-SmsPcIisWebSiteConfiguration** PowerShell command is executed or **SMS PASSCODE ISAPI Service** has been restarted.

25.4.3 The IlsAdministration PowerShell Module

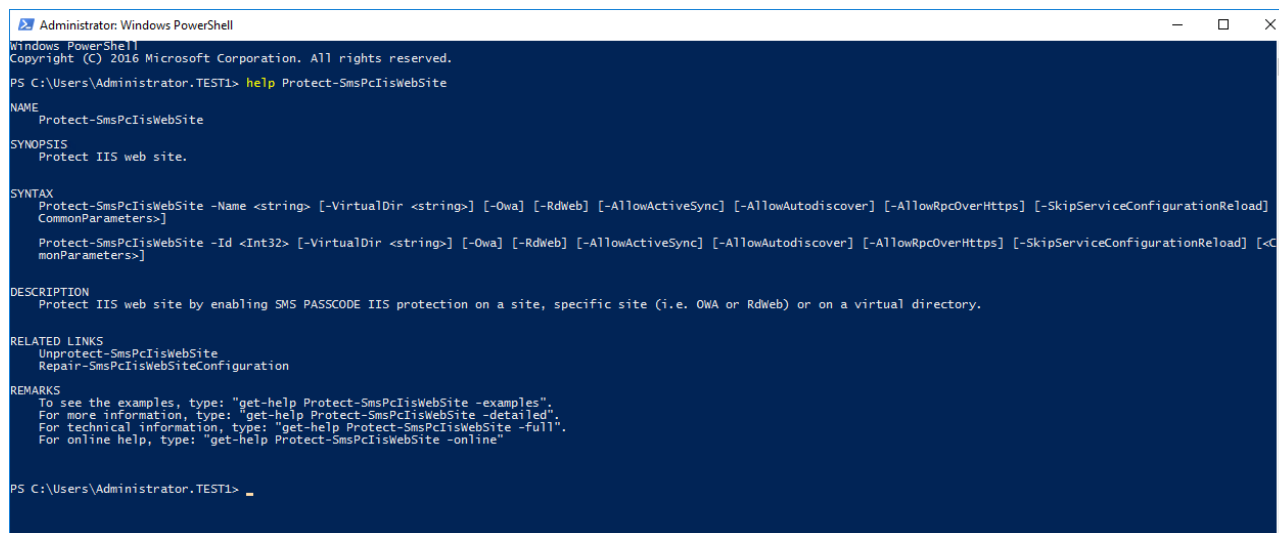
This module has three main features:

- Enable SMS PASSCODE authentication for a specific website or virtual directory on the local IIS.
- Disable SMS PASSCODE authentication for a specific website on the local IIS.
- Refresh the IIS Website protection configuration file to include any newly added websites on the local IIS.

The following sub-sections describe the syntax of the **IlsAdministration** module. The syntax is also well described using PowerShell help system.

25.4.3.1 Enable Protection of a Website

To enable SMS PASSCODE authentication for a specific website, use the `Protect-SmsPcIisWebSite` command in one of the following two ways:



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.TEST1> help Protect-SmsPcIisWebSite

NAME
    Protect-SmsPcIisWebSite

SYNOPSIS
    Protect IIS web site.

SYNTAX
    Protect-SmsPcIisWebSite -Name <string> [-VirtualDir <string>] [-Owa] [-RdWeb] [-AllowActiveSync] [-AllowAutodiscover] [-AllowRpcOverHttps] [-SkipServiceConfigurationReload] [-CommonParameters]
    Protect-SmsPcIisWebSite -Id <Int32> [-VirtualDir <string>] [-Owa] [-RdWeb] [-AllowActiveSync] [-AllowAutodiscover] [-AllowRpcOverHttps] [-SkipServiceConfigurationReload] [-CommonParameters]

DESCRIPTION
    Protect IIS web site by enabling SMS PASSCODE IIS protection on a site, specific site (i.e. OWA or RdWeb) or on a virtual directory.

RELATED LINKS
    Unprotect-SmsPcIisWebSite
    Repair-SmsPcIisWebSiteConfiguration

REMARKS
    To see the examples, type: "get-help Protect-SmsPcIisWebSite -examples".
    For more information, type: "get-help Protect-SmsPcIisWebSite -detailed".
    For technical information, type: "get-help Protect-SmsPcIisWebSite -full".
    For online help, type: "get-help Protect-SmsPcIisWebSite -online".

PS C:\Users\Administrator.TEST1>
  
```

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

Argument	Description
-Name	<p>This argument is used to specify the name of the website to protect. Example:</p> <pre>Protect-SmsPcIisWebSite -Name "Default Web Site"</pre>
-Id	<p>This argument is used to specify the IIS ID of the website to protect. The default website always has ID 1. Example:</p> <pre>Protect-SmsPcIisWebSite -Id 1</pre> <p>Use IIS administration PowerShell module command <code>(Get-IISServerManager).Sites</code> to get a list of the IDs of the different websites.</p>
-VirtualDir (optional)	<p>This optional argument is used to specify the name of the virtual directory under the website. Only this virtual directory will be protected. Example:</p> <pre>Protect-SmsPcIisWebSite -Name "Default Web Site" -VirtualDir "MyDirectory"</pre>
-Owa (optional)	<p>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.</p>
-AllowActiveSync (optional)	<p>This argument is only allowed together with the <code>-Owa</code> argument. It instructs the HTTP module to disable SMS PASSCODE authentication for ActiveSync connections.</p>
-AllowAutoDiscover (optional)	<p>This argument is only allowed together with the <code>-Owa</code> argument. It instructs the HTTP module to disable SMS PASSCODE authentication for ActiveSync AutoDiscover requests.</p>
-AllowRpcOverHttps (optional)	<p>This argument is only allowed together with the <code>-Owa</code> or <code>-RdWeb</code> arguments. It instructs the HTTP module to disable SMS PASSCODE authentication for RPC over HTTP/HTTPS connections.</p>
-RdWeb	<p>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.</p> <p>Please note that in order to protect an RD Web Access site, additional actions are required (cf. section 12.2.2, page 55).</p>

Examples:

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

```
Protect-SmsPcIisWebSite -Name "Default Web Site" -Owa -AllowActiveSync
```

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

```
Protect-SmsPcIisWebSite -Id 1 -Owa -AllowActiveSync
```

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

```
Protect-SmsPcIisWebSite -Name "SMS PASSCODE Admin"
```

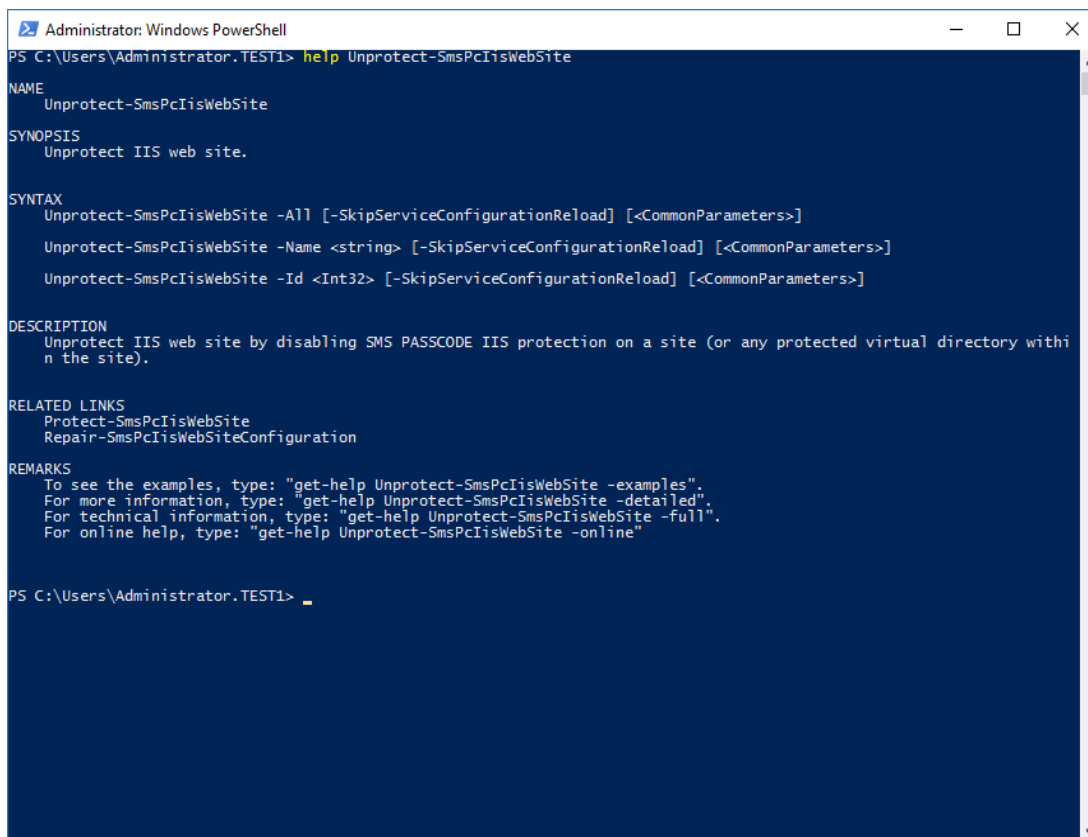
- Enable SMS PASSCODE authentication for an OWA site using Basic or Integrated Windows Authentication:

```
Protect-SmsPcIisWebSite -Name "Default Web Site"
```

25.4.3.2 Disable Protection of a Website

To disable SMS PASSCODE authentication for a specific website, use the

`Unprotect-SmsPcIisWebSite` PowerShell command in one of the following ways:



```
Administrator: Windows PowerShell
PS C:\Users\Administrator.TEST1> help Unprotect-SmsPcIisWebSite

NAME
    Unprotect-SmsPcIisWebSite

SYNOPSIS
    Unprotect IIS web site.

SYNTAX
    Unprotect-SmsPcIisWebSite -All [-SkipServiceConfigurationReload] [<CommonParameters>]
    Unprotect-SmsPcIisWebSite -Name <string> [-SkipServiceConfigurationReload] [<CommonParameters>]
    Unprotect-SmsPcIisWebSite -Id <Int32> [-SkipServiceConfigurationReload] [<CommonParameters>]

DESCRIPTION
    Unprotect IIS web site by disabling SMS PASSCODE IIS protection on a site (or any protected virtual directory within the site).

RELATED LINKS
    Protect-SmsPcIisWebSite
    Repair-SmsPcIisWebSiteConfiguration

REMARKS
    To see the examples, type: "get-help Unprotect-SmsPcIisWebSite -examples".
    For more information, type: "get-help Unprotect-SmsPcIisWebSite -detailed".
    For technical information, type: "get-help Unprotect-SmsPcIisWebSite -full".
    For online help, type: "get-help Unprotect-SmsPcIisWebSite -online".

PS C:\Users\Administrator.TEST1> _
```

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

Argument	Description
-Name	This argument is used to specify the name of the website to unprotect. Example: <code>Unprotect-SmsPcIisWebSite -Name "Default Web Site"</code>
-Id	This argument is used to specify the ID of the website to unprotect. The default website always has ID 1. Example: <code>Unprotect-SmsPcIisWebSite -Id 1</code> Use IIS administration PowerShell module command <code>(Get-IISServerManager).Sites</code> to get a list of the IDs of the different websites.
-All	This argument is used to completely remove IIS Website protection from all the websites. In this case, config.xml file is not modified and protection can be restored afterwards by using <code>Repair-SmsPcIisWebSiteConfiguration</code> command. (Please see 25.4.3.3)

Examples:

- Disable SMS PASSCODE authentication for an OWA site:

```
Unprotect-SmsPcIisWebSite -Name "Default Web Site"
```

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

```
Unprotect-SmsPcIisWebSite -Id 1
```

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

```
Unprotect-SmsPcIisWebSite -Name "SMS PASSCODE Admin"
```

25.4.3.3 Refresh the Configuration File

The IIS Website protection 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 IIS Website protection configuration file, then by default the HTTP module will allow access to this site.

IMPORTANT: Starting from SMS PASSCODE version 2018, the default behavior for a non-listed website is to allow ordinary access (without requiring multi-factor authentication). In earlier SMS PASSCODE versions, access was blocked by default.

If you want newly added websites to be configured explicitly in the ISAPI filter configuration file, you can use the following command:

```
Repair-SmsPcIisWebSiteConfiguration
```

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.

In addition, this command can be used to repair the SMS PASSCODE IIS Website protection component configuration based on the state of the IIS Website protection configuration file. In other words, manual and advanced configuration can be done in the IIS Website protection configuration file and then applied by running this PowerShell command.

25.4.4 IIS Website Protection Configuration File Syntax

The configuration of the HTTP module is stored in an 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 not take effect until **Repair-SmsPclisWebSiteConfiguration** command (described in the section above) is executed or the **SMS PASSCODE ISAPI Service** has been restarted.

25.4.4.1 <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.

25.4.4.2 <SITE> Element

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

```
<SITE name="Web Site Name" smspasscodedir="virtual dir name" >
  <URL />
  ...
  <URL />
</SITE>
```

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 HTTP module during SMS PASSCODE authentication. Recommended value is **"/SmsPasscodeLogon/"**. It is recommended to enable SMS

PASSCODE authentication for a website using the PowerShell module because this tool will automatically create the required virtual directory and configure it correctly (please read section 25.4.3.1, page 408).

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.

25.4.4.3 <URL> Element

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

```
<URL path="URL path" smspasscode="true|false"
credentials="credentials source" logoutUrl="URL path" >
    <host />
    ...
    <host />
</URL>
```

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:

- /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 PowerShell module with the -owa or -rdweb option to protect an OWA site or RD Web access site, respectively (please read section 25.4.3.1, page 408).

- **logoutUrl**: This is an **optional** attribute. It should be used to specify the logout URL for the ASP.Net Form Based Authentication. If this URL is navigated by the user's browser, then session is marked as expired by the SMS PASSCODE IIS Website protection.

For example, if SMS PASSCODE Self Service Web Site is set to form based authentication (please read section 22.5, page 328) and is protected by the IIS Website protection, then the following URL should be used to make logout functionality work properly:

- /FBA/Logout

25.4.4.4 <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).

25.4.4.5 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:

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

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

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

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

```
<CONFIG>
  <SITE name="Default Web Site" smspasscodedir="/SmsPasscodeLogon/" >
    <URL path="/" smspasscode="true">
      <HOST ip="192.168.*" smspasscode="false" />
    </URL>
  </SITE>
</CONFIG>
```

```

        </URL>
    </SITE>
</CONFIG>

```

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

```

<CONFIG>
  <SITE name="Default Web Site" smspasscodedir="/SmsPasscodeLogon/" >
    <URL path="/" smspasscode="false" />
    <URL path="/OWA" smspasscode="true"
      type="FormAuthentication" credentials="OWA" />
    <URL path="/rpc" smspasscode="true" >
      <host ip="localhost" smspasscode="false" >
    </URL >
  </SITE>
</CONFIG>

```

25.5 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**.

25.5.1 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 local⁴⁹ 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 not 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.

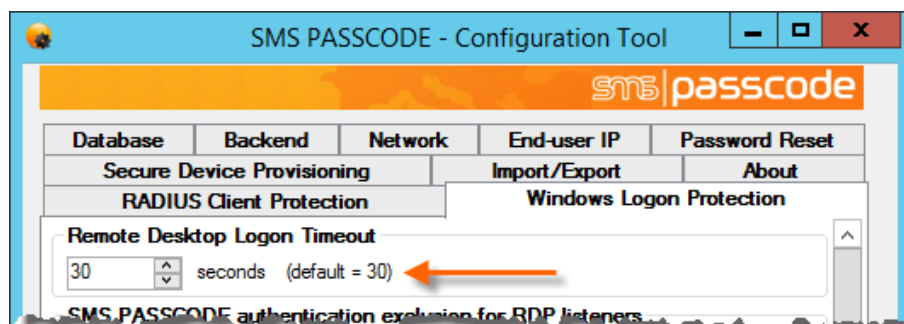
By default, all users being member of the local Administrators group are automatically added during installation to the **SMS PASSCODE console exclusion** group. This ensures that local administrators will always be able to log on using the local console.

25.5.2 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

⁴⁹ 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.

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:



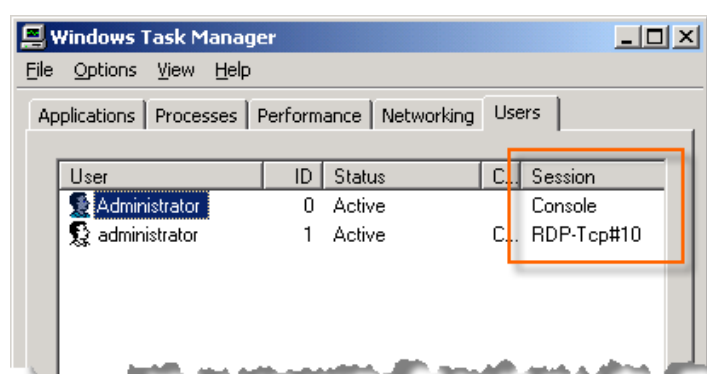
IMPORTANT

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

25.5.3 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**.

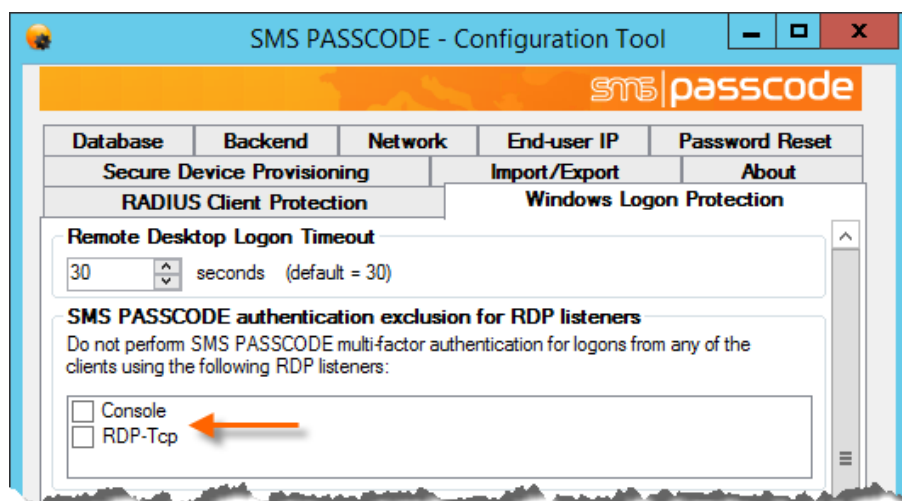
You can see which **WinStation** has been used to establish each session on a machine by inspecting the **Users** tab in the **Task Manager**. Each session will be named using the name of the corresponding **WinStation**.



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 25.5.1, page 415).

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:



25.5.3.1 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.

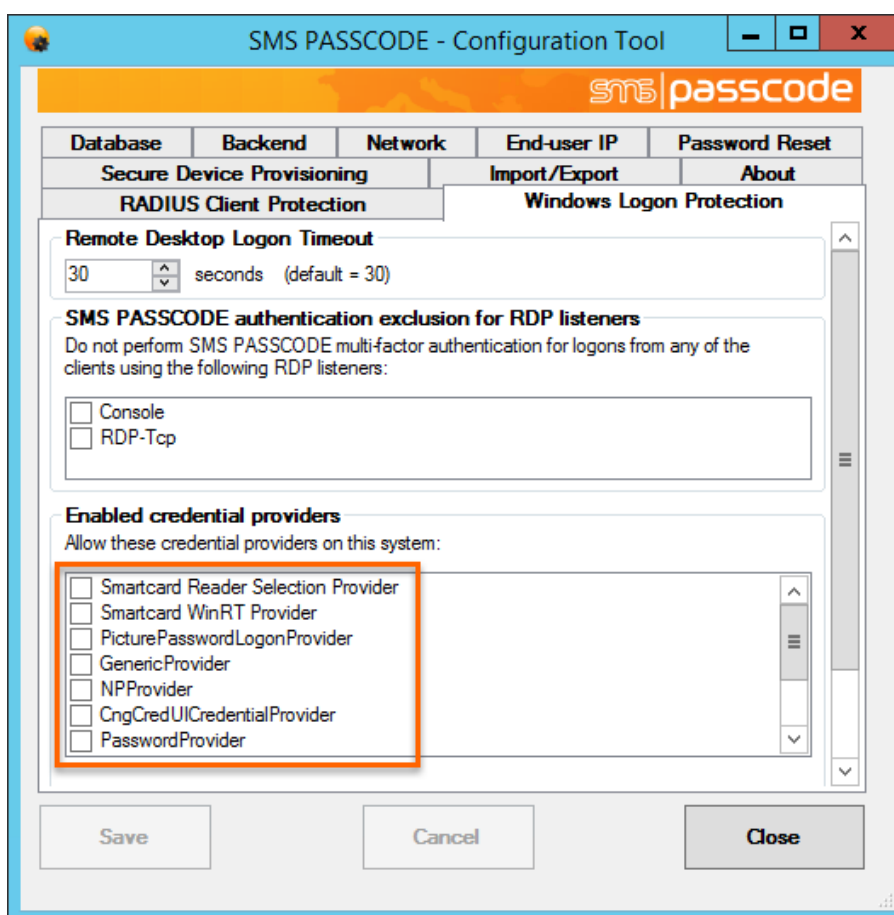
4. Open the exported file. Change the name of the key "RDP-Tcp" to a new name of own choice. This will be the name of the custom RDP Listener. Additionally, change any other required settings, e.g. **PortNumber**. Save the file.
5. Import the modified file into the registry. The registry will now contain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

25.5.4 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 providers⁵⁰ 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:



⁵⁰ 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.

25.5.5 Users' Cached Credentials

The SMS PASSCODE Windows Logon protection validates user passwords by using the Windows API. By default, the *network logon* type is used which is intended for high performance servers to authenticate passwords. This logon type provides high performance; however, it is not suitable for all situations. For example, if caching of user credentials is required (i.e. if the domain controller is unavailable, users with cached credentials on the server can still logon) then the default behavior can be changed to *interactive logon* type.

To change password validation to *interactive logon* type, 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\SOFTWARE\SMS PASSCODE\WinLogon

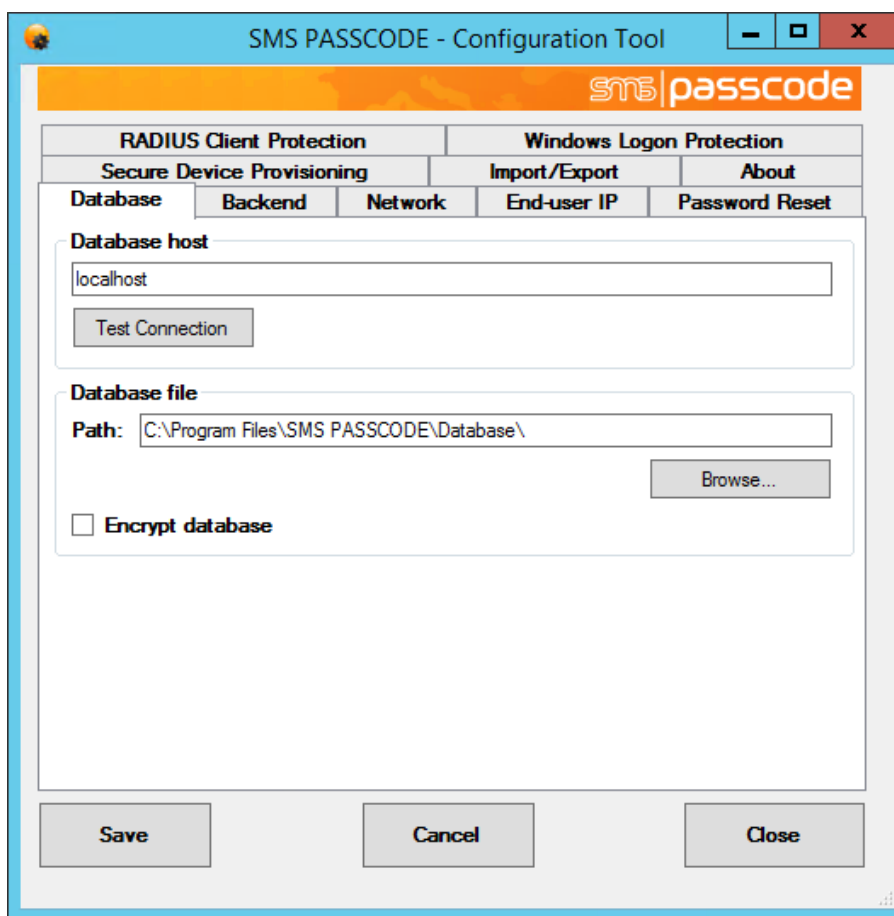
Right-click the key, select New and then DWORD (32-bit) value option.

4. Name the new setting as following **UseNetworkLogonType** and leave the default value of 0.

26 CONFIGURATION TOOL

The SMS PASSCODE **Configuration Tool** is used to configure machine specific SMS PASSCODE settings. A link to start the tool is located in the SMS PASSCODE folder of 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:

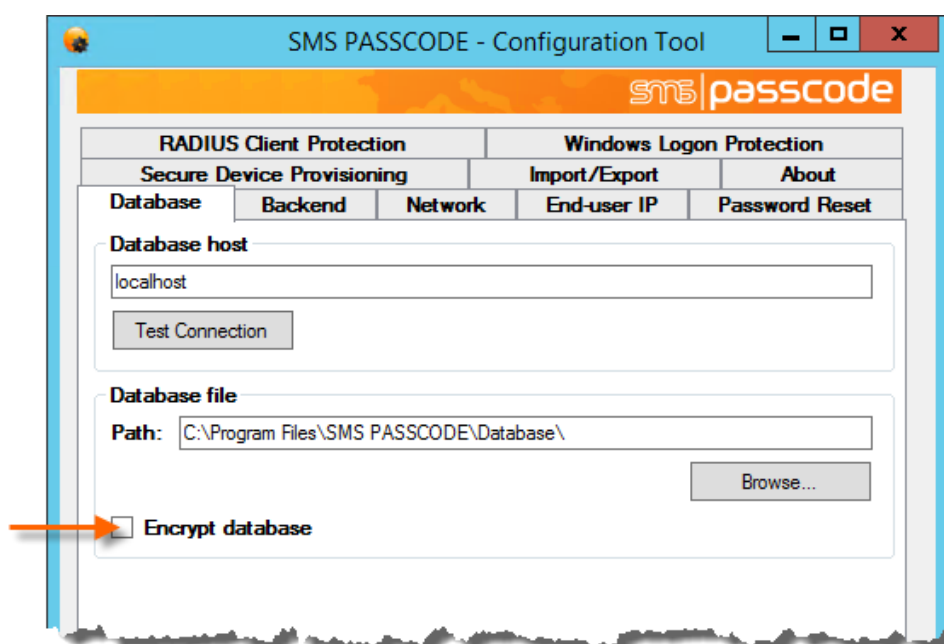
Tab	Explanation
Database	<p>This tab appears during an On-premise or Hybrid Setup, not for a Cloud Setup.</p> <p>You can specify the server on this tab, on which the SMS PASSCODE Database Service is located. This tab also contains a button Test Connection, which will perform a test whether the connection to the specified database server operates properly.</p> <p>On the server with the SMS PASSCODE Database component installed, this tab also includes an option for enabling strong encryption of the SMS PASSCODE database (cf. section 26.1).</p>

Tab	Explanation
Backend	<p>This tab appears when an SMS PASSCODE authentication client or SMS PASSCODE Password Reset Backend Service has been installed.</p> <p>First of all, you can specify on this tab, whether to connect to an on-premise SMS PASSCODE backend (using an On-premise or Hybrid Setup), or whether to connect directly to the IntelliTrust™ cloud service (using a Cloud Setup).</p> <p>On-premise/Hybrid Setup: In this case, you can furthermore specify a list of SMS PASSCODE Authentication Backend Service hosts that the authentication client(s) or PRBS on the local machine must use for handling authentication attempts. In addition, the priority is specified, i.e. in which order the authentication client(s) should attempt to communicate with the specified hosts. This tab also contains a button Test Connection, which will test whether the connections to the specified hosts operate properly.</p> <p>Cloud Setup: In this case, you can furthermore specify the URL to the IntelliTrust™ tenant to which you want to connect, and the ID(s) of the relevant Application(s) of type "Authentication API" in IntelliTrust™. This tab also contains a button Test Connection, which will test whether the connection to the specified IntelliTrust™ tenant operates properly (but will not test, whether the Application IDs are valid).</p>
Network	<p>This tab appears during an On-premise or Hybrid Setup, not for a Cloud Setup.</p> <p>On this tab you can specify which TCP ports must be used by the different SMS PASSCODE components and specify a shared secret (password) that is used for encrypting all communication between the different machines with SMS PASSCODE components installed. Please ensure that the TCP ports and shared secret are configured identically on all involved SMS PASSCODE machines. If this is not observed, communication between the machines will fail.</p>
Proxy Settings	<p>This tab only appears during a Cloud Setup.</p> <p>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 IntelliTrust™ cloud service via such a proxy.</p>
End-user IP	<p>This tab appears only when at least one SMS PASSCODE authentication client or the SMS PASSCODE Password Reset Website has been installed on the local machine. The tab allows you optionally to enable collection of end-user IP addresses. Collection of end-user IP addresses is required, if you would like to forward such IP addresses to IntelliTrust™, or if you would like to make use of <i>location and behavior aware authentication</i>. Please read section 26.2 (page 424) for more details.</p>
Password Reset	<p>This tab appears only when the SMS PASSCODE Password Reset Website and/or SMS PASSCODE Password Reset Backend Service component has been installed on the local machine. The tab allows configuring different settings related to the PRWS and PRBS components. Please read sections 23.6.1 (page 349) and 23.7.2 (page 357), respectively, for more details.</p>
RADIUS Client Protection	<p>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 25.2.2 (page 380) for more details.</p>

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 25.5 (page 415) for more details.
Secure Device Provisioning	This tab appears only when SMS PASSCODE Secure Device Provisioning has been installed on the local machine. The tab allows configuring the connection to the relevant Exchange Server to become protected. Please read section 24.2 (page 364) 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 that include a shared secret, you will be prompted to enter a password that is used for protecting (encrypting) the shared secret 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 network settings including a shared secret to all these clients. The syntax for importing and exporting settings is described in section 26.3 (page 428).

26.1 DB Encryption

On a server with the SMS PASSCODE Database component installed, the **Database** tab of the SMS PASSCODE Configuration Tool includes an option for enabling strong encryption of the SMS PASSCODE database files.



To enable encryption, proceed as follows:

- a. Select the checkbox **Encrypt database**
- b. Enter an encryption password
- c. Click the **Save** button

The screenshot shows a dialog box titled "Set encryption password to:". It contains a checkbox labeled "Encrypt database" which is checked. Below the checkbox are two text input fields: "Password:" and "Verify password:", both filled with dots. At the bottom of the dialog are three buttons: "Save", "Cancel", and "Close". Red circles with letters 'a', 'b', and 'c' are overlaid on the image to indicate the steps: 'a' points to the checkbox, 'b' points to the password fields, and 'c' points to the "Save" button.

To disable encryption, clear the **Encrypt database** checkbox and click the **Save** button. You will be asked to enter the same encryption password again that was used when enabling the encryption.

IMPORTANT: When enabling encryption of the SMS PASSCODE Database, please make sure to keep the encryption password in a safe place. Without this password, you will not be able to disable encryption again or to perform a disaster recovery afterwards.

Encryption can be enabled, no matter if the SMS PASSCODE Database Service is running or is stopped. If the database service is running, encryption will be enabled on-the-fly, i.e. there is no need to restart the database service.

Disabling encryption is only possible while the SMS PASSCODE Database Service is running. Decryption of the database files will occur on-the-fly, i.e. there is no need to restart the database service.

26.2 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, SMS PASSCODE Self-service Website, or SMS PASSCODE Password Reset Website should collect end-user IP addresses during authentication attempts.

By default, collection of end-user IP addresses is disabled for all clients, for the Self-service Website and for the Password Reset Website. However, if you would like to make use of *location and behavior aware authentication* (cf. section 16.1, page 96) a pre-requisite is that end-user IP addresses must be collected and reported to the SMS PASSCODE backend.

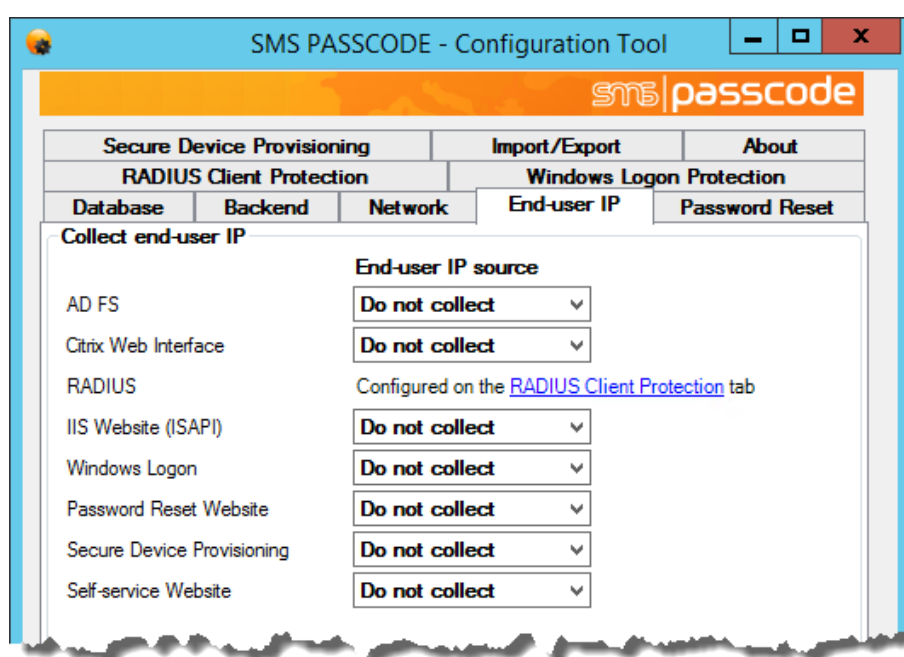
Enabling collection of end-user IP addresses can be done independently for any authentication client, Self-service Website and Password Reset Website installed locally.

IntelliTrust™ Integration

In case of a **Cloud Setup** or a **Hybrid Setup**, if collection of end-user IP addresses is enabled, such collected IP addresses will be forwarded to IntelliTrust™ as well, where they can be taken into account during evaluation of risk-based authentication. However, this only works, if the **Authentication API** application being used in IntelliTrust™ has been configured correctly to receive such IP addresses (cf. section 16.2, page 99).

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 only appears, if at least one SMS PASSCODE authentication client, the SMS PASSCODE Self-service Website, or the SMS PASSCODE Password Reset Website is installed locally. The tab will show a list of the clients available for configuration on the local machine:

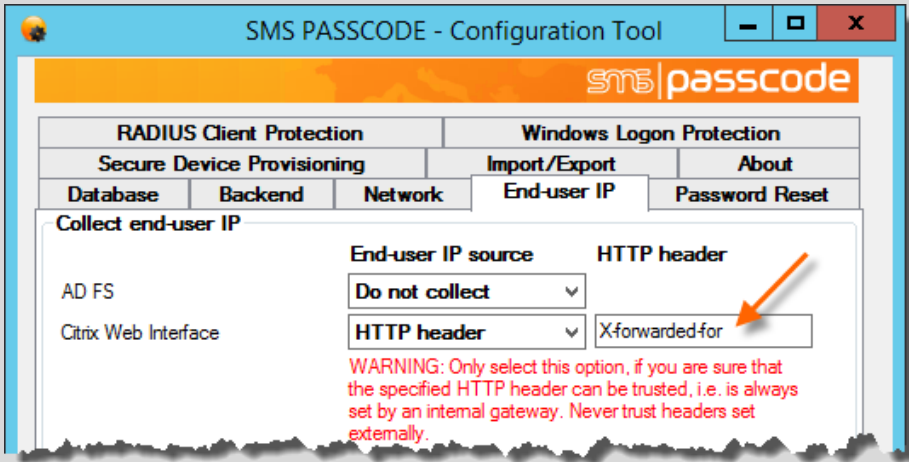


Note: As can be seen from the screenshot above, end-user IP collection for SMS PASSCODE RADIUS Protection is not configured on the **End-user IP** tab, but on the **RADIUS Client Protection** tab. This is due to the fact, that end-user IP collection can be configured differently per Connection Request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

End-user IP source option	Explanation
Network connection	<p>This option configures the client to report the end-user IP address according to the IP address of the source socket of the network connection. This is the recommended option, but only in case your network infrastructure is configured in such a way that the client recognizes the real end-user IP address.</p> <p>When selecting this option, it is recommended to perform some initial tests from different internal and external IP sources to ensure, that the correct IP addresses are reported.</p>

End-user IP source option	Explanation
HTTP Header	<p>This option is only available for services hosted by a Microsoft Internet Information Server (IIS), meaning:</p> <ul style="list-style-type: none"> • SMS PASSCODE Citrix Web Interface Protection • SMS PASSCODE IIS Website Protection • SMS PASSCODE AD FS Protection • SMS PASSCODE Secure Device Provisioning • SMS PASSCODE Password Reset Website • SMS PASSCODE Self-service Website <p>In this case, you may configure the authentication client to collect the end-user IP address from an HTTP header of your own choice. By default, the header X-forwarded-for⁵¹ is suggested, but you can enter any other name into the textbox, that appears:</p>  <p>This option should be used, when the authentication client is located behind a reverse proxy that hides the real end-user IP address, but at the same time stores the original end-user IP address into an HTTP header. Examples of such reverse proxies are Citrix Secure Gateway/Citrix Access Gateway Standard⁵², Bluecoat⁵³ and NetScaler.</p> <p>When selecting this option, it is recommended to perform some initial tests from different internal and external IP sources to ensure, that the correct IP addresses are reported.</p> <div style="background-color: red; color: white; padding: 10px;"> <p>WARNING!</p> <p>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.</p> </div>

⁵¹ 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.

⁵² HTTP header **X-forwarded-For** is hard-coded and enabled by default

⁵³ Please read KB2996 on <http://kb.bluecoat.com> for how to enable

26.3 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 the shared secret during export and import, respectively. The password must contain at least 5 characters. This argument is only required if the exported/imported settings contain a shared secret.
-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 the shared secret using the password **1234567890ABCDE**:

```
Config.exe -export:"mySettings.xml" -password:"1234567890ABCDE"
```

- Export all current settings to a file named **mySettings.xml**. Encrypt the shared secret using the password **1234567890ABCDE**. Perform the action quietly, i.e. do not open the Configuration Tool:

```
Config.exe -export:"mySettings.xml" -password:"1234567890ABCDE" -quiet
```

- Open the Configuration Tool and import settings from a file named **mySettings.xml**. Decrypt the shared secret using the password **1234567890ABCDE**:

```
Config.exe -import:"mySettings.xml" -password:"1234567890ABCDE"
```

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

- Import settings from a file named **mySettings.xml**. Decrypt the shared secret using the password **1234567890ABCDE**. 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:"1234567890ABCDE" -quiet
```

27 BACKUP AND RECOVERY

This section describes what files to backup to be able to perform a recovery of an SMS PASSCODE installation.

NOTE: In case of a **Cloud Setup**, only subsection 27.2 is relevant.

27.1 Backup of Database Files

The most important thing to backup is the SMS PASSCODE database. The database files are normally located on the server where the SMS PASSCODE Database component is installed (unless the database location has been moved to a file share). The default location of the folder containing the SMS PASSCODE database files is:

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

You should backup all files located in this folder. The folder should contain at least two files:

- The main database file:
SMSPASSCODE_DB.xml:
- The database transaction log file:
SMSPASSCODE_DB_TRANSLOG.xml:

The procedure for a database recovery depends on the fact, whether encryption was enabled for the backed up database files or not (cf. section 26.1, page 423).

If the backed up database files are not encrypted, or if the backed up files are encrypted, but are being restored to the same server as they were backed up from (with the same encryption password still in place), then the procedure for a database recovery is quite simple:

1. Stop the SMS PASSCODE Database Service.
2. Restore both the main database file and the database transaction log file from your backup.
3. Start the SMS PASSCODE Database Service.

On the other hand, if the backed up files were encrypted and should now be recovered to a new database server, then proceed as follows:

1. Install the SMS PASSCODE Database Service on the new server (if not already done).
2. Stop the SMS PASSCODE Database Service.
3. Using the SMS PASSCODE Configuration Tool, enable database encryption and enter the same encryption password as used previously (i.e. the encryption password used, when the database files were backed up).
4. Restore both the main database file and the database transaction log file from your backup.
5. Start the SMS PASSCODE Database Service.

IMPORTANT: If you have enabled encryption of your SMS PASSCODE Database using the SMS PASSCODE Configuration Tool (cf. section 26.1, page 423), then it is very important to keep the encryption password in a safe place. You might need it in case of a recovery.

27.2 Backup of Configuration Tool Settings

On every machine containing any SMS PASSCODE component you can use the SMS PASSCODE Configuration Tool to set machine specific configuration settings. If you want a backup of these settings, you should use the Configuration Tool on each machine to export the settings to a file, and then store these files in a safe place.

In case of a recovery, the Configuration Tool must be used to import the previously exported files.

Please read section 25.5.5 (page 420) for a description of the Configuration Tool export and import feature.

27.3 Backup of Authentication Monitoring Archive

If you have enabled the **Authentication Monitoring** feature on the **General Settings** page of the WAI (cf. section 17.3.3, page 114), then it is recommended to back up the archive as well, in case the archived data is of importance to you.

- If the archiving feature is set to store archived data to either CSV or XML files, then you simply need to back up all files stored in the archive folder, which is defined on the **General Settings** page as part of the archiving setup. The default path to the archive folder is:

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

Please note, that there is no automatic clean-up of the files in the archive folder. You should plan to remove the old files that are outdated according to the policy of your organization.

- If the archiving feature is set to store archived data to an SQL Server, then you must back up the destination table, which is defined on the **General Settings** page as part of the archiving setup. Please refer to the manual of your backup software regarding the procedure of backing up data from an SQL Server. Remember to ensure, that the SQL transaction log of the archive database is shrunk on a regular basis, preferable after each backup.

27.4 Backup of Self-service Notification Templates

If you are using the SMS PASSCODE Self-service Website and have enabled Self-service notifications on some User Group Policies, you might have customized your own templates for the notification contents (cf. section 17.6.1.3.1, page 168). If you have performed any such customization, then it is recommended to perform a backup of the customized template files. The template files are located on the server where the SMS PASSCODE Database component is installed. The default location of the folder containing the template files is:

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

However, you should verify the actually used paths by inspecting the configuration of your User Group Policies.

In case of a recovery of the template files, you just need to restore the backup of the template files.

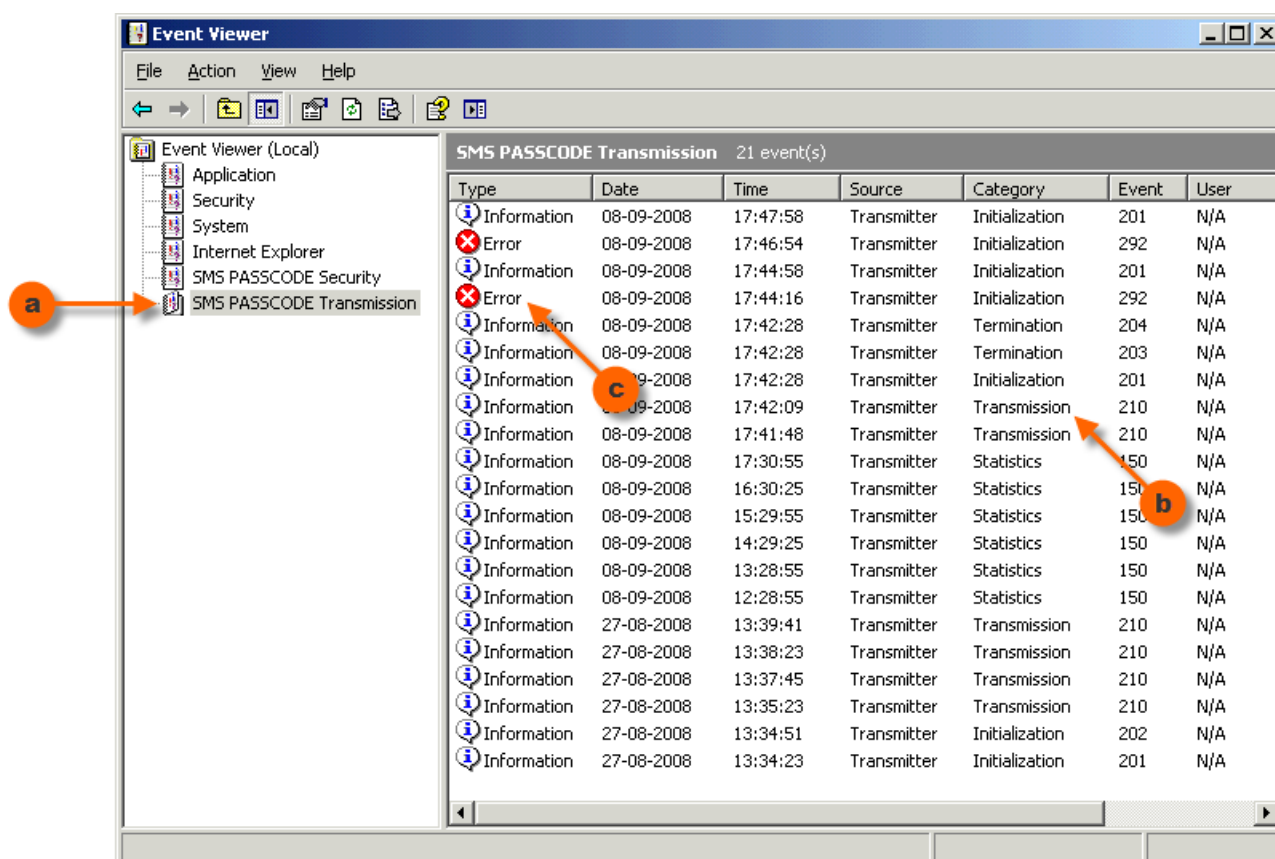
28 TROUBLESHOOTING

This section describes some common errors and the corresponding solutions:

- **No SMS is received during SMS PASSCODE authentication:**
Section 28.1 (page 432)
- **Error message “Unknown user” is shown during authentication:**
Section 28.2 (page 435)
- **Component communication problems:**
Section 28.4 (page 435)
- **User Store Integration (Active directory integration) does not work as expected:**
Section 28.3 (page 436)
- **Users cannot save changes in the Self-Service Website:**
Section 28.4 (page 437)
- **Users cannot access the Password Reset Website:**
Section 28.6 (page 440)
- **Users do not receive any quarantine email or an incorrect quarantine email when using the SMS PASSCODE Secure Device Provisioning component:**
Section 28.7 (page 440)
- **Token Authentication does not work:**
Section 28.8 (page 440)
- **RD Web Protection does not work:**
Section 28.9 (page 441)

28.1 SMS Transmission Problems

In case of SMS Transmission issues, please always start with opening the Windows Event Viewer on the SMS PASSCODE Transmitter Service host(s) and check the **SMS PASSCODE Transmission** event log (a) to verify whether any SMS was sent. Look for “Transmission events” (b). Also look, if any initialization errors have occurred (c). In case of any error or warning events, please inspect these events for details.



Problem	Error message in the SMS PASSCODE Transmission event log	Possible reasons
SMS transmissions fail permanently	<p>Unable to send SMS</p> <p>Or</p> <p>Error during initialization of SMS Modem (COMx): Device not found on COMx.</p> <p>Event ID: 11001</p>	<p>No connection to the modem due to:</p> <ul style="list-style-type: none"> Modem not powered on Modem not connected to the COM port specified in the SMS PASSCODE setup COM port is damaged Modem is damaged

Problem	Error message in the SMS PASSCODE Transmission event log	Possible reasons
SMS transmissions fail permanently	Com port is occupied or does not exist Event ID: 11001	No connection to the modem due to: <ul style="list-style-type: none"> • A different application is using the COM port specified in the SMS PASSCODE setup • COM port is damaged • The specified COM port does not exist
SMS transmissions fail permanently	Error during initialization of SMS Modem (COMx): ERROR: Could not register PIN code. Event ID: 11001	Initialization of modem fails because an incorrect SIM PIN code has been entered. Please correct the PIN code in the SMS PASSCODE Web Administration interface.
SMS transmissions fail permanently or periodically	Unable to send SMS (Mobile: xxxx). Modem reply=... Event ID: 11008	This could be due to a deactivated SIM card, insufficient signal strength or other cellular network problems. To determine the exact reason, please power off the modem, pull out the SIM card and verify that it works (e.g. put it into a mobile phone and try to send a SMS). If the SIM card does not work in a mobile phone, then replace it with another SIM card. If it works fine in a mobile phone, then the problem is most probably due to insufficient signal strength. You can inspect the signal strength on the Modem Monitoring page in the Web Administration Interface. In case of low signal strength, please try to move the modem to a location with better signal strength or try a better antenna.
A specific user does not receive SMS, even though it has been sent correctly according to the event log	None	The user's mobile phone might not support flash SMS. Please try to disable flash SMS for this user (you can disable flash SMS for a specific user in the SMS PASSCODE Web Administration interface).

28.2 Error Message “Unknown user” during Authentication

This error message is shown in the event log (and Authentication Monitor), if a user, who has not been created as an SMS PASSCODE user, tries to authenticate. This might be due to different reasons:

- If users are created manually in the SMS PASSCODE Web Administration interface, please check if the user in question is in fact present in the user grid.
- If users are imported using a User Integration Policy, please check if the user in question is in fact present in the user grid of the SMS PASSCODE Web Administration interface. If the user is not present, then please read section 28.3 below.

28.3 User Store Integration does not Work as Expected

When importing users from an Active Directory, it is recommended to install the SMS PASSCODE Database Service on a domain member server (or a domain controller). Enabling User Store Integration is very easy in this case (cf. section 17.5.2, page 128).

If User Store Integration does not work, please use the button **Verify settings** on the **User Integration Policies** page of the SMS PASSCODE Web Administration interface and check the result:

SMS|passcode Policies > User Integration Policies

Edit User Integration Policy: Default User Integration Policy (test.dom)

General Settings | **Data Source** | Data Mapping | Data Filtering | Data Transformations

Protocol

☒ LDAP
☐ Global Catalog
☐ Encrypt communication using SSL

Select whether to connect to the LDAP or Global Catalog.

Server name (Optional)

If necessary: Specify the name or IP address of the domain controller (the domain name is not necessary if the service runs on a member server).

Credentials (Optional)

Login:
 Password:

If necessary: Specify the credentials for the service account (necessary if the service account is not a member of the domain).

User selection

☒ Group membership (default)
☐ Custom LDAP filter (advanced)

Import users that are direct or indirect members of the group specified below.

Group name:
 SMS PASSCODE Users

Specify the name of the group (security group) containing the PASSCODE users. The group is "SMS PASSCODE Users". In case you do not have a unique name for the group in an AD forest, or you need authorization to search for the group, then please specify the complete distinguished name (DN) of the group.

Connection test **Verify settings**

Click the button to test the connection with the settings above.

© SMS PASSCODE A/S

Common problems regarding User Store Integration:

- Error message "User group xxx not found": Please verify that the group name is spelled identically in the SMS PASSCODE Web Administration interface and in the LDAP Store (Active Directory). Also, in case of Active Directory, please ensure that the group has been replicated to the domain controller, to which SMS PASSCODE is connecting.

- A specific user is not synchronized to the SMS PASSCODE Web Administration interface: Please verify in the User Store that the user is a direct or indirect member of the selected user group and that all required data (as defined on the **Data Filtering** tab) has been entered on this user's account.
- No users are synchronized to the SMS PASSCODE Web Administration interface when using Global Catalog: Please ensure that the fields containing required data are replicated to the Global Catalog.

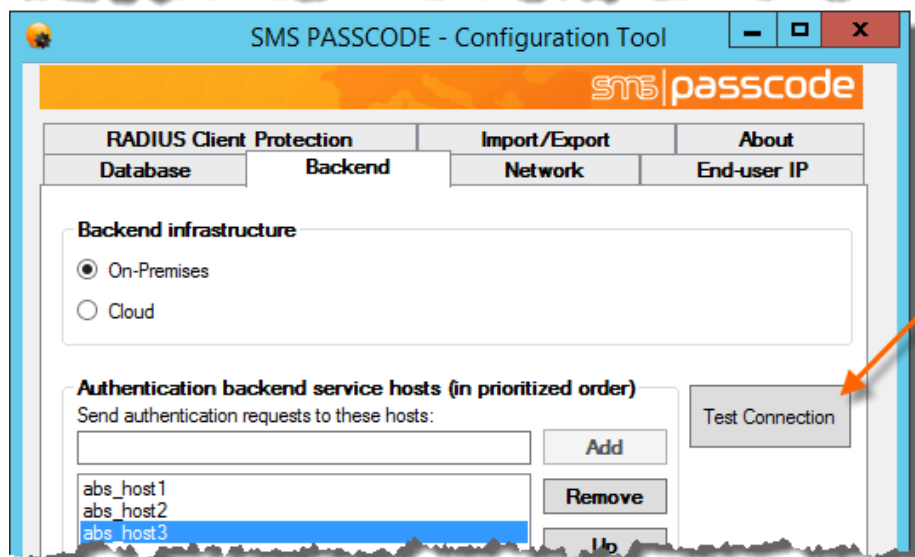
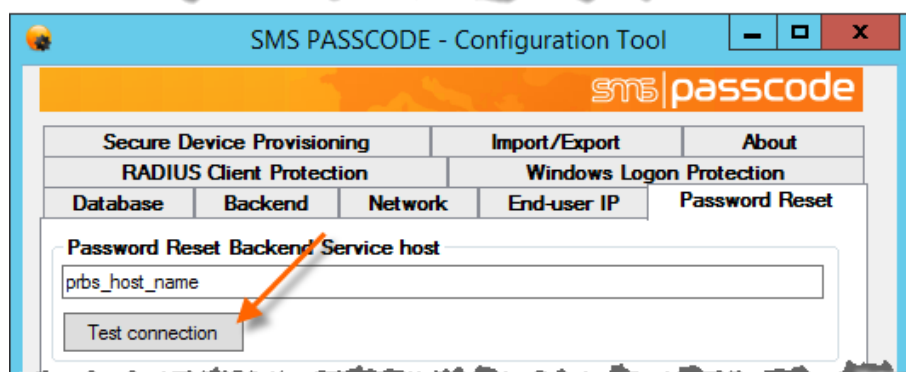
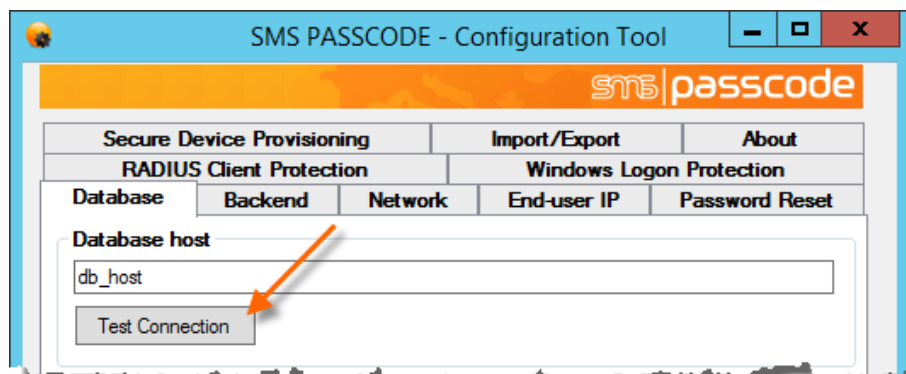
28.4 Component Communication Problems

If you are experiencing problems related to communication between components, please note the following requirements:

- All machines must run the same version of SMS PASSCODE.
- The same **shared secret** must be entered on all machines.
- The TCP ports used for communication must be open between the different machines (please read section 11.1, page 44, for TCP port details). If any default TCP port is changed to a different port number during installation, then this port change must be performed on all involved machines.

Diagnosing component communication

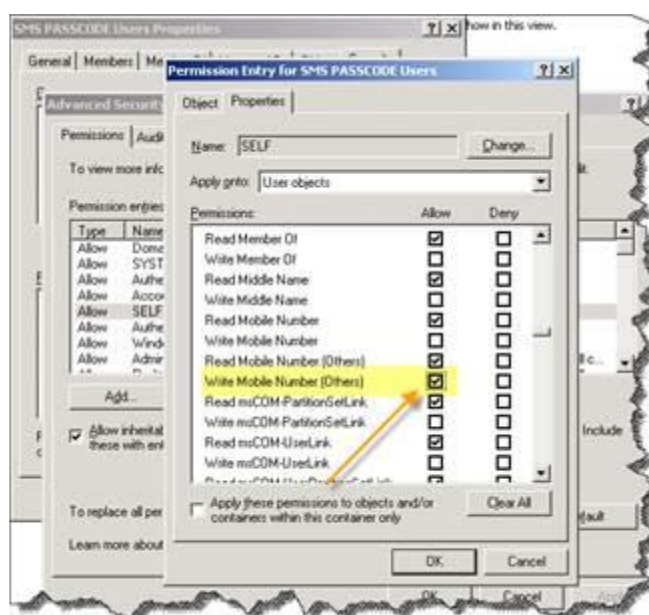
If you wish to check whether the communication between different machines works correctly, you can test the communication using the SMS PASSCODE **Configuration Tool**. The tabs **Database**, **Backend** and **Password Reset** contain **Test Connection** buttons for diagnosing component communication.



28.5 Self-service Website

If the SMS PASSCODE Self-service Website is configured to use Integrated Windows Authentication, and users get an error message when trying to save any changes, then this could be due to one of the following two reasons:

- If the error message says “Saving xxx failed. Reason: An operations error occurred”, then the problem might be due to missing configuration of authentication **delegation**. Please refer to section 22.5.1 (page 330).
- If the error message says “Saving xxx failed. Reason: Access is denied”, then the problem might be due to lack of write permissions in the AD. Please check the effective permissions in the AD, whether the user in question has write permissions to the specific LDAP attribute in question. In AD, find the user group used for importing the user (the group is called “SMS PASSCODE Users” by default), select **Properties**, **Security**, **Edit**, **Advanced**, **Self**, **Edit**, tab **Properties**, apply onto **User objects**:



28.6 Password Reset Website

This section describes different errors that can occur regarding the SMS PASSCODE Password Reset Website, and how to solve them.

28.6.1 Fatal Error when Accessing the Password Reset Website

If you try to access the SMS PASSCODE Password Reset Website, and you get a FATAL error, this is most probably due to the reason that you have not enabled HTTPS correctly for the site yet. Please read section 23.6.2 (page 350) for more details.

28.6.2 Access Denied when Accessing the Password Reset Website

If a user tries to log in to the SMS PASSCODE Password Reset Website, and gets an “Access Denied” error message, then please inspect the Password Reset event log on the Password Reset Backend Service host. It should contain an event log entry describing in more detail, what went wrong (cf. section 23.8, page 362).

28.7 Secure Device Provisioning

This section describes different possible reasons for issues that may occur when using the SMS PASSCODE Secure Device Provisioning (SDP) component.

28.7.1 Fatal Error when Accessing the Secure Device Provisioning Website

If you try to access the SMS PASSCODE Secure Device Provisioning Website, and you get a FATAL error, this is most probably due to the reason that you have not enabled HTTPS correctly for the site yet.

28.7.2 No Quarantine Emails Received

If no users receive quarantine emails, then this is most likely because the Exchange Server has not been configured correctly to send out quarantine emails for new ActiveSync devices. Please review section 24.2.1, page 368, in this case.

28.8 Token Authentication

This section describes several reasons, why token authentication might not work.

- If token authentication does not work in general, i.e. all users are affected:
 - Has token authentication been allowed on the UGP of the affected users?
 - Has the Token Policy of the users been configured correctly? Moreover, has the correct Token Policy been assigned to the users?
 - If you are using USB Keys:
 - Have you signed up for the 3rd party web service from Yubico?
 - Is the web service up and running (please contact the 3rd party provider for info)?
 - If you are using OATH tokens:
 - Is the SMS PASSCODE Database Service up and running?
- If token authentication does not work for selected users:
 - Has token authentication been allowed on the UGP of the affected users?

- Has the Token Policy of the users been configured correctly? Moreover, has the correct Token Policy been assigned to the users?
- Has a token ID been assigned to the users?
- The token might be out of sync. Please try to perform several authentications in a row. If this does not help, try to resync the token (the administrator can do this on the user maintenance page in the WAI, or the end-user can do this in the SMS PASSCODE Self-service Website, if permission has been granted).

28.9 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 2016/2019: 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
```

```
Get-RDSessionCollection | Set-RDSessionCollectionConfiguration -CustomRdpProperty "gatewaycredentialssource: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-RDSessionCollection | Set-RDSessionCollectionConfiguration -CustomRdpProperty "`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 Entrust Datacard prior to disclosing information from this document.