



**PUBLIC**

SAP Single Sign-On 3.0 SP02

Document Version: 1.9 – 2020-03-17

# Secure Login for SAP Single Sign-On Implementation Guide

# Content

<b>1</b>	<b>Introduction to Secure Login.</b>	<b>10</b>
<b>2</b>	<b>System Overview.</b>	<b>11</b>
2.1	Cryptographic Library for SAP Single Sign-On.	12
2.2	Clients for Authentication.	12
	Authentication Methods of Secure Login Client.	12
	Authentication Methods of Secure Login Web Client.	13
2.3	System Overview with Secure Login Server.	13
2.4	PKI Structure.	14
	Out-of-the-Box PKI Login Server.	14
	PKI Integration.	14
2.5	Secure Communication.	15
2.6	Policy Server Overview.	16
2.7	Digital Signing with Secure Store and Forward (SSF).	17
2.8	Authentication Profiles.	17
<b>3</b>	<b>Basic Scenarios.</b>	<b>18</b>
3.1	Environment Using Secure Login Client.	18
	Authentication Methods without Secure Login Server.	19
	Workflow with X.509 Certificate without Secure Login Server.	20
	Workflow with Kerberos Token without Secure Login Server.	21
3.2	Environment Using Secure Login Client and Secure Login Server.	21
	Authentication Methods with Secure Login Server.	22
	Workflow with X.509 Certificate Request Using Secure Login Server.	23
3.3	SNC X.509 Configuration.	24
	Configuring SNC Parameters for X.509 Certificates.	24
	Configuring X.509 Certificates Using the Trust Manager.	25
3.4	SNC Kerberos Configuration.	27
	Microsoft Windows Account for SAP Server.	28
	Create a Microsoft Windows Account.	32
<b>4</b>	<b>Advanced Scenarios.</b>	<b>33</b>
4.1	Logging on with Secure Login Client Using SNC.	33
	Enabling Secure Login Client to Smartly Select an SNC Mode.	34
	Rolling out General Availability of SNC-Encrypted Logon.	35
	Manually Switching to Encryption Only for Logging on Using SNC.	36
	SNC Configuration Options in the Secure Login Client.	36
4.2	Providing X.509 Certificates to Secure Login Client Using JavaScript Web Client.	38

	Elements Required in Secure Login Client for JavaScript Web Client. . . . .	39
	Elements Required in Secure Login Server for JavaScript Web Client. . . . .	40
	Extending JavaScript Web Client to Multiple SAP GUI Logins. . . . .	41
	Extending JavaScript Web Client to Multiple Portal Logins. . . . .	41
	Configuring the Secure Login Client for JavaScript Web Client. . . . .	42
	Configuring the Secure Login Server for JavaScript Web Client. . . . .	43
4.3	Using a Remote Certification Authority in Secure Login. . . . .	46
	Prerequisites for Using a Remote Certification Authority . . . . .	46
	Configuring a Remote Certification Authority for Secure Login. . . . .	48
4.4	Remote Certification Authority Certificate Templates. . . . .	54
4.5	Using the Secure Login Server to Provide Trusted Certification Authorities. . . . .	54
	Configuration Information for Trusted Certification Authorities Provided by the Secure Login Server. . . . .	55
4.6	Certificate Lifecycle Management Using the Secure Login Server. . . . .	57
	The sapslscli Command Line Interface. . . . .	58
4.7	Browser-Based Enrollment of Secure Login Client Using a Secure Login Server Profile. . . . .	58
	API Methods for Profile Enrollment. . . . .	59
	HTML Code Example with Secure Login Server Profile and SNC Name. . . . .	61
4.8	Using Secure Login Client as SSH Agent. . . . .	62
	Restricting the Use of Secure Login SSH Agent. . . . .	63
4.9	Digital Client Signature (SSF). . . . .	64
	How to Test SSF Client Signature. . . . .	64
	SSF User Configuration in SAP GUI. . . . .	66
	System Signature Using Microsoft Active Directory Authentication. . . . .	66
4.10	X.509 and Kerberos Authentication. . . . .	69
	Authentication with X.509 Certificates and Kerberos. . . . .	69
	Supporting Authentication with Kerberos and X.509 on SAP NetWeaver AS ABAP. . . . .	70
4.11	Kerberos Authentication for HTML-Based User Interfaces Using AS ABAP with SPNego. . . . .	72
	System Landscape for Kerberos Authentication on AS ABAP. . . . .	73
	Setting the AS ABAP Profile Parameters. . . . .	74
	Configuring a Service Account. . . . .	75
	Creating a keytab. . . . .	78
	Troubleshooting SPNego on AS ABAP. . . . .	80
4.12	Configuring Secure Login Web Client Connections to SAP GUI. . . . .	80
	Connection with Redirect to URL. . . . .	81
	Direct SAP GUI Connection with Secure Login Web Client. . . . .	82
	Load-Balanced SAP GUI Connection with Secure Login Web Client (Using the Message Server) . . . . .	83
	Launch SAP Logon Pad. . . . .	85
4.13	Using Secure Login Client in Web Adapter Mode. . . . .	85
	Configuring Web Adapter Mode for Secure Login Client. . . . .	86

4.14	Using Secure Login Server for SAML 2.0 Authentication. . . . .	86
	Configuring SAML 2.0 Authentication in the Secure Login Server. . . . .	87
4.15	Certificate Lifecycle Management in the AS ABAP Using Secure Login Server. . . . .	88
	PSE Infrastructure Involved in Certificate Renewal Using Secure Login Server. . . . .	89
	Prerequisites for Certificate Renewal Using Secure Login Server. . . . .	90
	Configuring Certificate Lifecycle Management in the AS ABAP Using Secure Login Server. . . . .	90
	Preparing a Certificate Renewal at Regular Intervals. . . . .	95
4.16	Certificate Lifecycle Management in the AS Java Using Secure Login Server. . . . .	97
	Infrastructure Involved In Certificate Renewal Using Secure Login Server. . . . .	98
	Prerequisites for Certificate Renewal Using Secure Login Server. . . . .	99
	Configuring Certificate Lifecycle Management in the AS Java Using Secure Login Server. . . . .	99
	Renewing Certificates at Regular Intervals for AS Java Clients. . . . .	103
4.17	Issuing Certificates for iOS Devices. . . . .	109
	Configuring an Authentication Profile for iOS Devices. . . . .	110
4.18	Kerberos Authentication with SPNego. . . . .	110
	Configuring Kerberos Authentication with SPNego for Secure Login Client. . . . .	112
	Enabling Kerberos Authentication with SPNego for Secure Login Web Client. . . . .	112
	Configuring SPNego on SAP NetWeaver Administrator. . . . .	113
4.19	LDAP User Authentication. . . . .	114
	Importing LDAP Server CAs or Certificates into the SAP NetWeaver Key Storage. . . . .	115
4.20	Deleting a Configuration. . . . .	116
4.21	User Authentication against SAP Netweaver Application Server for ABAP. . . . .	117
	Creating a Destination with an RFC Destination Type. . . . .	118
4.22	RADIUS User Authentication. . . . .	119
	Using a Customer-Specific securid.ini Server Message File. . . . .	120
4.23	Identification Using RFID Tokens. . . . .	121
	Security Aspects of RFID Identification. . . . .	121
	Implementation Concept of RFID Identification. . . . .	122
	RFID Identification Example. . . . .	122
	Prerequisites for RFID Identification in the Kiosk PCs. . . . .	124
	Configuring Identification with RFID Tokens. . . . .	124
<b>5</b>	<b>Secure Login Client. . . . .</b>	<b>132</b>
5.1	Secure Login Client Installation. . . . .	132
	Unattended Installation with SAPSetup Installation Server. . . . .	134
5.2	Uninstalling Secure Login Client. . . . .	135
	Uninstalling Secure Login Client with Microsoft Windows Control Panel. . . . .	135
	Uninstalling Secure Login Client with SAPSetup. . . . .	135
	Uninstalling Secure Login Client with a Command Line Tool. . . . .	136
5.3	Updating the Secure Login Client to the Support Package. . . . .	137
5.4	Adding Root Certificates during Installation. . . . .	138
	Option 1: Installing Root CA Certificates on a Windows Client. . . . .	139

	Option 2: Distributing Root CA Certificates on Microsoft Domain Server. . . . .	140
	Option 3: Distribute Secure Login Server Root CA Certificates Using Microsoft Group Policies . . . . .	140
5.5	Downloading Policies to the Secure Login Client. . . . .	142
	Downloading Policies to Secure Login Client Using Profile Groups. . . . .	142
	Downloading Policies to Secure Login Client Using the Policy Download Agent. . . . .	143
	Creating a Profile Group of Authentication Profiles. . . . .	145
5.6	Getting User-Specific Profiles for Certificate Enrollment. . . . .	146
	Configuring User-Specific Profile Download in Secure Login Client. . . . .	146
	Downloading User-Specific Profile Groups to the Secure Login Client. . . . .	147
5.7	Configuration Options. . . . .	148
	Enable SNC in SAP GUI. . . . .	148
	User Mapping. . . . .	151
	Overview of Registry Configuration Options. . . . .	154
	Automatically Using the Proxy Configuration of Microsoft Internet Explorer for Secure Login Client. . . . .	154
	Using Secure Login Client Profiles for Kerberos and Microsoft Cryptography API Tokens. . . . .	157
	Smart Card Integration. . . . .	158
	Tracing Secure Login Client. . . . .	158
	Enabling the Display of LDAP Messages in Secure Login Client. . . . .	159
	SAP Business Client with Secure Login Client. . . . .	161
5.8	Secure Login Client for Citrix XenApp. . . . .	162
	Secure Login Client with a Published Desktop. . . . .	163
	Secure Login Client with a Published SAP Logon. . . . .	163
	Other Features of Secure Login Client. . . . .	164
5.9	Secure Login Client for macOS. . . . .	164
	Installing Secure Login Client on a Mac Client. . . . .	165
	Uninstalling Secure Login Client from a Mac Client. . . . .	165
	Configuring Secure Login Client on a Mac Client. . . . .	166
<b>6</b>	<b>Secure Login Server. . . . .</b>	<b>168</b>
6.1	Installation and Installation File Names. . . . .	168
	Prerequisites for Installing Secure Login Server. . . . .	169
	Authentication Servers Supported by Secure Login Server. . . . .	169
	Secure Login Server Installation with Software Update Manager. . . . .	170
	Secure Login Server Installation with Telnet. . . . .	171
	Secure Login Server Uninstallation. . . . .	173
6.2	Initial Configuration Wizard. . . . .	174
	Prerequisites for Running the Initial Configuration Wizard. . . . .	175
	Initial Configuration. . . . .	175
6.3	Administration. . . . .	179
	Starting the Secure Login Administration Console. . . . .	180

	Changing Password. . . . .	180
	Stopping and Starting Secure Login Server with Telnet. . . . .	181
	Stopping and Starting Secure Login Server Using SAP Management Console. . . . .	181
6.4	Secure Login Web Client. . . . .	182
	Enabling SAP GUI to Use Credentials with Secure Login Web Client. . . . .	183
	Security Features of Secure Login Web Client. . . . .	183
	Secure Login Security Device for Mozilla Firefox. . . . .	189
	Rebranding Secure Login Web Client. . . . .	191
	Export Restrictions. . . . .	192
6.5	Configuration. . . . .	192
	Overview of Login Modules Supported by SAP Single Sign-On. . . . .	192
	Adding a Policy Configuration. . . . .	194
	Creating an Authentication Profile Pointing to a Policy Configuration. . . . .	195
	Creating Destinations. . . . .	197
	Setting the Enrollment URL for Secure Login Client. . . . .	198
	Configuring Actions at Policy Download. . . . .	199
	Configuration of User Certificate Names. . . . .	200
	Managing Destinations . . . . .	214
	Archiving Certificate Requests, Issued Certificates, and User Certificates. . . . .	216
	Adding Certification Authorities. . . . .	219
	Using External User Certification Authorities. . . . .	220
	Using Certificate Templates. . . . .	221
	Configuring Secure Communication. . . . .	223
	Checking the Availability of Secure Login Server Configuration. . . . .	224
6.6	Configuration Examples. . . . .	225
	Verify Authentication Server Configuration. . . . .	225
	Integrate into Existing PKI. . . . .	226
	High Availability and Failover for Secure Login Server and Secure Login Client. . . . .	227
<b>7</b>	<b>Secure Login Library. . . . .</b>	<b>231</b>
7.1	Installing Additional Features for Secure Login. . . . .	231
<b>8</b>	<b>SAP Cryptographic Library. . . . .</b>	<b>232</b>
8.1	SAP Cryptographic Library for Secure Login. . . . .	232
	Configurable Features of SAP Cryptographic Library. . . . .	233
8.2	Downloading the Installation Package. . . . .	234
8.3	Standard and FIPS 140-2 Certified Crypto Kernel of the SAP Cryptographic Library. . . . .	235
	Using the FIPS 140-2 Certified Secure Login Crypto Kernel. . . . .	236
8.4	Configuration for the AS ABAP. . . . .	237
	Using the Single Sign-On Wizard to Configure SNC and SPNego. . . . .	239
	Digital Signatures (SSF) with a Hardware Security Module. . . . .	240
8.5	Configuring the SAP Cryptographic Library. . . . .	240

	Enabling Configuration of the SAP Cryptographic Library Using AS ABAP Profile Parameters	242
	Setting Profile Parameters for the SAP Cryptographic Library.	243
8.6	Enabling Certificate Verification.	243
8.7	Using Certificate Revocation Lists.	244
	Downloading CRLs with the CRL Tool.	245
	Getting a CRL from a CRL Distribution Point.	246
8.8	Configuration Options.	248
	Configuring Tracing for the Cryptographic Library.	248
<b>9</b>	<b>Parameter Reference.</b>	<b>250</b>
9.1	Parameter Overview for Secure Login Client.	250
	Registry Configuration Options.	250
	SSF Parameters for Digital Signatures.	268
9.2	Parameter Overview for Secure Login Server.	270
	Parameters for Initial Configuration (PKI Certificates).	270
	Parameters for Signing Certificate Requests.	272
	Secure Login Client Policy and Profiles.	273
	Parameters for the Policy Configuration.	281
	Parameters for User Authentication in the Authentication Profile.	295
	Parameters for Certificate Configuration in the Authentication Profile.	297
	Parameters for Destination Management Configuration.	308
	Parameters for Certificate Renewal Using Secure Login Server.	311
9.3	Parameter Overview for the SAP Cryptographic Library.	314
	SNC Parameters for the SAP Cryptographic Library.	314
	Parameters for Certificate Revocation Lists.	324
<b>10</b>	<b>Troubleshooting.</b>	<b>326</b>
10.1	Troubleshooting Secure Login Client.	326
	Error in SNC.	327
	User Name Not Found.	328
	Invalid Security Token.	329
	Wrong SNC Library Configured.	330
	No Display of Password Expiration Warning.	331
	SNC Error Codes in the Secure Login Client.	331
10.2	Troubleshooting SAP Cryptographic Library.	332
	SNC Library Not Found.	332
	Credentials Not Found.	333
	No Credentials Found at Start of Application Server ABAP.	334
	No User Exists with SNC Name.	335
	Monitoring the SAP Cryptographic Library.	335
	Error Occurred with sapgenpse.	335




	SNC Error Codes. . . . .	335
10.3	Troubleshooting Secure Login Server. . . . .	336
	Secure Login Web Client Authentication Failed. . . . .	336
	Trust Warnings in Secure Login Web Client. . . . .	337
	Error Codes of SAP Stacktrace Errors. . . . .	337
	Checklist User Authentication Problem. . . . .	340
	Enable Fully Qualified Distinguished Name in Enrollment URL. . . . .	340
	Locking and Unlocking. . . . .	343
	Secure Login Server SNC Problem. . . . .	344
	Secure Login Authentication Profile Lock and Unlock. . . . .	345
	Internal Server Message. . . . .	345
	Error Codes. . . . .	345
	Monitoring Secure Login Server. . . . .	348
	Logging and Tracing Secure Login Server with the Log Viewer of SAP NetWeaver Administrator . . . . .	348
<b>11</b>	<b>List of Abbreviations. . . . .</b>	<b>352</b>
<b>12</b>	<b>Glossary. . . . .</b>	<b>354</b>
<b>13</b>	<b>Secure Login Security Guide. . . . .</b>	<b>361</b>
13.1	Before You Start. . . . .	362
13.2	Component Overview. . . . .	362
13.3	FIPS 140-2 Crypto Kernel. . . . .	363
13.4	Secure Login Client. . . . .	364
	Installation Procedures and Settings for Secure Login Client. . . . .	364
	Initialization Procedures for Secure Login Client. . . . .	365
	Configuration Procedures and Settings for Secure Login Client. . . . .	366
	Runtime Security Considerations for Secure Login Client. . . . .	366
13.5	Secure Login Server. . . . .	366
	Installation Procedures and Settings for Secure Login Server. . . . .	367
	Initialization Procedures and Settings for Secure Login Server. . . . .	367
	Configuration Procedures and Settings for Secure Login Server. . . . .	370
	Runtime Security Considerations for Secure Login Server. . . . .	373
	Secure Login Web Client. . . . .	373
13.6	SAP Cryptographic Library. . . . .	374
	Installation Procedures and Settings for the SAP Cryptographic Library. . . . .	374
	Initialization Procedures for the SAP Cryptographic Library. . . . .	375
	Configuration Procedures and Settings for the SAP Cryptographic Library. . . . .	378
	Runtime Security Considerations for the SAP Cryptographic Library. . . . .	378
13.7	Microsoft Windows Server Domain Controller. . . . .	379
13.8	Microsoft Windows Server Active Directory. . . . .	379
13.9	LDAP Directory Server. . . . .	379



13.10	RSA Authentication Server. ....	380
-------	---------------------------------	-----

# 1 Introduction to Secure Login

Secure Login is an innovative software solution specifically created for improving user and IT productivity and for protecting business-critical data in SAP business solutions by means of secure single sign-on to the SAP environment.

Secure Login provides strong encryption, secure communication, and single sign-on between a wide variety of SAP components. For more information, see the central SAP Note [2300234](#) .

- SAP GUI and SAP Single Sign-On 3.0 with Secure Network Communications (SNC)
- HTML-based user interfaces and SAP Single Sign-On 3.0 with Secure Socket Layer – SSL (HTTPS)
- Third-party application servers supporting Kerberos and X.509 certificates

In a default SAP setup, users enter their SAP user name and password on the SAP GUI logon screen. SAP user names and passwords are transferred through the network without encryption.

To secure networks, SAP provides a “Secure Network Communications” interface (SNC) that enables users to log on to SAP systems without entering a user name or password. The SNC interface can also direct calls through the SAP Cryptographic Library to encrypt all communication between SAP GUI and the SAP server, thus providing secure single sign-on to SAP.

Secure Login allows you to benefit from the advantages of SNC without being obliged to set up a public-key infrastructure (PKI). Secure Login allows users to authenticate with one of the following authentication mechanisms:

- Windows Domain (Active Directory Server)
- RADIUS server
- LDAP server
- SAP Single Sign-On 3.0
- Smart card authentication
- RFID identification

If a PKI has already been set up, the digital user certificates of the PKI can also be used by Secure Login.

Secure Login also provides single sign-on for Web browser access to the SAP Single Sign-On 3.0 (and other HTTPS-enabled Web applications) with SSL.

## 2 System Overview

Secure Login consists of several components: Secure Login Client, Secure Login Server, and Secure Login Library.

Secure Login is a client/server software system integrated with SAP software to facilitate single sign-on, alternative user authentication, and enhanced security for distributed SAP environments.

The Secure Login solution includes several components:

- **Secure Login Client**  
Client application that provides security tokens (Kerberos and X.509 technology) for a variety of applications. You can optionally run the Secure Login Client as an SSH agent. It uses the functions of the SAP Cryptographic Library, which is the default cryptographic library of the Application Server ABAP (see the related link). For more information on the SAP Cryptographic Library, see SAP Note [1848999](#). The SAP Cryptographic Library supports both X.509 and Kerberos technology.
- **Secure Login Server**  
Central service that provides X.509v3 certificates (out-of-the-box PKI) to users and application servers. The Secure Login Web Client is an additional function. It also enables web-based clients to use certificates after an authentication at an identity provider using Security Assertion Markup Language (SAML) 2.0. Secure Login Server also provides fast RFID identification for users of kiosk PCs on the shop floor (see the related link).
- **Secure Login Library**  
The Secure Login Library is a library that contains a toolset for Secure Login. It contains the `saplscli` command line tool for certificate lifecycle.

### Note

- The cryptographic library `SAPCRYPTOLIB` is not a part of Secure Login anymore. Secure Login is now using the default SAP Cryptographic Library of the Application Server ABAP. You do not need to make an SNC configuration of a separate `SAPCRYPTOLIB`.
- The component `NWSSO for CommonCryptoLib 2.0` has been removed. The previous CRL utility is now integrated in the `sapgenpse` command (see the related link).

### → Tip

You do not need to install all of the components. The components that you require depend on your use case scenario.

## Related Information

[SAP Cryptographic Library for Secure Login \[page 232\]](#)

[Identification Using RFID Tokens \[page 121\]](#)

[Downloading CRLs with the CRL Tool \[page 245\]](#)

[The saplscli Command Line Interface \[page 58\]](#)

## 2.1 Cryptographic Library for SAP Single Sign-On

We recommend that you run SAP Single Sign-On with the latest version of SAP Cryptographic Library provided by SAP.

- SAP Cryptographic Library (CommonCryptoLib), which comes with the kernel of AS ABAP (see SAP Note [1848999](#)). For more information, see the related link.

### Related Information

[SAP Cryptographic Library for Secure Login \[page 232\]](#)

## 2.2 Clients for Authentication

Secure Login runs with the following clients for authentication:

### Related Information

[Authentication Methods of Secure Login Client \[page 12\]](#)

[Authentication Methods of Secure Login Web Client \[page 13\]](#)

### 2.2.1 Authentication Methods of Secure Login Client

The Secure Login Client is integrated with SAP software to provide single sign-on capability and enhanced security.

Secure Login Client can be used with Kerberos technology, an existing public key infrastructure (PKI), or together with the Secure Login Server for certificate-based authentication without having to set up a PKI.

The Secure Login Client can use the following authentication methods:

- Smart cards and USB tokens with an existing PKI certificate  
Secure Login Server and authentication server are not necessary.
- Microsoft Crypto Store with an existing PKI certificate  
Secure Login Server and Authentication Server are not necessary.
- Microsoft Windows Credentials  
The Microsoft Windows Domain credentials (Kerberos token) can be used for authentication. The Microsoft Windows credentials can also be used to receive a user X.509 certificate with the Secure Login Server.

- User name and password (several authentication mechanisms)  
The Secure Login Client prompts you for your user name and password and authenticates with these credentials using the Secure Login Server in order to receive a user X.509 certificate.

All of these authentication methods can be used in parallel. A policy server provides authentication profiles that specify how to log on to the desired SAP system.

## Related Information

[Environment Using Secure Login Client \[page 18\]](#)

## 2.2.2 Authentication Methods of Secure Login Web Client

This client is based on a Web browser and is part of the Secure Login Server. The Secure Login Web Client has the same authentication methods as the standalone Secure Login Client, but with the following limited functions:

- Limited integration with the client environment (interaction required)
- Limited client policy configuration

## Related Information

[Secure Login Web Client \[page 182\]](#)

## 2.3 System Overview with Secure Login Server

This topic gives you an overview of an environment using Secure Login Server.

The main feature of the Secure Login Server is to provide an out-of-the-box PKI for users and application server systems (for example, SAP NetWeaver).

Users receive short term X.509 certificates. For the application server, long term X.509 certificates are issued. Based on the industry standard X.509v3, the certificates can be used for non-SAP systems as well.

In order to provide user certificates, the user needs to be authenticated (verified by the Secure Login Server). Therefore the Secure Login Server supports several authentication servers.

## 2.4 PKI Structure

You can integrate the PKI in different ways.

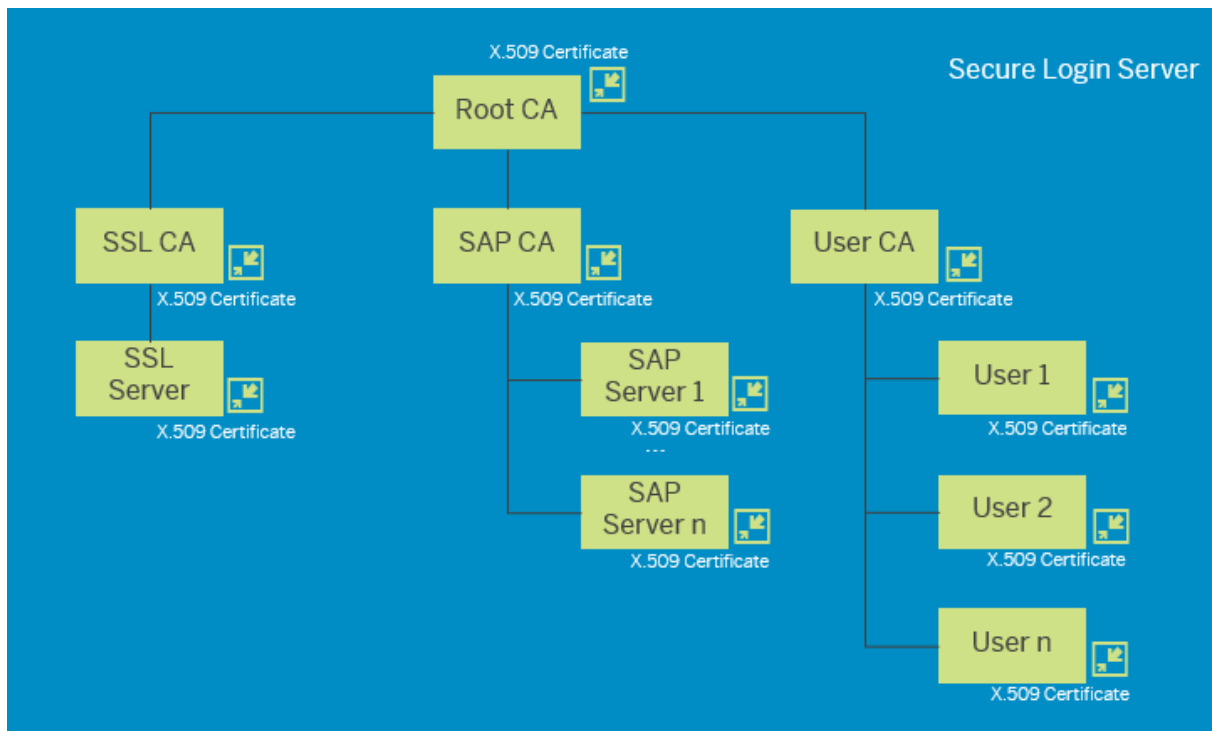
There are different integration scenarios available for Secure Login Server:

- out-of-the-box PKIs
- integrations into existing PKIs
- registration authorities using remote certificate authorities

SLS is a multi-PKI system, and all types of CAs can co-exist and be mixed multiple times.

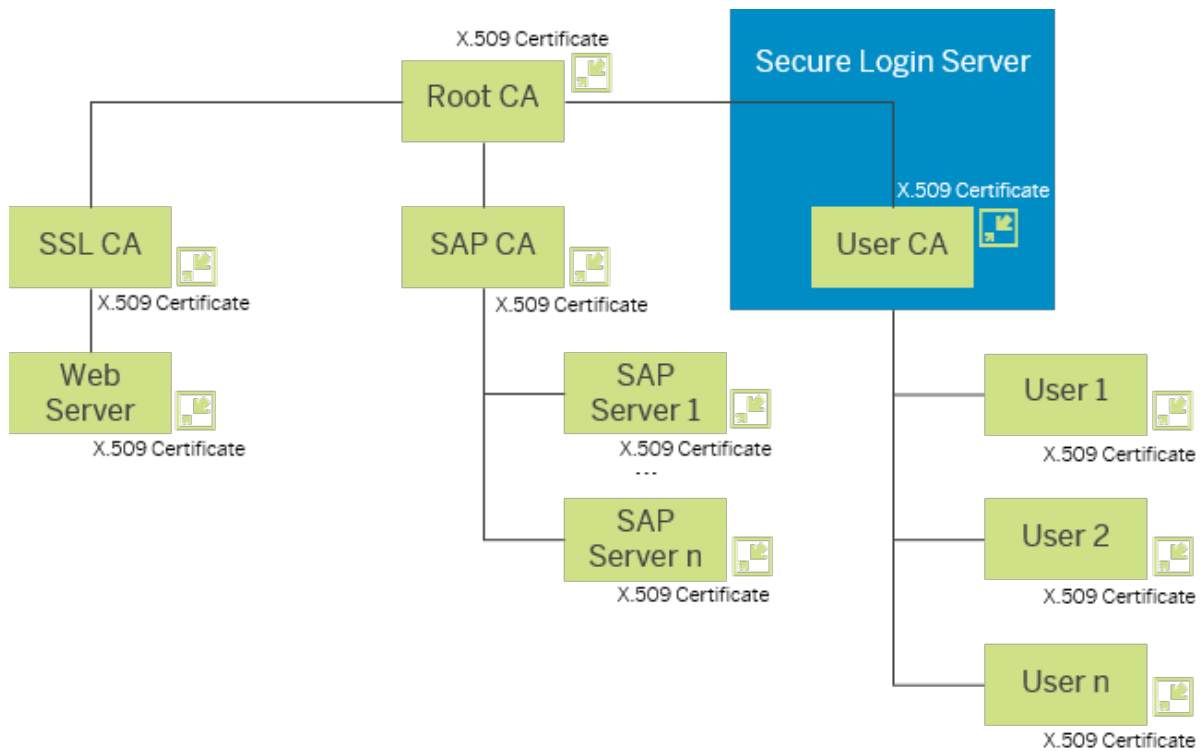
### 2.4.1 Out-of-the-Box PKI Login Server

Secure Login Server provides standard X.509 certificates for users (short term) and application server (long term). The following out-of-the-box PKI structure can be delivered with the Secure Login Server.



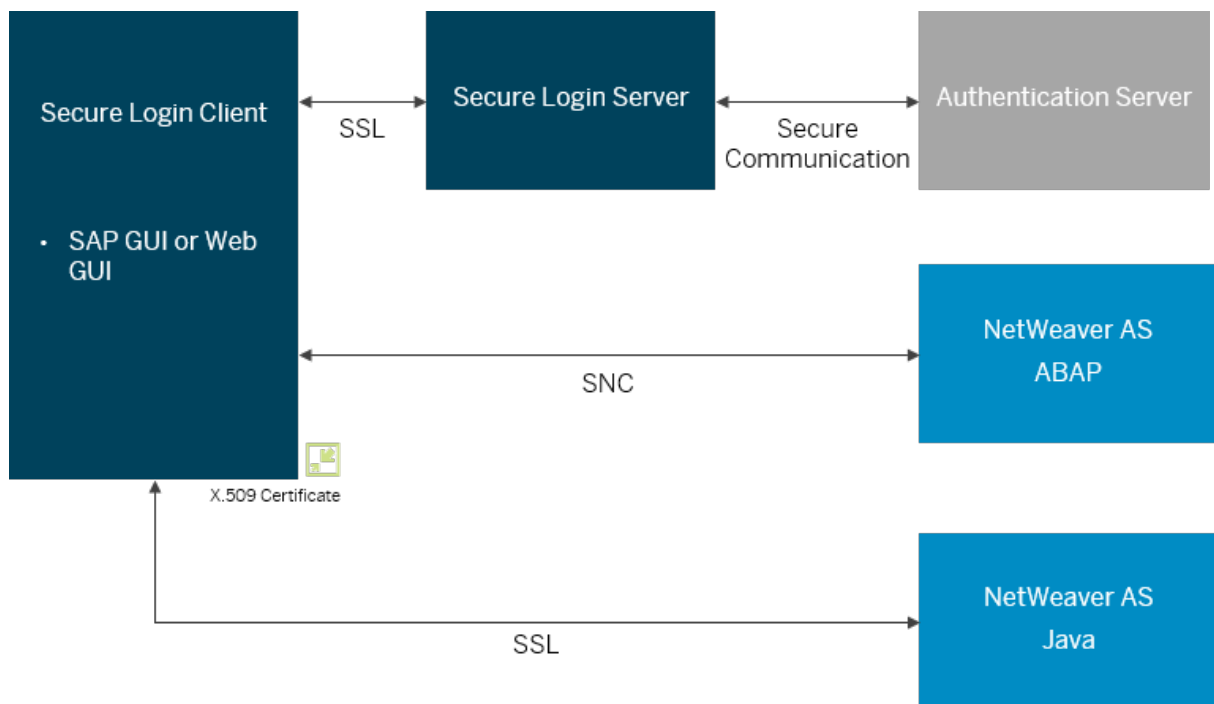
### 2.4.2 PKI Integration

As the Secure Login Server is based on industry standard X.509v3, it is possible to integrate the Secure Login Server to an existing PKI. The required minimum is to provide a user CA certificate to the Secure Login Server.



## 2.5 Secure Communication

The goal of the Secure Login solution is to establish secure communication between all required components:





The following table displays the security protocol or interface that is used for secure communication between various components.

Technology Used for Secure Communication

From	To	Security Protocol / Interface
SAP GUI	SAP NetWeaver	DIAG/RFC (SNC)
Business Explorer	SAP NetWeaver	DIAG/RFC (SNC)
Business Client	SAP NetWeaver	DIAG/RFC (SNC)
Web GUI	SAP NetWeaver	DIAG/RFC (SNC), HTTPS
Secure Login Client	Secure Login Server	HTTPS (SSL)
Secure Login Server	LDAP server	HTTPS (SSL)
Secure Login Server	SAP NetWeaver	RFC (SNC)
Secure Login Server	RADIUS server	RADIUS (shared secret)

## 2.6 Policy Server Overview

Secure Login Client configuration is profile-based. You can configure the application contexts to provide a mechanism for automatic application-based profile selection.

The system then searches the application contexts for specific personal security environment universal resource identifiers (PSE URIs).

If no matching PSE URI is found, a default application context that links to a default profile can be defined.

The application contexts and profiles are stored in the Microsoft Windows Registry of the client. You define these parameters in the XML policy file.

### Example

The following tables shows an example for dependencies of application contexts and profiles:

Dependencies of Application Contexts and Profiles

Application Contexts		
Application A.1	PSE URI (A.1)	Profile P.x
Application A.2	PSE URI (A.2)	Profile P.y
Application A.3	PSE URI (A.3)	Profile P.x
Application A.4	Default PSE URI	Default Profile P.z

Application A.4 does not have a PSE URI that is specifically assigned to application A.4. For this reason, a default PSE URI is used. It links to a default profile with settings are configurable in the XML policy file.

Profiles and Related Settings

#### Profiles and Related Settings

Profile P.x	Settings P.x
Profile P.y	Settings P.y
Default Profile P.z	Settings for Default Profile P.z

## 2.7 Digital Signing with Secure Store and Forward (SSF)

SAP Single Sign-On supports digital signing using the Secure Store and Forward (SSF) interface of the Application Server ABAP.

- Secure Login Client enables you to make system signatures with your SAP user and your Microsoft Windows password from Microsoft Active Directory.
- The SAP Cryptographic Library provides digital signatures (SSF) with encryption keys that are embedded in a hardware security module.

For more information, see the related links.

### Related Information

[Digital Client Signature \(SSF\) \[page 64\]](#)

[Digital Signatures \(SSF\) with a Hardware Security Module \[page 240\]](#)

## 2.8 Authentication Profiles

The authentication profile feature of Secure Login allows you to determine a certain user authentication method.

An authentication profile uses a user CA and an authentication method against a certain client type. You can select either the type Secure Login Client, Secure Login Web Client, or Application Server Profile. The enrollment URL, PKI, and the client behavior is downloaded to each client. You can define the user certificates, for example, with LDAP user mapping using attributes from LDAP or Active Directory, or user logon ID padding and archive certificate requests. You are free to change the Distinguished Name in many ways.

SAP NetWeaver Administrator organizes the authentication profiles in authentication stacks with login modules. Using authentication stacks makes sure that Secure Login is a failover solution.

## 3 Basic Scenarios

The following section contains basic scenarios for single sign-on and authentication.

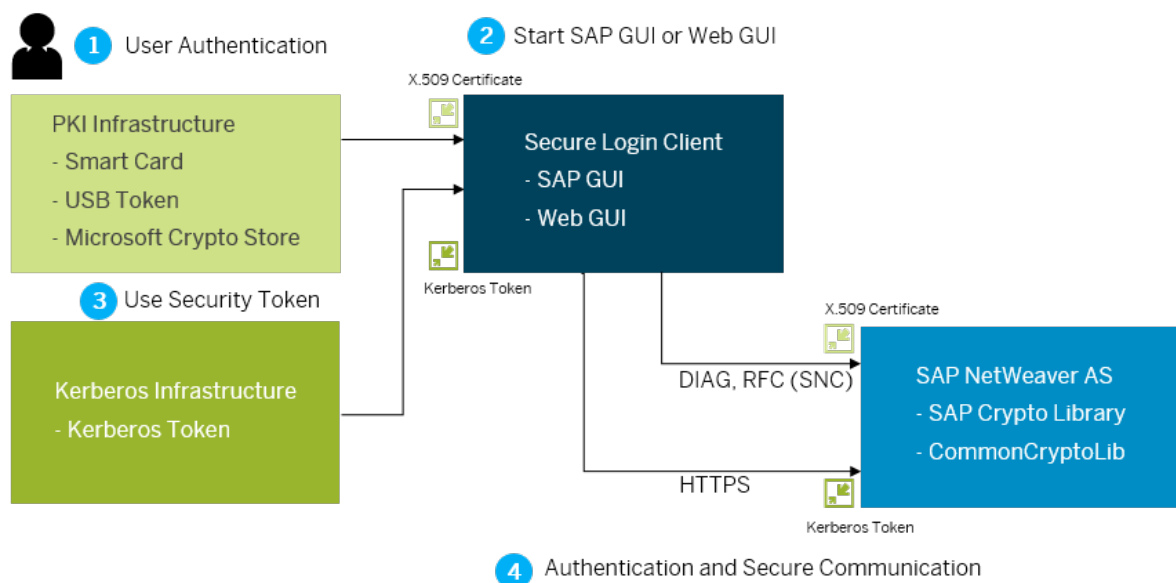
You are using the Secure Login Client with X.509 certificates or Kerberos tokens.

You can also use both components of Secure Login, the Secure Login Client and the Secure Login Server. The Secure Login Server provides authentication profiles to the Secure Login Client, Secure Login Web Client, or to the application server. It enables you to flexibly configure user authentication according to the needs of your enterprise.

### 3.1 Environment Using Secure Login Client

You can set up Secure Login in an environment using the Secure Login Client without Secure Login Server.

The following figure shows the Secure Login system environment using the Secure Login Client and the SAP Cryptographic Library.



The Secure Login Client is responsible for the certificate-based and Kerberos-based authentication to the SAP NetWeaver AS.

## 3.1.1 Authentication Methods without Secure Login Server

In a system environment without Secure Login Server, the Secure Login Client supports the following authentication methods:

Authentication Methods without Secure Login Server

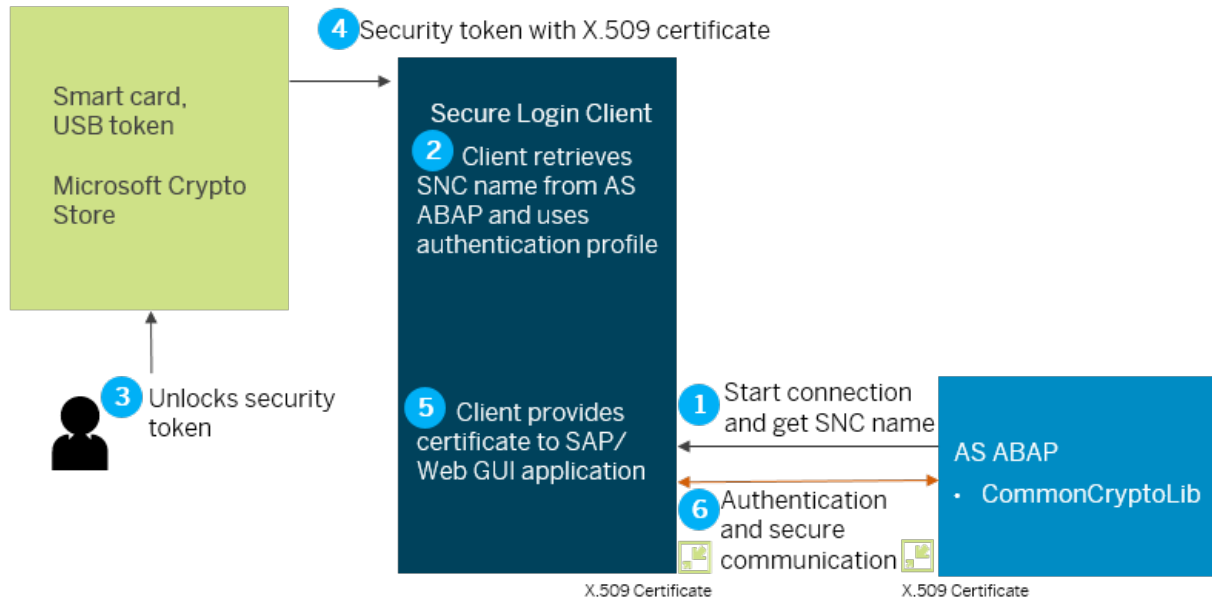
Authentication Method	Details
Authentication with X.509 certificates	<p>The certificate provider sends the X.509 certificates through secure network communication (SNC). The following certificate providers work with X.509 certificates:</p> <ul style="list-style-type: none"><li>• Smart card and USB tokens with an existing PKI certificate</li><li>• Microsoft Crypto Store (Certificate Store)</li></ul> <p>In SNC the Secure Login Client can perform authentication with encryption and digital signing certificates. The Secure Login Client supports RSA and DSA keys.</p>
Authentication with Kerberos tokens	<p>For more information about the authentication with a Kerberos token, see the related link.</p>

### Related Information

[Workflow with Kerberos Token without Secure Login Server \[page 21\]](#)

### 3.1.2 Workflow with X.509 Certificate without Secure Login Server

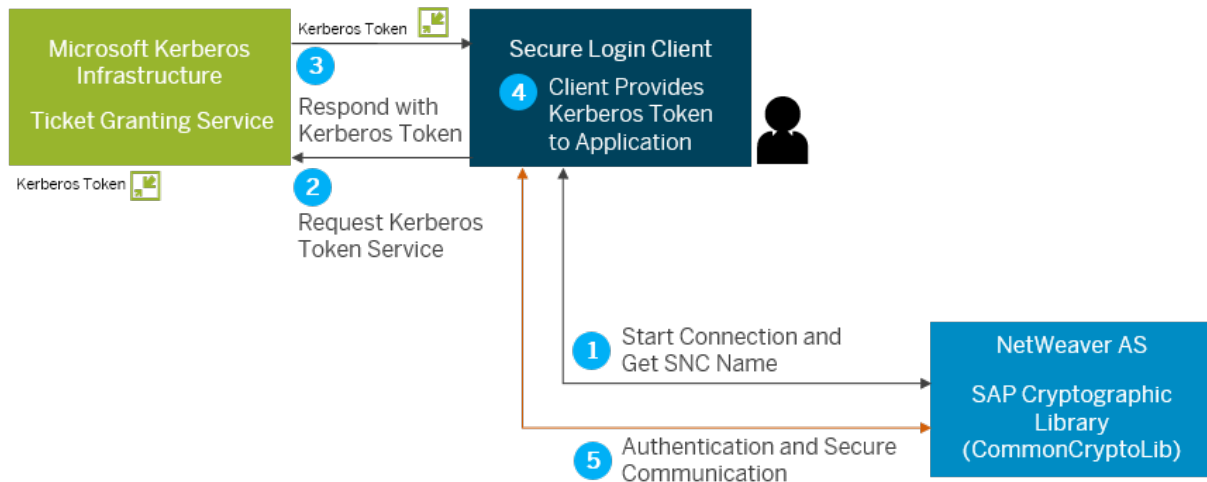
The following figure shows the principal workflow and communication between the individual components.



1. Upon connection start, the Secure Login Client retrieves the SNC name from the SAP NetWeaver AS ABAP.
2. The Secure Login Client uses the authentication profile for this SNC name.
3. The user unlocks the security token, for example, by entering the PIN or password.
4. The Secure Login Client receives the X.509 certificate from the user security token.
5. The Secure Login Client provides the X.509 certificate for single sign-on and secure communication between SAP GUI or Web GUI and the AS ABAP.
6. The user is authenticated and the communication is secured.

### 3.1.3 Workflow with Kerberos Token without Secure Login Server

The following figure shows the principal workflow and communication between the individual components.

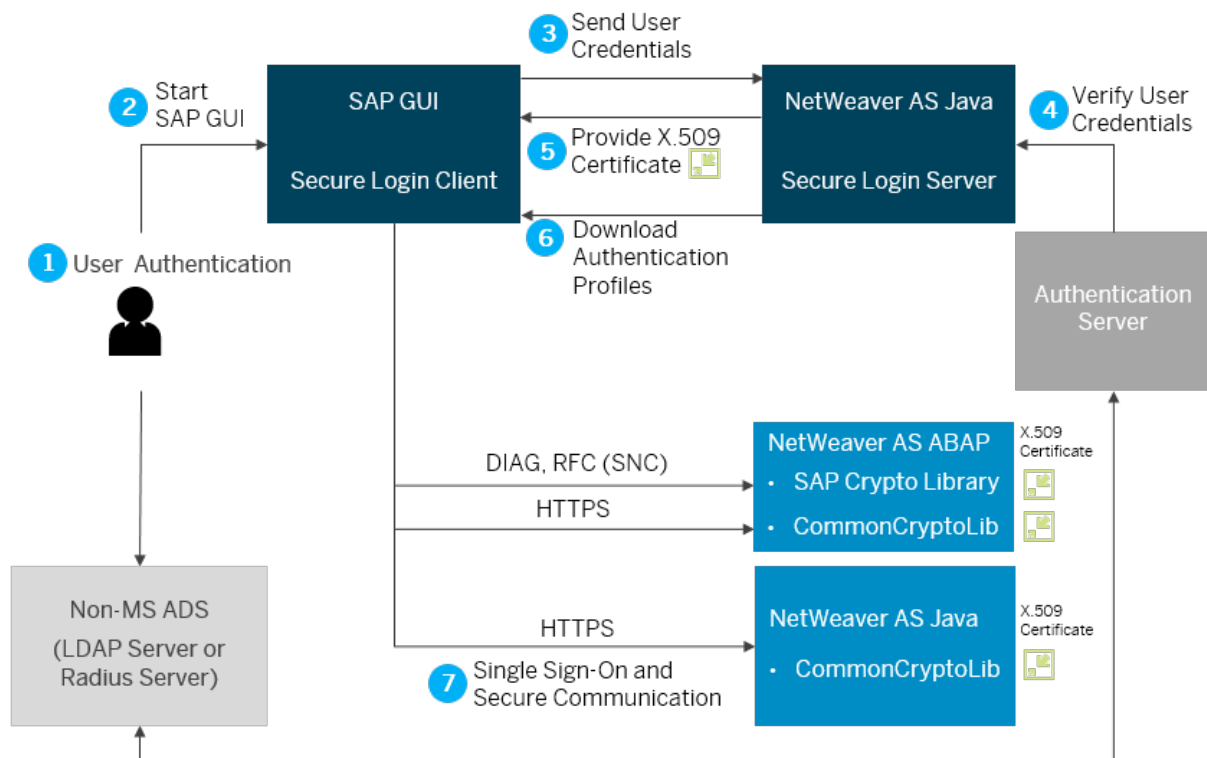


1. Upon connection start, the Secure Login Client retrieves the SNC name (User Principal Name of the service user) of the respective SAP server system.
2. The Secure Login Client starts at the Ticket Granting Service a request for a Kerberos Service token.
3. The Secure Login Client receives the Kerberos Service token
4. The Secure Login Client provides the Kerberos Service token for SAP single sign-on and secure communication between SAP Client and SAP server.
5. The user is authenticated and the communication is secured.

## 3.2 Environment Using Secure Login Client and Secure Login Server

You can also set up Secure Login in an environment with Secure Login Client, Secure Login Server, and the SAP Cryptographic Library.

The following figure shows the Secure Login system environment with these system components if an existing PKI or Kerberos infrastructure is used.



The Secure Login Client is responsible for the certificate-based authentication and Kerberos-based authentication to the SAP application server.

The Secure Login Server is the central server component that connects all parts of the system. It enables authentication against an authentication server and provides the Secure Login Client with a short term certificate. The Secure Login Server is a pure Java application. It consists of a servlet and a set of associated classes and shared libraries. It is installed on an SAP NetWeaver Application Server. You can set the initial configuration and administration in the Secure Login Administration Console. The configuration data is stored in the database and can be displayed using the J2EE Engine GUI Config Tool in the path [SecureLoginServer](#).

The Secure Login Server provides authentication profiles to the Secure Login Client, Secure Login Web Client, or to the application server. It allows flexible user authentication configurations (for example, which authentication type should be used for which SAP application server).

### 3.2.1 Authentication Methods with Secure Login Server

Secure Login supports several authentication methods. It uses the Java Authentication and Authorization Service (JAAS) as a generic interface for the different authentication methods.

For each supported method, there is a corresponding configurable JAAS module.

The following authentication methods are supported:

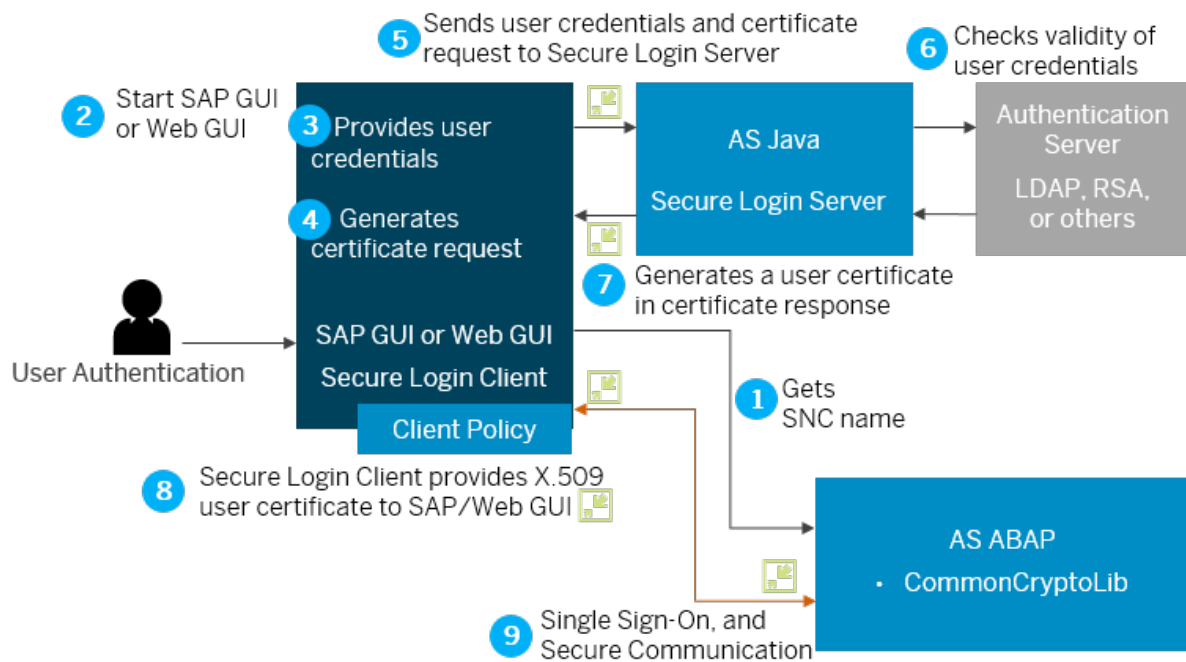
- Microsoft Active Directory Service (ADS)
- RADIUS
- RSA SecurID token (via RADIUS)
- LDAP



- ABAP-based logon
- SAP NetWeaver AS for Java User Management Engine
- SAP NetWeaver AS for Java SPNego

### 3.2.2 Workflow with X.509 Certificate Request Using Secure Login Server

The following figure shows the principal workflow and communication between the individual components.



1. Upon connection start, the Secure Login Client retrieves the SNC name from the SAP NetWeaver Application Server ABAP (AS ABAP).
2. To generate this SNC name, the Secure Login Client uses the client policy of the Secure Login Server.
3. The Secure Login Client provides the user credentials.
4. The Secure Login Client generates a certificate request.
5. The Secure Login Client sends the user credentials and the certificate request to the Secure Login Server.
6. The Secure Login Server forwards the user credentials to the authentication server (for example, an LDAP or RSA server) and receives a response indicating whether the user credentials are valid or not.
7. If the user credentials are valid, the Secure Login Server generates a certificate response and provides it to the Secure Login Client.
8. Secure Login Client provides the user certificate to SAP GUI.
9. This user certificate is used to perform single sign-on and secure communication (SNC) between the SAP GUI or web GUI client and the AS ABAP.

#### Note

Microsoft Internet Explorer uses the Microsoft Crypto API (CAPI) for cryptographic operations. The Microsoft Crypto API has a plug-in mechanism for third-party crypto engines. The Crypto Service Provider (CSP) from SAP is such a plug-in. It provides the user keys to all CAPI-enabled applications.

## 3.3 SNC X.509 Configuration

This section describes the SNC X.509 certificate configuration.

### Prerequisites

You need X.509 certificates signed by a trusted Certification Authority for the SNC configuration. This certificate must be integrated in the SNC SAPCryptolib PSE.

The Secure Login Library uses X.509 client or server certificates for SNC connections. It supports either no key usage in X.509 certificates or one or more supported key usages. The supported key usages depend on whether the X.509 certificate is used for client-server or server-server communication. Make sure the X.509 certificates are configured with supported values.

For a list of the key usages the Secure Login Library supports for SNC, see the following tables.

Key Usage for X.509 Client Certificates for Client-Server Communication

Certificate Fields	Values	Mode
[No key usage field]	[No values]	[No mode]
<i>Key Usage</i>	<i>Digital Signature</i>	sigsession, ParallelSessions mode
<i>Key Usage</i>	<i>Data Encipherment</i>	Encryption
<i>Key Usage</i>	<i>Key Encipherment</i>	Encryption

Key Usage for X.509 Server Certificates for Client-Server and Server-Server Communication

Certificate Fields	Values	Mode
[No key usage field]	[No values]	[No values]
<i>Key Usage</i>	<i>Digital Signature</i>	sigsession, ParallelSessions mode (client-server only) Encryption

### 3.3.1 Configuring SNC Parameters for X.509 Certificates

Configuration of SNC parameters for X.509 certificates

#### Procedure

1. Log on to the SAP Netweaver Application Server using SAP GUI.

2. Use the SAP Single Sign-On wizard for SNC and SPNego (transaction `SNCWIZARD`) to set the SNC parameters.

#### **i Note**

If the SAP Single Sign-On wizard is not available, start transaction `RZ10` and define the SNC parameters in the [default profile](#).

For more information, see the related links.

## **Related Information**

[SNC Parameters for X.509 Configuration \[page 314\]](#)

[Using the Single Sign-On Wizard to Configure SNC and SPNego \[page 239\]](#)

## **3.3.2 Configuring X.509 Certificates Using the Trust Manager**

The default tool for the configuration of X.509 certificates and PSE management is the trust manager in the SAP GUI. It enables you to create and import PSEs and to add certificates to the certificate list of the relevant PSEs.

### **Context**


For more information on the recommended way on how you configure an SNC configuration for X.509 certificates, see the SAP Help Portal in the *SAP NetWeaver Library* under [Application Help > Function-Oriented View > Security > Network and Transport Layer Security > Transport Layer Security on the AS ABAP > Using the SAP Cryptographic Library for SNC > Configuring the Use of the SAP Cryptographic Library for SNC > Configuring SNC for Using the SAP Cryptographic Library on the AS ABAP](#).

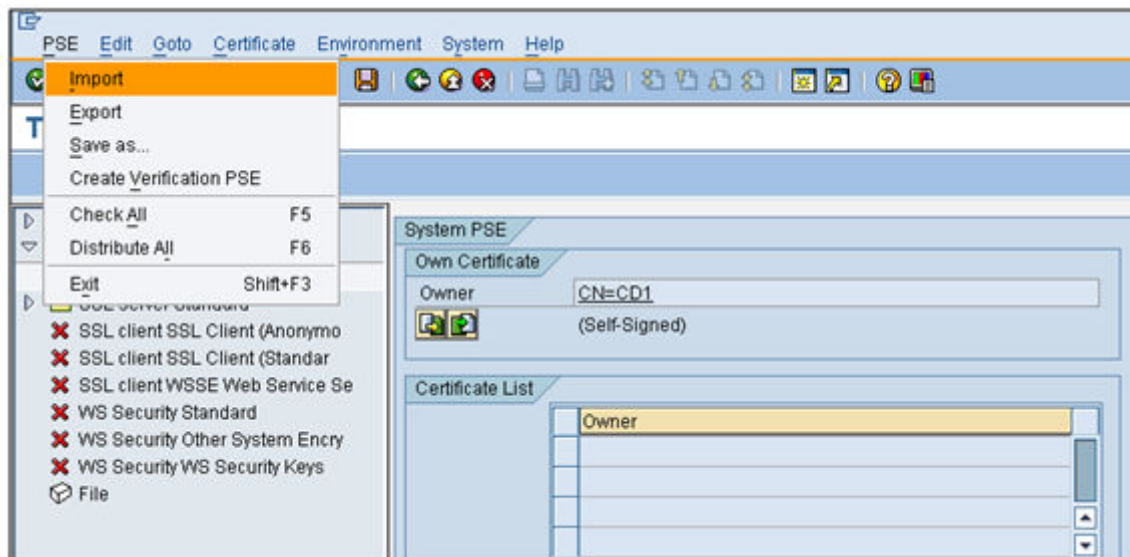
### **Procedure**


1. Open SAP GUI.
2. Start transaction `STRUST` and import the SAP server certificate.

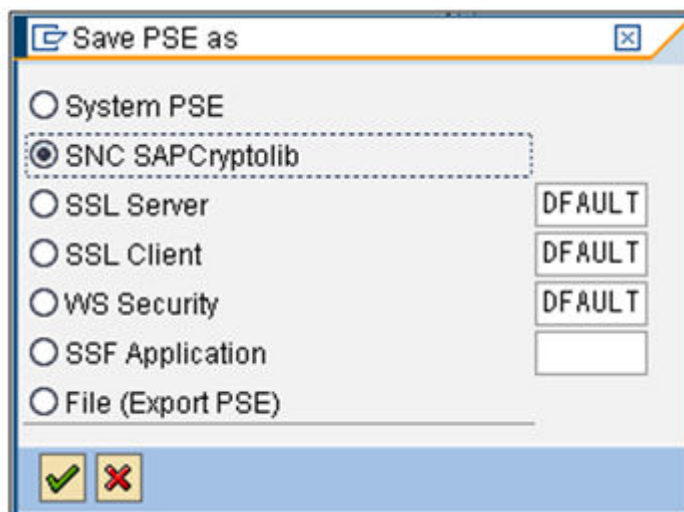
The SAP server certificate must be available in a PSE format. If this is not the case, create a PSE with the trust manager (transaction `STRUST`). The new certificate must be signed by a Certification Authority.

For a client/server communication, the certificates must be provided by a Public Key Infrastructure (PKI). If no PKI is available the Secure Login Server (out of the box PKI) can be used to provide certificates.

3. Toggle to change mode using the  button.
4. From the *PSE* menu, choose *Import*.



5. Load the PSE file.
6. (If required) Enter the PSE password.
7. Choose the *PSE* > *Save as...*.
8. Select *SNC SAPCryptolib* and choose .



If the certificate distinguished name of the PSE file does not match the SNC name configuration set in the default profile parameter (*snc/identity/as*), an error message appears. This verification check is performed only if SNC is activated.

## 3.4 SNC Kerberos Configuration

Configuring SNC for Kerberos includes the creation of an X.509 PSE and of setting the relevant profile parameters.

### Context

You want to protect, for example, internal and external server-to-server communication with SNC. This topic describes how you create the relevant PSE and how you configure the SNC parameters for Kerberos in an AS ABAP.

### Procedure

1. Log on to the Application Server ABAP using SAP GUI or SAP GUI for HTML.
2. Start transaction `STRUST` (trust manager).
3. (For SAP NetWeaver 7.4 SP05 or higher) Choose the [Change](#) button.
4. Select the SNC `SAPCryptolib` PSE.
5. Choose [Create](#). For more information on creating a PSE, see ► [SAP NetWeaver Library: Function-Oriented View](#) ► [Security](#) ► [System Security](#) ► [System Security for SAP NetWeaver AS ABAP Only](#) ► [Trust Manager](#) ► [Creating PSEs and Maintaining the PSE Infrastructure](#) ► [Creating or Replacing a PSE](#) ►.
6. Set the relevant parameters and choose [Continue \(Enter\)](#).
7. Save your changes.
8. Use the SAP Single Sign-On wizard for SNC and SPNego (transaction `SNCWIZARD`) to set the SNC parameters.

#### i Note

If the SAP Single Sign-On wizard is not available, start transaction `RZ10` and define the SNC parameters in the [default profile](#).

For more information, see the related links.

Using this configuration, you make sure that you can at least generate a self-signed X.509 certificate. You can import your own certificate if available.

### Related Information

[SNC Parameters for Kerberos Configuration \[page 316\]](#)

[Using the Single Sign-On Wizard to Configure SNC and SPNego \[page 239\]](#)

## 3.4.1 Microsoft Windows Account for SAP Server

In order to verify user Kerberos authentication, the Secure Login Library requires a Kerberos keytab which you can create using the command line tool, provided by Secure Login Library.

The Kerberos keytab contains Kerberos principals and encrypted keys that are derived from the Microsoft Windows user password. Therefore a Microsoft Windows account in Microsoft Active Directory is required.

### 3.4.1.1 Define Service Principal Name

#### Context

The Service Principal Name will be used to provide Kerberos service tokens to the requested users. This Service Principal Name is also required for the SNC name configuration.

#### Procedure

1. Start the Microsoft Windows tool [ADSI Edit](#).

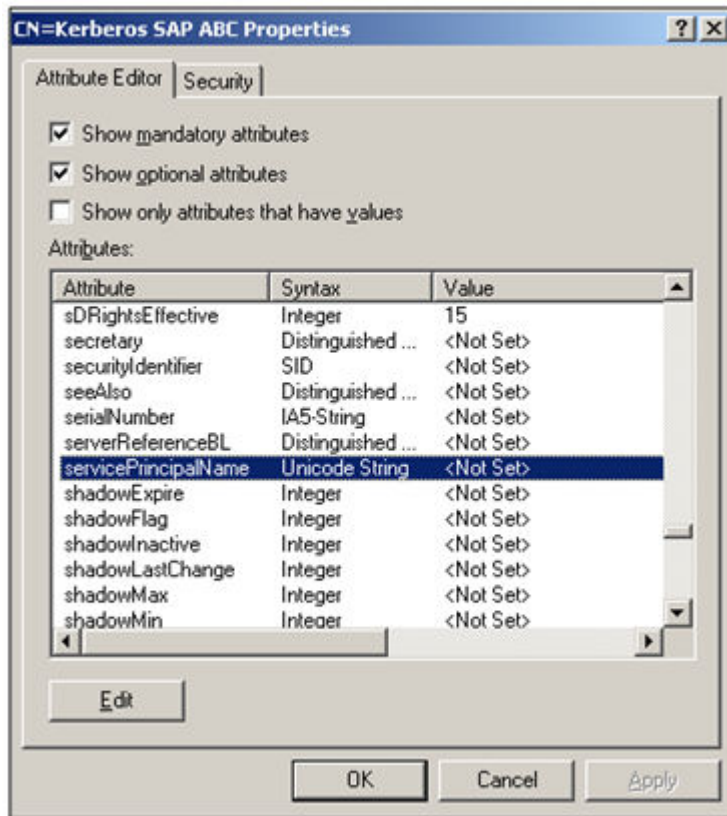
##### ❖ Example

Enter `adsiedit.msc` in the start menu of Microsoft Windows.

##### i Note

If this tool is not available, see the related link.

2. Choose the Microsoft Windows user (in our example: SAPServiceABC).
3. Define the field [servicePrincipalName](#).



#### i Note

The mandatory format is SAP/SAPService<SID>.

## Related Information

[Configuring a Service Account \[page 75\]](#)

### 3.4.1.2 Check for Multiple Service Principal Names

If the Secure Login Client does not get a service ticket from the domain server, this may be due to the fact that the Service Principal Name used has been assigned several times in the Active Directory system. Use the following command to check this:

#### Example

```
setspn -T * -T foo -X
```



### 3.4.1.3 Creating Keytab for Kerberos

You need a keytab file to use SNC with Kerberos authentication.

#### Context

If you want to use SNC with Kerberos authentication, you need to create a keytab file. The default procedure for creating a keytab file is the SAP GUI transaction [SPNego Configuration](#) (transaction code `SPNEGO`). For more information, see the related link.

You can still use the `sapgenpse` command as a fallback or legacy solution. For more information, use the following command:

```
sapgenpse -h
```

#### Related Information

[Creating a keytab \[page 78\]](#)

[No Credentials Found at Start of Application Server ABAP \[page 334\]](#)

### 3.4.1.4 Verifying keytabs for SNC Authentication

The SAP Cryptographic Library provides a function to make a keytab available for SNC configuration.

You can provide a keytab in the following ways:

- Using [SPNego Configuration](#) (transaction `SPNEGO`) or the SAP Single Sign-On configuration wizard (transaction `SNCWIZARD`) in SAP GUI to provide a global keytab
- Creating a keytab located in the `SAPSNCSKERB.pse` file using the `sapgenpse` command

With SAP Cryptographic Library 8.4.20 and AS ABAP 7.4 SP08 or higher, both cryptographic libraries verify the global keytab created with [SPNego Configuration](#) (transaction `SPNEGO` or `SNCWIZARD`) first and then the keytab located in the `SAPSNCSKERB.pse` file generated by `sapgenpse`. This makes sure that the cryptographic library uses a keytab that is suitable for the SNC authentication.

## ! Restriction

In an environment with SAP Cryptographic Library 8.4.19 or AS ABAP 7.4 SPO7 or lower, the library verifies the keytab differently. For more information, see SAP Note [2029258](#). If you activate the SAP Cryptographic Library trace, it contains some of the following messages:

Trace Messages for keytab Verification Issues

Trace Message	keytab Veri- fication	Description
Kerberos ticket verified successfully with global keyTab configured in SPNEGO (have global keyTab configured in SPNEGO and keyTab from PSE)	Successful	The cryptographic library has found the global keytab provided by the SPNEGO or SNCWIZARD transaction and the keytab located in the SAPSNCSKRB.pse file. Verification was successful using the global keytab.
Kerberos ticket verified successfully with global keyTab configured in SPNEGO (have only this one)	Successful	The library has found and verified the global keytab provided by the SPNEGO or SNCWIZARD transaction, and no keytab located in the SAPSNCSKRB.pse file is available.
Kerberos ticket verified successfully with keyTab from PSE (have global keyTab configured in SPNEGO and keyTab from PSE)	Successful	The library has found and verified the keytab located in the SAPSNCSKRB.pse file and has found the global keytab (provided by the SPNEGO or SNCWIZARD transaction).
Kerberos ticket verified successfully with keyTab from PSE (have only this one)	Successful	The library has found and verified the keytab located in the SAPSNCSKRB.pse file. No global keytab provided by either the SPNEGO or SNCWIZARD transaction) is available.
Kerberos ticket verification failed with global keyTab configured in SPNEGO	Failed	The library failed to verify the global keytab provided by either the SPNEGO or SNCWIZARD transaction.
Kerberos ticket verification failed with keyTab from PSE	Failed	The library failed to verify the keytab located in the SAPSNCSKRB.pse file.
Kerberos ticket verification not successfully because no global keyTab configured through SPNEGO nor a PSE with a keyTab is existing	Failed	The library failed to verify a global keytab and a file-based keytab (in SAPSNCSKRB.pse) because none of these keytabs is available.

### 3.4.1.5 Using Kerberos for SNC with Users in Multiple Domains

Solution for users in multiple Active Directory domains using Kerberos for SNC

You use Kerberos for SNC and you have users in multiple Active Directory domains. In such an environment, it is the best to have a trust relationship between the different domains. Every user is then able to receive an authentication ticket from the Domain Controller for this user's domain. As a consequence, the user can use this ticket for the server, which might be in a different domain.

#### i Note

If there is no trust relationship between the different domains, create a service account and a keytab for every domain.

### 3.4.2 Create a Microsoft Windows Account

#### Procedure

1. Create a new Microsoft Windows Account.

We recommend the format SAPService<SID>.

2. Define a password and choose the option *User cannot change password* and *Password never expires*.

#### i Note

Make sure the password is as complex as possible.

## 4 Advanced Scenarios

This section contains a number of advanced scenarios. An advanced scenario may serve a special use case, which might be suitable for a specific enterprise or industry, for example, but might not be suitable for other enterprises.

Advanced scenarios require considerable configuration effort. Configuration is usually performed in multiple systems. Sometimes different administrators are involved, for example, LDAP and AS ABAP administrators.

### 4.1 Logging on with Secure Login Client Using SNC

SAP Single Sign-On 3.0 enables you to log on with SAP GUI using encrypted communication but without single sign-on.

There are cases when users do not have single sign-on credentials for a target system, for example when they have forgotten their smart card or RSA token. In this case, the target system is untrusted. However, the users still want to log on to the target system using SNC because it is required by the security policy of your company.

To run SNC in encryption only mode, the server needs to authenticate with an X.509 certificate. In the client, only the Root Certification Authority certificate of the server's PKI must be installed as trusted authority.

In exceptional circumstances, a user may need to log on to an untrusted system using SNC.

As an administrator of the application servers, you want to offer a solution for this emergency situation. Users without single sign-on credentials should be enabled to use SNC when logging on to SAP Netweaver Application Servers (ABAP or Java), which are untrusted because they do not know the users' credentials. The users should not encounter an SNC error. As an administrator, you can roll out an encryption only mode for SNC to all employees. This configuration enables users to log on to untrusted application servers using SNC.

The following options are available:

- As an administrator, you can enable legacy compatibility mode. This is SNC-protected login on the side of the server. It is also possible to use server session keys or manual server trust. Legacy compatibility mode is available with CommonCryptLib 8.5.x or lower und SAPCRYPTOLIB 5.5.5.
- As an administrator, you can enable Secure Login Client to select an authentication method (smart mode) if most application servers use SAP Cryptographic Library CommonCryptoLib 8.5 or higher. It is also possible to use server session keys or manual server trust.  
We recommend this option because the Secure Login Client always selects the best authentication method.
- As an administrator, you can permanently roll out encryption only using SNC for all users or a group of users.
- Users can manually switch to encryption only for logging on using SNC.

## Prerequisites

- Client PCs are running the Secure Login Client of SAP Single Sign-On 3.0 or higher.
- The back-end systems are running Application Server ABAP with the SAP Cryptographic Library CommonCryptoLib 8.5 or higher.

## Related Information

[SNC Configuration Options in the Secure Login Client \[page 36\]](#)

### 4.1.1 Enabling Secure Login Client to Smartly Select an SNC Mode

As an administrator, you want to enable the Secure Login Client to automatically select an authentication method.

## Prerequisites

- Client PCs are running the Secure Login Client of SAP Single Sign-On 3.0 or higher.
- The back-end systems are running Application Server ABAP with the SAP Cryptographic Library CommonCryptoLib 8.5 or higher or 8.4.x.

## Context

Your company has a heterogenous landscape with multiple SAP systems. Some of them run with CommonCryptoLib 8.5 or higher, 8.4.x, or SAPCRYPTOLIB 5.5. SNC is in place. Users access the systems using either Kerberos tokens, or X.509 certificates. When users want to log on to a specific SAP Netweaver Application Server, they obviously do not want to think about which authentication method their Secure Login Client is using during logon.

As an administrator of the SAP systems, you want to make life easy for your colleagues. You want to configure the Secure Login Client so that SNC-encrypted logon is always possible no matter what authentication method the respective application server uses.

#### → Recommendation

In heterogenous landscapes, we recommend that you configure the Secure Login Client to use smart mode for selecting the authentication mode.

If this setting is activated, the Secure Login Client and the server negotiate the best common SNC mode:

- Authentication using Kerberos tokens
- Authentication using X.509 certificates
- Encryption only (no single sign-on)

To configure this smart selection of authentication methods, proceed as follows:

## Procedure

1. Open Secure Login Client.
2. In **File > Options...**, choose the **SNC** tab.
3. Select **Smart Mode**.

### Note

If most application servers in the landscape support Kerberos, you can choose the checkbox **Prefer Kerberos**. As a result, the Secure Login Client tries to use the Kerberos authentication method before it goes to the next authentication method. This configuration is also required if some back ends do not use the SAP Cryptographic Library CommonCryptoLib 8.5 or higher.

4. You can distribute this policy among all the other relevant clients - for example, with Microsoft Group Policies or other suitable means.

## 4.1.2 Rolling out General Availability of SNC-Encrypted Logon

As an administrator, you want to help users in an emergency situation and offer them a permanently available way to log on to the untrusted systems using SNC.

## Context

In this case, users do not need to manually switch to encryption only for SNC.

## Procedure

1. Open the Secure Login Client.
2. In **File > Options...**, choose the **SNC** tab.
3. Choose **Encryption Only Mode** and apply the settings.
4. You can distribute this policy among all other relevant clients - for example, with Microsoft Group Policies or other suitable means.

### 4.1.3 Manually Switching to Encryption Only for Logging on Using SNC

In exceptional cases, end users need to log on to an untrusted application server using SNC. One example of this is when employees forget their smart cards. This means they do not have single sign-on credentials.

#### Context

When end users without single sign-on credentials get an SNC error and cannot log on to Application Server ABAP, they can switch the Secure Login Client's encryption only emergency mode only for the current logon.

As an administrator, you might want to inform your end users about this manual mode. The following procedure describes how end users use the Secure Login Client to manually switch to encryption only mode for logging on using SNC.

After an unsuccessful logon attempt to an application server, the users receive an SNC error. Tell end users to proceed as follows:

#### Procedure

1. Open the Secure Login Client.
2. Choose the profile *Encryption only emergency mode is not active*.
3. To switch to encryption only mode, do one of the following:
  - Right-click this profile and choose *Toggle Encryption Only Mode*.
  - Double-click this profile.
  - Use the Return key.

End users get an SNC-encrypted connection to log on. The profile list of the Secure Login Client indicates that the encryption mode for SNC is on. The icon of the Secure Login Client and the encryption only profile is red. The application server prompts them for their user name and password.

### 4.1.4 SNC Configuration Options in the Secure Login Client

The Secure Login Client provides the following SNC configuration options for legacy compatibility mode and for smart mode.

## 4.1.4.1 Using Server Session Key Mode for SNC

Every time users use a token (smart card or soft token) to authenticate, they must enter a PIN. You do not want to force users to enter this PIN every time they open a session.

### Context

The Secure Login Client provides an option for handling smart cards or soft tokens for sessions of applications that run as plugins in the back end.

You open a session of an application (for example, Business Explorer Analyzer) which is embedded in Microsoft Excel and is running with RFC connections in the back end. You can log on to the back end using SNC. Of course, you also want to open the application session using SNC communication. A temporary session key is created, which is reused by the applications. This means users are not forced to enter a PIN for example, whenever they open this type of application session.

Administrators can enable SNC-protected sessions of applications.

### Procedure

1. Open the Secure Login Client.
2. Go to the [Options...](#) menu to choose the [SNC](#) tab.
3. Choose [Server Session Key Mode](#).

Administrators can enable the creation of a temporary session key for each application.

- a. List the applications separated by commas. All these applications use one common session key until its validity ends.

In the case below, the session key of the back end session is not shared with the applications listed.

- a. List the applications separated by commas. All these applications use their own session key until its validity ends.

### Results

Distribute this policy among all the other relevant clients - for example, with Microsoft Group Policies or other suitable means.

For more information, see the related link.



## Related Information

[SNC Settings \[page 267\]](#)

### 4.1.4.2 Allowing Manual Server Trust

Administrators have the option to allow a manual trust exception, in order to resolve a situation where a back end's X.509 certificate cannot be verified automatically.

#### Context

The trust exception is valid until the current Windows session ends.

#### Procedure

1. Open the Secure Login Client.
2. Go to the [Options...](#) menu to choose the [SNC](#) tab.
3. Choose [Allow Manual Server Trust](#).

Distribute this policy among all the other relevant clients - for example, with Microsoft Group Policies or other suitable means.

For more information, see the related link.

## Related Information

[SNC Settings \[page 267\]](#)

## 4.2 Providing X.509 Certificates to Secure Login Client Using JavaScript Web Client

JavaScript Web Client uses Secure Login Web Adapter to provide the Secure Login Client with certificates for SAP GUI login.

Your company portal, which runs in a web browser, provides multiple services, for example, there is a service provider for Human Resources or a service provider for opening internal support tickets. To use these services,

open your browser, log on to the company portal, and choose the link to the relevant service provider. An SAML 2.0 identity provider manages the users. TLS-protected single sign-on is possible within the portal landscape.

Of course, you also want to use single sign-on when you start SAP GUI. Here, the communication is protected by SNC. However, SAP GUI with SNC requires X.509 certificates. The setup varies according to the browser.

Browsers supporting plugins	<p>In some browsers, Secure Login Web Client can use a Java applet to trigger authentication at the SAP GUI without using Secure Login Client.</p> <p>For more information, see <a href="#">Using Secure Login Client in Web Adapter Mode [page 85]</a>.</p>
(Advanced) Browsers without plugin support	<p>Advanced browsers, however, do not allow Java applets as plugins since plugins are regarded as vulnerable. For security reasons, we recommend that you use advanced browsers.</p>

If you use these advanced browsers without plugin support, for example, for your company portal and want to log on to SAP GUI applications, you must roll out the Secure Login Client 3.0 or higher. You must run it with a set of JavaScript and Secure Login Web Adapter profiles provided by the Secure Login Server. The Secure Login Client communicates in a secure way with SAP GUI using SNC. The Local Security Hub makes sure that there is a secure communication channel with the JavaScript Web Client using TLS. A JavaScript Web Client enables the web browser to enroll certificates for web-based applications or applications that are installed locally. Administrators configure these profiles in the Secure Login Server.

## 4.2.1 Elements Required in Secure Login Client for JavaScript Web Client

The Secure Login Client profiles come with a dedicated user profile group for the JavaScript Web Client.

### Prerequisites

- You have installed Secure Login Client 3.0 with Secure Login Server support.

Secure Login Client uses a user profile group that is relevant for the JavaScript Web Client. You can see the profiles listed in the Secure Login Client. The user profile group contains the following authentication profiles:

- Secure Login Client Web Adapter profile with a port (requests and accepts X.509 certificates)
- Local Security Hub profile (this profile manages the browser communication)
- Secure Login Client profile (for example, for basic login with user name and password)

Moreover, the Secure Login Client needs an authentication profile for the JavaScript Web Client.

- Secure Login Web Client profile for a JavaScript Web Client (manages the upload and update of the Secure Login Client Web Adapter profiles)

## 4.2.2 Elements Required in Secure Login Server for JavaScript Web Client

To enable the JavaScript Web Client, the Secure Login Server must have special authentication profiles and a user profile group, which are uploaded to the Secure Login Client.

What you need in the Secure Login Server are the following elements:

- JavaScript Web Client profile
- A dedicated user profile group with at least the following authentication profiles:
  - Local Security Hub
  - Secure Login Web Adapter

If you want to log on to multiple SAP systems using SAP GUI and if these systems have different user certificate mappings or authentication policies, you must use a Secure Login Web Adapter profile for each connection.

The Secure Login Client gets new or updated profiles from the Secure Login Server, which is configured as the host in the Secure Login Client.

### 4.2.2.1 JavaScript Web Client

A component of Secure Login Server and Secure Login Client 3.0 that allows web browsers to enroll certificates for locally installed or web-based applications.

Single sign-on sessions of the current web application can be re-used, such as SAML 2.0 or portal logins. Interactive logon inside the web page is supported as well. This new technology is web-browser independent, and does not require any extensions or plugins.

#### i Note

Firefox requires a security module to access the operating system's local certificate store if Secure Login Server certificates are used for TLS.

#### i Note

For security reasons, Microsoft Edge runs with network isolation in the default settings. With version 25.10158x or higher, you can use Edge for the JavaScript Web Client. You must enable loopback for localhost 127.0.0.1. Run the following command in the command prompt (as administrator):

```
CheckNetIsolation LoopbackExempt -a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe
```

A JavaScript Web Client profile is associated with one Local Security Hub profile and one Web Adapter profile. Multiple JavaScript Web Client profiles can be configured independently, for example with different user certificate mappings or authentication policies.

## 4.2.2.2 Local Security Hub

A component of Secure Login Client 3.0 that allows web browsers to run JavaScript Web Clients.

The Local Security Hub provides an HTTPS REST API and is secured by TLS and CORS. The required TLS server certificate is implemented as a Secure Login Server profile. One Local Security Hub profile is sufficient to support one or more JavaScript Web Clients and their associated Secure Login Web Adapter profiles.

### i Note

This component is not provided in a terminal server environment (CITRIX or Windows Terminal Server).

## 4.2.2.3 Secure Login Web Adapter

A component of Secure Login Client 3.0 that allows web browsers to run Secure Login 3.0 JavaScript Web Clients

A Secure Login Web Adapter acts as a container for a single Secure Login Server certificate (only one certificate at any one time) but may receive certificates from multiple JavaScript Web Clients. Multiple Secure Login Web Adapter profiles are possible if multiple JavaScript Web Client certificates are required at the same time.

## 4.2.3 Extending JavaScript Web Client to Multiple SAP GUI Logins

You can extend JavaScript Web Client to support multiple logins.

If you are using SAP GUI to access multiple SAP systems (for example, an ERP system and an SRM system) at the same time with different user certificate mappings or authentication policies, your Secure Login Client must have multiple JavaScript Web Client profiles. You need one profile for one SAP GUI connection. In this case, you can use, for example, multiple SNC names, different authentication modes, and different certificate configurations.

### i Note

The Secure Login Client needs only one Local Security Hub. It provides a communication channel to the JavaScript Web Client using TLS.

## 4.2.4 Extending JavaScript Web Client to Multiple Portal Logins

Your company runs multiple portal applications that are reachable from the corporate portal. There is a Human Resources portal and an Employee Self-Service portal. However, these two portals require two different

certificates. Using JavaScript Web Client allows you to receive dedicated certificates for these different portal applications.

When you are running Secure Login Web Client in the JavaScript Web Client, you need a second Web Adapter profile and the related Secure Login Web Client profile for authentication.

You can still use the user profile group you configured for JavaScript Web Client. All you have to do is add a second Secure Login Web Adapter profile and a second Secure Login Web Client profile that specifies the authentication. This means that, in total, your user profile group has the following profiles:

- Local Security Hub
- Secure Login Web Adapter profile (Human Resources portal)
- Secure Login Web Client profile for authentication (Human Resources portal)
- Secure Login Web Adapter profile (Employee Self-Service portal)
- Secure Login Web Client authentication profile for authentication (Employee Self-Service portal)

You can easily extend this by adding another login to another portal application by simply adding the required profiles (Secure Login Web Adapter profile and Secure Login Web Client authentication profile for authentication).

## 4.2.5 Configuring the Secure Login Client for JavaScript Web Client

The Secure Login Client is using the authentication profiles that you have configured in the Secure Login Server.

### Context

The following authentication profiles must be available in the Secure Login Server:

- Local Security Hub
- Secure Login Web Adapter
- Authentication profile for logging on to an AS ABAP, for example using SPNego

A dedicated user profile group in the Secure Login Server contains all these authentication profiles. You distribute this user profile group to the clients. In the Secure Login Client, enter the URL to the Secure Login Server host and choose the user profile group that contains the profiles for JavaScript Web Client.

To configure the Secure Login Client manually, proceed as follows:

### Procedure

1. Open the Secure Login Client.
2. Go to the *Policy Groups* tab.

3. Enter the URL of the Secure Login Server host.
4. Go to [Group](#) and choose the user profile group you have created for the JavaScript Web Client.
5. Go to [Update Policy](#) and choose *at startup*.
6. Choose OK.
7. (If applicable) Choose the [Refresh](#) button to update the user profile group settings.

## 4.2.6 Configuring the Secure Login Server for JavaScript Web Client

The Secure Login Server requires a couple of dedicated authentication profiles to enable JavaScript Web Client in clients.

### Procedure

1. Create a Secure Login Client Web Adapter profile.
2. Create a Local Security Hub profile.
3. Create a Secure Login Web Client profile.
4. Create a user profile group for Secure Login Web Adapter and the Local Security Hub profile.

Two new profiles appear in the list of profiles of the Secure Login Client. They come with the user profile group for JavaScript Web Client you created earlier. You can recognize by their icons.

- Icon with blue arrows: default profile (the Secure Login Client can create certificates locally)
- Icon with yellow arrows: Secure Login Web Client profile (for certificates by the browser)

### 4.2.6.1 Creating an Authentication Profile for Secure Login Web Adapter

The Secure Login Client uses a Secure Login Web Adapter profile to get certificate information from the JavaScript Web Client, which is provided by the Secure Login Server.

### Procedure

1. Open the Secure Login Administration Console and go to the [Authentication Profiles](#) tab.
2. Choose [Create](#).
3. Enter a name and a description for your authentication profile and choose the client type [Secure Login Web Adapter Profile](#).
4. Choose [Next](#) to continue with the enrollment configuration.

5. Enter the following data:
  - Host name of your Secure Login Server
  - Port number with client authentication mode *Do Not Request*
  - The profile type is *webadapter*.
6. To complete the authentication profile, choose *Finish*.

## 4.2.6.2 Creating a Local Security Hub

For JavaScript Web Client, the Secure Login Client needs a signed TLS-protected communication channel with your browser.

### Context

To create a Local Security Hub profile, proceed as follows:

### Procedure

1. Open the Secure Login Administration Console and go to the *Authentication Profiles* tab.
2. Choose *Create*.
3. Enter a name and a description for your authentication profile and choose the client type *Local Security Hub Profile*.
4. Choose a policy configuration. The standard policy configuration is *Anonymous*, which is only available for this type of profile. Clients will get certificates without authentication and without interaction.
5. Enter the configuration for the certificate. The default validity period is 181 days because a long-term certificate is required. It is only used for the initial signing during the setup of the communication channel.
6. Enter a port that is available in all clients. The default port number is **34443**. The IP address is 127.0.0.1.
7. Choose *Next* to continue with the enrollment configuration.
8. Enter the following data:
  - Host name of your Secure Login Server
  - The port number you used for the JavaScript Web Client profile. Client authentication mode *Do Not Request*. *Auto-Enroll* is set to on.
9. To complete the authentication profile, choose *Finish*.

### 4.2.6.3 Creating a User Profile Group for JavaScript Web Client

The Secure Login Client uses a user profile group for the JavaScript Web Client.

#### Procedure

1. Open the Secure Login Administration Console and go to the [User Profiles Group](#) tab.
2. Choose [Create](#).
3. Enter a name and a description.
4. To create the user profile group, choose [OK](#).
5. Go to the [Profiles](#) tab and choose [Edit](#).
6. Add the following authentication profiles:
  - Local Security Hub
  - Secure Login Web Adapter
7. Save your changes.

You have configured a user profile for JavaScript Web Client. You can go to the Secure Login Client and configure it to use this user profile group. For more information, see the related link.



#### Related Information

[Configuring the Secure Login Client for JavaScript Web Client \[page 42\]](#)

### 4.2.6.4 SAML Support for JavaScript Web Client

When you open a SAP GUI SNC connection, Secure Login Client will launch a browser-based single sign-on procedure through a Web Client profile with SAML authentication.

#### Prerequisites

- You have installed SAP Single Sign-On with Secure Login Server 3.0 SP02 Patch 1 (see [2491884](#) ) and Secure Login Client 3.0 SP02 Patch 2 (see [2532366](#) .
- You have configured a JavaScript Web Client. For more information, see [Providing X.509 Certificates to Secure Login Client Using JavaScript Web Client \[page 38\]](#).
- You have configured a Web Client profile with SAML authentication.
- For the Web Client Profile, a user profile group with a mapped local security hub and a Web adapter profile exists. For more information, see [Creating a User Profile Group for JavaScript Web Client \[page 45\]](#).



## Context

Secure Login Client launches the Web Client profile in JavaScript Web Adapter mode when an SNC connection is launched. This requires some configuration steps on server-side and on client-side.

## Procedure

1. Configure a Web Client Profile for initiating an authentication in a Web Adapter profile and ensure that you choose one that is attached to a SAML profile for authentication with an identity provider.

To do so, in the Secure Login Administration Console, under [<Profile Management>](#) → [<Authentication Profiles>](#) → [<Web Adapter>](#), on the [Enrollment Configuration](#) tab, use the [SAP GUI initiated browser SSO](#) option.

2. Optionally, you can force reauthentication everytime the user accesses the Web Client Profile.
  - a. Enable the *forceAuthn* policy in the configured SAML service provider.
  - b. In the [Secure Login Administration Console](#), under [<Profile Management>](#) → [<User Profile Groups>](#) → [<Details of Web Adapter>](#) → [< Profiles>](#) → [<Web Adapter>](#), check the [Enable Re-Authentication](#) option.

## 4.3 Using a Remote Certification Authority in Secure Login

You want to use PKIs of Remote Certification Authorities (CAs) provided by the Active Directory Certificate Service or by a product with CMC interface. You also want to benefit from the advantages Secure Login Server offers, advantages like short-lived certificates and trust.

### 4.3.1 Prerequisites for Using a Remote Certification Authority

Before the configuration in Secure Login Server can be started., certain preparations are required. These preparations depend on the respective product and protocol:

- [Configuring Microsoft AD CS Web Enroll \[page 47\]](#)

## 4.3.1.1 Configuring Microsoft ADCS Web Enroll

### Context

Secure Login Server as registration authority requires additional configurations of Microsoft ADCS Web Enroll. For details on how to set up the ADCS role "Certification Authority Web Enrollment", see the current documentation in MSDN .

Configure the following settings:

### Procedure

1. Use HTTPS for the Web Enroll URL .
2. Configure a domain user that acts as RA agent in Secure Login Server with appropriate permissions, e.g. "DOMAIN\SLSRA".
3. Create a certificate for the domain user.
4. Configure the certificate and private key to be exported as PFX file for later import into AS JAVA.  
HTTPS Server Authentication with Basic Authentication is also supported, but not recommended.
5. Add "Security > Autoenroll" for the domain user. Do so for all ADCS certificate templates that shall be used by Secure Login Server.
6. Set the desired "Cryptography" properties.

### Related Information

[Prerequisites for Using a Remote Certification Authority \[page 46\]](#)

[Configuring a Remote Certification Authority for Secure Login \[page 48\]](#)

[Remote Certification Authority Certificate Templates \[page 54\]](#)

## 4.3.2 Configuring a Remote Certification Authority for Secure Login

To use Remote CAs in the Secure Login Client, you need to configure them in the SAP NetWeaver AS for Java and in the Secure Login Server.

### Context

Proceed as follows:

### Procedure

Steps in the SAP NetWeaver Administrator

1. (If required) Define the key storage and import certificate and key information of your Registration Authority, issued by the Remote CA.
2. Create HTTPS destinations for remote CAs.
3. (If required) Configure the respective proxies.
4. (If the proxy configuration has been changed) Restart SAP NetWeaver AS for Java.

Steps in the Secure Login Server

5. Create a remote CA in the Secure Login Server using the destinations created in the AS Java.
6. Create or change a Secure Login Client profile to use remote CAs.
7. Add the Secure Login Client profile to a user profile group and upload the policy to the Secure Login Client (see the related link).

Steps in the Secure Login Client

8. If the Secure Login Client uses a new user profile group, refresh the policy groups and choose the user profile group where you have configured the remote CA.

After a policy has been downloaded, the Secure Login Client uses the policy group with the remote CA.

### Related Information

[Creating a Profile Group of Authentication Profiles \[page 145\]](#)

### 4.3.2.1 Adding the Certificate and Key Information of the Remote Certification Authority

Your Remote CA administrator provides credentials for HTTPS authentication to enable Registration Authority function. The credentials could be either a user name and password, or an X.509 certificate with private key. In

In addition, you may get the SSL/TLS root CA certificate, import the certificates and key information of the Remote CA into the SAP NetWeaver AS for Java.

## Context

Proceed as follows:

## Procedure

1. Open the SAP NetWeaver Administrator and choose the [Configuration](#) tab.
2. Choose [Certificates and Keys](#).
3. Add the key storage view for your Registration Authority credentials.
4. To add the certificates and private keys, choose [Import Entry](#).
5. Select the entry type [X.509 Certificate](#) and import the certificate file.
6. Select the entry type [PKCS#12 Key Pair](#) and import the key file.

### 4.3.2.2 Configuring a Destination for a Remote Certification Authority

The destinations of SAP NetWeaver AS for Java contain the connection information of the Remote CAs.

## Context

If you want to use Remote CAs, configure separate destinations in the SAP NetWeaver Administrator and include the URL, the certificate type, and the authentication of the Remote CA.

## Procedure

1. Open the SAP NetWeaver Administrator and choose the [Configuration](#) tab.
2. To create a new destination, go to [Destinations](#) and choose [Create...](#)
3. Enter a destination name that indicates the Remote CA and choose the destination type [HTTP Destination](#).
4. Choose [Next](#) to continue.
5. Enter the URL of the Remote CA service.
6. Deactivate [Ignore SSL Server Certificates](#) and choose the trusted server certificate key storage of the Remote CA you want to use.

7. Choose [Next](#) to continue.
8. Choose the authentication of the Remote CA. Choose either [Basic \(User ID and Password\)](#) or [X509 Client Certificate with SSL](#).

#### ❖ Example

Values for Remote CA Authentication

Authentication	Client Certificate Authentication
<a href="#">Basic (User ID and Password)</a>	User name and password
<a href="#">X509 Client Certificate with SSL</a>	Key storage view
	Certificate

9. To test the connection to the Remote CA, choose [Ping Destination](#). A message in the SAP NetWeaver Administrator tells you whether the Remote CA was reached.
10. To complete, choose [Finish](#).

### 4.3.2.3 Configuring Proxies for a Remote Certification Authority

Your remote CA must communicate with the SAP NetWeaver AS for Java from outside your company intranet. For this reason, you need to configure proxies for the AS Java.

#### Context

Enter the proxy settings in the [Java System Properties](#) section of the SAP NetWeaver Administrator.

#### Procedure

1. Open the SAP NetWeaver Administrator. Then choose the [Configuration](#) tab and select [Infrastructure](#).
2. Go to [Java System Properties](#) and choose the [System VM Parameters](#) tab.
3. Add the Java system properties of your AS Java.

#### ❖ Example

Java System Properties for Remote CA Proxies

Name	Custom Calculated Value
http.nonProxyHosts	localhost *.company.corp
http.proxyHost	proxy
http.proxyPort	8080
https.nonProxyHosts	localhost *.company.corp
https.proxyHost	proxy
https.proxyPort	8080

4. Restart SAP NetWeaver AS for Java.

You have completed the configuration in the SAP NetWeaver Administrator.

### 4.3.2.4 Defining a Remote Certification Authority in the Secure Login Server

You must add and enable the Remote CA you configured in the SAP NetWeaver AS for Java in the Secure Login Server.

#### Context

You must add a Remote CA with its adapter type and destination as a new CA to the Secure Login Server.

#### Procedure

1. Open the Secure Login Administration Console.
2. Go to the *PKI Structure* section of the *Certificate Management* tab.
3. Choose the *Create Remote CA* button.
4. Enter a name for the Remote CA.
5. Choose the adapter type and the HTTP destination in accordance with the type of your Remote CA.

#### ❖ Example

Active Directory Certificate Service

Parameter	Value
Alias Name	ADCS Remote CA
Adapter Type	ADCS - WebEnroll
HTTP Destination	<HTTP_destination_name>

#### ❖ Example

CMC Remote CA

Parameter	Value
Alias Name	CMC
Adapter Type	CMC - Simple
HTTP Destination	<HTTP_destination_name>

6. Choose the row of your newly created Remote CA.
7. Choose [Enable Remote CA](#). This builds up a first connection from the Secure Login Server to your Remote CA and displays the details of the Remote CA certificate in the Certificate Management view of the Secure Login Server.
8. The Secure Login Server prompts you to specify a distinctive name for the connection test - for example **CN=test**.

If the enabling the Remote CA is successful, you will see a green status indicator, the certificate type **REMOTE CA**, an algorithm, and a period of validity. The details pane at the bottom displays the details of the X.509 certificate.

You can now enter the Remote CA in the respective authentication profiles.

### 4.3.2.5 Using a Remote Certification Authority for Secure Login Client

When you use authentication profiles and perform a policy upload, the Secure Login Server distributes the new or updated policy with the Remote CA to the clients.

#### Context

To use the Remote CAs that are available in the Secure Login Server, integrate them into new or existing authentication profiles. Use a new or already existing user profile group to update the policy to multiple clients.

The policy download automatically updates the policy groups in the Secure Login Client. This ensures that the Secure Login Client is going to use the updated policy with the Remote CA.

#### **i Note**

If the Secure Login Client is to use a new user profile group that comes with the Remote CA, you must manually select the respective profile in the Secure Login Client. For more information, see the related link.

## **Procedure**

1. Choose the [Authentication Profiles](#) section in the [Profile Management](#) tab and select the relevant authentication profiles.
2. Choose [Edit](#) in the [Certificate Configuration](#) tab.
3. Go to the field [CA for Issuing Certificates](#) and choose the Remote CA.
4. Save your changes.
5. (Optional) To see the key and certificate details of the Remote CA, choose [View Properties](#).

From now on, the policy download mechanism updates the authentication profile in the Secure Login Client. You don't need to do anything. The profile with the Remote CA appears in the list of profile of the Secure Login Client. You can see the details if you right-click the profile and choose [Show Certificate...](#)

## **Related Information**

[Manual Choice of User Profile Group in the Secure Login Client \[page 53\]](#)

### **4.3.2.6 Manual Choice of User Profile Group in the Secure Login Client**

If the Secure Login Client uses a new user profile group that comes with the Remote CA, you must manually select the respective profile in the Secure Login Client.

## **Context**

#### **i Note**

You only need to perform the following procedure once.



## Procedure

1. To manually update the policy in the Secure Login Client, open the Secure Login Client.
2. Choose the *Policy Groups* tab in **File > Options...**
3. Choose *Refresh* to make sure that the Secure Login Client gets the most recent policies.
4. Go to the *Group* field and choose the user profile group that comes with the Remote CA.

The profile with the Remote CA appears in the list of profiles of the Secure Login Client. You can see the details if you right-click the profile and choose *Show Certificate...*

From this point onwards, the policy download mechanism updates the authentication profile in the Secure Login Client. You need not do anything further.

## 4.4 Remote Certification Authority Certificate Templates

Like Secure Login Server, a remote CA also supports multiple certificate templates, depending on the respective product and service. The certificate template of a Remote CA is always overriding any attributes sent by SLS in the name of the client. The main purpose of selecting a template in SLS is to tell the Remote CA which kind of certificate shall be issued.

## 4.5 Using the Secure Login Server to Provide Trusted Certification Authorities

The Secure Login Server can take over the entire trust management for an Application Server ABAP. It provides trusted CAs with the respective trust anchors. Therefore, you no longer need to use the trust manager of AS ABAP.

The Secure Login Server can import a CA with its own trusted issuer certificate - for example, its own root CA certificate with a number of certificates that belong to a special PSE. This trusted issuer certificate replaces the previous CA's own certificate in the trust manager (*STRUST* transaction in AS ABAP). Thus, the Secure Login Server takes over the entire trust management of a special PSE - for example, the SSL server PSE.

The CA certificate provided by the Secure Login Server comes with a list of trust anchors stored in the key storage of SAP NetWeaver Application Server for Java. The Secure Login Server uses an application server profile group with the AS Java key storage view, which contains the certificates of the trust anchors in a list.

### Note

Administrators of the Secure Login Administration Console must have the appropriate permission in the SAP NetWeaver Application Server for Java to use the key storage view.

## 4.5.1 Configuration Information for Trusted Certification Authorities Provided by the Secure Login Server

To be able to use trusted CAs provided by the Secure Login Server, you will need to configure them in the SAP NetWeaver AS for Java and in the Secure Login Server.

### Prerequisites

Administrators who configure trusted CAs in the Secure Login Administration Console must have the following role in the SAP NetWeaver Administrator because they enable the Secure Login Server to read the key storage view with the trusted CA certificates.

- SLAC\_SUPERADMIN

### Context

Proceed as follows:

### Procedure

In the SAP NetWeaver Administrator

1. Create a key storage view for the Secure Login Server and import or copy CA entries into the key storage view you want to use in the Secure Login Server.
2. Restart SAP NetWeaver AS for Java.

In the Secure Login Server

3. Activate the trusted CA key storage view in the respective application server profile group and add the key storage view created (in the SAP NetWeaver Administrator) to the application server group.

### 4.5.1.1 Configuring the Trusted CA Key Storage View for the Secure Login Server

The Secure Login Server needs a key storage view that contains the list of trust anchors that the Secure Login Server is supposed to use as trusted CAs.

#### Context

Proceed as follows:

#### Procedure

1. Open SAP NetWeaver Administrator.
2. Go to *Certificates and Keys* in the *Configuration* tab.
3. To create a new key storage view, choose *Add View* in the *Content* section of the *Key Storage* tab
4. Import or copy the entries, for example, of the root CA certificate and other CA certificates. You can import certificates from the file system or copy already existing certificates from other key storage views. Use either the *Import Entry* or *Copy Entry* button.

Your key storage has all the required CA certificates.

### 4.5.1.2 Defining a Trusted Certification Authority in the Secure Login Server

The Secure Login Server must know the key storage view you created in the SAP NetWeaver Application Server for Java. As an administrator, you enter the key storage view into a dedicated application server profile and mark it as the key storage view with the trusted CAs.

#### Prerequisites

The Secure Login Server Remote CA adapter for Microsoft Active Directory Certificate Services - Web Enrollment needs a specific certificate template in the Certification Authority of the Active Directory settings. Currently, only a single template is supported, its name must be *SecureLoginServerUser*. The display name of the template can be different.

For more information, see the Microsoft Windows Server documentation about managing certificate templates.

## Context

Proceed as follows:

## Procedure

1. Open the Secure Login Administration Console.
2. Go to the [Application Server Profile Groups](#) section of the [Profile Management](#) tab.
3. Create a new application server profile group or choose an existing one.
4. To add a key storage view, go to the [Trusted CAs](#) tab and choose the [Edit](#) button.
5. Activate the [Select a Key Storage View](#) checkbox.
6. Select the key storage view with the trusted CAs in the dropdown box.

### Note

You can use [Certificate and Keys](#) to see the key storage view in SAP NetWeaver Application Server for Java, the certificates, and the details of the certificates.

7. Save your changes.

## 4.6 Certificate Lifecycle Management Using the Secure Login Server

The Secure Login Server can manage the certificate lifecycle - for example, renew long-lived certificates. It uses application server profile groups with authentication profiles where you can configure the renewal of certificates.

The Secure Login Server provides multiple options for this:

- Certificate renewal supported by the Application Server ABAP and the AS Java
- The `saplscli` command line interface for managing the certificate lifecycle using operating system means

## Related Information

[Certificate Lifecycle Management in the AS ABAP Using Secure Login Server \[page 88\]](#)

[The saplscli Command Line Interface \[page 58\]](#)

[Installing Additional Features for Secure Login \[page 231\]](#)

[Certificate Lifecycle Management in the AS Java Using Secure Login Server \[page 97\]](#)

## 4.6.1 The sapslscli Command Line Interface

SAP Single Sign-On 3.0 comes with the `sapslscli` command line tool, which enables administrators to manage the certificate lifecycle without using an AS ABAP. It provides certificate lifecycle management, a function that enables you to directly renew certificates (in PSEs). You configure application server profile groups. Each application server profile group contains profiles of the type "application server profile". Assign these profile groups to the system IDs (SIDs).

An application server profile group like this requires a "registration agent" profile for the initial enrollment certificate for the administrator's logon with credentials. It also contains application type-specific profiles - for example, the SNC PSE, PSEs of the SSL Server PSE type. It also includes all trusted TLS root certificates that are required to run secured communication with the Secure Login Server.

As an administrator, you can trigger a renewal of the relevant certificates in the command line.

For more information, see the command line interface help using `sapslscli -h`.

## 4.7 Browser-Based Enrollment of Secure Login Client Using a Secure Login Server Profile

You want to start SAP GUI using a browser shortcut, but you do not have a suitable certificate. For this reason, you need a browser-supported enrollment of the Secure Login Client.

### ! Restriction

- This function is only available for Microsoft Windows clients running Microsoft Internet Explorer.
- Only web sites from trusted hosts can use the front-end control.

A user who uses the Secure Login Client wants to get an SNC connection to an Application Server ABAP with a specific SNC name, but no suitable certificate is available. The user wants to use the user certificate configuration of a dedicated Secure Login Server profile. Using a front-end control in the browser, the Secure Login Client initiates an enrollment with a Secure Login Server profile. The enrolled certificate is meant to be used for connections to an AS ABAP with a given SNC name. The front-end control determines that this Secure Login Server profile is used for connections with a specific AS ABAP, which is identified by the SNC name.

When you log off from the current Secure Login Client session, or when the certificate lifetime has expired, you remove the certificate that is tied to the specified Secure Login Server profile.

This temporary setting overrides the current application policies in the client's registry.

## Prerequisites

You need to fulfill the following requirements on the side of your clients:

- You have installed the Secure Login Client 2.0 or higher with the [Secure Login Server Support](#) option. The front-end control `slsax.dll` comes with the Secure Login Client. After the installation, the front-end

control is located in the installation folder of the Secure Login Client. For more information, see the related link.

- Your client uses Microsoft Internet Explorer.
- You have installed SAP GUI.
- You are using Secure Login Server profiles.

Observe the following server-side prerequisites:

- You are running Application Server ABAP and Java.
- You have installed Secure Login Server 2.0 or higher on an AS Java.
- You are using SAP Cryptographic Library on an AS ABAP.
- You have configured Secure Login Server profiles.

## Related Information

[Secure Login Client Installation \[page 132\]](#)

## 4.7.1 API Methods for Profile Enrollment

The front-end control `s1sax.dll` implements a number of methods for enrolling Secure Login Server profiles at the Secure Login Client.

### ProfileIsEnrolled

This method displays whether a profile exists and is enrolled.

Syntax

```
bool ProfileIsEnrolled(BSTR szProfile)
```

Return Values	Description
true	The relevant profile exists and is enrolled.
false	All other situations

### ProfileEnroll

This method executes an enrollment for an authentication with user name and password or for an authentication where credentials are provided by Microsoft Windows. The method sends an exception if `szProfile` is too long or contains invalid characters.

## Syntax

```
bool ProfileEnroll (BSTR szProfile)
```

## ProfileEnrollSNC

This method binds the SNC name to the relevant profile. This binding overrides the registry settings provided by the application policies. The method sends an exception if the profile is too long or contains invalid characters.

For more information, see the related link.

## Syntax

```
bool ProfileEnrollSNC(BSTR szProfile, BSTR SNCname)
```

Return Values	Description
true	The relevant profile exists and is enrolled.
false	All other situations

## ProfileLogout

This method triggers a logout of the relevant Secure Login Server profile without any return values. As a consequence, any call of `ProfileIsEnrolled` returns `false`.

## Syntax

```
void ProfileLogout(BSTR szProfile)
```

## ClearSSLCache

This method deletes the SSL cache of the Microsoft Internet Explorer.

## Syntax

```
void ClearSSLCache()
```

## Related Information

[HTML Code Example with Secure Login Server Profile and SNC Name \[page 61\]](#)

## 4.7.2 HTML Code Example with Secure Login Server Profile and SNC Name

If you want to use this function, integrate the front-end control, for example, into your portal page.

The front-end control `slsax.dll` enables you to force the Secure Login Client to initiate an enrollment with a dedicated Secure Login Server profile at an AS ABAP having a specific SNC name. For this reason, you define at least the following things in your front-end control:

- Secure Login Server profile you want to use
- SNC name of the AS ABAP for which the certificate is meant to be used

### Example

The following simple HTML code example tells you how to tie a dedicated Secure Login Server profile to an SNC name of the AS ABAP you want to connect to. The user interface displays a pushbutton where you can trigger the enrollment with the Secure Login Server profile called `MyProfile` that is tied to the SNC name `CN=my_SNC_server` of the AS ABAP.

```
<html>
<head><title>SlcAx Test Page</title></head>
<script language="javascript">
doEnroll = function()
{
  var retval = slsax.ProfileEnrollSNC("MyProfile", "CN=my_snc_server");
}
</script>
<body>
  <form name="form">
    <input type="button" name="cmdEnroll" value="Enroll" onClick="doEnroll()" />
  </form>
  <object id="slsax" classid="CLSID:E3D89180-3104-414B-9807-6E778E0103E3"
width="0" height="0" />
</body>
</html>
```

The result is a web site with an [Enroll](#) pushbutton.

When you choose [Enroll](#), the Secure Login Client enrolls the Secure Login Server profile, prompts you for your credentials, and issues a certificate.

After having entered the user credentials, the user gets the certificate of the Secure Login Server profile name (`MyProfile`), and can log on to the AS ABAP with the SNC name `CN=my_snc_server`.



## 4.8 Using Secure Login Client as SSH Agent

The Secure Login Client can run as an SSH agent, which provides a secure way to use keys and certificates stored in the Microsoft Crypto Store for SSH public key authentication.

### Context

You want to reuse keys and certificates that have been rolled out locally and that are stored in the Microsoft Crypto Store for SSH terminal sessions, such as PuTTY or Cygwin. In this case, the Secure Login Client acts as an SSH agent. This replaces the SSH agent of PuTTY (Pageant).

#### ! Restriction

The Secure Login Client only supports RSA keys.

After having activated the Secure Login SSH Agent in the Secure Login Client, you must add your public key to the `authorized_keys` file on the side of the SSH target system.

### Procedure

1. Make sure that no other SSH agent is active.

#### ⚠ Caution

If another SSH agent is running, and you enable the Secure Login SSH Agent, you get the following message:

```
Another SSH Agent is running. It will not be possible to start the Secure Login SSH Agent.
```

2. Open the Secure Login Client. You find the tray icon in the taskbar of Microsoft Windows.
3. Go to the *SSH Agent* tab in ► *File* ► *Options...* ►

#### i Note

This tab only displays local certificates with the relevant key information.

4. Make sure the checkbox *Enable Secure Login SSH Agent* is enabled.
5. Choose *Apply* to start the Secure Login SSH Agent.

The Secure Login SSH Agent is active. You see the following notification in the tray:

#### *SAP Secure Login Client*

This is your SSH Agent. Press CTRL-ALT-C to get a certificate's public SSH key.

6. Choose the certificate you want to use for the SSH agent.

7. Use Ctrl-Alt-C or the [Copy to Clipboard](#) button to copy the public key into the clipboard.
8. Log on to the Linux/UNIX server using SSH by entering the user name and password.
9. Open the authentication configuration file `authorized_keys` in the `$HOME/.ssh/` directory in your target system.
10. Add the public key from the Secure Login Client certificate to the file and save your changes.

Test the configuration by starting a new SSH session with the target system.

#### → Tip

This authentication setting can be used for SSH sessions on multiple servers if you allow agent forwarding.

## 4.8.1 Restricting the Use of Secure Login SSH Agent

Developers or administrators want to restrict the use of the SSH agent.

### Context

The user of the client PCs should not be able to switch between SSH agent modes. The user should either always use the Secure Login SSH Agent or never use it.

- Always use Secure Login Client as an SSH agent.
- Never use the Secure Login SSH Agent.

### Procedure

1. Open the registry of Microsoft Windows and go to `[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\Common]`.
2. Create the new registry key **TurnOnSSHAgent** of the type `REG_DWORD`.
3. To switch on the SSH agent mode in your Secure Login Client, enter the value **1**. To disable the Secure Login SSH Agent, enter the value **0**.
4. Log off from your Microsoft Windows session and log on again.

When the Secure Login Client starts again, your settings are permanent.

5. If you want to always use Secure Login Client as an SSH agent, select the local certificate you want to use and add its public key to your SSH terminal application.

## 4.9 Digital Client Signature (SSF)

The Secure Login Client can use X.509 certificates for digital signatures in an SAP environment.

The supported interface is Secure Store and Forward (SSF). This option is part of the default installation. The prerequisite for using SSF is that SSF is configured in the SAP instance profile.

### 4.9.1 How to Test SSF Client Signature

You can test the SSF client signature in a SAP GUI using, for example, Secure Login Server, smart-card, or soft-token profiles as SSF profiles. For more information, see related link.

#### Procedure

1. Log on to the SAP system using SAP GUI and start transaction `SE38`.
2. Enter the program name `SSF01` and execute this program.
3. Choose a desired function you want test, for example, *Signing*.
4. For the parameter *RFC destination*, enter the value `SAP_SSFATGUI`.
5. For the parameter *SSF format*, enter the value `PKCS7`.

You have the following configuration options:

- If you use smart card, enter the Distinguished Name of the smart card certificate in the *ID* field.

❖ Example

CN=Smartcard User, OU=SAP Security

User profile (sign and develop)	
ID	CN=Smartcard User, OU=SAP Security
SSF Profile	
Password	

In the *SSF Profile* field, enter the token ID.

❖ Example

tokcapi:\*(\*)

- If you use Secure Login Client profile provided by Secure Login Server, enter the Distinguished Name of the user certificate in the *ID* field.

CN=Username, OU=SAP Security

Syntax:

<profile\_name> is the profile name defined in Secure Login Server. In this example the profile name is SSF.

- ### Example

### Example

- Execute the program and choose the *Sign* button.

```
SST Test Program
```

---

Additional operation:

---

	Sign	RFC target:	SAP_SSFATG01
--	------	-------------	--------------

---

Input date: 398

!!!!!!! This text should be signed !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! This  
!!! This text should be signed !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! This text should be signe

User profile (sign and develop)

CN=SSTEST, O=SAP, L=Waldorf, C=DE  
tokswimm//securelogin/SSE

Result: SSF\_API\_OK

Results for the signatory:

CN=SSTEST, O=SAP, L=Waldorf, C=DE  
SSF\_API\_SIGNER\_OR\_RECIPIENT\_CN

Output date: 2.420

G.p.\*H#...#.aC.j....l.O..\*\*H#.....C.#.\*\*H#...##.#.#.!!!!!!!!!!!!!!! This text should  
should be signed !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! This text should be signed !!!!!!!!!!

AP TIP CORE IDM and Cryptool.0...U...NW 7.21.0...User CA FMO...110527132045Z..110527232045Z081.0...  
#EPV.S==#####c####Y#Z#O.U.####.#!1:(~:#Ag..B#....#uoS0.U...#....#0...U...#.0.C...U...  
epS\*.m.c.,leC..LzKx.#.#...#jCVv.N###e#"\$.IsHYd#####S-;.;#b.#xx##.#fNM\*v#d####).DHed.z.#cRdT  
.SAP TIP CORE IDM and Cryptool.0...U...NW 7.21.0...Root CA Demo FMO...110321090453Z..210321090453ZOM  
zp#:!.##3#.###0.l+##.#.#.#.#.vApR###00.#.X(.WNT####kde.#el=L.).g###zQ##?#0.h.b.LQ###.###  
0...#0...#@#.#.....#.k.kCC###k.#.-#6.YM#####=-###.S.-# hTY###LeP.##b##.X####Zvy#&!@#?#Vy..#.  
.#.##.--#+\$k#.#GJ-WC..1#.-#0.Z..0ZMLSD".U...SAP TIP CORE IDM and Cryptool.0...U...NW 7.21.0...U...U  
#\*-##m1.-#PQi###Q#./.#j}.ij}#.l##.###.##\*"###k.v#S###T5.##BHDX#.#####T.##G.#.##k####.#\*\*\*.z#.

Results of GUI-Download:

File name: C:\temp\IsSigned.txt  
Length of file in bytes: 2.420

## Related Information

[SSF Parameters for Digital Signatures \[page 268\]](#)

### 4.9.2 SSF User Configuration in SAP GUI

This topic tells you how you configure a user for the SSF in SAP GUI.

#### Context

Use this configuration step to define which Secure Login Client profile is used for the SSF interface. This is defined for each SAP user.

#### Procedure

1. Log on to the SAP system using SAP GUI and start transaction `SU01`.
2. Edit the desired user and, on the *Address* tab, choose the *Other Communication* button.
3. Choose the *SSF* option and define the desired parameters. For details about the parameters, see the related link.

## Related Information

[SSF Parameters for Digital Signatures \[page 268\]](#)



### 4.9.3 System Signature Using Microsoft Active Directory Authentication

The AS ABAP provides you with a tool for signing and approving data with a digital signature. By default, you use your SAP user ID and password to do so. Using a BAdI and an front-end control in the Secure Login Client, however, enables you to provide a system signature for documents using your SAP user and your Microsoft Windows password.


#### **i** Note


We do not recommend that you use this system signature mechanism. Use signatures based on X.509 certificates instead.

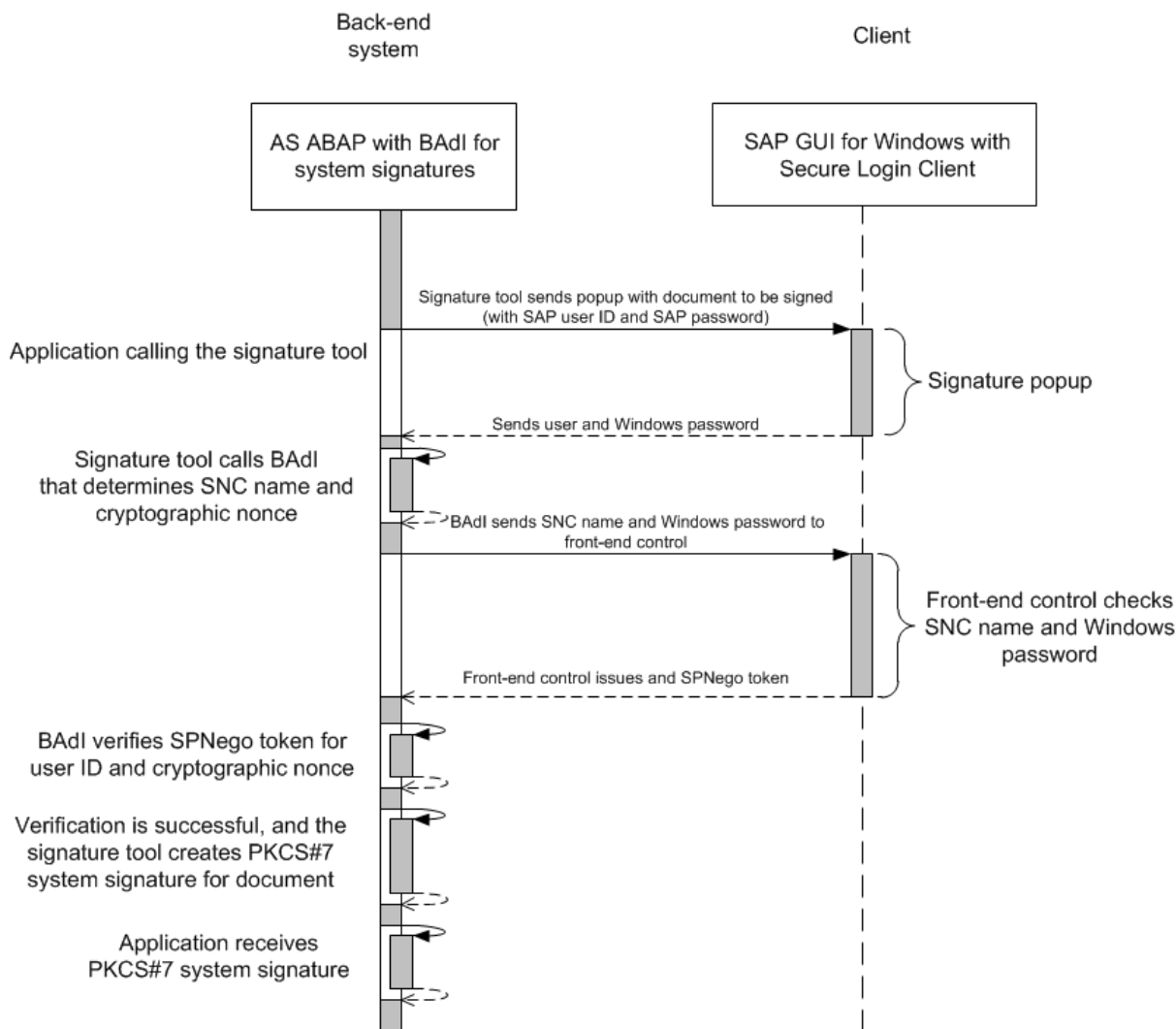
## Prerequisites

- You have applied SAP Note [1862737](#) .
- You are running SAP GUI for Windows on the client.
- SAP NetWeaver Single Sign-On 2.0 SP2 or higher is installed. During the installation of Secure Login Client, you activated the *Kerberos Single Sign-On* installation component. A front-end control called `slcax.dll` is available on the Secure Login Client (in this case, SAP GUI for Windows).
- You are using the SAP Cryptographic Library (see SAP Note [1848999](#) ) , or you have set the path to the cryptographic library you use as SSF provider. If required, use transaction `RZ10` to change the following profile parameters:
  - `ssf/ssfapi_lib=<path_to_cryptographic_library>`
  - `ssf/name=SAPSECULIB`
- You have configured SNC for Kerberos. The AS ABAP user has a Kerberos SNC name. For more information, see the related link.

## Scenario

In a Microsoft Windows environment (Microsoft Active Directory), a user is using an AS ABAP and logged on using single sign-on. In the application, the user calls the signature tool. When the user creates a system signature, he or she must re-authenticate with his or her SAP user ID and Microsoft Windows password. Now he or she is able to provide a system signature for documents to prove that he or she reviewed the document was reviewed by him or herself during the workflow process. For more information on digital signing, see the relevant related link and SAP Note [700495](#) , which describes how you create digital signatures with the user and password of an ABAP user account. However, since the user has logged on with SAP NetWeaver Single Sign-On, the user might not have a password on the AS ABAP.

Using the BAdI from SAP Note [1862737](#) , you can provide system signatures for documents with the SAP user and the Microsoft Windows password. This BAdI in the AS ABAP determines the SNC name and sends the SNC name with the password to the SAP GUI for Windows client. The `slcax.dll` front-end control in the Microsoft Windows environment on the client side verifies the user name and password. Once it has done so, it issues an SPNego token that is retrieved from the BAdI in the AS ABAP. The BAdI then verifies the SPNego token. If the verification is successful, the digital signature is created for the document.



Client tracing logs certain activities and any errors that might occur during the signing process. For more information, see the relevant related link.

### ! Restriction

End users of SAP GUI for Windows should not have administration rights for their clients. This makes sure that the configuration of the Secure Login Client remains unchanged.

## Related Information

[http://help.sap.com/saphelp\\_nw74/helpdata/en/a7/75745b9bc84d86ad83edbd671f02d7/frameset.htm](http://help.sap.com/saphelp_nw74/helpdata/en/a7/75745b9bc84d86ad83edbd671f02d7/frameset.htm)  
 SNC Kerberos Configuration [page 27]  
 Tracing Secure Login Client [page 158]

### 4.9.3.1 Digital Client Signatures for SAP UI5 Applications

This JavaScript-based Web signer functionality allows Secure Login Client to create digital signatures in SAP UI5 applications, such as SAP Fiori or SAP Cloud Platform, in browsers on both Windows and macOS.

#### Context

This Web Signer is based on the JavaScript Web Client, and it allows to create SSF compatible PKCS#7 SignedData. Note that for the integration into your own UI5 apps, you have to contact SAP support. It is available in all standard browsers on Windows and macOS (for example, Chrome, Firefox, Safari, Internet Explorer, Edge). For more information, see the Product Availability Matrix at <http://support.sap.com/pam>.

#### Procedure

On Secure Login Client, change the local security configuration. For more information, see [Providing X.509 Certificates to Secure Login Client Using JavaScript Web Client \[page 38\]](#).

## 4.10 X.509 and Kerberos Authentication

This topic describes how you can combine X.509 and Kerberos authentication.

### 4.10.1 Authentication with X.509 Certificates and Kerberos

Users can authenticate to an AS ABAP with X.509 certificates and Kerberos using SNC communication.

You already have an authentication method in place that is based on SNC server certificates. All users use the message server to authenticate at the application server. During the authentication process, the message server always sends the same SNC name since it is only able to use one single name. This means that the SNC name in the [Network](#) tab is a fixed entry entered by the CA for certificate-based authentication.

To add users who are able to log on with Kerberos, you need to have a name in the CN part (of the SNC name) that enables users to perform a Kerberos authentication as well.

Depending on the authentication method of the client, the Secure Login Client uses the existing CN part for certificate-based authentication or tries to map the CN part to a Service Principal Name that can be used for Kerberos authentication.

If this is not possible, the Secure Login Client converts the CN part as described in the related link.



## Related Information

[SAP Note 1696905](#) 

### 4.10.2 Supporting Authentication with Kerberos and X.509 on SAP NetWeaver AS ABAP

You want to use Kerberos authentication technology for the client-to-server communication and thus enable single sign-on and secure server-to-server communication using SNC.

#### Prerequisites

- You have installed Secure Login Client on the client workstations in a Microsoft domain and have enabled SNC in SAP GUI.
- The SAP Cryptographic Library is installed on AS ABAP systems ONE and TWO. This makes an SNC communication with X.509 certificates possible.

#### **i** Note

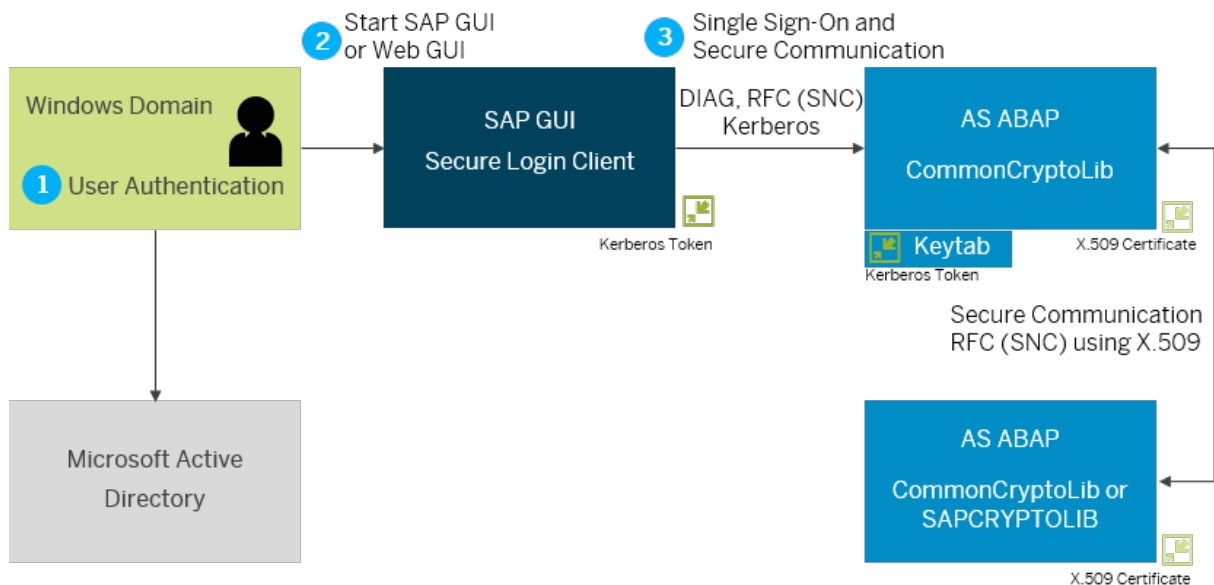
This setup is also possible if the SAP Cryptographic Library or SAPCRYPTOLIB is installed on AS ABAP system TWO.

- The following SAP Single Sign-On components are installed in the environment shown in the following table.

Systems	Software Components
Microsoft Windows client	Secure Login Client
AS ABAP system ONE	SAP Cryptographic Library (SNC library)
AS ABAP system TWO	SAP Cryptographic Library or SAPCRYPTOLIB (SNC library)

#### Context

We assume that there is a Microsoft domain account who requests authentication at a Secure Login Client. The Secure Login Client issues a Kerberos service token and authenticates at AS ABAP system ONE with SNC. The server-to-server communication uses X.509 certificates.



## Procedure

1. In Microsoft Active Directory, create a service account that can be used by AS ABAP. Specify a Service Principal Name for this user. (See options 1 and 2).
2. Use *Edit Profiles* (transaction *RZ10* on AS ABAP systems (ONE and TWO) to configure the SNC parameters in the default profile.
3. On AS ABAP system ONE, use the service account of the Microsoft Active Directory, create a Kerberos keytab file in the SAP Cryptographic Library as described in [SNC Kerberos Configuration \[page 27\]](#).
4. On AS ABAP system ONE, generate X.509 certificates in the *Trust Manager* (transaction *STRUST*).
  - Option 1
  - a. Create an X.509 certificate for AS ABAP.

### ❖ Example

**CN=SAPServiceABC, OU=SAP Security, C=DE**

- b. Start *Edit Profiles* (transaction *RZ10*).
- c. Choose an default profile.
- d. Choose *Extended Maintenance* and then the *Change* pushbutton.
- e. Under *snc/identities/as*, enter **CN=SAPServiceABC, OU=SAP Security, C=DE**.

Secure Login Client converts the SNC name for use by Kerberos. If SAP GUI receives the SNC name `p:CN=SAPServiceABC, OU=SAP Security, C=DE`, the Secure Login Client rebuilds the service account SPN, for example, to `CN=SAP/SAPServiceABC@DOMAIN.LOCAL`. This happens if the Secure Login Client uses a Kerberos profile, and SAP GUI has no Kerberos name.

- Option 2
- a. Create an X.509 certificate for AS ABAP.

#### ❖ Example

**CN=SAPServiceABC@DOMAIN.LOCAL**

Unlike some PKI vendors, Secure Login Server can generate a certificate with special characters, for example (@) at sign.

5. On AS ABAP system TWO, generate X.509 certificate in *Trust Manager* (transaction *STRUST*).  
If you use self-signed certificates, import them from AS ABAP system ONE.
6. Restart AS ABAP systems ONE and TWO.
7. Configure SNC user mapping in *User Maintenance* (transaction *SU01*) on AS ABAP system ONE.
8. Depending on the communication direction, configure secure network communication (SNC) in *Configuration of RFC Connections* (transaction *SM59*) on AS ABAP systems ONE and TWO.

## Related Information

[Installing Additional Features for Secure Login \[page 231\]](#)

[http://help.sap.com/saphelp\\_nw73ehp1/helpdata/en/49/236897bf5a1902e10000000a42189c/frameset.htm](http://help.sap.com/saphelp_nw73ehp1/helpdata/en/49/236897bf5a1902e10000000a42189c/frameset.htm)

[http://help.sap.com/saphelp\\_nw73ehp1/helpdata/en/4c/5bdb17f85640f1e10000000a42189c/frameset.htm](http://help.sap.com/saphelp_nw73ehp1/helpdata/en/4c/5bdb17f85640f1e10000000a42189c/frameset.htm)

[http://help.sap.com/saphelp\\_nw73ehp1/helpdata/en/7e/6ca46b1ee4468a98280ff00db4d97d/frameset.htm](http://help.sap.com/saphelp_nw73ehp1/helpdata/en/7e/6ca46b1ee4468a98280ff00db4d97d/frameset.htm)

## 4.11 Kerberos Authentication for HTML-Based User Interfaces Using AS ABAP with SPNego

Kerberos authentication on SAP Netweaver Application Server (SAP NetWeaver AS) ABAP with a web client requires Simple and Protected GSS API Negotiation Mechanism (SPNego) for AS ABAP.

Many company employees who use Microsoft Windows operating systems and SAP business applications for their daily work want to have Single Sign-On for their employees. The employees use PCs in a Microsoft Windows environment. They log on, for example to a Microsoft Windows operating system, which gets the respective Windows accounts, for example from the domain controller of Active Directory. Kerberos is the authentication method used. The Kerberos key distribution center, which is integrated in the Microsoft environment, grants a Kerberos ticket to the account users who log on.

When a user tries to access the Application Server ABAP with a web browser (using HTTPS), the AS ABAP requests a Kerberos service ticket from the browser. The browser forwards this request to Active Directory. The Kerberos key distribution center in the domain controller of Active Directory grants a Kerberos service ticket for the AS ABAP and the user can log on using his or her browser.

## Related Information

[Workflow with Kerberos Token without Secure Login Server \[page 21\]](#)

### 4.11.1 System Landscape for Kerberos Authentication on AS ABAP

Kerberos authentication requires several systems in your landscape, which negotiate the outcome transparently for the user.

#### ⚠ Caution

SPNego does not provide transport layer security. We recommend that you use transport layer security mechanisms, such as Secure Sockets Layer (SSL) / Transport Layer Security (TLS), to ensure confidentiality and integrity of the communication with AS ABAP.

Component Required for SPNego on AS ABAP

Component	Description
Web client	The web client requests a service or a resource from AS ABAP and authenticates against the Kerberos Key Distribution Center. For example, users use a web browser as a web client to access web applications running on AS ABAP. The web client of the user must support SPNego.
Kerberos Key Distribution Center (KDC)	AS ABAP uses the single sign-on authentication mechanism, integrated, for example, into Microsoft Windows 2003 and higher. The Microsoft Windows Domain Controller (DC) acts as a KDC, enabling Microsoft Windows integrated authentication in a Microsoft Windows domain, which includes, among others, support for Simple and Protected GSSAPI Negotiation Mechanism (SPNego). It authenticates the user and grants a token that is used for the communication between the user's web client and AS ABAP.
AS ABAP	For the supported releases of AS ABAP, see SAP Note <a href="#">1798979</a> . For further information, see also SAP Note <a href="#">1819808</a> .
<b>i Note</b> Secure Network Communication (SNC) must be activated.	
SAP Cryptographic Library	You have licenses for SAP Single Sign-On (see SAP Note <a href="#">1848999</a> ) and you use the default SAP Cryptographic Library on the host AS ABAP. For more information, see the related link.

## Related Information

<https://support.sap.com/pam> 

[Installing Additional Features for Secure Login \[page 231\]](#)

[SAP Cryptographic Library for Secure Login \[page 232\]](#)

### 4.11.2 Setting the AS ABAP Profile Parameters


To enable authentication with SPNego for ABAP you must set profile parameters in the Application Server ABAP.

#### Procedure

1. Start SAP GUI or SAP GUI for HTML.
2. Start [Edit Profiles](#) (transaction RZ10).
3. Choose default profile.
4. Select [Extended maintenance](#).
5. To edit or add profile parameters, choose the [Change](#) button.
6. Set the following profile parameters as required.

Profile Parameters for SPNego

Parameter	Setting
<a href="#">spnego/enable</a>	Set to <b>1</b> .
<a href="#">spnego/krbspnego_lib</a>	Set to the path to the Kerberos library (SAP Cryptographic Library).
Kerberos Library File Names	
File Name	Operating System
sapcrypto.dll	Microsoft Windows
libsapcrypto.so	UNIX platforms
libsapcrypto.sl	HP-UX on PA-RISC only

Parameter	Setting
<a href="#">spnego/construct_SNC_name</a>	<p>If you use a Kerberos-based SNC product that is not SAP Single Sign-On, use this parameter to determine the format for the translation of Kerberos user name to SNC name. Default value is <b>111</b>.</p> <p>For more information, see <a href="#">1819808</a> .</p> <div> <p><b>Note</b></p> <p>Changing this dynamic profile parameter does not require a restart.</p> </div>

7. Save and activate your entries.
8. Restart AS ABAP.
9. Start *SPNego Configuration* (transaction *SPNEGO*).  
If the transaction starts without error message, then you have set up the SPNego library correctly and you know the kernel supports SPNego.

### 4.11.3 Configuring a Service Account

The Simple and Protected GSS-API Negotiation Mechanism (SPNego) configuration enables you to maintain and derive new symmetric keys with a Kerberos service account and password.

#### Context

Find the exact steps in the Microsoft documentation.

#### Procedure

1. Create a service account on the Windows domain controller.

##### → Tip

We recommend the format **Kerberos<SID>**. You can use the same service account as for SNC.

You can also use another service account. We recommend that you do not use **SAPService<SID>** because the *Password Never Expires* option is not set for this account by default. If the password for this account expires, single sign-on fails.

#### ❖ Example

**KerberosAB1.**

2. Enable the *Password Never Expires* option for this account.
3. Register the Service Principal Names (SPNs) for the service account for the host name of the AS ABAP and all AS ABAP aliases. Thus you associate the AS ABAP aliases **hades.customer.de** and **su3x24.customer.de** with the AS ABAP service account on the Microsoft Windows Domain Controller. Ensure that all SPNs are unique. You can either register the Service Principal Names by means of the Active Directory (see the related links) or you use the `setspn` command as in the following example:

#### ❖ Example

```
setspn -A HTTP/hades.customer.de IT.CUSTOMER.DE\KerberosAB1  
setspn -A HTTP/su3x24.customer.de IT.CUSTOMER.DE\KerberosAB1
```

4. To check the association between the AS ABAP service account and service principal name, use one of the following commands:
  - To easily find out in the client which service account is assigned to which service principal name, use the following command in the domain of the service account:

#### ❖ Example

```
setspn -L KerberosAB1
```

- To check the result of the configuration on the side of the Service Principal Name, enter the following command at the command line for each SPN you registered, for example:

#### ❖ Example

```
ldifde -r serviceprincipalname=HTTP/hades.customer.de -f out.ldf
```

## Related Information

[Registering Service Principal Names for a Kerberos Service Account in Active Directory \[page 77\]](#)

[Define Service Principal Name \[page 28\]](#)

### 4.11.3.1 Registering Service Principal Names for a Kerberos Service Account in Active Directory

You need to register the Service Principal Names in Active Directory for the host names of the Application Server ABAP and all AS ABAP aliases.

#### Context

The Service Principal Names identify, for example, dialog instances or servers of the AS ABAP. To make Kerberos authentication with SPNego possible, you have a unique assignment from a Service Principal Name to a Kerberos service account in the *SPNego Configuration* (transaction *SPNEGO*). In Active Directory, however, you can register several Service Principal Names for one Kerberos service account.

To register Service Principal Names for a Kerberos Principal Name, perform the following steps:

#### Procedure

1. Start *Active Directory Users and Computers*.
2. Go to your domain controller.
3. To enable the attribute editor, choose *View* and select *Advanced Features*.
4. Choose *Users* and select your Kerberos service account, for example **Kerberos<SID>**.
5. Right-click the Kerberos service account and select *Properties*.
6. Choose the *Attribute Editor* tab.
7. Select the attribute *servicePrincipalName*.
8. Choose the *Edit* button.
9. To add your Service Principal Names, enter the respective names and choose *Add*.
10. To make your changes permanent, choose *OK* and *Apply*.

### 4.11.3.2 Creating Kerberos Keytab Files on the Microsoft Windows Domain Controller

The keytab for Kerberos-based SNC and SPNego establishes trust between the Key Distribution Center and AS ABAP.

#### Procedure

Create a keytab for Kerberos-based SNC and SPNego on your Microsoft Windows Domain Controller using Active Directory means.



Find the exact steps in the Microsoft documentation.

## 4.11.4 Creating a keytab

Using a keytab file, you can add the Kerberos service account of the Key Distribution Center to configure trust for SAP NetWeaver AS ABAP.

### Context

#### Note

After having performed this procedure, you do not need to restart the application server if the keytab was updated or configured for the first time. Wait two minutes for all instances to synchronize.


### Procedure

1. Start SAP GUI or SAP GUI for HTML.
2. Start *SPNego Configuration* (*SPNEGO* transaction).
3. Switch to Edit mode.
4. Confirm the license disclaimer.

SAP NetWeaver AS ABAP only supports SPNego with a valid license for SAP Single Sign-On 2.0 or higher.

5. Add the Kerberos service account manually or from a keytab file.

Enter the Kerberos service account manually if you know the password of the service user. Otherwise import the keytab file.

- Create a keytab for Kerberos-based SNC and SPNego by adding a Kerberos service account manually. Choose  (*Add*) and enter the Kerberos Principal name and password. Save your changes.

#### Note

The Kerberos service account is case-sensitive, but the Microsoft Windows domain is always in uppercase. Use the following format for the Kerberos principal:

<sAMAccountName>@<WINDOWS-2000-DOMAIN-UPPERCASE>

#### Example

AD\_KerbAdminABC@IT.CUSTOMER.COM

- To import a keytab file, choose  (*Import keytab file*). Save your changes.

### **i** Note

Keep in mind that you must have enabled SNC and maintained the user's SNC Name in the [SU01](#) transaction. For more information, see the related link.

6. If you have not already done so, perform a user mapping on the [SNC](#) tab of [User Maintenance](#) (transaction [SU01](#)).
7. Save your entries.

## Results

After you have configured the Key Distribution Center and the trust configuration, your users can log on to Microsoft Windows and authenticate at the AS ABAP if SAP Single Sign-On is already used for SNC-based authentication.

The token contains the Kerberos User Principal Name (UPN), which does not match the ABAP user name. The UPN from the Active Directory has the following format:

Format: `<AD_user_name>@<REALM>`

Example: `Smith@IT.CUSTOMER.DE`

During SPNego authentication, the token received from the Key Distribution Center is transferred by the way of the user's web client to the AS ABAP. This token contains the Kerberos UPN, which consists of two parts: a user name part and a domain part, separated by the at-sign (@) (for example `Smith@IT.CUSTOMER.DE`). To authenticate the user with such a token, the UPN must be mapped to an existing ABAP user. SPNego re-uses the existing SNC mapping string that can be configured in transaction `SU01`.

You can use arbitrary Kerberos-based SNC products in combination with SPNego. Unfortunately, the various SNC products differ in how they construct an SNC name for a given Kerberos User Name. This requires a configuration option to control prefixing and uppercase or lowercase conversion of the user name and domain parts. This is controlled by profile parameter `spnego/construct_snc_name`. (See SAP Note [1819808](#) - SPNego: Collective Corrections.)

## Related Information

[Creating Kerberos Keytab Files on the Microsoft Windows Domain Controller \[page 77\]](#)

[SNC Parameters for the SAP Cryptographic Library \[page 314\]](#)

[Profile Parameters for SPNego \[page 317\]](#)

## 4.11.5 Troubleshooting SPNego on AS ABAP

To analyze SPNego authentication failures, use the SPNego tracing function.

### Procedure

1. Start *SPNego Configuration* (transaction *SPNEGO*).
2. Choose **► Goto ► SPNego Tracing ►**.

### Related Information

[SAP Note 1732610](#) 

[SAP Note 1819808](#) 

## 4.12 Configuring Secure Login Web Client Connections to SAP GUI

You can use the Secure Login Web Client to launch an SAP GUI connection using a configuration that, for example, does not use a local `saplogon.ini` configuration file.

### Context

Configure the way you want your Secure Login Web Client to start an SAP GUI. You do so by defining the post authentication actions of the Secure Login Web Client and the relevant parameters. Only one connection action is possible per Secure Login Web Client profile.

### Procedure

1. Start the Secure Login Administration Console.
2. Choose the relevant authentication profile.
3. Select the *Secure Login Web Client Settings* tab.
4. Using the *Post Authentication Actions* section, choose the action you want to use.

As an option for the connection types for direct connection, load balanced connection, and SAP logon pad, you can also define that the Secure Login Web Client redirects to a given URL after successful authentication.

Several types of connections to SAP GUI are available. For more information, see the related links.

- Simple redirect to URL
  - Direct connection with Secure Login Web Client (Redirect to URL option also available)
  - Load-balanced SAP GUI connection using the message server (Redirect to URL option also available)
  - Launching your SAP logon pad directly (Redirect to URL option also available)
5. Save your configuration.
  6. Expand the tray [Web Client URL](#). The [URL](#) field contains the URL you use to start the Secure Login Web Client. The authentication profile generates the web client URL automatically.
  7. Select the web client URL and copy it to your clipboard.
  8. Start the Secure Login Web Client.

The start of the Secure Login Web Client is profile-dependent. The GUID identifies your authentication profile. To start the Secure Login Web Client, use the URL you copied to your clipboard. It already contains the profile (GUID), which is the last element of the URL.

```
https://<host_name>:<ssl_port>/SecureLoginServer/webclient/webclient.html?
profile=<GUID>
```

Example:

```
https://nwssoexample.dhcp.wdf.abc.corp:50201/SecureLoginServer/webclient/
webclient.html?profile=cd468f6c-ff00-f479-8021-9d811040556e
```

## Related Information

[Connection with Redirect to URL \[page 81\]](#)

[Direct SAP GUI Connection with Secure Login Web Client \[page 82\]](#)

[Load-Balanced SAP GUI Connection with Secure Login Web Client \(Using the Message Server\) \[page 83\]](#)

[Launch SAP Logon Pad \[page 85\]](#)

### 4.12.1 Connection with Redirect to URL

Enter a URL for certificate-based login. After successful user authentication, this URL is called.

You can use this URL to configure a location where SSL client-based authentication with the enrolled X.509 certificate is required, for example, in the SAP Enterprise Portal.

Choose the action [Redirect to URL](#) and enter the relevant URL in the mandatory field.

## Post Authentication Actions

Action	Parameters
* <a href="#">Redirect to URL</a>	Enter the URL to which the Secure Login Web Client is redirected after successful authentication, for example, to an enterprise portal.

## 4.12.2 Direct SAP GUI Connection with Secure Login Web Client

A direct connection to an SAP GUI (ABAP) under Microsoft Windows uses the SAP GUI description to address the ABAP server.

You can combine a connection action with a URL redirect, which allows you to leave the Secure Login Web Client page after successful authentication.

## Post Authentication Actions

Actions	Parameters	Connection String
<a href="#">Log On to ABAP System</a>	<ul style="list-style-type: none"> <li>* <a href="#">IP Address/Host Name</a></li> </ul> <p>IP address or fully qualified host name of the ABAP System. (We recommend that you use host names). SAP GUI starts with the connection string <code>/H/&lt;host&gt;</code>.</p>	<code>/H/&lt;host&gt;</code>
	<ul style="list-style-type: none"> <li>* <a href="#">Port</a></li> </ul> <p>Port of ABAP server: Default is 3200. SAP GUI starts with the connection string <code>/S/&lt;port&gt;</code>.</p>	<code>/S/&lt;port&gt;</code>
	<ul style="list-style-type: none"> <li>* <a href="#">SNC Name</a></li> </ul> <p>SNC name of ABAP server. SAP GUI starts with SNC_PARTNERNAME</p> <div> <p>❖ Example</p> <p><b>p:CN=ABAP System</b></p> </div>	<code>SNC_PARTNERNAME=&lt;SNC_name&gt;</code>
<a href="#">Redirect to URL and Log On to ABAP System</a>	<ul style="list-style-type: none"> <li>* <a href="#">Redirect to URL</a></li> </ul> <p>Enter the URL to which the Secure Login Web Client is redirected after successful authentication, for example, to an enterprise portal.</p>	

Actions	Parameters	Connection String
Optional Parameters		
	<p><i>SAP GUI Description</i></p> <p>Name of the server profile in SAP GUI for Microsoft Windows (<i>Description</i> field in SAP GUI). If you are using SAP GUI for Microsoft Windows, you need to enter the SAP GUI description to enable direct logon to an ABAP system. This means that you need the <code>&lt;saplogon.ini&gt;</code> file with the respective entry.</p>	

### 4.12.3 Load-Balanced SAP GUI Connection with Secure Login Web Client (Using the Message Server)

You can use the Secure Login Web Client to launch a load-balanced SAP GUI connection using a configuration that, for example, does not use a local `saplogon.ini` configuration file.

Moreover, you profit from the load balancing function of the message server.

#### ❖ Example

If you want to have a load-balanced connection using the message server, start the Secure Login Web Client with the following connection string:

```
/M/<host_name>/S/<service>/G/<group>
```

You can also configure the Secure Login Web Client to redirect to a given URL after successful authentication.

To configure the post authentication actions, go to your authentication profile.

Post Authentication Actions

Actions	Parameters	Connection String
<i>Log On to ABAP Message Server</i>	<ul style="list-style-type: none"> <li><i>Message Server</i></li> </ul> <p>IP address or fully qualified host name of the ABAP Message Server. SAP GUI starts with an <code>/M/host</code> connection string.</p>	<code>/M/&lt;host&gt;</code>
	<ul style="list-style-type: none"> <li><i>* Message Server Service</i></li> </ul> <p>The service (port) that identifies this service.</p>	<code>/S/&lt;port&gt;</code>

Actions	Parameters	Connection String
	<p><i>* Group</i></p> <p>The ABAP group. SAP GUI starts with a /G/&lt;group&gt; connection string.</p>	/G/<group>
<p><i>Redirect to URL and Log On to ABAP Message Server</i></p>	<p><i>* Redirect to URL</i></p> <p>Enter the URL the Secure Login Web Client is redirected to after successful authentication, for example, to an enterprise portal.</p>	
Optional Parameters		
<p><i>SAP GUI Description</i></p> <div> <p><b>! Restriction</b></p> <p>This parameter is only relevant for SAP GUI (ABAP) for Microsoft Windows. SAP GUI for Java ignores this field. We recommend that you leave this field empty.</p> </div> <p>Name of the server profile in SAP GUI for Microsoft Windows (<i>Description</i> field in SAP GUI). If you are using SAP GUI for Microsoft Windows, you need to enter the SAP GUI description to enable direct logon to an ABAP system. This means that you need the &lt;saplogon.ini&gt; file with the respective entry.</p>		
	<p><i>Gateway Host</i></p> <p>Specifies the SAP router for the connection to the ABAP server. SAP GUI starts with an /H/&lt;host&gt; connection string.</p>	/H/<host>
	<p><i>Gateway Port</i></p> <p>Specifies the port of the SAP router. SAP GUI starts with an /S/&lt;port&gt; connection string.</p>	/S/<port>

## 4.12.4 Launch SAP Logon Pad

You can also launch a direct connection with your SAP Logon Pad by configuring the following post-authentication actions.

You can also configure that the Secure Login Web Client redirects to a given URL after successful authentication.

Post Authentication Actions

Action	Parameter
<a href="#">Launch SAP Logon Pad</a>	
<a href="#">Redirect to URL and Launch SAP Logon Pad</a>	<p><i>* Redirect to URL</i></p> <p>Enter the URL to which the Secure Login Web Client is redirected after successful authentication, for example, to an enterprise portal.</p>

## 4.13 Using Secure Login Client in Web Adapter Mode

The key management of Secure Login Client in Web Adapter mode is highly secure.

Web Adapter mode ensures a high security level because it enables the Secure Login Client to manage private keys for Secure Login Web Client. However, the client system does not store the keys persistently, but they are temporarily stored in a secure way in the memory of the clients. The SNC and key management libraries are not downloaded. When the Secure Login Client user has restarted or logged out, the Secure Login Client removes all Single Sign-On keys. Web Adapter mode also enables you to use a logout function in the Secure Login Client.

### Prerequisites

- You have installed Secure Login Client with Secure Login Server Support.

If you configured a Secure Login Web Client profile in the Secure Login Administration Console, you can, after the enrollment, choose a Secure Login Web Client profile, which you can use for SNC in the Secure Login Client. This profile is not persistent. It is only available after an enrollment and for the client session.

### Related Information

[Secure Login Client Installation \[page 132\]](#)



## 4.13.1 Configuring Web Adapter Mode for Secure Login Client

### Procedure

1. Open the Secure Login Administration Console.
2. Choose the relevant client authentication profile.
3. Go to [Secure Login Web Client Settings](#).
4. Expand the [Client Behavior](#) section.
5. Choose Edit.
6. Activate [Web Adapter Mode \(requires Secure Login Client installation\)](#).

Web Adapter mode is immediately active after changing the configuration for the next web client enrollment on this profile.

## 4.14 Using Secure Login Server for SAML 2.0 Authentication

You want to enable web-based clients to use authentication provided by an identity provider using Security Assertion Markup Language (SAML) 2.0.

SAML 2.0 requires an identity provider that is a separate resource for users and identities, and provides authentication. It can be configured in the SAP NetWeaver Administrator. An identity provider provides authentication for a number of trusted service providers.

In this scenario, mutual trust must exist between the identity provider and the host of the Secure Login Server. Secure Login Server is considered by the identity provider to be one of its service providers.

For more information about SAML 2.0, see the relevant SAP NetWeaver release in the SAP Help Portal under [► Application Help ► SAP NetWeaver Library: Function-Oriented View ► Security ► User Authentication and Single Sign-On ► Authentication Concepts ► Authentication for Web-Based Access ► SAML 2.0 ►](#)

### Prerequisites

- You have configured a policy configuration for SAML 2.0 with a SAML 2.0 login module (for example, [SAML2LoginModule](#) in the SAP NetWeaver Administrator).
- You have set up an identity provider with the host of the Secure Login Server as a trusted service provider (see the related link).

## Authentication Scenario with Secure Login Server

A user submits an authentication request to the Secure Login Server in the Secure Login Web Client URL. The browser redirects the request to the identity provider, which manages the users, credentials, and identities for multiple systems. The identity provider responds to the request by executing an initial authentication using a SAML 2.0 artifact with the user's credentials and redirects it to the Secure Login Server. The Secure Login Server issues a certificate, which enables the users to authenticate, for example, on an SAP GUI.

### Related Information

[Configuring the Identity Provider for SAP Single Sign-On and SAP Identity Management implementation guide](#)

## 4.14.1 Configuring SAML 2.0 Authentication in the Secure Login Server

To enable SAML 2.0 authentication with Secure Login Server, you must create an authentication profile for SAML 2.0 that points to a special policy configuration containing an SAML 2.0 login module. In particular, you must configure the authentication profile to use the standard SAP NetWeaver login screen.

### Context

Secure Login Server enables SAML 2.0 authentication of web-based clients. A separate authentication profile for Secure Login Web Client points to a policy configuration in the SAP NetWeaver Administrator that uses the inbuilt SAML 2.0 login module. This authentication profile is configured to use the standard SAP NetWeaver logon screen. It points to a policy configuration in the SAP NetWeaver Administrator, which uses an inbuilt SAML 2.0 login module. The authentication profile tells the Secure Login Web Client to log on to the identity provider using the logon screen of AS ABAP.

### Procedure

1. To create an authentication profile for SAML 2.0, open the Secure Login Administration Console.
2. Go to the [Authentication Profiles](#) section of the [Profile Management](#) tab.
3. Choose [Create](#).
4. Enter a name and a description for the SAML 2.0 authentication profile.
5. Choose [Secure Login Web Client Profile](#) in the [Client Type](#) field.
6. It is mandatory that you select [Standard Authentication Form](#) in the [User Authentication](#) section. This ensures that you use the identity provider as a resource for authentication. The identity provider uses the SAP NetWeaver logon screen.

7. Choose [Use Policy Configuration](#) and select the SAML 2.0 policy configuration (containing the SAML 2.0 login module) that you configured earlier in the SAP NetWeaver Administrator.
8. Choose [Next](#) and enter the data of the user certificate that the Secure Login Server is supposed to issue.
9. Choose [Next](#), specify the post-authentication action, and choose [Finish](#) to complete the configuration.
10. You can proceed to the [Web Client URL](#) section of the [Secure Login Web Client Settings](#) tab and distribute the Secure Login Web Client URL to the clients for SAML 2.0-based authentication.  
You have now created a authentication profile for the Secure Login Web Client that enables users to authenticate with SAML 2.0. For more information about the parameters, see the related link.

## Related Information

[Parameters for User Authentication in the Authentication Profile \[page 295\]](#)

## 4.15 Certificate Lifecycle Management in the AS ABAP Using Secure Login Server

You want to automatically renew long-lived X.509 certificates, which are stored in the trust manager of Application Server ABAP. Usually, administrators renew certificates individually, for example for a set of systems in your system landscape. Using Secure Login Server, administrators are able to manage the certificates of the development systems, quality systems, and/or production systems separately.

Using certificate lifecycle management, you can schedule a certificate renewal automatically in AS ABAP. This means that you can automatically renew any protocol-specific or application-specific PSE certificates, like SSL server or client, and SNC SAPCryptolib in regular intervals without any manual interaction. A background job in the AS ABAP monitors the certificates, detects the expired ones, and requests their renewal.

It is easy to manage the lifecycle of application server PSEs, and you can align key and certificate lifetimes to state-of-the-art cryptographic recommendations, regulations, and compliance standards.

## Implementation

Secure Login Server provides certificate lifecycle management, a function that enables you to directly renew certificates (in PSEs). You configure application server profile groups, for example for the development systems, quality systems, or production systems. Each application server profile group contains profiles of the type "application server profile". Assign these profile groups to the system IDs (SIDs), for example of your development systems.

An application server profile group like this requires a "registration agent" profile for the initial enrollment certificate for the administrator's logon with credentials. It also contains application type specific profiles, for example the SNC PSE, PSEs of the SSL Server PSE type. It also includes all trusted TLS root certificates that are required to run secured communication with Secure Login Server.

As an administrator, you can trigger a renewal of the relevant certificates per PSE type (for example, for all SSL Server PSEs) by running the reports `SSF_CERT_ENROLL` (gets a certificate for the "registration agent") and `SSF_CERT_RENEW` (renews or generates the certificates) in the AS ABAP.

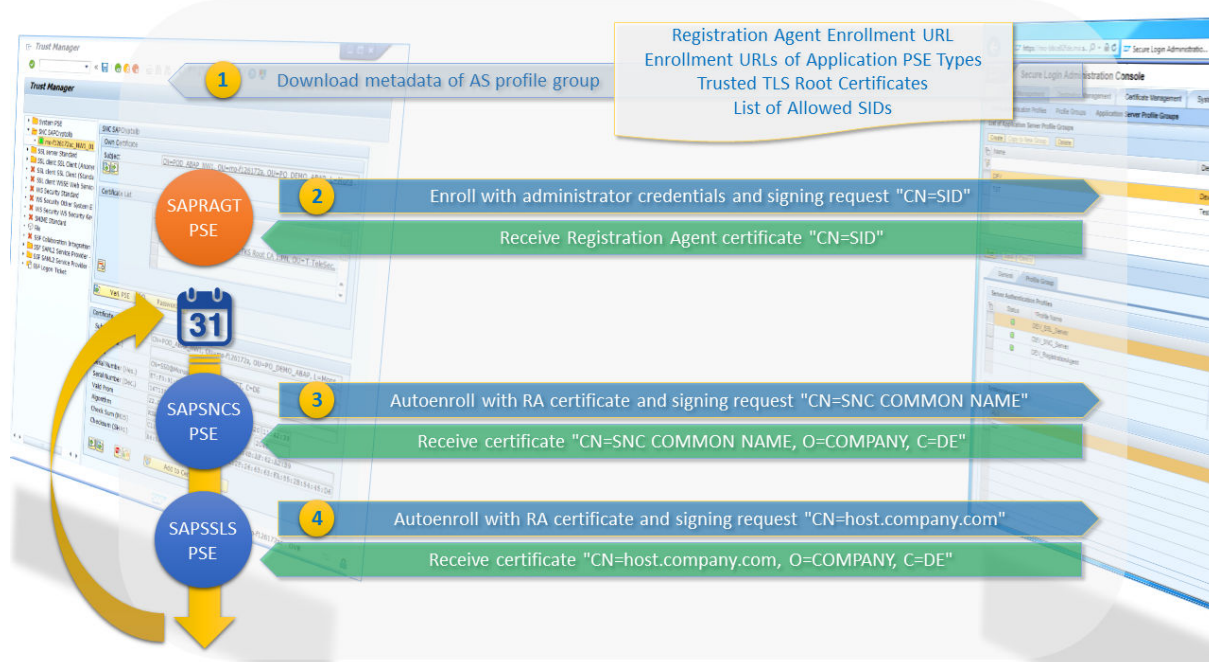
For more information, see SAP Note [2260733](#) and [2316487](#).

## 4.15.1 PSE Infrastructure Involved in Certificate Renewal Using Secure Login Server

Application Server ABAP centrally stores the PSEs in the trust manager. For example, to renew the SNC PSE and the PSEs of the SSL Server PSE type, AS ABAP needs to enroll in the application server profiles on Secure Login Server (using the report `SSF_CERT_ENROLL`). For the renewal of the certificates, the AS ABAP gets the relevant renewal data from the metadata URL of the application server profile group (provided on Secure Login Server).

The report `SSF_CERT_ENROLL` enrolls for a "registration agent" certificate and writes it into the PSE list of the trust manager. This certificate is used to enroll for the authentication profiles of the Secure Login Server. This report also contains the list of profiles with the PSE types you want to renew or generate.

The application server profile group includes authentication profiles for every PSE type. When the AS ABAP requests a certificate renewal using the report `SSF_CERT_RENEW`, it gets the updated certificate data from the relevant application server profile of the Secure Login Server.



#### PSEs Involved in the Process of Renewing Long-Lived X.509 Certificates

PSE-Related Action (of AS ABAP Trust Manager Client)	PSE File Involved (Trust Manager) PSE Type	Action in Secure Login Server
AS ABAP initially enrolls with administrator credentials and signing request	SAPRAGT . PSE	Issues registration agent certificate with CN=<SID>
Auto-enrolls with RA certificate on SLS	SAPSNCS . PSE (SNC PSE type)	Sends (renews) certificate in SNC PSE(s) with CN=SNC COMMON NAME, O=COMPANY, C=DE
Auto-enrolls with RA certificate on SLS	SAPSSLS . PSE (SSL Server PSE type)	Sends (renews) certificate in SSL PSE(s) with CN=host.company.com, O=COMPANY, C=DE
Auto-enrolls with RA certificate on SLS	Any other PSEs	Sends (renews) certificate in any other PSE(s) with CN=subject, O=SUBJECT, C=DE

## 4.15.2 Prerequisites for Certificate Renewal Using Secure Login Server

If you want to automatically renew long-lived X.509 certificates with Secure Login Server means, you must fulfill a number of prerequisites.

- You have installed SAP Single Sign 2.0 SP06 or higher with Secure Login Server.
- You are using SAP NetWeaver 7.31 SP 17, 7.4 SP13 or 7.5 SP00 higher.

## 4.15.3 Configuring Certificate Lifecycle Management in the AS ABAP Using Secure Login Server

If you want to automatically renew long-lived X.509 certificates with Secure Login Server means using certificate lifecycle management, you must configure Secure Login Server and use reports in the Application Server ABAP.

### Procedure

On the Secure Login Server

Create new application server profiles and configure application server profile groups with the corresponding application server profiles on Secure Login Server. It makes sense to use an application server profile group for

a set of SAP systems, for example, for your development systems. The report `SSF_CERT_ENROLL` retrieves the content of the application server group in the metadata URL.

### 4.15.3.1 Configuring Secure Login Server for Certificate Lifecycle Management

To enable certificate renewal, an administrator must configure application server profiles and application server profile groups in the Secure Login Server.

#### 4.15.3.1.1 Configuring an Application Server Authentication Profile of the Profile Type "Registration Agent"

You want to renew certificates of a group of SAP systems (AS ABAP), for example, all development systems of your landscape.

#### Context

In Secure Login Administration Console, you can configure an application server profile group that covers all system IDs of your development systems.

#### Procedure

1. In Secure Login Administration Console, you can configure an application server profile group that covers all system IDs of your development systems.
2. Go to the [Authentication Profiles](#) section of the [Profile Management](#) tab.
3. Choose [Create](#) to open the wizard that helps you to create a new authentication profile.
4. Enter the authentication profile name. It makes sense to choose a meaningful name that reveals the purpose of the authentication profile. It could be a good idea to include, for example, the PSE type, for which you want to renew the certificates.
5. Choose [Application Server Profile](#) in [Client Type](#).
6. Go to the [Authentication Configuration](#) field and choose a policy configuration for the authentication step.
7. Choose [Next](#) to configure the properties of the user certificates.
8. Make sure that you selected the correct CA in the field [CA for Issuing Certificates](#).
9. Choose [Next](#) to go to the enrollment configuration. The enrollment URL is automatically provided by Secure Login Server.

### **i** Note

The enrollment port configured in the SSL configuration of the SAP NetWeaver Administrator must have the type *Request* in the *Client Authentication Mode* column.

10. Choose the profile type *Registration Agent*. The *Certificate Template* field has the fixed value *SSL Client Template* (see the related link), which appears in the metadata information.
11. Choose *Finish* to complete the configuration.

## **Related Information**

[Using Certificate Templates \[page 221\]](#)

### **4.15.3.1.2 Configuring an Application Server Authentication Profile of the Profile Type "Application"**

You want to renew certificates of a group of SAP systems (AS ABAP), for example, all development systems of your landscape.

## **Context**

In Secure Login Administration Console, you can configure an application server profile group that covers all the system IDs of your development systems. This application server group contains the application server authentication profiles of the required certificate types you plan to renew.

## **Procedure**

1. Open Secure Login Administration Console to configure Secure Login Server.
2. Go to the *Authentication Profiles* section of the *Profile Management* tab.
3. Choose *Create* to open the wizard that helps you to create a new authentication profile.
4. Enter the authentication profile name. It makes sense to choose a meaningful name that reveals the purpose of the authentication profile. It could be a good idea to include, for example, the PSE type for which you want to renew the certificates.
5. Choose *Application Server Profile* in *Client Type*.
6. Go to the *User Authentication* field and make sure that you use a policy configuration that contains a certificate-based login module.
7. Choose *Next* to configure the properties of the user certificates.
8. Make sure that you selected the correct CA in the field *CA for Issuing Certificates*.

9. Choose [Next](#) to go to the enrollment configuration. The enrollment URL is automatically provided by Secure Login Server.

#### **i Note**

The enrollment port configured in the SSL configuration of the SAP NetWeaver Administrator must have the type [Required](#) in the [Client Authentication Mode](#) column.

10. Choose the profile type [Application](#).
11. Choose the suitable certificate template for the relevant PSEs. For example, [SSL SERVER Template](#) refers to the certificate of the SSL Server PSEs. For more information, see the related link.
12. Choose [Finish](#) to complete the configuration.

#### **i Note**

(Optional) If you want to renew certificates of other PSE types, create further application server authentication profiles by repeating this procedure accordingly.

13. Include the application server profiles into an application server profile group (see the related link).

## **Related Information**

[Setting Up an Application Server Profile Group for Multiple Application Servers for ABAP/SAP Systems \(ABAP\)](#)  
[\[page 93\]](#)

[Using Certificate Templates](#) [\[page 221\]](#)

### **4.15.3.1.3 Setting Up an Application Server Profile Group for Multiple Application Servers for ABAP/SAP Systems (ABAP)**

You want to renew certificates of a group of SAP systems (AS ABAP), for example, all development systems of your landscape.

## **Context**

In Secure Login Administration Console, you can configure an application server profile group that covers all the system IDs of your development systems. This application server profile group contains the application server authentication profiles for the PSE types of the certificates you plan to renew and a registration agent authentication profile for enrollment on Secure Login Server.



## Procedure

1. Open Secure Login Administration Console to configure.
2. Go to the [Application Server Profile Groups](#) section of the [Profile Management](#) tab.
3. Choose [Create](#).
4. Enter a name for the application server profile group. We recommend that you use a meaningful name that reveals for which group of SAP systems you plan to renew certificates (for example, all development systems).
5. Select the name of your new application server profile group.
6. (If applicable) If the [Sync Trust Anchors](#) button is not grayed out, choose it to synchronize the trust anchors of the SSL configuration in the SAP NetWeaver Administrator. This may happen if the SSL configuration of the AS Java changed. This SSL configuration change needs to be updated in the Secure Login Server. The [Sync Trust Anchors](#) button enables you to synchronize with the changed SSL configuration of the AS Java.
7. Choose [Edit](#).
8. Choose [Add](#) to add the application server profiles you created earlier. Select the down-arrow to see the list of the application server profiles.
9. Select the profiles you want to add.
  - a. Add an application server profile of the type `Registration Agent`.

### **i** Note

It is mandatory to include an application server profile of the type `Registration Agent`. It enables the AS ABAP to enroll on Secure Login Server.

- b. Add, for example, profiles for SNC PSEs and for certificates of SSL server PSEs.
10. Go to the [System Identifiers](#) tray to enter, for example, the system IDs (SIDs) of all your development systems for which you want to renew the certificates.
  11. Save your changes.

## 4.15.4 Preparing a Certificate Renewal at Regular Intervals

You can renew your certificates using Secure Login Server means in the Application Server ABAP using certificate lifecycle management. To do so, use two ABAP reports.

### Context

If you want to automatically renew long-lived X.509 certificates using Secure Login Server means, you must proceed as follows:

### Procedure

1. Start the report `SSF_CERT_ENROLL` once to enroll on Secure Login Server using your administrator credentials and the metadata URL. You are prompted to decide whether you want the AS ABAP to trust the certificate from the Secure Login Server. In some cases, a new PSE is created. After that, the enrollment is complete and is valid from this point onwards. It establishes a trust relationship between the AS ABAP and the Secure Login Server. This is a prerequisite for renewing the certificates using the report `SSF_CERT_RENEW`.

#### i Note

You only need to perform this step once.

2. Set up the report `SSF_CERT_RENEW` to renew your user certificates and/or server certificates for the selected application server profile group, which covers a set of SIDs. It makes sense to schedule a repetitive certificate renewal. Create variants for different PSE types. The variants contain the relevant metadata URL, the number of days until certificate expiration, and the PSE types for which you want to renew the certificates. Use the ABAP job scheduling function (for example, using [Define Job](#), transaction `SM36`) to determine the conditions for the execution of your `SSF_CERT_RENEW` report variants.

For more information, see SAP Note [2452425](#) .


### 4.15.4.1 Defining a Variant for Certificate Renewal

We recommend that you use variants when defining the renewal information for the certificates.

### Context


The variants of the report `SSF_CERT_RENEW` contain the metadata URL of the Secure Login Server, the number of days until the expiration of the current certificates, and the relevant PSE types. Moreover, you define whether you merely want to renew certificates or whether you want to generate a new private key.

## Procedure

1. Open program SSF\_CERT\_RENEW with SE38 transaction.
2. Create a variant for this program using the  **Variants** button.
3. Enter a name for the variant and choose **Create**.
4. Enter the metadata URL from the Secure Login Server in the **SLS Metadata URL** field (see the related link).
5. Define when you want to renew your certificates by entering the number of days until the expiration of your certificates.

### Example

You define 20 days until expiration. Let's assume that the certificates will expire on November 11. The scheduled report will run on October 21 and renew the relevant certificates.

6. Leave the value **All** in the field **PSE Context**.
7. Choose the **Attributes** button and enter a description of the variant.
8. Save your variant.
9. Go back and start your report with the variant you created earlier.
10. Choose  **Execute (F8)** to run the program.

You get a list of all the PSE types configured in the application server profile group of the Secure Login Server. This list is stored in the location the metadata URL points to.

11. By activating the checkboxes in the columns **New Cert** and **New Key**, you determine that you want to renew certificates of a certain PSE type (in the column **PSE Description**).

Column	Description
<b>New Cert</b>	The report renews the certificates.
<b>New Key</b>	The report renews the certificates and generates a new private key.

12. Save your changes.

At this stage, it makes sense to schedule the report SSF\_CERT\_RENEW so that it runs in regular intervals.

## Related Information

[PSE Infrastructure Involved in Certificate Renewal Using Secure Login Server \[page 89\]](#)

## 4.15.4.2 Setting Up a Scheduled Job for Certificate Renewal

You want to schedule the report `SSF_CERT_RENEW` with the information as to which certificates you want to renew.

### Context

Your variants already contain the metadata URL of the Secure Login Server, the relevant PSE types, and the period until the expiration of the current certificates.

### Procedure

1. Start *Define Job* (transaction `SM36`) in the AS ABAP.
2. Enter a job name.
3. Choose the *Step* button.
4. Choose `SSF_CERT_RENEW` in the ABAP Program section.
5. Choose the variant you created earlier.
6. Choose the *Start Condition* button.
7. Define the job as a periodic job that is repeated regularly.
8. Save your scheduled job.

From now on, your scheduled job automatically renews the certificates regularly. You can check your job in the job overview (transaction `SM37`).

## 4.16 Certificate Lifecycle Management in the AS Java Using Secure Login Server

You want to automatically renew long-lived X.509 certificates, which are stored in the Key Storage Service of AS Java, in the SAP NetWeaver Administrator under *Certificates and Keys*. Usually, administrators renew certificates individually, for example for a set of systems in your system landscape. Using Secure Login Server, administrators are able to manage the certificates of the development systems, quality systems, and/or production systems separately.

Using certificate lifecycle management, you can schedule automatic certificate renewal in AS Java. This means that you can automatically renew any protocol-specific or application-specific certificates, like SSL server or client in regular intervals without any manual interaction. A task in the AS Java monitors the certificates, detects the expired ones, and requests their renewal.

It is easy to manage the lifecycle of key storage views of the AS Java, and you can align key and certificate lifetimes to state-of-the-art cryptographic recommendations, regulations, and compliance standards.

## Implementation

Secure Login Server provides certificate lifecycle management, a function that enables you to directly renew certificates (in key storage views). You configure application server profile groups, for example for the development systems, quality systems, or production systems. Each application server profile group contains profiles of the type "application server profile". Assign these profile groups to the system IDs (SIDs), for example of your development systems.

An application server profile group like this requires a "registration agent" profile for the initial enrollment certificate for the administrator's logon with credentials. It also contains application type specific profiles. It also includes all trusted TLS root certificates that are required to run secured communication with Secure Login Server.

As an administrator, you can trigger a renewal of the relevant certificates by enrolling a registration agent (getting a registration certificate) and scheduling a task to renew or generates the certificates in the AS Java.

### 4.16.1 Infrastructure Involved In Certificate Renewal Using Secure Login Server

AS Java centrally stores the key storage views in the Keystore Service of the SAP NetWeaver Administrator. For example, to renew the key storage views of the SSL Server, AS Java needs to enroll in the application server profiles on Secure Login Server. For the renewal of the certificates, the AS Java gets the relevant renewal data from the metadata URL of the application server profile group (provided on Secure Login Server), for example, it contains the list of templates and profiles of the certificates you want to renew or generate.

Using the Secure Login Certificate Lifecycle Management Cockpit, you enroll a "registration agent" to receive a certificate and write it into the key storage view list of the Keystore Service. This certificate is used to enroll for the authentication profiles of the Secure Login Server.

The application server profile group includes authentication profiles for every keystore view. When the AS Java requests a certificate renewal, it gets the updated certificate data from the relevant application server profile of the Secure Login Server.

Keystorage Views Involved in the Process of Renewing Long-Lived X.509 Certificates

Action (in AS Java CLM Cockpit)	Key Storage Views	Action in Secure Login Server
AS Java initially enrolls with administrator credentials and signing request	SLCLM	Issues registration agent certificate with CN=<SID>
Auto-enrolls with RA certificate on SLS	ICM_SSL_nnnnn_<port number>	Sends (renews) certificate in SSL PSE(s) with CN=host.company.com, O=COMPANY, C=DE
Auto-enrolls with RA certificate on SLS	Any other key storage views	Sends (renews) certificate in any other PSE(s) with CN=subject, O=SUBJECT, C=DE

## 4.16.2 Prerequisites for Certificate Renewal Using Secure Login Server

If you want to automatically renew long-lived X.509 certificates with Secure Login Server means, you must fulfill a number of prerequisites.

- You have installed SAP Single Sign-On 3.0 SP01 or higher with Secure Login Server
- You are using SAP NetWeaver 7.31 SP 17, 7.4 SP13 or 7.5 SP00 higher.

## 4.16.3 Configuring Certificate Lifecycle Management in the AS Java Using Secure Login Server

If you want to automatically renew long-lived X.509 certificates with Secure Login Server means using certificate lifecycle management, an administrator must configure application server profiles and application server profile groups in the Secure Login Server.

### Context

Create new application server profiles and configure application server profile groups with the corresponding application server profiles on Secure Login Server. It makes sense to use an application server profile group for a set of SAP systems, for example, for your development systems. You then provide the metadata URL in the CLM Cockpit to retrieve the content of the application server group.

### Procedure

1. [Configuring an Application Server Authentication Profile of the Profile Type "Registration Agent" \[page 100\]](#)
2. [Configuring an Application Server Authentication Profile of the Profile Type "Application" \[page 101\]](#)
3. [Setting Up an Application Server Profile Group for Multiple Application Servers for Java/SAP Systems \(Java\) \[page 102\]](#)

### 4.16.3.1 Configuring an Application Server Authentication Profile of the Profile Type "Registration Agent"

You want to renew certificates of a group of SAP systems (AS Java), for example, all development systems of your landscape.

#### Context

In Secure Login Administration Console, you can configure an application server profile of the type "Registration Agent" that will be used to get a registration certificate.

##### i Note

The profile type "Registration Agent" supports authentication configuration with password based authentication. SPNego, ticket or certificate-based login are not supported.

#### Procedure

1. In Secure Login Administration Console, you can configure an application server profile group that covers all system IDs of your development systems.
2. Go to the [Authentication Profiles](#) section of the [Profile Management](#) tab.
3. Choose [Create](#) to open the wizard that helps you to create a new authentication profile.
4. Enter the authentication profile name. It makes sense to choose a meaningful name that reveals the purpose of the authentication profile. It could be a good idea to include, for example, the key storage view, for which you want to renew the certificates.
5. Choose [Application Server Profile](#) in [Client Type](#).
6. Go to the [Authentication Configuration](#) field and choose a policy configuration for the authentication step.
7. Choose [Next](#) to configure the properties of the user certificates.
8. Make sure that you selected the correct CA in the field [CA for Issuing Certificates](#).
9. Choose [Next](#) to go to the enrollment configuration. The enrollment URL is automatically provided by Secure Login Server.

##### i Note

The enrollment port configured in the SSL configuration of the SAP NetWeaver Administrator must have the type [Request](#) in the [Client Authentication Mode](#) column.

10. Choose the profile type [Registration Agent](#). The [Certificate Template](#) field has the fixed value [SSL Client Template](#) (see the related link), which appears in the metadata information.
11. Choose [Finish](#) to complete the configuration.

## Related Information

[Using Certificate Templates \[page 221\]](#)

### 4.16.3.2 Configuring an Application Server Authentication Profile of the Profile Type "Application"

You want to renew certificates of a group of SAP systems (AS Java), for example, all development systems of your landscape.

## Context

In Secure Login Administration Console, you can configure an application server profile group that covers all the system IDs of your development systems. This application server group contains the application server authentication profiles for the required certificate types you plan to renew.

## Procedure

1. Open Secure Login Administration Console to configure Secure Login Server.
2. Go to the [Authentication Profiles](#) section of the [Profile Management](#) tab.
3. Choose [Create](#) to open the wizard that helps you to create a new authentication profile.
4. Enter the authentication profile name. It makes sense to choose a meaningful name that reveals the purpose of the authentication profile. It could be a good idea to include, for example, the PSE type for which you want to renew the certificates.
5. Choose [Application Server Profile](#) in [Client Type](#).
6. Go to the [User Authentication](#) field and make sure that you use a policy configuration that contains a certificate-based login module.
7. Choose [Next](#) to configure the properties of the user certificates.
8. Make sure that you selected the correct CA in the field [CA for Issuing Certificates](#).
9. Choose [Next](#) to go to the enrollment configuration. The enrollment URL is automatically provided by Secure Login Server.

#### Note

The enrollment port configured in the SSL configuration of the SAP NetWeaver Administrator must have the type [Required](#) in the [Client Authentication Mode](#) column.

10. Choose the profile type [Application](#).
11. Choose the suitable certificate template for the relevant PSEs. For example, [SSL SERVER Template](#) refers to the certificate of the SSL Server PSEs. For more information, see the related link.



12. Choose *Finish* to complete the configuration.

#### **i Note**

(Optional) If you want to renew certificates of other PSE types, create further application server authentication profiles by repeating this procedure accordingly.

13. Include the application server profiles into an application server profile group (see the related link).

## **Related Information**

[Using Certificate Templates \[page 221\]](#)

[Setting Up an Application Server Profile Group for Multiple Application Servers for Java/SAP Systems \(Java\) \[page 102\]](#)

### **4.16.3.3 Setting Up an Application Server Profile Group for Multiple Application Servers for Java/SAP Systems (Java)**

You want to renew certificates of a group of SAP systems (AS Java), for example, all development systems of your landscape.

## **Context**

In Secure Login Administration Console, you can configure an application server profile group that covers all the system IDs of your development systems. This application server profile group contains the application server authentication profiles for the required certificate types you plan to renew and a registration agent authentication profile for enrollment on Secure Login Server.

## **Procedure**

1. Open Secure Login Administration Console to configure.
2. Go to the *Application Server Profile Groups* section of the *Profile Management* tab.
3. Choose *Create*.
4. Enter a name for the application server profile group. We recommend that you use a meaningful name that reveals for which group of SAP systems you plan to renew certificates (for example, all development systems).
5. Select the name of your new application server profile group.

6. (If applicable) If the [Sync Trust Anchors](#) button is not grayed out, choose it to synchronize the trust anchors of the SSL configuration in the SAP NetWeaver Administrator. This may happen if the SSL configuration of the AS Java changed. This SSL configuration change needs to be updated in the Secure Login Server. The [Sync Trust Anchors](#) button enables you to synchronize with the changed SSL configuration of the AS Java.
7. Choose [Edit](#).
8. Choose [Add](#) to add the application server profiles you created earlier. Select the down-arrow to see the list of the application server profiles.
9. Select the profiles you want to add.
  - a. Add an application server profile of the type `Registration Agent`.

#### **i Note**

It is mandatory to include an application server profile of the type `Registration Agent`. It enables the AS Java to enroll on Secure Login Server.

- b. Add, for example, profiles for certificates of SSL servers.
10. Go to the [System Identifiers](#) tray to enter, for example, the system IDs (SIDs) of all your development systems for which you want to renew the certificates.
11. Save your changes.

## **4.16.4 Renewing Certificates at Regular Intervals for AS Java Clients**

You can create recurring tasks for certificate renewals in Java clients in the Secure Login Certificate Lifecycle Management Cockpit.

### **Prerequisites**

- You have installed SAP Single Sign-On 3.0 SP02 or higher with Secure Login Server and Secure Login Certificate Lifecycle Management on AS Java
- You are using SAP NetWeaver 7.31 SP 17, 7.4 SP13 or 7.5 SP00 higher.
- You have the *Administrator* role.
- For setting up a new configuration, your *Administrator* user needs the `SLCLM_OPERATOR` role. To reset the configurations, you need the `SLCLM_ADMIN` role.

### **Context**

## Procedure

1. Access the Secure Login Certificate Lifecycle Management at the following URL: `https://<host>.<domain>./sapso/clm`.
2. Enroll a registration agent to get a registration certificate from Secure Login Server: [Enrolling a Registration Agent \[page 104\]](#).
3. Enroll an application certificate and create a task for its renewal: [Enrolling an Application Certificate and Creating a Task \[page 105\]](#).
4. Change the task configuration or review the tasks in the scheduler: [Changing the Task Configuration in the Scheduler \[page 107\]](#).
5. Reset the configurations (with administrator authorization only): [Changing the Task Configuration in the Scheduler \[page 107\]](#).

### 4.16.4.1 Enrolling a Registration Agent

To be able to ask for renewals of long-lived X.509 certificates, the Secure Login Certificate Lifecycle Management Cockpit must make itself known to the Secure Login server. This is done through the enrollment of a registration certificate.

## Prerequisites

An application server group that includes your system ID and application profiles is defined in Secure Login Server.

## Context

For the renewal of the certificates, the AS Java gets the relevant renewal data from the metadata URL of this application server group. It first requests a registration certificate that is used to enroll for the authentication profiles of the Secure Login Server. When it requests a certificate renewal in the next step, it gets the updated certificate data from the respective application server profile of the Secure Login Server.

## Procedure

1. In the Secure Login Certificate Lifecycle Management Cockpit, choose the [Registration](#) tile.
2. To enroll on Secure Login Server, enter the metadata URL of an application server group that contains the SID of your system.

```
https://slshost.domain:443/SecureLoginServer/appserverprofiles/groupsmetadata?  
groupId=GroupWithYourSID
```

3. To get the metadata of this application server group, choose [Fetch](#).
4. Review the metadata to ensure that they are correct. This includes the SIDs, the RA and the app profiles.
5. Enroll the registration agent by providing user credentials of a user that has administrative authorizations on Secure Login Server.  
  
A registration certificate with CN=<SID> is created.
6. Ensure that the registration certificate is correct and choose [Save](#).
7. Go back to the Secure Login Certificate Lifecycle Management Cockpit, either by choosing the [Back](#) button in the upper left corner or the [Home](#) button in the lower right corner.

## Results

You only need to perform this step once. The registration certificate is valid for the entire system. Now, you can enroll application certificates and define a task that requests new certificates at regular intervals from Secure Login Server.

### 4.16.4.2 Enrolling an Application Certificate and Creating a Task

You enroll the renewed certificates and then create a recurring task so the system will renew the certificates automatically in the future.

## Procedure

1. In the Secure Login Certificate Lifecycle Management Cockpit, choose the [Enrollment](#) tile.
2. Select the keystore view.

Note that only keystores that include certificates with private keys are listed.

Each keystore view can include more than one private key.

3. Select certificates and the correct combination of template profiles from the dropdown list.
4. For each certificate, specify whether a new private key should be generated.

#### **i** Note

You can enroll one or more certificates simultaneously.

If you select a certificate that is already signed by a certificate authority, the system will warn you and ask you to double-check your choice.

Certificates will become active immediately. If the certificate is used by an external process such as Internet Connection Manager (ICM), a restart of this application may be required to make use of the new certificate.

5. Choose [Enroll Certificates](#).
6. Review the renewed certificates by checking that the enrollment has status [OK](#).

Check the details of the certificate by choosing [Show Details](#).

7. If the status is [OK](#), choose [Next](#) to create a task.

Note that each view must be administered in a separate task. You can, however, create more than one task for the same certificate.

8. To configure your system to automatically renew the certificates regularly, enter the required data and choose [Create Task](#).

The grace period defines the days until expiration of your certificates. Let's assume that the task is carried out daily, it will renew the certificate 14 days before expiration. In case of a system downtime or other error, 14 days should be sufficient to ensure the task to successfully renew the certificate prior to its expiration.

#### → Recommendation

To test if the task is set up correctly, you can enter 0 (zero) as grace period and schedule the task for a minute in the future. Then you can immediately check the Job Log of the Java Scheduler.

9. (Optional) Repeat this procedure for all certificates that you want to be renewed automatically.
10. Go back to the Secure Login Certificate Lifecycle Management Cockpit by choosing the [Back](#) button in the upper right corner or the [Home](#) button in the lower right corner.

## 4.16.4.2.1 Inserting a TLS Server Host Name Into a Certificate

### Context

If you create your own certificate, you need to make sure that it contains the host name of the TLS/SSL Server, if the profile template demands one. The details view of the certificate shows the DNS name. There is the following procedure to manually include these DNS names in the certificate as subject alternative names.

### Procedure

1. In the NetWeaver Administrator, on the [Configuration](#) tab, choose [Keys and Certificates](#).
2. Select your key storage view.  
  
You can either create a certificate for each port or for the general port.
3. On the [View Entries](#) tab below, choose [Create](#).
4. Specify a name.

Do not check [Store Certificate](#).

5. Choose [Next](#).
6. To add a subject property, choose [Add](#).
7. From the dropdown list of predefined subject properties, select [unstructuredName](#) and choose [Add](#).
8. For the unstructured name, enter the host name or full qualified host name of the TLS server so it will be found in the DNS. To enter more than one, separate them by a colon (":").
9. Enter the common name.
10. Choose [Next](#) and skip the step to sign a key pair by choosing [Next](#) again.
11. Choose [Finish](#).

## Results

You can now create a task for certificate renewal of this certificate in the Secure Login Certificate Lifecycle Management Cockpit. We recommend to test if the task is successful by scheduling it for a minute into the future and entering a grace period of zero days. Then check if the task is listed in the Java Job Scheduler.

### 4.16.4.3 Changing the Task Configuration in the Scheduler

Use the [Scheduler](#) tile of the Secure Login Certificate Lifecycle Management Cockpit to change the configuration of the tasks for the automatic renewal of certificates or to review the tasks configured in your system.

## Prerequisites

You have enrolled a new certificate and created a task.

## Procedure

1. In the Secure Login Certificate Lifecycle Management Cockpit, choose the [Scheduler](#) tile.
2. For each task, you can do the following:
  - To edit a task, choose the [Edit](#) icon.
  - To delete a task, choose the [Delete](#) icon. You can also delete a task in the Java Scheduler on the [Tasks](#) tab.
3. Go back to the Secure Login Certificate Lifecycle Management Cockpit by choosing the [Back](#) button in the upper right corner or the [Home](#) button in the lower right corner.

## Results

Check the Job Scheduler in the AS Java to see if the tasks have been carried out correctly.

### 4.16.4.4 Resetting All Configurations

As an administrator, you can delete all local configurations for the Certificate Lifecycle Management with just one click.

## Prerequisites

You have an *Administrator* user with the `SLCLM_ADMIN` role.

## Context

This step will delete the registration certificate (keystore view SLCLM) and all related tasks.

## Procedure

In the Secure Login Certificate Lifecycle Management Cockpit, choose the [Reset Configurations](#) tile.

## Results

This step will set back the cockpit to its original state.

## 4.17 Issuing Certificates for iOS Devices

Secure Login Server can issue medium-lived or long-lived certificates for iOS devices.

### Context

Since the Secure Login Server is familiar with the SCEP protocol, iOS client devices can use it to enroll on the Secure Login Server. A special Secure Login Web Client profile is available. It uses the Apple iOS SCEP protocol for user authentication.

#### ! Restriction

There are restrictions that apply to the key size of the certificates. For more information, see the related link.

#### i Note

As an administrator, you can also enable provisioning of short-lived certificates for iOS device users using the SAP Authenticator app. You can configure this in the One-Time Password Administration UI.

For more information, see the One-Time Password Authentication Administration Guide. Go to the Administrator Setup for SAP Authenticator Users in the [Using Mobile Single Sign-On](#) section.

To set up authentication of an iOS client device using Secure Login Server methods, an administrator must do the following:

### Procedure

1. Install the root certificate in the iOS client device.
2. Create an authentication profile on the Secure Login Server to provide the relevant enrollment URL that is suitable for iOS devices using the SCEP protocol.

### Related Information

<http://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html> 



## 4.17.1 Configuring an Authentication Profile for iOS Devices

If you want to enroll iOS client devices on the Secure Login Server, you must configure a Secure Login Web Client profile for the Apple iOS SCEP protocol.

### Context

Since the Secure Login Server can use the SCEP protocol, you can specify that the Secure Login Server issues certificates for iOS client devices. To do this, an administrator needs to create authentication profiles for the Apple iOS SCEP protocol on the Secure Login Server.

### Procedure

1. Open the Secure Login Administration Console.
2. Go to the [Authentication Profiles](#) tab under [Profile Management](#).
3. Choose [Create](#).
4. Enter a name and a description of the authentication profile.
5. Choose the client type [Secure Login Web Client](#).
6. Choose the [Apple iOS SCEP](#) authentication form in the [User Authentication](#) section.
7. Choose [Next](#) to continue.
8. Enter the values of the certificate configuration (see the related link) and choose [Next](#).
9. Finish the authentication profile configuration by defining the post-authentication actions.

### Related Information

[Parameters for Certificate Configuration in the Authentication Profile \[page 297\]](#)

## 4.18 Kerberos Authentication with SPNego

In this configuration example, the user authentication is verified against a Microsoft Windows domain.

### Prerequisites

- Secure Login Server is installed and the initial wizard has been completed.

- In Certificate Management at least the User CA is available.
- To use HTTPS, you must enable SSL on the SAP NetWeaver server.
- You have configured and enabled SPNego on SAP NetWeaver Administrator.

## Procedure

1. Log on to the Secure Login Administration Console and choose [Profile Management](#).
2. Go to [Certificate Configuration](#) and check whether a user CA is available in this [Certificate Issuer](#) section.
3. Configure your [Secure Login Client Settings](#). For more information, see related links. For [Secure Login Web Client Settings](#), see [Creating a Profile Group of Authentication Profiles \[page 145\]](#).
4. If you use Secure Login Client, choose [Profile Management](#) and configure the client policy. For [Secure Login Client Settings](#), see [Creating a Profile Group of Authentication Profiles \[page 145\]](#).
5. Go to [User Profile Groups](#).
6. Choose the profile group that contains the SPNego authentication profile in the [User Profile Group](#) tab.
7. Choose the [Download Policy](#) button. This export the files `ProfileGroup<profilegroup>.reg` and `ProfileDownloadPolicy<profilegroup>.reg`.
8. Export the client policy which is used for the Secure Login Client installation.
9. Choose this profile in the Secure Login Client, and an X.509 certificate is provided without further user interaction.

After a successful authentication, an X.509 user certificate is provided. This user certificate is available in the Microsoft Certificate Store (User Certificate Store).

10. If you use the Secure Login Web Client, log on with the corresponding profile URL.

## Related Information

[Applications and Profiles \[page 276\]](#)

[Parameters for Client Configuration \[page 281\]](#)

[Downloading Policies from the Secure Login Server \[page 144\]](#)

## 4.18.1 Configuring Kerberos Authentication with SPNego for Secure Login Client

In this configuration example, the user authentication is verified against a Microsoft Windows domain.

### Procedure

1. Log on to the Secure Login Administration Console and choose [Profile Management](#).
2. Go to [Certificate Configuration](#) and check whether a user CA is available in this [Certificate Issuer](#) section.
3. Configure your [Secure Login Client Settings](#). For more information, see related links. For [Secure Login Client Settings](#), see [Creating a Profile Group of Authentication Profiles \[page 145\]](#).
4. Go to [User Profile Groups](#).
5. To add the default SPNego authentication profile, choose [Add](#).
6. If you use the Secure Login Client, distribute the policy URL to the clients, for example by downloading the policies using the [Download Policy](#) button. For more information, see related link.
7. Choose this profile in the Secure Login Client, and an X.509 certificate is provided without further user interaction.

After a successful authentication, an X.509 user certificate is provided. This user certificate is available in the Microsoft Certificate Store (User Certificate Store).

8. If you use the Secure Login Web Client, log on with the corresponding profile URL.

### Related Information

[Applications and Profiles \[page 276\]](#)

[Parameters for Client Configuration \[page 281\]](#)

[Downloading Policies from the Secure Login Server \[page 144\]](#)

## 4.18.2 Enabling Kerberos Authentication with SPNego for Secure Login Web Client

Kerberos authentication is also possible for Secure Login Web Client.

### Context

You use the default SPNego authentication profile as a template to create your own SPNego authentication profile, but you must change the client type to Secure Login Web Client profile.

## Procedure

1. Log on to the Secure Login Administration Console and choose the node [Profile Management](#).
2. Verify whether the authentication mechanism in [Authentication Profile](#) is configured correctly.
3. Select the default SPNego authentication profile.
4. Choose [Copy to New Profile](#).
5. Enter a name for your new authentication profile.
6. Set the type of the new authentication profile to [Secure Login Web Client Profile](#).
7. For more information, see related link.

## Related Information

[Kerberos Authentication with SPNego \[page 110\]](#)

### 4.18.3 Configuring SPNego on SAP NetWeaver Administrator

SPNegoLoginModule works in close conjunction with the user management engine (UME).

## Context

Remember that you may need to configure the mapping mode of the Kerberos Principal Name to the UME or to change Customizing settings of the UME data source configuration. For more information, see the SAP NetWeaver Library 7.3 under ► [SAP NetWeaver Library: Function-Oriented View](#) ► [Security](#) ► [User Authentication and Single Sign-On](#) ► [Integration in Single Sign-On \(SSO\) Environments](#) ► [Single Sign-On for Web-Based Access](#) ► [Using Kerberos Authentication](#) ► [Configuring the UME for Kerberos Mapping](#) ►.

#### **i** Note

If you have an Active Directory environment with parent and child domains, you should configure the keytab file for the parent and child domain when you set up SPNego in SAP NetWeaver AS for Java.

## Procedure

To configure SPNego, use the appropriate configuration wizard. For more information, see the SAP NetWeaver Library 7.3 under ► [SAP NetWeaver Library: Function-Oriented View](#) ► [Security](#) ► [User Authentication and Single Sign-On](#) ► [Integration in Single Sign-On \(SSO\) Environments](#) ► [Single Sign-On for Web-Based Access](#) ► [Using Kerberos Authentication](#) ►.

### ⚠ Caution

If you do not use an LDAP as data source in the user management engine (UME), you must choose **Principal@REALM** as mapping mode and **virtual user** as source.

If your LDAP server is connected with the user management engine (UME), choose **Principal Only** as mapping mode and **LoginID** as source.

## 4.19 LDAP User Authentication

In this configuration example, the user authentication is verified against a Microsoft Active Directory System or LDAP server.

### Prerequisites

- Secure Login Server is installed and the initial wizard has been completed.
- In [Certificate Management](#) at least the User CA is available.
- To use HTTPS, you must enable SSL on the SAP NetWeaver AS for Java.

### Procedure

1. Log on to the Secure Login Administration Console and choose the [Authentication Profile](#) tab.
2. Choose [Certificate Management](#) and check whether a user CA is available.
3. Choose a user CA.
4. If you use Secure Login Client, choose [Profile Management](#) and configure the client policy. For [Secure Login Client Settings](#), see [Creating a Profile Group of Authentication Profiles \[page 145\]](#).
5. Go to [User Profile Groups](#).
6. Choose the profile group that contains the relevant authentication profile.
7. Choose the [Download Policy](#) button. This exports the files `ProfileGroup<profilegroup>.reg` and `ProfileDownloadPolicy<profilegroup>.reg`.
8. Export the client policy which is used for the Secure Login Client installation.
9. Create an LDAP destination. For more information, see related link. This LDAP destination must exist in the SAP NetWeaver Administrator.
10. Define the connection parameters for the login module [SecureLoginModuleLDAP](#). For more information, see related link.
11. Install the Secure Login Client application on the client PC. Import the files `ProfileGroup<profilegroup>.reg` and `ProfileDownloadPolicy<profilegroup>.reg` to the client registry. Verify whether the certificate chain (trust relation) of the SSL server certificate is in the Microsoft Certificate Store (Computer Certificate Store). Import missing certificates.

12. Restart your client PC.
13. In the Secure Login Client, the profile defined in [Authentication Profile](#) is displayed in Secure Login Client Console. Choose this profile and enter the user name and password (Active Directory System or LDAP server).  
  
After successful authentication, an X.509 user certificate is provided. This user certificate is displayed in the Secure Login Client Console and is available in the Microsoft Certificate Store (User Certificate Store).
14. If you use the Secure Login Web Client, log on with the corresponding profile URL.

## Related Information

[Importing LDAP Server CAs or Certificates into the SAP NetWeaver Key Storage \[page 115\]](#)

[Creating Destinations \[page 197\]](#)

[Parameters for LDAP Login Modules \[page 287\]](#)

### 4.19.1 Importing LDAP Server CAs or Certificates into the SAP NetWeaver Key Storage

You establish a trust relationship with your SAP Netweaver Application Server by importing CAs or certificates into the Key Storage.

## Context

To establish a trust relationship with the SAP Netweaver Application Server, you import your CA certificate of the LDAP server into the Key Storage of SAP Netweaver Application Server. Take the following steps:

## Procedure

1. Start SAP NetWeaver Administrator.
2. Go to the [Configuration](#) tab.
3. Choose [Views](#) in [Certificates and Keys](#).
4. Select [Key Storage](#).
5. Select the Key Storage view `TrustedCAs`.

You display the details of the TrustedCAs view in the [View Entries](#) tab.

6. Choose [Import Entry](#).
7. Select the file format of your CA or certificate.
8. Browse to your file.

9. To import your file, choose [Import](#).

## Results

You have now established a trust relationship by having imported CAs or certificates files.

For more information, see the SAP Help Portal under ► [SAP NetWeaver Library: Function-Oriented View](#) ► [Security](#) ► [Security](#) ► [System Security](#) ► [System Security for AS Java Only](#) ► [Using the AS Java Key Storage](#) ►.

## 4.20 Deleting a Configuration

You can delete the configuration in the Secure Login Certificate Lifecycle Management Cockpit by choosing the corresponding tile.

### Prerequisites

You have administrator authorizations with the `SLCLM_ADMIN` role.

### Context

### Procedure

1. In the Secure Login Certificate Lifecycle Management Cockpit, choose [Delete Configuration](#).
2. Confirm the confirmation message.

## Results

The configuration is deleted. To create a new one, start by enrolling a registration agent.

## Related Information

[Enrolling a Registration Agent \[page 104\]](#)

## 4.21 User Authentication against SAP Netweaver Application Server for ABAP

In this example, the user authentication is verified against the user management of SAP Netweaver Application Server for ABAP.

### Prerequisites

- Secure Login Server is installed and the initial wizard has been completed.
- In [Certificate Management](#), at least the user CA is available.
- To use HTTPS, enable SSL on SAP Netweaver Application Server.

### Context

Take the following steps:

### Procedure

1. Verify whether the authentication mechanism in the client authentication profile is configured correctly.  
**SecureLoginDefaultPolicyConfigurationABAP.**
2. Create a destination with an RFC destination value in the SAP NetWeaver Administrator. For more information, see related link.
3. Choose [Certificate Management](#) and check if a user CA is available for this authentication profile.
4. Choose a user CA.
5. Choose [Profile Management](#) and configure the client policy.
6. Go to [Certificate Configuration](#).
7. Configure your [Secure Login Client Settings](#). For more information, see related links. For [Secure Login Client Settings](#), see [Creating a Profile Group of Authentication Profiles \[page 145\]](#).
8. Go to [User Profile Groups](#).
9. Choose the profile group that contains the relevant authentication profile in the [Profile Group](#) tab.
10. Choose the [Download Policy](#) button. This exports the files `ProfileGroup<profilegroup>.reg` and `ProfileDownloadPolicy<profilegroup>.reg`.



11. Export the client policy which is used for the Secure Login Client installation.
12. Create an RFC destination. For more information, see related link. This RFC destination must exist in the SAP NetWeaver Administrator.
13. Define the connection parameters for the login module [SecureLoginModuleABAP](#). For more information, see related link
14. Install the Secure Login Client application on the client PC. Import the files `ProfileGroup<profilegroup>.reg` and `ProfileDownloadPolicy<profilegroup>.reg` to the client registry. Verify whether the certificate chain (trust relation) of the SSL server certificate is in the Microsoft Certificate Store (Computer Certificate Store). Import missing certificates. You can also use Secure Login Web Client.
15. Restart your client PC.
16. In the Secure Login Client, the profile defined in [Authentication Profile](#) is displayed in Secure Login Client Console. Choose this profile and enter the user name and password (AS ABAP).  
  
After successful authentication, an X.509 user certificate is provided.  
  
This user certificate is displayed in the Secure Login Client Console and is available in the Microsoft Certificate Store (User Certificate Store).
17. If you use the Secure Login Web Client, log on with the corresponding profile URL.

## Related Information

[Secure Login Client Installation \[page 132\]](#)

[Creating a Destination with an RFC Destination Type \[page 118\]](#)

### 4.21.1 Creating a Destination with an RFC Destination Type

#### Procedure

1. Start the SAP NetWeaver Administrator.
2. Go to [Destinations](#).
3. Choose [Create...](#)
4. Enter a destination name. You must enter this name in the [Login Module](#) options in Secure Login Administration Console.
5. Choose the destination type [RFC Destination](#).
6. Continue with [Next](#) and follow the steps of the destination wizard SAP NetWeaver Administrator.

## 4.22 RADIUS User Authentication

In this configuration example, the user authentication is verified against a RADIUS server.

### Prerequisites

- An RSA Authentication Manager (with a RADIUS server) is installed and running. The versions currently supported are 6.1, 7.1., 8.0, and 8.1. It communicates with the Secure Login Server through its RADIUS protocol using its own RADIUS server. The Secure Login Server supports new SecurID PINs and the next token code of RSA SecurID tokens.  
For more information, see the corresponding RSA Authentication Manager documentation.  
For more information about the parameters for RADIUS, see [Parameters for RADIUS Login Modules \[page 289\]](#).
- Secure Login Server is installed and the initial wizard was completed.
- In [Certificate Management](#) at least the User CA is available.

### Procedure

1. Verify in SAP NetWeaver Administrator whether the policy configuration for RADIUS authentication was set up correctly.
2. Log on to the Secure Login Administration Console and choose a authentication profile.
3. Verify whether the RADIUS destination of the authentication profile is configured correctly.
4. Choose [Certificate Configuration](#) and check if the a user CA is available in this [Certificate Issuer](#) section.
5. Configure your [Secure Login Client Settings](#). For more information, see related links. For [Secure Login Client Settings](#), see [Creating a Profile Group of Authentication Profiles \[page 145\]](#).
6. In the RADIUS Server, configure [Radius Client](#) for Secure Login Server.  
This means that the Secure Login Server can establish communication to the RADIUS Server. Use the Shared Secret for this connection.
7. Install the Secure Login Client application on the client PC (see [Secure Login Client Installation \[page 132\]](#)) or use Secure Login Web Client.
8. If you use Secure Login Client, choose [Profile Management](#) and configure the client policy. For [Secure Login Client Settings](#), see [Creating a Profile Group of Authentication Profiles \[page 145\]](#).
  - a. Go to [Profile Groups](#).
  - b. Choose the profile group that contains the relevant authentication profile.
  - c. Choose the [Download Policy](#) button. This export the files `ProfileGroup<profilegroup>.reg` and `ProfileDownloadPolicy<profilegroup>.reg`.
  - d. Export the client policy which is used for the Secure Login Client installation.
9. If you use the Secure Login Client and you have downloaded the policy for the relevant authentication profile, the defined profile appears in Secure Login Client Console.

Choose this profile and enter the user name and password (RADIUS user database).

After successful authentication, an X.509 user certificate is provided.

This user certificate is displayed in the Secure Login Client Console and is available in the Microsoft Certificate Store (User Certificate Store).

10. If you use the Secure Login Web Client, log on with the corresponding profile URL.

## Related Information

[Parameters for Client Configuration \[page 281\]](#)

[Parameters for Secure Login Web Client Configuration \[page 286\]](#)

### 4.22.1 Using a Customer-Specific securid.ini Server Message File

This topic describes how you provide a server message file for RSA authentication to a RADIUS destination.

## Context

You can import or configure the customer-specific `securid.ini` server message file in the RADIUS destination of the Secure Login Administration Console.

## Procedure

1. Open the Secure Login Administration Console.
2. Go to the [Destination Management](#) tab.
3. Select a destination with the type RADIUS Destination.
4. Choose the [Edit](#) button.
5. Expand the [Advanced Configuration for RSA Authentication](#) section in the [Settings](#) tab below the list of destinations.
6. If you want to use your own `securid.ini` server message file that has already been customized, proceed as follows:
  - a. Use [Import Server Message File](#) to browse to your file.
  - b. Import the `securid.ini` file.
7. If you want to enter the parameters for the `securid.ini` server message file manually, proceed as follows:
  - a. Enter the required values in the parameters of the [Advanced Configuration for RSA Authentication](#) section.
8. Save your changes.

## Related Information

[SAP Help Portal for Enhancement Package 3 for SAP Netweaver Application Server release 7.0](#)

### 4.23 Identification Using RFID Tokens


Multiple users want to quickly log on to a kiosk application using RFID tokens and perform short tasks.

A typical use case for this is a hardened kiosk PC on the shop floor. Multiple employees, such as production workers, use it to perform tasks in SAP GUI or in a browser-based application provided by an application server or any other X.509-based back end. A typical task could be, for example, ordering new material. The employees would use RFID tokens because an RFID identification is very fast. Closing SAP GUI or the application they have used triggers a logoff.

When they place their RFID tokens on the reader, they get an X.509 certificate, which will be available until they pick up the RFID token. A dedicated RFID token identifies them. All the employees who want to log on to a kiosk application do is place their tokens on the reader to receive a certificate, start SAP GUI or an application for login, and remove their tokens. When they finish their work, they close the application they worked with. When the next employee performs identification using his or her token, he or she gets a new certificate.

You can use RFID tokens to identify at the following back ends:

- Application Server ABAP using X.509-based SNC
- Application Server Java using SSL client authentication
- Any X.509-based back end or web server

For more information, see SAP Note [1970286](#) .

#### 4.23.1 Security Aspects of RFID Identification

Using RFID tokens enables employees to quickly log on to a kiosk application on a kiosk PC. There they can perform tasks. RFID identification alone was not designed for secure authentication. This means that you must ensure a high level of security by various means.

To provide a high level of security, you must guarantee the following:

1. Harden the kiosk PCs by sealing them physically, for example, to make sure that no one can plug in any devices.
2. Use forgery-proof RFID systems.
3. After identification of the RFID token, the kiosk PC performs either a Kerberos or an SSL-based certificate authentication using the Microsoft Windows account. The kiosk PC's Microsoft Windows user authenticates in a secure way at the Secure Login Server using Kerberos or SSL-based X.509 certificates.
  - If your kiosk PCs belong to a Microsoft Windows domain, the domain user of the kiosk desktop authenticates using Kerberos against the Microsoft Windows domain.
  - If your kiosk PCs do not belong to a Microsoft Windows domain, the Microsoft Windows users running the kiosk desktop authenticate with SSL using X.509 certificates.

## 4.23.2 Implementation Concept of RFID Identification

RFID tokens provide a unique identifier (UID), which the Secure Login Server uses for mapping the employees who want to log on to the kiosk application. Using X.509 certificates or Kerberos authentication, the kiosk PC makes sure that the authentication is secure. The employees can now perform their tasks in a kiosk application and log off.

### Prerequisites

Server	<ul style="list-style-type: none"><li>Secure Login Server 2.0 SP04 or higher on an SAP NetWeaver Application Server for Java</li><li>SPNego or X.509 client certificate authentication is enabled on the AS Java</li><li>A directory server that can map a UID to a user name</li></ul>
Client	<ul style="list-style-type: none"><li>Secure Login Client 2.0 SP04 or higher (running on a Microsoft Windows platform) with a dedicated RFID-enabled authentication profile</li></ul>

Secure Login Client can only handle data from an RFID token if dedicated RFID profiles are available in the Secure Login Client. These profiles are provided by the Secure Login Server. Distribute the RFID profiles to the respective kiosk PCs using the policy downloader and/or the profile groups. Using these profiles, the Secure Login Client monitors the connected RFID readers. When an employee places the RFID token on the reader, the Secure Login Client enrolls for a certificate. Then the employee works the kiosk application on the kiosk PC, for example, an SAP GUI or a browser-based application.

The RFID profiles depend on the RFID reader hardware you are using.

### i Note

To make sure that only authorized kiosk PCs can perform such an operation without user authentication, the Microsoft Windows (domain) user running the kiosk desktop needs to authenticate either using an X.509 certificate (SSL) or Kerberos (SPNego).

## Related Information

[Configuring Identification with RFID Tokens \[page 124\]](#)

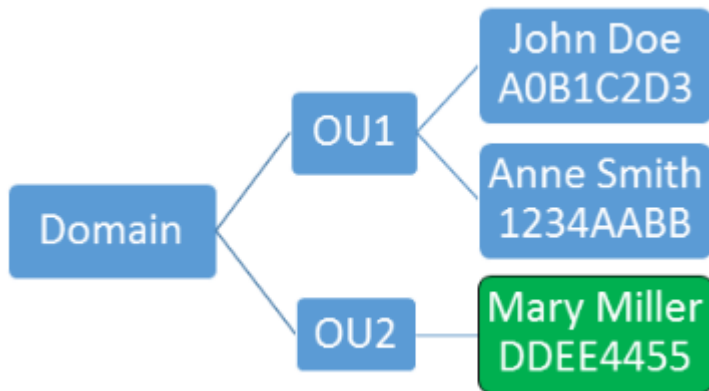
## 4.23.3 RFID Identification Example

An employee called Mary Miller wants to use a kiosk PC on the shop floor, order material in a SAP GUI application quickly, and continue with her daily work like many of her colleagues.

### i Note

This kiosk PC's technical desktop user is authenticated in Mary Miller's domain in Active Directory with CN=KIOSKUSR001@DOMAIN.COM with Kerberos or with an X.509 certificate (arrow 1).

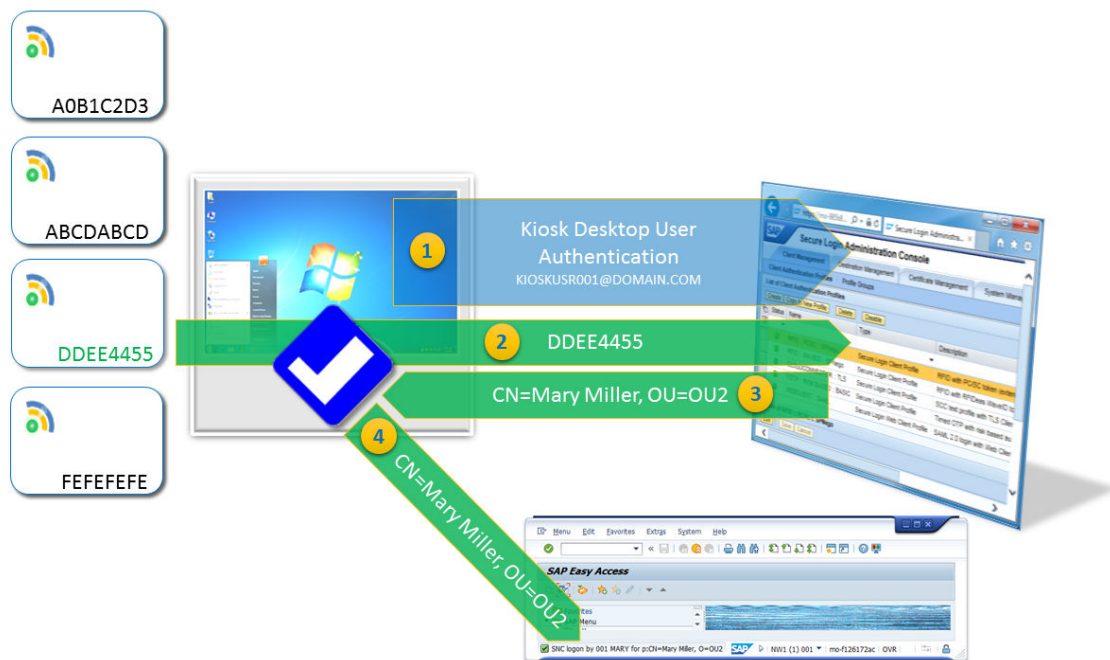
Mary Miller has an RFID token with the UID DDEE4455 (arrow 2). Her user account "Mary Miller" belongs to the organizational unit "OU2" in a Microsoft Windows domain called "Domain".



She places her RFID token on the RFID reader and the reader transmits the UID DDEE4455 to the Secure Login Server. The Secure Login Server finds her UID in the configured attribute in Active Directory and retrieves further attributes from this directory entry, such as a given name, last name, and organizational unit. It issues an X.509 certificate with the following elements in the user's subject name (arrow 3):

- CN=Mary Miller
- OU=OU2

The Secure Login Client receives this X.509 certificate, which is only valid for this session, and Mary Miller uses it to log on to her SAP GUI application (arrow 4), where she orders the material.



## 4.23.4 Prerequisites for RFID Identification in the Kiosk PCs

Depending on the RFID identification (reader type) you use, you must make sure that your readers are connected and installed properly at the kiosk PCs.

Secure Login supports the following kinds of RFID identification (reader types):

- PC/SC
- Wave ID

Prerequisites in the Kiosk PC

Prerequisites	Description
Secure Login Client 2.0 SP04	<ul style="list-style-type: none"><li>• You have installed Secure Login Client 2.0 SP04 or higher on your kiosk PCs.</li></ul>
PC/SC (reader type)	<ul style="list-style-type: none"><li>• You have installed the respective device drivers for PC/SC readers.</li><li>• A Microsoft Windows smart card service is active.</li></ul>
Wave ID (reader type)	<ul style="list-style-type: none"><li>• You have installed the respective device drivers for Wave ID readers.</li><li>• You have placed the runtime DLL of RF IDEas (file name <code>pcProxAPI.dll</code>) in the folder <code>C:\Windows\System32</code> (32-bit Microsoft Windows) or <code>C:\Windows\SysWOW64</code> (64-bit Microsoft Windows) of the kiosk PCs, and you have registered the DLL.</li></ul>

## 4.23.5 Configuring Identification with RFID Tokens

If you want to use RFID tokens during Secure Login Client sessions, you need to make settings in the Active Directory domain controller, in the SAP NetWeaver Administrator, in the Secure Login Server, and in the Secure Login Client.

To enable employees to use RFID tokens for identification at a kiosk PC, you need to connect the reader hardware properly and configure a number of systems.

1. Active Directory domain controller  
The Active Directory domain controller must know the employees who want to log on to the kiosk application using the RFID tokens at the kiosk desktop. Add the unique identifiers of the RFID tokens user attributes in Active Directory.
2. SAP NetWeaver Administrator (of SAP NetWeaver Application Server for Java)  
The Microsoft Windows (domain) user running the kiosk desktop can authenticate either using Kerberos or X.509 certificates (SSL). In both cases, you must create custom configurations in the policy configuration of the SAP NetWeaver Administrator, include the suitable login modules, add rule attributes for the Service Principal Name, or configure the certificate subject and issuer name to restrict the kiosk PCs.
3. Secure Login Server (Secure Login Administration Console)  
Create an LDAP destination for the relevant subtree of your directory in [Destination Management](#) using LDAP server authentication for the mapping of the employees who want to log on to the kiosk application (see the related link). During RFID authentication, the Secure Login Server tries to find the their user names by searching for the unique identifiers of the RFID tokens in the given search base DN and in all subtrees.

Use a new client authentication profile for Secure Login Client with the profile type of the RFID reader (PC/SC or Wave ID) and configure the user mapping using the LDAP search attributes, the user name mapping attributes, and the user certificate attributes.

4. Secure Login Client

Use the policy download agent to upload the suitable RFID client authentication policies from the Secure Login Server.

## Related Information

[Applications and Profiles \[page 276\]](#)

[Adding a Policy Configuration \[page 194\]](#)

[Managing Destinations \[page 214\]](#)

### 4.23.5.1 Setting User Attributes for RFID Tokens in Active Directory

Active Directory must know the UIDs of the RFID tokens.

## Context

Active Directory handles the entire user management of the employees who want to log on to the kiosk application.

## Procedure

To enter the UIDs of the RFID tokens into Active Directory, proceed as follows:

1. Use a new or existing user attribute in Active Directory.
2. Enter the value of the UID as `DirectoryString` as displayed by the Secure Login Client.

#### Example

```
"extensionAttribute15"="31EADA58"
```

#### Note

Make sure that these user attributes are unique in the directory subtree of the search base DN.

When the Secure Login Server finds a UID of an RFID token, Active Directory returns the requested user attributes.



## 4.23.5.2 Configuring Kiosk PC Authentication at a Domain

The Microsoft Windows (domain) users running the kiosk desktops must authenticate either using Kerberos (SPNego) or a client certificate (X.509).

Perform the respective configuration in the SAP NetWeaver Administrator of the SAP NetWeaver Application Server for Java.

In the subsequent steps, you must use the respective login module(s) with the `REQUIRED` flag. Use rule attributes to restrict kiosk PC access to domains and clients.

### 4.23.5.2.1 Configuring Kerberos (SPNego) Authentication at Kiosk PCs

You want your Microsoft Windows (domain) users running the kiosk desktops for RFID-based identification to authenticate at the Microsoft Windows domain using Kerberos (SPNego).

#### Context

To configure Kerberos (SPNego) authentication of the Microsoft Windows (domain) users running the kiosk desktops for RFID identification at the Microsoft Windows domain controller, you must configure a realm and policies in the SAP NetWeaver Administrator of the AS Java. You then restrict access to the domains and the kiosk PCs' authorization by setting rule attributes in the Secure Login Administration Console.

#### Procedure

1. Open the SAP NetWeaver Administrator in the domain controller.
2. Go to [► Configuration ► Authentication and Single Sign-On ► SPNEGO](#) and create a Kerberos realm for a system account.
3. Configure the Service Principal Name as required by the AS Java. For more information, see the SAP Help Portal under [► Application Help ► Function-Oriented View ► Security ► User Authentication and Single Sign-On ► Integration in Single Sign-On \(SSO\) Environments ► Single SignOn for Web-Based Access ► Using Kerberos Authentication ► Using Kerberos Authentication on SAP NetWeaver AS Java](#).
4. Go to [► Configuration ► Authentication and Single Sign-On ► Authentication](#) and create a new custom policy configuration with the following login modules and the [Required](#) flag.
  1. SPNegoLoginModule
  2. SecureLoginModuleUserDelegationWithSPNego

#### i Note

Enter the login modules exactly in this sequence.

5. Select the login module `SecureLoginModuleUserDelegationWithSPNego` and choose [Edit](#).
6. Go to the [Login Module Options](#) tab.
7. Restrict the kiosk PCs and domains that your kiosk PCs can access.
  - a. To specify the allowed Microsoft Windows (domain) user names, edit the login module option `Rule1.principal` (or add a new option) and enter the allowed user names in the [Value](#) tab.
  - b. To restrict the domains that the kiosk PC is allowed to access, edit the `Rule1.realm` option (or add a new option) and specify the allowed domains in the [Value](#) tab.

#### ❖ Example

Values for Login Module Options

Value	Description
<code>( . * )</code>	Allow access to all realms or all Microsoft Windows (domain) users
<code>ABC ( . * )</code>	Allow access to all Microsoft Windows (domain) users or realms starting with ABC
<code>ABC</code>	Allow access only to a Microsoft Windows (domain) user or realm called ABC

If no rule value matches, the authentication fails.

Login Module Option Configuration Examples

Option	Value	Description
<code>Rule1.principal</code>	<code>KIOSK ( . * )</code>	This configuration allows the user principal name
<code>Rule1.realm</code>	<code>DOMAIN . LOCAL</code>	<code>KIOSK02@DOMAIN . LOCAL</code> , but not <code>K . IOS@DOMAIN . LOCAL</code> .

8. Save your changes.  
You have now configured Kerberos (SPNego) authentication of your Microsoft Windows (domain) user running the kiosk desktop at a Microsoft Windows domain controller.

## 4.23.5.2.2 Configuring X.509 Certificate Authentication at Kiosk PCs

You want your kiosk PCs for RFID-based identification to authenticate at the Microsoft Windows domain using X.509 certificates (SSL).

### Context

To configure SSL-based X.509 certificate authentication of the Microsoft Windows domain users running the kiosk desktop for RFID identification at the Microsoft Windows domain controller, you must create an LDAP destination in the SAP NetWeaver Administrator of the AS Java.

## Procedure

1. Open the SAP NetWeaver Administrator in the domain controller.
2. Go to ► [Configuration](#) ► [Security](#) ► [SSL](#) ► and create an HTTPS port with the value *Required* in the *Client Authentication Mode* column.

For more information, see the SAP Help Portal under ► [Application Help](#) ► [Function-Oriented View](#) ► [Security](#) ► [User Authentication and Single Sign-On](#) ► [Integration in Single Sign-On \(SSO\) Environments](#) ► [Single Sign-On for Web-Based Access](#) ► [Using X.509 Client Certificates](#) ► [Using X.509 Client Certificates on the AS Java](#) ►.

3. Go to ► [Configuration](#) ► [Authentication and Single Sign-On](#) ► [Authentication](#) ► and create a new custom policy configuration with the following login module and the *Required* flag.
  - SecureLoginModuleUserDelegationWithSSL
4. Select the login module SecureLoginModuleUserDelegationWithSSL and choose *Edit*.
5. Go to the *Login Module Options* tab.
6. Restrict the Microsoft Windows domain users and the domains that your kiosk PCs can access.
  - a. To specify the allowed issuer names of the Microsoft Windows domain users, edit the login module option Rule1.issuerName (or add a new option) and enter the allowed X.509 certificate name of the issuer in the *Value* tab.
  - b. To restrict the subject names of the Microsoft Windows domain users running the kiosk desktop that are allowed to access, edit the Rule1.subjectName option (or add a new option) and specify the allowed X.509 certificate name of the subject in the *Value* tab.

### ❖ Example

Values for Login Module Options

Value	Description
(. *)	Allow access to all issuer or subject names
CN=ABC (. *)	Allow access to all issuer or subject names starting with CN=ABC
CN=ABC	Allow access only to issuer or subject name called CN=ABC

If no rule value matches, the authentication fails.

Login Module Option Configuration Examples

Option	Value	Description
Rule1.subjectName	CN=KIOSK (. *)	This configuration allows the distinguished name CN=KIOSK02, O=SHOP, C=US issued by CN=KIOSK ISSUING CA, O=LOCAL, C=DE, but not CN=KIOSK02, O=SHOP, C=US issued by CN=KIOSK ISSUING CA, O=TEST, C=UK.

Option	Value	Description
Rule1.issuerName	CN=KIOSK ISSUING CA, O=LOCAL, C=DE	

7. Save your changes.

You have now configured SSL-based X.509 certificate authentication of your domain user running the kiosk desktop at a Microsoft Windows domain controller.

### 4.23.5.3 Configuring Secure Login Server for RFID Identification

The Secure Login Server needs a dedicated LDAP destination for the user mapping of the user attributes you set in Active Directory. This makes sure that the UIDs from the RFID tokens of the employees who want to log on to the kiosk application are identified as authorized users in the authentication profile stored in a policy configuration. The policy download agent pushes this profile to the kiosk PCs.

#### Context

You must create an LDAP destination with connection data and an LDAP server authentication for user mapping. The Secure Login Server searches for UIDs of RFID tokens in the defined search base DN and in its subtrees. If you want to perform user login ID mapping in multiple domains, see the related link.

#### Procedure

1. Open the Secure Login Administration Console.
2. Go to the [Destination Management](#) tab and create an LDAP destination (see the related link).
3. Enter the required connection data and the LDAP server authentication (see the related link).
4. Go to the [Authentication Profile](#) tab to create a authentication profile for the Secure Login Client.
  - a. Choose [Create](#), and the wizard for the creation of a authentication profile starts.
  - b. Choose the respective policy configuration name in the [User Authentication](#) section.
  - c. Choose the profile type for RFID identification in the [Client Configuration](#) section of the wizard. Depending on the reader type you are using, you choose one of the following values:
    - o [RFID \(WaveID based\)](#)
    - o [RFID \(PCSC based\)](#)
  - d. Complete the creation of the client authentication in the wizard.
5. To configure user mapping for the employees who want to log on to the kiosk application, edit the authentication profile once again.
6. Go to the [Certificate Configuration](#) tab, expand the [User Logon ID Mapping \(Optional\)](#) section, and activate [Enable User Logon ID Mapping](#).

- a. Add the LDAP destinations to the [Mapping Destinations](#) table.
- b. Enter the user attribute in the [LDAP Search Attribute](#) field. You configured the user attribute earlier in Active Directory. It contains the UIDs of the employees' RFID tokens. The user attribute provides the user name for user mapping.

#### ❖ Example

extensionAttribute15

- c. Choose the search value ([PKCS10:CN](#)).
  - d. Go to the [Mapping Attributes](#) section and enter all the LDAP attributes you want to appear in your certificates. For more information on mapping with added attributes, see the related link.
  - e. Configure the user certificate attribute and save the authentication profile.
7. Go to the [User Profile Groups](#) section to create a profile group (see the related link) and add the authentication profile for RFID tokens.
- You have now configured the authentication profile for the RFID tokens of the employee who want to log on to the kiosk application, and you prepared it for being downloaded to the kiosk PCs.

## Related Information

[Creating Destinations \[page 197\]](#)

[Parameters for Destination Management Configuration \[page 308\]](#)

[\(Optional\) Configuring the User Logon ID Mapping with Added Attributes \[page 210\]](#)

[Creating a Profile Group of Authentication Profiles \[page 145\]](#)

[LDAP User Mapping with Multiple Search Base DNs \[page 215\]](#)

## 4.23.5.4 Enabling Secure Login Client for RFID Identification

The authentication profile for RFID identification you created earlier in the Secure Login Server contains all the settings the Secure Login Client of the kiosk PCs needs for RFID identification.

### Context

Distribute the RFID client authentication policy to the kiosk PCs that are intended to support RFID identification.

### Procedure

Use the policy download agent or profile groups to download Secure Login Server policies to the registry of the kiosk PCs. For more information, see the related link.

## Related Information

[Downloading Policies to the Secure Login Client \[page 142\]](#)

# 5 Secure Login Client

The Secure Login Client is a client application that provides security tokens (Kerberos and X.509 technology) for a variety of applications.

## 5.1 Secure Login Client Installation

This section explains the installation and the installation options of the Secure Login Client.

### Context

An installation of the Secure Login Client in a Citrix XenApp environment does not require any special steps or settings.

(Optional) If, in the case of a new installation, you want to use the policy download agent for getting the client policy configuration from Secure Login Server to Secure Login Client, you must take care that you fulfill the following prerequisites.

- You have deployed the new policy URL (located in the policy group settings) before you execute SAPSetup. SAPSetup restarts the policy download service and pulls the client configuration from Secure Login Server.
- You have established SSL trust in the clients by having imported the SSL host certificate. For more information, see related link.

### Procedure

1. To download the SAP Single Sign-On software from the ONE Support Launchpad, go to <https://support.sap.com/swdc>.
2. Go to the ONE Support Launchpad and choose ► [Software Downloads](#) ► [Support Package and Patches](#) ► [By Category](#) ► [SAP NetWeaver and complementary products](#) ► [SAP Single Sign-On](#) ► [SAP Single Sign-On 3.0](#) ►. Choose SAP Single Sign-On 3.0 and download the package.

#### i Note

You find the most recent installation package in ► [Support Packages and Patches](#) ► [Comprised Software Component Versions](#) ►.

3. You find the installation package `SAPSetupSLC.exe` in the compressed download file.

4. Extract it and start `SAPSetupSLC.exe` to install Secure Login Client.

The Secure Login Client installation package of the Secure Login Client component contains the following options

Installation Options of Secure Login Client

Option	Description
<a href="#">SAP Secure Login Client</a>	This option installs the basic components of Secure Login Client. This feature is mandatory.
<a href="#">Start during Microsoft Windows login</a>	Option for an installation under Citrix XenApp, see related link.
<a href="#">Secure Login Server Support</a>	This option installs authentication support with Secure Login Server. Based on the provided user credentials, the Secure Login Server provides user certificates to the Secure Login Client. If you choose <a href="#">Secure Login Server Support</a> , it comes together with the options <a href="#">Crypto &amp; Certificate Store Providers</a> , <a href="#">Policy Download Agent</a> , and Web Adapter mode. In the integrated Web Adapter mode, you enable the Secure Login Client to create and store private keys for the Secure Login Web Client.
<a href="#">Kerberos Single Sign-On</a>	This feature installs the Kerberos authentication support. To hide the Kerberos profile, do not install this feature.

5. To continue, choose [Next](#).
6. Choose [Install](#).

Close the window of the installation package. The Secure Login Client starts automatically when a user logs on.

7. (If applicable) Distribute the installation with SAPSetup means.

## Related Information

[Secure Login Client for Citrix XenApp \[page 162\]](#)

[Option 1: Installing Root CA Certificates on a Windows Client \[page 139\]](#)



## 5.1.1 Unattended Installation with SAPSetup Installation Server

This topic describes how you run an unattended installation of Secure Login Client with the SAPSetup Installation Server.

### Context

You use the SAPSetup Installation Server to distribute SAP front-end software on multiple workstations across the network. You can create your own installation package or deploy Secure Login Client on multiple clients.

An administrator has several possibilities to distribute Secure Login Client to various clients.

- Create a dedicated installation package for distribution among multiple clients using SAPSetup Installation Server.
- Deploy Secure Login Client on multiple clients using SAPSetup Installation Server.

#### i Note

If you customize the installation paths in the SAP Installation Server, you must take care that the paths for the 64-bit and 32-bit versions of Microsoft Windows point to different destination directories. The following variables contain the installation paths:

- `<SapSLCDestDir>`  
Installation path for Microsoft Windows 32-bit
- `<SapSLC64BitDestDir>`  
Installation path for Microsoft Windows 64-bit

#### ! Restriction




An unattended installation with SAPSetupSLC package delivered by SAP only includes the preselected (default) installation options. An administrator cannot select or unselect options.

As an example, an administrator can create a dedicated installation package on a central installation server and then distribute it among the clients.

#### ⚠ Caution

When you install Secure Login 2.0, you uninstall an old MSI-based Secure Login Client 1.0.

### Procedure

1. Start SAPSetup as described in <http://service.sap.com/sltoolset>  *Software Logistics Toolset 1.0*  *SAPSetup* .
2. Use the method that suits you best to distribute Secure Login Client to the client workstations.

## 5.2 Uninstalling Secure Login Client

There are multiple ways to uninstall Secure Login Client.

- Using Control Panel in your Microsoft Windows operating system
- Using SAP Setup
- Using a command line tool

### 5.2.1 Uninstalling Secure Login Client with Microsoft Windows Control Panel

You can uninstall Secure Login Client using Control Panel of Microsoft Windows.

#### Procedure

1. Start [Control Panel](#) in your Microsoft Windows operating system.
2. Choose the option for uninstalling a program
3. Select the row for Secure Login Client.
4. Choose the button for uninstallation.
5. Follow the instruction of the wizard.

You have now uninstalled your Secure Login Client.

### 5.2.2 Uninstalling Secure Login Client with SAPSetup

Here you find a description how you uninstall Secure Login Client using SAPSetup.

#### Context

If you want to uninstall Secure Login Client, you can use SAPSetup. For more information on SAPSetup, see [related link](#).

#### i Note

SAPSetupSLC is a default SAPSetup. It support all default parameters and arguments.

## Procedure

1. Start `SAPSetupSLC.exe`.
2. Unselect all options.
3. The wizard guides you through the uninstallation.

## Related Information

[Secure Login Client Installation \[page 132\]](#)

<http://service.sap.com/sltoolset> 

## 5.2.3 Uninstalling Secure Login Client with a Command Line Tool

Here you find a description how you uninstall Secure Login Client using a command line tool.

## Context

You can uninstall Secure Login Client with the command `NwSapSetup.exe`. It is located in the installation directory.

Microsoft Windows 32 bit:

```
%ProgramFiles%\SAP\SapSetup\setup
```

Microsoft Windows 64 bit:

```
%ProgramFiles(x86)%\SAP\SapSetup\setup
```

### **i** Note

`NwSapSetup.exe` also offers a repair function. Use the following command:

```
NwSapSetup.exe /product:"SLC" /repair
```

For an uninstallation, proceed as follows:

## Procedure

1. Start a command prompt.

2. Enter the uninstallation command.

#### ❖ Example

```
NwSapSetup.exe /product:"SLC" /uninstall /nodlg
```

You have uninstalled Secure Login Client.

## 5.3 Updating the Secure Login Client to the Support Package

To update the Secure Login Client to the current support package, take the following steps.

### Context

You can download the support package software from the SAP Service Marketplace. You do not need to uninstall the existing version of the Secure Login Client. You simply run the installation software and overwrite your existing Secure Login Client.

### Procedure

1. Go to <https://support.sap.com/swdc>.
2. Choose ► *Support Package and Patches* ► *Software Downloads* ► *By Category* ► *SAP NetWeaver and complementary products* ► *SAP Single Sign-On* ► *SAP Single Sign-On 3.0* .

#### i Note

The file name of the installation kit indicates the support package, the patch level number, and a temporary download ID is appended.

3. Start the installation as described in the related link.
4. To display the version number of your software, right-click the blue diamond of the Secure Login Client in the Microsoft Windows notification area.
5. Choose *About Secure Login...*. The version number 3.0, support package, and the patch level are displayed.

### Related Information

[Secure Login Client Installation \[page 132\]](#)

## 5.4 Adding Root Certificates during Installation

This section describes how to integrate the installation of the Secure Login Server root CA certificate (Microsoft Certificate Store) for the Secure Login Client into software distribution tools.

### Context

#### i Note

The customized aspects of this installation are associated only with the integration with Secure Login Server.

To export a root CA certificate from the Secure Logon Server, proceed as follows:

### Procedure

1. Open the Secure Login Administration Console.

```
https://<host_name>:<port>/webdynpro/resources/sap.com/securelogin.ui/Main
```

#### Example

```
https://example.com:50001/webdynpro/resources/sap.com/securelogin.ui/Main
```

2. Go to the [Certificate Management](#) tab.
3. Select the root CA you want to export.
4. Choose the [Export Entry](#) button.
5. Choose the export format [X.509 Certificate](#). This means that the exported certificate file has the file extension .cert.

The dialog box displays the file name, type, size, and the download link.

#### i Note

You might be prompted to enter and confirm a password to encode the entry file.

6. Choose [Download](#) button.
7. (Optional) Rename the file so that it indicates the origin of the root CA certificate.
8. Save it in a location of your choice.

## 5.4.1 Option 1: Installing Root CA Certificates on a Windows Client

To ensure secure communication and a trust relationship, you install root CA certificates on Windows clients.

### Context

In the client environment, you need to install the root CA certificate from Secure Login Server or the certificate of the SSL root CA. The root CA certificate is used to establish secure communication to the Secure Login Server.

To make sure that you can download policies from Secure Login Server to the clients using the policy download agent, you must establish SSL trust by importing an SSL host CA certificate to the clients.

### Procedure

Use the Microsoft CertMgr tool, which is part of the Microsoft Windows Software Development Kit (SDK,) to import certificates. In a system with a Secure Login Client installation, use the following command to import a certificate:

Syntax

```
certmgr.exe /add /all /c <root_CA_file> /s ROOT /r localMachine
```

The root CA certificate is provided by the Secure Login Server.

#### ❖ Example

```
certmgr.exe /add /all /c SLS_RootCA.crt /s ROOT /r localMachine
```

```
certmgr.exe /add /all /c SSL_host_RootCA.crt /s ROOT /r localMachine
```

## 5.4.2 Option 2: Distributing Root CA Certificates on Microsoft Domain Server

### Context

To distribute Secure Login Server root CA certificates to all clients in Active Directory, proceed as follows:

### Procedure

1. Log on to the Microsoft Domain Server as administrator.
2. Start the command prompt in Microsoft Windows.
3. Use the following command:`certutil -dsPublish -f <root_CA_file> RootCA`
4. Restart your client.  
After a restart the group policies are updated. This pushes the certificates to the client. To do so, you can also use the command `gpupdate /force`.

## 5.4.3 Option 3: Distribute Secure Login Server Root CA Certificates Using Microsoft Group Policies

This topic shows you how to distribute Secure Login Server root CA certificates using Microsoft Group Policies

Use the corresponding procedure in the related link.

### Related Information

[Distributing Root CA Certificates Using Microsoft Group Policies with Microsoft Windows Server 2008/2008 R2 \[page 141\]](#)

[Distributing Root CA Certificates Using Microsoft Group Policies with Microsoft Windows Server 2003/2003 R2 \[page 141\]](#)

### 5.4.3.1 Distributing Root CA Certificates Using Microsoft Group Policies with Microsoft Windows Server 2008/2008 R2

These steps describe how to distribute root CA certificates using Microsoft Group Policies.

#### Context

To distribute Secure Login Server root CA certificates using Microsoft Group Policies, take the following steps:  
Microsoft Windows Server 2008/2008 R2

#### Procedure

1. Open the Control Panel in Microsoft Windows.
2. Go to the administrative tools.
3. Open the Group Policy Management Editor.
4. Navigate to ► *Forest* ► *Domain* ►. Choose the domain name. To edit the default domain policy, right-click *Edit...*
5. Go to ► *Computer Configuration* ► *Policies* ► *Windows Settings* ► *Security Settings* ► *Public Key Policies* ► *Trusted Root Certification Authorities* ►.
6. Import the root CA certificate of the Secure Login Server.
7. Restart your client.  
After a restart the public key and group policies are updated. This pushes the certificates to the client. To do so, you can also use the command `gpupdate /force`.

### 5.4.3.2 Distributing Root CA Certificates Using Microsoft Group Policies with Microsoft Windows Server 2003/2003 R2

These steps describe how to distribute root CA certificates using Microsoft Group Policies.

#### Context

To distribute Secure Login Server root CA certificates using Microsoft Group Policies, take the following steps:  
Microsoft Windows Server 2003/2003 R2



## Procedure

1. Open the Control Panel in Microsoft Windows
2. Go to *Administrative Tools*.
3. Open *Domain Security Policy*.
4. Go to ► *Security Settings* ► *Public Key Policies* ► *Trusted Root Certification Authorities* ►.
5. Import the root CA certificate of the Secure Login Server.
6. Restart your client.  
After a restart the public key and group policies are updated. This pushes the certificates to the client. To do so, you can also use the command `gpupdate /force`.

## 5.5 Downloading Policies to the Secure Login Client

If you have installed Secure Login Server and maintained the policies for client authentication there, the Secure Login Client needs the client authentication policies of the Secure Login Server.

Among other things, the client authentication policies contain the policy URL, the enroll URL, the client profile and the settings for the authentication of the client. You must download the policies to the Secure Login Client. After having downloaded the policies to the Secure Login Client, you have updated the registry of your client PCs with the new policy.

You can use different options for downloading the policies for the Secure Login Client.

### 5.5.1 Downloading Policies to Secure Login Client Using Profile Groups

The Secure Login Client needs the client authentication policies of the Secure Login Server.

## Context

You need to get the policies of the authentication profile from Secure Login Server for the Secure Login Client. This is possible if you use profile groups. A profile group contains one or several authentication profiles. Each authentication profile defines a number of policies that determine the behavior of the client. If you download the policies to the Secure Login Client, the Secure Login Administration provides registry files (\*.reg), two per profile group. Import these registry files into the clients you want to migrate to the policies of SAP Single Sign-On 3.0. The Secure Login Client uses the new policies after a restart.

Proceed as follows:

## Procedure

Create a profile group with the authentication profiles of Secure Login Server. For more information, see related link.

## Related Information

[Creating a Profile Group of Authentication Profiles \[page 145\]](#)

[Enable Fully Qualified Distinguished Name in Enrollment URL \[page 340\]](#)

## 5.5.2 Downloading Policies to Secure Login Client Using the Policy Download Agent

Secure Login Client gets the client authentication policies from the Secure Login Server in regular intervals using the policy download agent.

## Context

### ⚠ Caution

If the client PCs in your enterprise are connected using VPN or Wi-Fi, or if they are never shut down, it makes sense to choose a different policy update interval, for example, one of the following:

- Your average working hours in minutes
- The whole day in minutes

Prerequisites:

- You have checked the [Secure Login Server Support](#) option during the Secure Login Client installation. This activates the policy download agent.
- If you have clients on Microsoft Windows, you have established an SSL trust relationship with your clients by having imported the relevant SSL host CA certificates. For more information, see the related link.

## Procedure

1. Create a profile group with the client authentication profiles of Secure Login Server. For more information, see related link.

2. Download the file `ProfileDownloadPolicy_<profile_group>.reg` to import the policy URL and the settings into the clients.
3. Distribute the registry file with the distribution mechanisms you usually use.  
After the distribution, the registry file imports all the client authentication parameters into the registry of the respective clients.
4. Restart the client systems or restart the Secure Login service to get the configuration into the clients.

## Related Information

[Creating a Profile Group of Authentication Profiles \[page 145\]](#)

[Enable Fully Qualified Distinguished Name in Enrollment URL \[page 340\]](#)

[Option 1: Installing Root CA Certificates on a Windows Client \[page 139\]](#)

[Client Policy \[page 274\]](#)

### 5.5.2.1 Start during Windows login

The Secure Login Client starts automatically when a user logs on to a Microsoft Windows operating system. Remember that this automatic startup increases memory and CPU consumption.

If you unselect the installation option [Start during Windows login](#), the Secure Login Client does not start automatically.

### 5.5.2.2 Using Certificates for CAPI Applications

You only need this feature if you want to use certificates issued for CAPI applications by the Secure Login Server, such as for a client authentication with Internet Explorer. The CSP/CAPI service is registered during the installation.

### 5.5.2.3 Downloading Policies from the Secure Login Server

To automatically download client policies from the Secure Login Server, install the [Secure Login Server Support](#) feature. It includes the [Policy Download Agent](#). For more information, see related link.

## Related Information

[Secure Login Client Installation \[page 132\]](#)

## 5.5.3 Creating a Profile Group of Authentication Profiles

Profile groups in the Secure Login Server contain the authentication profiles.

### Context

Download the client authentication policies of the Secure Login Server to the Secure Login Client in a profile group. One client can only belong to one profile group.

To create a profile group and to download the profiles to clients, proceed as follows:

### Procedure

1. Open the Secure Login Administration Console of SAP NetWeaver Single Sign-On.

```
https://<host_name>:<port>/webdynpro/resources/sap.com/securelogin.ui/Main
```

#### ❖ Example

```
https://example.com:50001/webdynpro/resources/sap.com/securelogin.ui/Main
```

2. Go to the [Authentication Profiles](#) tab.
3. Select [User Profile Groups](#) in the toolbar below the tabs.
4. Choose the [Create](#) button.
5. Enter a name and a description for the profile group.
6. Enter the parameters for the download mode of the profile groups and policies.

Among other things, they contain the protocol, the port, the interval after which the policy is updated, the network timeout, and the setting when the policy is updated.

Consider that when Secure Login server is configured to allow only secure communication, you can only choose the HTTPS protocol.

For more information, see the corresponding documents in the related links.

7. If required, add more authentication profiles.
8. Choose [Download Policy](#). The subsequent popup displays the following registry files:
  - ProfileGroup\_<profile\_group\_name>.reg  
This file includes the configuration of all authentication profiles in the profile group. If there are any changes in the profiles, download the most recent registry file and re-install the Secure Login Client for the changes to take effect. You find an overview of the client authentication parameters in the related link.
  - ProfileDownloadPolicy\_<profile\_group\_name>.reg  
This file includes the policy URL that specifies the resource file that includes the latest configuration of all authentication profiles in the profile group. If there are any changes in the profiles, the most recent configuration is automatically updated in the Secure Login Client after a defined time (policy update interval).

9. Distribute the registry files with the distribution mechanisms you usually use.  
After the distribution, the registry file imports all the client authentication parameters into the registry of the respective clients.
10. Start the Secure Login Server. In intervals defined in the profile group parameters, the Secure Login Client retrieves the policies of respective profile group from the Secure Login Server.

## Related Information

[Parameters for Client Configuration \[page 281\]](#)

[Parameters for Downloading Policies Using Profile Groups \[page 292\]](#)

[Configuring Secure Communication \[page 223\]](#)

## 5.6 Getting User-Specific Profiles for Certificate Enrollment

On a specially configured Secure Login Client, users can quickly get a list of profiles to enroll with certificates by selecting a user-specific authentication profile from a list in the Secure Login Client. The profiles are downloaded from the Secure Login Server the users specify in the server URL.

Users who, for example, work in several projects simultaneously need to access several resources by using several user profiles. They can quickly get the relevant profiles for certificate enrollment by selecting a project-related profile group from a list in the Secure Login Client. All these profiles are stored in a profile group in the Secure Login Server, which the users identify by entering the host name and port number.

### 5.6.1 Configuring User-Specific Profile Download in Secure Login Client

User-specific profile download to a Secure Login Client is no default feature. For this reason, you must configure it individually in the registry of the client.

## Context

### Prerequisites

Server	<ul style="list-style-type: none"> <li>Secure Login Server 2.0 SP03 or higher on an SAP Application Server Java</li> </ul>
Client	<ul style="list-style-type: none"> <li>Secure Login Client 2.0 SP03 or higher (running on a Windows platform)</li> <li>SAP GUI</li> </ul>

To enable users to select a profile from the Secure Login Server in their Secure Login Client, take the following steps:

## Procedure

1. Go to the client's registry in administration mode and open it.
2. Enter the parameter **ShowUserPoliciesPage** with the value **1** in the registry path `[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\Common]`.

### ! Restriction

Since this is no default registry parameter, you must enter the parameter and the value manually. You cannot download the parameter from the Secure Login Server.

After this client configuration, your client displays the *Policy Groups* tab where users can select a profile group provided by the Secure Login Server. The profile group contains the profiles users can select in the Secure Login Client.

## 5.6.2 Downloading User-Specific Profile Groups to the Secure Login Client

In Secure Login Client, users can quickly get a list of profiles for certificate enrollment by selecting a user-specific profile from the list in the Secure Login Client.

## Context

For details on the policy download settings for the client, see the related link.

To download profile groups with the user-specific profiles to the Secure Login Client, take the following steps:

## Procedure

1. Choose **File > Options...** in the Secure Login Client.
2. Go to the *Policy Groups* tab.
3. You identify the Secure Login Server that provides the profiles.
  - a. Enter the server URL using host name and port number in the *Host* field.

### ❖ Example

```
https://<host_name>:<port>
```

- b. (If applicable) If your Secure Login Server uses the proxy settings stored in the Microsoft Internet Explorer, you only need to select [Use IE Proxy Settings](#).
  - c. If you want to any other proxy settings, select [Use Manual Proxy Settings](#) and enter them.
4. Choose [Refresh](#) to download the list with the predefined profile groups from this Secure Login Server. The [Group](#) field displays a dropdown list of all profile groups provided by the Secure Login Server.
5. Select a profile and choose [Apply](#) and/or [OK](#).  
The profiles of this profile group appear in your Secure Login Client, and you can choose one of the profiles for certificate enrollment.
6. (If applicable) If you want to delete the list of profile groups in the Secure Login Client, choose [Clear](#).

## Related Information

[Parameters for Downloading Policies Using Profile Groups \[page 292\]](#)

## 5.7 Configuration Options

This topic deals with several configuration options of the Secure Login Client.

Among other things, this section describes how to enable SNC in SAP GUI, how to define the user mapping in SAP user management, and how to support smart cards.

### 5.7.1 Enable SNC in SAP GUI

Using SNC in SAP GUI

#### Context

To establish secure communication between SAP GUI and SAP Netweaver Application Server; you need to enable the SNC option.

#### Procedure

Start the SAP GUI application, create or open a system entry; enable the SNC option, and define the SNC name of the Application Server ABAP.

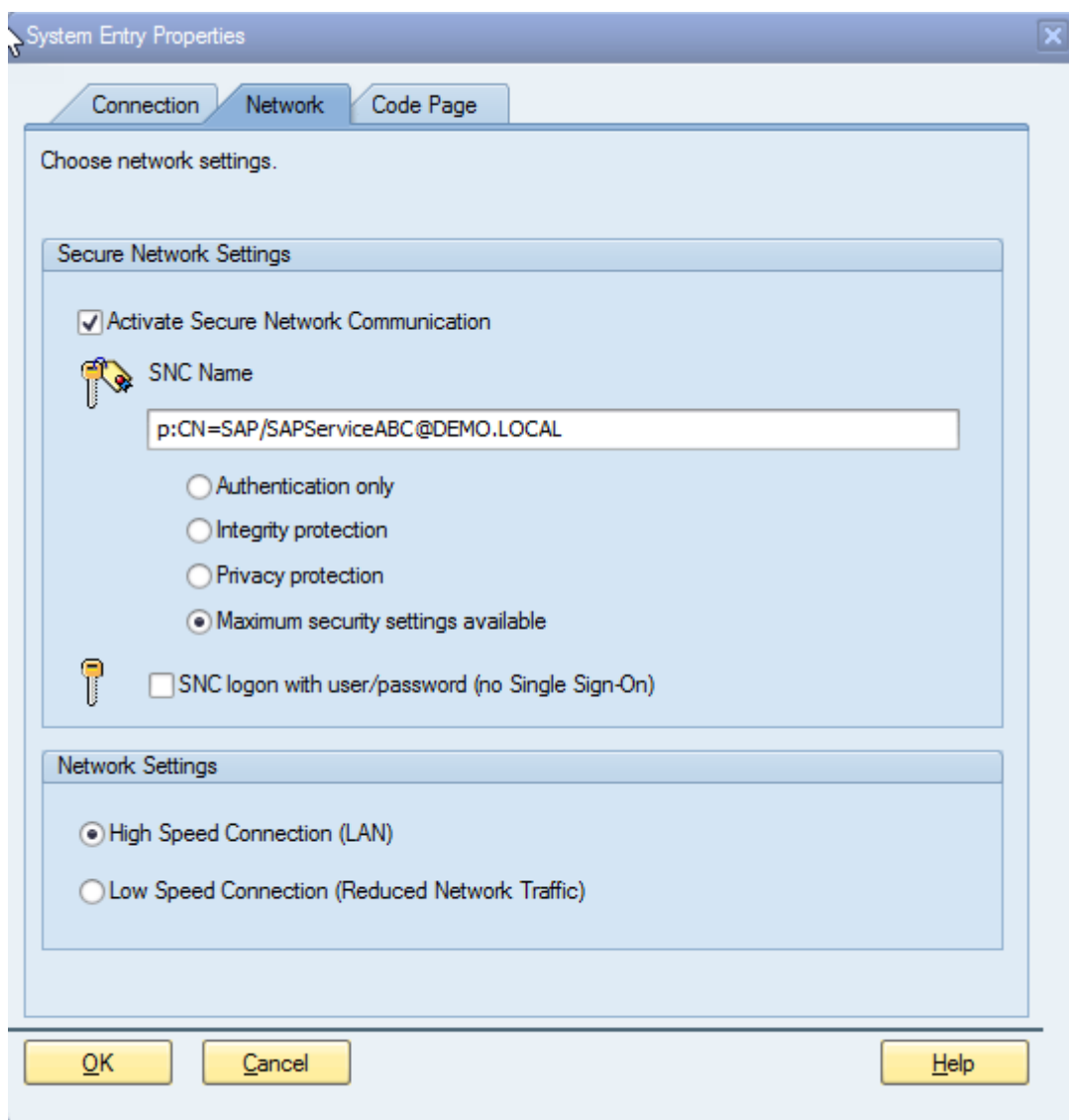
## 5.7.1.1 Kerberos SNC Name

### Procedure

1. Choose the option *Activate Secure Network Communication* and define the SNC Name as Service Principal Name.

Example SNC Name:

p:CN=SAP/SAPServiceABC@DEMO.LOCAL



The SNC name is provided by your SAP NetWeaver Administrator. Note that the definition of the SNC name is case-sensitive.



2. (If applicable) If your Secure Login Client has multiple profiles, you can determine that you want to use a selected profile for a specific application server. For more information, see the related link.

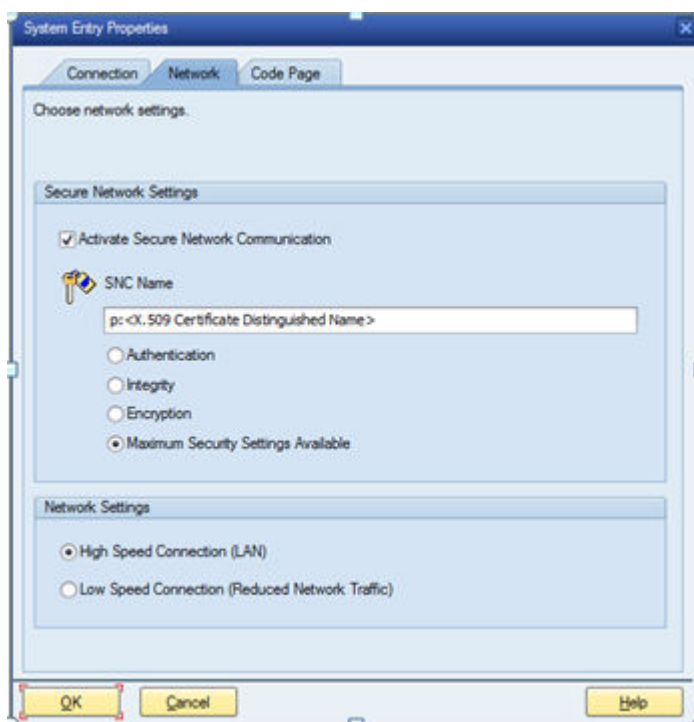
## Related Information

[Application Policy Settings for Kerberos and Microsoft Cryptography API \(CAPI\) Token \[page 254\]](#)

### 5.7.1.2 X.509 Certificate SNC Name

#### Procedure

1. Choose the option *Activate Secure Network Communication* and define the SNC name.



Example SNC Name:

p:CN=ABC, OU=SAP Security

The SNC name is provided by your SAP NetWeaver administrator. Note that the definition of the SNC Name is case-sensitive.

2. (If applicable) If your Secure Login Client has multiple profiles, you can determine that you want to use a selected profile for a specific application server. For more information, see the related link.

## Related Information

[Application Policy Settings for Kerberos and Microsoft Cryptography API \(CAPI\) Token \[page 254\]](#)

## 5.7.2 User Mapping

This section describes how to define the user mapping in SAP user management. For the user authentication using security tokens (X.509 certificate or Kerberos token), this mapping is required to define which security token belongs to which SAP user.

### → Tip

For smooth and straightforward integration, we recommend that you use the SAP Identity Management solution to manage user mapping.

### 5.7.2.1 Manual Configuration

The user management enables you to enter the SNC name in the AS ABAP.


## Procedure

1. Start the user management tool by calling transaction `SU01`. Choose the *SNC* tab.
2. If you are using Kerberos authentication, enter the Kerberos user name in the *SNC name* field.
3. If you are using *X.509* certificate based authentication, enter the X.509 certificate Distinguished Name in the *SNC name* field.

### i Note

Note that the definition of the SNC name is case-sensitive.

### i Note

You can enable only certain administrators to change the SNC name in `SU01` by implementing the SAP Note [1882254](#) .

### 5.7.2.1.1 Kerberos Example

In this example, the SNC name `p:CN=MICROSOFTUSER@DEMO.LOCAL` belongs to the user "SAPUSER".

**Maintain User**

User: SAPUSER

Last Changed On: DDIC 08.05.2011 20:11:23 Status: Saved

Address Logon data **SNC** Defaults Parameters Roles Profiles Gr...

**SNC Status**

OO ☒ SNC is active on this application server

Unsecure logon is allowed depending on the user (snc/accept\_insecure\_gui)

**SNC data**

SNC name: p:CN=MICROSOFTUSER@DEMO.LOCAL

☒ Canonical name determined

☐ Unsecure communication permitted (user-specific)

### 5.7.2.1.2 X.509 Certificate Example

In this example the *SNC name* **p:CN=SAPUSER, OU=SAP Security** belongs to the user "SAPUSER".

**Maintain User**

User: SAPUSER

Last Changed On: DDIC 08.05.2011 20:11:23 Status: Saved

Address Logon data **SNC** Defaults Parameters Roles Profiles Gr...

**SNC Status**

OO ☒ SNC is active on this application server

Unsecure logon is allowed depending on the user (snc/accept\_insecure\_gui)

**SNC data**

SNC name: p:CN=SAPUSER, OU=SAP Security

☒ Canonical name determined

☐ Unsecure communication permitted (user-specific)

### 5.7.2.2 Set External Security Name for All Users

You can use transaction SNC1 (report RSUSR300) to configure the SNC name in batch mode.

### i Note

Note that the definition of the SNC name is case-sensitive.

With this tool you can choose all SAP Users by specifying \*. You receive a list of SAP users or SAP user groups. You can use the option *Users without SNC names only* to overwrite SNC names.

This batch tool takes an SAP user and uses the components

<previous\_character\_string><SAP\_user\_name><next\_character\_string> to build the SNC name.

## 5.7.2.2.1 Kerberos Example

In this example, SNC names are generated with the following string for all users without an SNC name:

p:CN=<user\_name>@DEMO.LOCAL

The screenshot shows the 'Set External Security Name for All Users' tool interface. It has a title bar with a clock and a help icon. Below the title bar, there are two rows of input fields. The first row is labeled 'Users' and has a text box containing an asterisk (\*). To its right is a 'to' label and another empty text box. To the right of the 'to' label is a yellow button with a right-pointing arrow. The second row is labeled 'User group' and has an empty text box. To its right is a 'to' label and another empty text box. To the right of the 'to' label is a yellow button with a right-pointing arrow. Below these rows is a checkbox labeled 'Users without SNC names only' which is checked. At the bottom, there are two text boxes. The first is labeled 'Previous character string' and contains the text 'p:CN='. The second is labeled 'Following character string' and contains the text '@DEMO.LOCAL'.

## 5.7.2.2.2 X.509 Certificate Example

In this example SNC names are generated with the following string for all users without an SNC name:

p:CN=<user\_name>, OU= SAP Security

The screenshot shows the 'Set External Security Name for All Users' tool interface. It has a title bar with a clock and a help icon. Below the title bar, there are two rows of input fields. The first row is labeled 'Users' and has a text box containing an asterisk (\*). To its right is a 'to' label and another empty text box. To the right of the 'to' label is a yellow button with a right-pointing arrow. The second row is labeled 'User group' and has an empty text box. To its right is a 'to' label and another empty text box. To the right of the 'to' label is a yellow button with a right-pointing arrow. Below these rows is a checkbox labeled 'Users without SNC names only' which is checked. At the bottom, there are two text boxes. The first is labeled 'Previous character string' and contains the text 'p:CN='. The second is labeled 'Following character string' and contains the text ', OU=SAP Security'.

## 5.7.3 Overview of Registry Configuration Options

This section describes further configuration options in registry for the Secure Login Client.

You can make the following settings:

- Common settings
- Application policy settings for Kerberos and Microsoft Cryptography API (CAPI) token
- CAPI settings
- Single Sign-On settings for Kerberos-based SNC profile
- Single Sign-On settings for SPNego profile

For more information, see the related links.

### Related Information

[Common Settings \[page 251\]](#)

[Application Policy Settings for Kerberos and Microsoft Cryptography API \(CAPI\) Token \[page 254\]](#)

[CAPI Settings \[page 257\]](#)

[Single Sign-On Setting for Kerberos-Based SNC Profile \[page 262\]](#)

[Single Sign-On Setting for SPNego Profile \[page 265\]](#)

## 5.7.4 Automatically Using the Proxy Configuration of Microsoft Internet Explorer for Secure Login Client

For reasons of simplicity, you want use the proxy settings of your Microsoft Windows domain. Secure Login Client can auto-detect the proxy settings in the Internet connection configuration of Microsoft Internet Explorer.

Secure Login Server can use the following proxy server configuration options from Microsoft Internet Explorer:

- Automatic proxy server detection
- Using an automatic proxy configuration script URL

### **i** Note

These detection options correspond to the following proxy server settings in Microsoft Internet Explorer in

► [Tools](#) ► [Internet Options](#) ► [Connections](#) ► [LAN settings](#) ►:

- [Automatically detect settings](#)
- [Use automatic configuration script](#)

If the first detection option is not successful and does not return a proxy server, Secure Login Client continues and looks for a proxy URL in the automatic configuration script. If it does not find a valid proxy URL there either, it falls back on directly accessing the Internet without using a proxy server.

## ! Restriction

Using the proxy configuration of the operating system is only possible if you use Microsoft Internet Explorer in a Microsoft Windows environment with Secure Login Client and Secure Login Server, both 2.0 SP02 or higher. SAP Single Sign-On does not support a static proxy server setting for LANs.

## Related Information

[Configuring Automatic Proxy Server Detection \[page 155\]](#)

### 5.7.4.1 Configuring Automatic Proxy Server Detection

To configure automatic proxy server detection from Microsoft Internet Explorer for Secure Login Client enrollment URL, you must change your clients' configuration.

## Context

## Procedure

1. Start the Secure Login Administration Console.
2. Choose the authentication profile for which you want to configure proxy server auto-detection.
3. Choose the *Secure Login Client Settings* tab.
4. Choose the *Edit* button.
5. Choose the *HTTP Proxy URL* field and enter **AUTO**. For more information, see the related link.
6. Save your changes.

The Secure Login Server generates the configuration for automatically using the proxy settings of Microsoft Internet Explorer for the Secure Login Clients. The configuration flag is distributed with the policy download mechanism. The client registry gets the following new parameter in the Registry path

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\profiles  
\<authentication_profile_name>].
```

```
"useWindowsHttpProxy"=dword:00000001
```

## Related Information

[Parameters for Client Configuration \[page 281\]](#)

## 5.7.4.2 Configuring Proxy Auto-Config (PAC) Support for Policy Download

To configure the use of a proxy server using a proxy auto-config (PAC) URL for Secure Login Client policy download, you must change your clients' configuration.

### Context

You can configure the proxy URL settings for each profile group.

### Procedure

1. Start the Secure Login Administration Console.
2. Choose the *User Profile Groups* section in the *Profile Management* tab.
3. Select the relevant profile group.
4. Choose the *Edit* button.
5. Enter the URL of your proxy in the *HttpProxyURL* field.

#### ❖ Example

`http://example.address.com:8888/wpad.dat`

6. To use this proxy URL as a proxy auto-config (PAC) URL, select *Yes*.
7. Save your changes.  
At policy down, the client registry gets the following new parameter in the registry path  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\System].

```
"ProxyIsPACURL"=dword:00000001
```

```
"HttpProxyURL"="http://example.address.com:8888/wpad.dat"
```

For more information on the registry parameters, see the related link.

### Related Information

[Client Policy \[page 274\]](#)

## 5.7.5 Using Secure Login Client Profiles for Kerberos and Microsoft Cryptography API Tokens

You want clients in a Microsoft Windows environment to be able to log on to servers using Secure Login Client profiles for Kerberos and Microsoft Cryptography API tokens. The profiles have not been uploaded from the Secure Login Server. The registry of a client contains the parameters and values of the client profile that is assigned to a specific Application Server ABAP.

A customer wants to use Secure Login Client profiles that are not uploaded from the Secure Login Server (for more information, see the related link). For this reason, the Microsoft Windows registry must contain the respective registry parameters and values. The Secure Login Client uses all of the registry keys in `HKEY_LOCAL_MACHINE\Software\Policies\SAP\SecureLogin\applications` to determine the SNC application policy that is used to define the authentication method for a specific application. You therefore assign one Secure Login Client profile for a dedicated authentication method to a certain application, in this case an AS ABAP. It is possible to distribute these registry parameters to your clients, for example, with Microsoft Group Policies or other suitable means.

These Secure Login Client profiles in the registry enable the respective clients to log on using Kerberos or Microsoft Cryptography API certificates to certain Application Servers ABAP. Parameters specify the SNC names of the Application Servers ABAP, the type of login you want to establish, and the authentication profile.

### ❖ Example

The following examples show excerpts in Microsoft Windows registry format.

- Settings for Kerberos login

The clients use Kerberos to log on to servers whose SNC name contains the elements `CN=ABC`, `OU=TEST`, `O=SAP`, `C=DE`. Users can manually select the authentication profile in the Secure Login Client.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\applications\ABC_Kerberos]
"GssTargetName"="CN=ABC, OU=TEST, O=SAP, C=DE"
"TokenType"="kerberos"
"allowFavorite"=dword:00000001
```

- Settings for X.509 login

The clients use X.509 certificates to log on to servers whose SNC name contains the elements `O=SAP-AG`, `C=DE`. Only certificates in which the Distinguished Name contains `CN=SSO_CA`, `O=SAP-AG`, `C=DE` are used. Users cannot manually select the authentication profile in the Secure Login Client.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\applications\SAP AG_X.509]
"GssTargetName"="CN=CERT, O=SAP-AG, C=DE"
"TokenType"="tokcapi"
"CAPIFilterIssuerDN"="CN=SSO_CA, O=SAP-AG, C=DE"
"allowFavorite"=dword:00000000
```

## Related Information

[Application Policy Settings for Kerberos and Microsoft Cryptography API \(CAPI\) Token \[page 254\]](#)



## 5.7.6 Smart Card Integration

The Secure Login Client can use X.509 certificates stored in smart cards and supports 32-bit and 64-bit cryptographic service providers.

For smart card support, you need to install the relevant smart card middleware. Secure Login Client supports smart cards through the Microsoft Crypto API (CSP) or middleware that is based on mini drivers. The mini drivers automatically publish the certificates, for example, in the Microsoft Certificate Store.

These interfaces are typically also supported by the smart card middleware software.

Checklist for smart card support:

- If required, install smart card reader hardware and PC/SC driver. Typically the smart card reader is usually automatically recognized by the operating system.
- Install smart card middleware software. This middleware software should support the desired smart card. Some smart card vendors provide their own middleware software, and there are some middleware software vendors available who support different kinds of smart cards.

PIN management is handled by the middleware software. A typical situation is a user logging on to a Microsoft operating system using the smart card. This user needs to re-enter the PIN in the browser or in SAP GUI.

Whether the user is able to do this depends on the smart card middleware, which might close the smart card after the logon to Microsoft Windows. For more information, contact your smart card middleware vendor.

## 5.7.7 Tracing Secure Login Client

You can switch on tracing of your Secure Login Client with different trace levels. Analyzing the trace files helps you to find the cause of issues that might occur with the Secure Login Client.

### Context

By default, tracing of the Secure Login Client is disabled. The user does not need administrator rights.

#### → Recommendation

Only use the Secure Login Client trace if an error has occurred and you are investigating the cause of the error. Deactivate the trace after the error was remedied.

The client trace function writes the trace into rotation files located in the trace folder. The maximum size of all trace files for each process is 110 MB (ten backup files and one trace file). Since each Secure Login Client and each SAP GUI gets a new process ID, for example, when it starts up again, you may end up with a large number of trace files. Make sure that you provide enough disk space for the client trace function.

You can perform the following actions for client tracing:

- Configure the trace level
- Determine the trace folder

- Delete all traces
- Open the trace folder, for example, to view the trace files

To switch on and configure client tracing, proceed as follows:

## Procedure

1. Start Secure Login Client.
2. Choose the *Tracing* tab in ► *File* ► *Options* ►.
3. Execute the relevant Secure Login Client trace function.

Secure Login Client Trace Functions

Screen Element	Description
<i>Trace Level</i>	Set the trace level. The following trace levels are available: <ul style="list-style-type: none"> <li>○ Deactivated (no tracing)</li> <li>○ Errors only</li> <li>○ Errors and Warnings</li> <li>○ Errors, Warnings, and Information</li> <li>○ Developer Traces (in the case of issues that must be solved by support staff)</li> </ul>
<i>Location</i>	Path of the trace files
<i>Delete All Traces</i>	This function enables you to delete all trace files at once. You cannot delete traces that are currently in use.
<i>Open Trace Folder</i>	If you choose this, Microsoft Windows Explorer opens, showing the folder where your client traces are located.

4. Choose *OK* or *Apply*.

## 5.7.8 Enabling the Display of LDAP Messages in Secure Login Client

In a Microsoft Windows environment, you can display messages from LDAP in Secure Login Client. If LDAP generates messages, the Secure Login Server interprets them and sends its own messages to the Secure Login Client.

### Context

If LDAP generates a message that has an effect on the authentication, the Secure Login Server receives the LDAP error code. The Secure Login Server produces a message with a text that comes from Secure Login

Server. It sends this text to the client(s). Users who get such a message take action or can contact their administrators and ask them for LDAP support.

The messages from LDAP refer to the following situations:

- After a period of time defined in the LDAP password policy, a user's password has expired.
- The user must perform a password change after a period of time defined in the LDAP password policy.
- The user account is locked, for example, because someone entered a wrong password too often. The LDAP locks this user account after a defined number of unsuccessful password entries.
- After an employee left the company, LDAP locks this employee's user account to prevent unauthorized login.
- A user logs on with correct user name and password at a workstation this user is not authorized for.

### ❖ Example

A user tries to authenticate at a Secure Login Client and gets a message saying that this user's password has expired. The origin of this message is LDAP, where the users are managed. Obviously the password policy in LDAP enforces a password change after a certain period of time. This period of time has expired. LDAP sends the respective message code to SAP Single Sign-On. The Secure Login Server interprets the message code and sends the message `Password expired`. Now the user knows that he or she is supposed to change the password.

### i Note

SAP Single Sign-On supports the following LDAP servers:

- Active Directory (default)
- Oracle Directory Server

Take the following steps to set the parameter for the display of LDAP messages in the Secure Login Client.

## Procedure

1. Start SAP NetWeaver Administrator.
2. Choose the [Configuration](#) tab.
3. Choose [Authentication and Single Sign-On](#).
4. Choose [Components](#).
5. Select the relevant policy configuration of your LDAP server.
6. Choose the [Edit](#) button.
7. Go to the [Login Module Options](#) section of your LDAP policy configuraton.
8. Select **LdapServerType** in the [Name](#) field.
9. Enter the value for your LDAP server.

### ❖ Example

**AD** for Active Directory (default).

**ODSEE** for Oracle Directory Server.

For more information, see the related link.

10. Save your changes.

## Related Information

[Parameters for LDAP Login Modules \[page 287\]](#)

### 5.7.9 SAP Business Client with Secure Login Client

Integration of Secure Login Client in SAP Business Client

Prerequisites

You have installed SAP NetWeaver Business Client 4.0 Patch Level 5 as User Interface Add-On for SAP NetWeaver.

You are using SAP Single Sign-On 2.0 or higher.

You are using on-demand short-term certificates from Secure Login Server.

You can integrate Secure Login Client in SAP Business Client. This means that you can log on to SAP Business Client using the secure login features of SAP Single Sign-On 2.0 or higher.

For more information about the configuration of SAP Business Client, see the relevant SAP NetWeaver release in the SAP Help Portal under ► [Application Help](#) ► [SAP NetWeaver Library: Function-Oriented View](#) ► [Application Server](#) ► [Application Server ABAP](#) ► [UI Technologies in ABAP](#) ► [SAP NetWeaver Business Client](#) ► [Installation and Client Configuration](#) ►.

## 5.7.9.1 Integrating Secure Login Client into SAP Business Client

Use the configuration file to configure that SAP NetWeaver Business uses Client Secure Login Client for authentication.

### Context

As an administrator, you can configure a Secure Login integration by adding the attribute `slc` to the system connection. To add the attribute to the SAP UI Landscape service, proceed as follows:

### Procedure

1. Access the `administrator` configuration file in the SAP UI Landscape format. For more information on how to provide the administrator configuration file, see [Administrator Configuration](#).
2. Create or change your SAP UI Landscape service for system connection, which uses Secure Login Client, and add the attribute `slc="1"`.

#### ❖ Example

```
<Service type="NWBC" uuid="d5bf6876-0ee9-4ae2-8c68-9aeb07081a5e"
name="ABC" url="abcd.acme.com:3206" slc="1">
```

For more information on how to configure SAP UI Landscape services, see [SAP UI Landscape Configuration Guide](#).

## 5.8 Secure Login Client for Citrix XenApp

This section describes how to use the Secure Login Client in a Citrix XenApp environment.

The Secure Login Client supports only 64-bit Microsoft Windows operating systems. See the related link to the Product Availability Matrix for an overview of the supported platforms.

### Use Case

The customer wants to run Secure Login Client in a Citrix XenApp environment.

### Note

Some components are not available in a terminal server installation. For more information, see [Local Security Hub \[page 41\]](#).

## Related Information

<http://support.sap.com/pam>

### 5.8.1 Secure Login Client with a Published Desktop

Secure Login client runs with a published desktop, which similarly to a standard Microsoft Windows desktop.

A published desktop behaves similarly to a standard Microsoft Windows desktop. You can install the Secure Login Client in the same way as on a local Microsoft Windows operating system. To minimize memory and CPU consumption, we recommend that you unselect the feature *Start during Windows login*.

### 5.8.2 Secure Login Client with a Published SAP Logon

The Secure Login Client does not start automatically when a user logs on to a published SAP Logon in a Citrix XenApp environment. When installing, you may unselect the features *Start during Windows login*.

#### 5.8.2.1 How to Enable Automatic Startup with a Published SAP Logon

This topic describes how you automatically start up Secure Login Client with a published SAP logon.

## Context

To automatically start the Secure Login Client, create a user login script called `usrlogon_slc.cmd` in the Microsoft Windows directory and insert it into the Microsoft Windows Registry.

## Procedure

1. Install the Secure Login Client.
2. Create the file `usrlogon_slc.cmd` in the Microsoft Windows directory.
3. Insert the following content into the file `usrlogon_slc.cmd`:

```
@ECHO OFF
rem starting Secure Login Client, remove the next line if you do not want the
SLC to start automatically
start "Launch SLC"
"%ProgramFiles(x86)%\SAP\FrontEnd\SecureLogin\bin\sbus.exe"
rem register CSP, remove the next two lines if no CSP/CAPI support is required
regsvr32.exe /s
"%ProgramFiles(x86)%\SAP\FrontEnd\SecureLogin\lib\sbussto.dll"
regsvr32.exe /s
"%ProgramFiles%\SAP\FrontEnd\SecureLogin\lib\sbussto.dll"
```

4. Add the script to the Microsoft Windows Registry to make sure that the Secure Login Client starts automatically at startup. Open the Microsoft Windows Registry and go to the following path:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`
5. Open the key [AppSetup](#) and append the reference to the file `usrlogon_slc.cmd` to the value with a simple comma as a separator (without any space).

### ❖ Example

Registry value name:

[AppSetup](#)

Registry value:

`ctxhide.exe usrlogon.cmd,cmstart.exe,usrlogon_slc.cmd`

You must keep the sequence as shown in the example above because, when starting up, the system proceeds from one file to the next.

## 5.8.3 Other Features of Secure Login Client

Secure Login Client supports a number of additional features, such as automatic startup when a user logs on to Microsoft Windows, certificate issued for CAPI applications, and automatic download of client policies.

## 5.9 Secure Login Client for macOS

You can run Secure Login Client on Mac client computers with the macOS operating system.

SAP Single Sign-On 3.0 SP02 or higher can be used with Kerberos technology, an existing public key infrastructure (PKI), or together with the Secure Login Server for certificate-based authentication without

having to set up a PKI. It allows you to use SAP GUI with SNC or browser-based authentication on a macOS client with macOS 10 or higher.

## 5.9.1 Installing Secure Login Client on a Mac Client

The installation of Secure Login Client on a Mac client uses the default macOS installation procedure.

### Procedure

1. Download the PKG file of the Secure Login Client from the SAP Support Portal under Software Downloads.
2. Start the default installation wizard on your Mac client. For more information, see the relevant documentation of Apple Inc.  
You have completed the installation of the Secure Login Client. Secure Login Client can use Kerberos to authenticate against an SAP GUI using an SNC connection. You do not need to reboot your Mac client to run single sign-on with SAP GUI.
3. Start Secure Login Client from *Applications* to make its icon appear in the status menu bar.

## 5.9.2 Uninstalling Secure Login Client from a Mac Client

You uninstall Secure Login Client from your Mac client using the normal macOS uninstallation procedure.

### Procedure

1. Under *Applications*, drag and drop the Secure Login Client icon to the trashcan.
2. Provide the admin password twice in order to complete the uninstallation.

You have completely uninstalled Secure Login Client without having left any remains on your Mac client.



## 5.9.3 Configuring Secure Login Client on a Mac Client

Secure Login Client supports Kerberos, x.509 certificates from Keychain, Java Script Web Client Profiles, and Secure Login Server Profiles.

### Context

The Secure Login Client is available in the Dock with a main menu. You can make a few settings, such as show/hide the icon, auto-start Secure Login Client after login, and quit Secure Login Client.

#### ! Restriction

In macOS 10.10 (Yosemite), the Secure Login Client icon cannot be kept in the Dock.

- x.509 Certificates from Keychain  
You can use certificate filters with the parameters you are probably familiar with from the Windows client, except for [CAPIProviderFilter](#), which is not applicable on macOS. You have to configure CAPI filters in the `settings.plist` file. For more information, see [CAPI Settings \[page 257\]](#).
- Secure Login Server Profile  
For a complete list of available parameters, please refer to [2400527](#). The `settings.plist` file that is attached to this SAP Note includes contains a complete list of supported parameters. You can use it as a template and set the desired parameters. Then you distribute the file on the clients under `/Library/Preferences/com.sap.SecureLoginClient/` using macOS means or a third-party tool.  
For more information about all parameters available for Windows. see [Common Settings \[page 251\]](#).
- Java Script Web Client  
For more information, see [Providing X.509 Certificates to Secure Login Client Using JavaScript Web Client \[page 38\]](#).

#### ! Restriction

Auto-logout is not possible on macOS.

### Procedure

In the status menu, choose the Secure Login Client and choose [Preferences](#) from the context menu to configure the following:

- SNC. For more information, see [SNC Settings \[page 267\]](#).
- Policy Groups. For more information, see [Manual Choice of User Profile Group in the Secure Login Client \[page 53\]](#).
- SSH Support.  
You can enable/disable SSH support and allow to automatically load the certificates in an SSH agent. Note that you have to copy the line from the [Preference](#) dialog to the config file in the SSH directory.

- Tracing. For more information, see [Tracing Secure Login Client \[page 158\]](#).

## Related Information

[Secure Login Client for macOS \[page 164\]](#)

## 6 Secure Login Server

The Secure Login Server is a central service that provides X.509v3 certificates (out-of-the-box PKI) to users and application servers. The Secure Login Web Client is a browser-based additional function.

### 6.1 Installation and Installation File Names

This chapter describes how to install Secure Login Server for different support packages of SAP Single Sign-On 3.0.

To download the software from the ONE Support Launchpad, go to <https://support.sap.com/swdc>. Install the software using Software Update Manager.

#### Note

The names of the installation files vary according to the version and support package of SAP Single Sign-On.

File Name for Installing Secure Login Server

Version and Support Package	Installation File Name
Secure Login Server 3.0 SP00	SLSERVER00_0.sca  This is the file name of the installation kit, which has not been patched.
Secure Login Server 3.0 SP03	SLSERVER03_0-<ID>.sca  The installation files have the following format:  SLSERVER<support_package_number_<patch_level>-<ID>.sca  <b>❖ Example</b>  SLSERVER03_0-10012314.sca  The ID attached to the file name is a temporary download ID.

Secure Login Server 3.0 SPx is integrated in SAP Solution Manager. You can update Secure Login Server 3.0 to higher support packages and patches using Maintenance Optimizer. For more information, see the SAP Help Portal under [SAP Solution Manager](#) > [Maintenance Optimizer](#).

If you run into problems when installing Secure Login Server, look into the trace files to identify the problem. For more information on tracing of Secure Login Server, see the related link.

## Related Information

[SAP Note 2341102](#)

### 6.1.1 Prerequisites for Installing Secure Login Server

This topic describes the prerequisites for an installation of the Secure Login Server.

During the installation of Secure Login Server, the SAP Netweaver Application Server must be up and running.

The installation of the SAP Cryptographic Library is optional and required for SAP user authentication only. The SAP Cryptographic Library will be used to establish secure communication to Application Server ABAP to verify SAP credentials.

Hardware and software requirements are described in the following documents:

- The Product Availability Matrix lists the software requirements for all components. For more information, see related link.
- The Sizing Guide contains the hardware requirements. For more information, see <http://help.sap.com/sso>.

## Related Information

<http://support.sap.com/pam>

[Authentication Servers Supported by Secure Login Server \[page 169\]](#)

### 6.1.2 Authentication Servers Supported by Secure Login Server

The Secure Login Server supports the following authentication servers:

Supported Authentication Servers

Supported by Secure Login Server	Details
LDAP server system	<ul style="list-style-type: none"><li>• Microsoft Active Directory System 2003, 2008, 2012</li><li>• openLDAP</li><li>• Oracle Directory Server Enterprise Edition</li></ul> <p>For more information, see the related link.</p> <p>Check the Product Availability Matrix for the most current releases.</p>
SAP server system	Application Server ABAP 6.20 or higher version

Supported by Secure Login Server	Details
RADIUS server system	RSA Authentication Manager 6.1, 7.1, 8.0 and 8.1 freeRADIUS Microsoft Network Policy and Access Services (NPA) Microsoft Internet Authentication Service (IAS)
SAP NetWeaver AS for Java User Management Engine (UME)	BasicPasswordLoginModule
SAP NetWeaver AS for Java SPNego	SPNegoLoginModule

## Related Information

<http://support.sap.com/pam>

[Enabling the Display of LDAP Messages in Secure Login Client \[page 159\]](#)

## 6.1.3 Secure Login Server Installation with Software Update Manager

This topic describes how you install Secure Login Server with the Software Update Manager.

### Context

Prerequisites:

- Your service user has administrator authorizations.
- You have downloaded the latest Software Update Manager for your operating system.
- You have downloaded the relevant installation file for Secure Login Server. For more information, see related link.
- You have met the requirements for the update. For more information, see related link.

#### → Tip

We recommend that you use this procedure to install Secure Login Server.

## Procedure

1. Start the Software Update Manager.
2. Install the installation file for Secure Login Server according to the steps in the wizard.
3. Choose the relevant components.

You have now installed the Secure Login Server.

## Related Information

<http://service.sap.com/sltoolset>

<https://service.sap.com/sap/support/notes/1563579>

<https://service.sap.com/sap/support/notes/1707161>

[Installation and Installation File Names \[page 168\]](#)

## 6.1.4 Secure Login Server Installation with Telnet

A Telnet installation is a fast, but insecure option for installing Secure Login Server. Use this installation method for support purposes only.

## Context

### ⚠ Caution

We recommend that you use the installation using the Software Update Manager. For more information, see related link.

## Procedure

1. Copy the relevant installation file to the target SAP Netweaver Application Server.
2. Start a Telnet session.

```
telnet localhost 5<instance_number>08
```

### ❖ Example

```
telnet localhost 50008
```

3. Deploy the Secure Login Server package.

For Secure Login Server 3.0 SP00:

```
deploy <source>\SECURELOGINSERVER00_0.sca
```

#### ❖ Example

```
deploy D:\InstallSLS\SECURELOGINSERVER00_0.sca
```

For Secure Login Server 3.0 SP03:

```
deploy <source>\SLSERVER<support_package_number>_<patch_level>-<ID>.sca
```

#### ❖ Example

```
deploy D:\InstallSLS\SLSERVER03_0-10012314.sca
```

The Secure Login Server application starts automatically when you open the login page of the Secure Login Administration Console for the first time. Start the initial configuration as described in the related link. You find a list of useful Telnet commands in the related link.

After the deployment of Secure Login Server, you have created the following components:

- SecureLoginServer.sda
- securelogin.ui.ear
- securelogin.ui.alias.ear
- securelogin.umep.ear
- securelogin.lib.jni

## Related Information

[Initial Configuration Wizard \[page 174\]](#)

[List of Useful Telnet Commands \[page 172\]](#)

[Secure Login Server Installation with Software Update Manager \[page 170\]](#)

### 6.1.4.1 List of Useful Telnet Commands

This topic contains a table with Telnet commands that are useful if you install Secure Login Server with Telnet.

List of Useful Telnet Commands

Action	Command
Deploy Secure Login Server	<b>deploy SECURELOGINSERVER00&lt;sp_pl&gt;.sca</b>  <sp_pl> stands for the support package number with two digits and the patch level number with one digit.

Action	Command
Undeploy Secure Login Server	<pre>undeploy name=securelogin.ui vendor=sap.com  undeploy name=securelogin.ui.alias vendor=sap.com  undeploy name=securelogin.umep vendor=sap.com  undeploy name=SecureLoginServer vendor=sap.com</pre>
List application	<pre>list_app   grep securelogin</pre>

### Note

If you want to undeploy the Secure Login Server, execute these commands. We recommend that you use the sequence displayed in this table.

## Related Information

[Secure Login Server Installation with Telnet \[page 171\]](#)

[Secure Login Server Uninstallation \[page 173\]](#)

## 6.1.5 Secure Login Server Uninstallation

This chapter describes how you uninstall Secure Login Server.

### Context

Uninstall the Secure Login Server in Telnet.

### Procedure

1. Start a Telnet session.

```
telnet localhost 5<instance_number>08
```

#### ❖ Example

```
telnet localhost 50008
```

2. Undeploy Secure Login Server. To do so, you undeploy the components individually.

```
undeploy name=<ear_file> vendor=sap.com
```



#### ❖ Example

```
undeploy name=securelogin.ui vendor=sap.com
```

#### ❖ Example

```
undeploy name=securelogin.ui.alias vendor=sap.com
```

#### ❖ Example

```
undeploy name=securelogin.umep vendor=sap.com
```

#### ❖ Example

```
undeploy name=SecureLoginServer vendor=sap.com
```

## Results

You have now uninstalled the Secure Login Server. The system keeps the configuration data in the database of the SAP Netweaver Application Server.

## Related Information

[List of Useful Telnet Commands \[page 172\]](#)

## 6.2 Initial Configuration Wizard

After the deployment of Secure Login Server an initial configuration is required

### ⚠ Caution

The initial configuration of the Secure Login Server can be performed on local host or on a remote host (with HTTPS only).

## 6.2.1 Prerequisites for Running the Initial Configuration Wizard

Prerequisites for running the initial configuration wizard of the Secure Login Server

### Prerequisites

- Verify that the Secure Login Server application is running.
- In the SAP NetWeaver AS for Java, you have assigned the role SLAC\_SUPERADMIN to your user. For more information about users and roles in AS Java, see the related link and *SAP Help Portal* under ► [SAP NetWeaver Library: Function-Oriented View](#) ► [Security](#) ► [Identity Management](#) ► [User Management of the Application Server Java](#) ► [Administration of Users and Roles](#) ► [Managing Users, Groups, and Roles](#) ►.

#### → Tip

For security reason, we recommend that you use SSL during the initial configuration process.

### Procedure

### Related Information

[Authorizations and Roles \[page 368\]](#)

## 6.2.2 Initial Configuration

This section describes the modes that are possible for the initial configuration wizard.

This section describes the initial configuration of the Secure Login Server. The initialization wizard sets the values for the PKI certificates and for the user certificates. The following configuration options are available:

- **Automatic**  
The initialization wizard generates the configuration of the PKI certificates and user certificates automatically. You can change the configuration in each configuration step.
- **Manual**  
In this option, you can configure the PKI certificates and user certificates manually. You can also import a CA certificate in a key-pair file and use the parameter and values from this file.  
If you want to use a hardware security module user CA (HSM), see the related link.

- [Migrate](#)  
You see this option if you have an older version of Secure Login Server. In the [Migrate](#) mode, the initial configuration wizard allows you to import the PKI as a file from the previous version. Thus you can migrate the configuration from your the previous version of the Secure Login Server.
- [Skip All](#)  
If you choose this option, the initialization wizard skips the PKI creation and generates the user certificate configuration with the default values. You do not want to enter individual values.

## Related Information

[Using External User Certification Authorities \[page 220\]](#)

### 6.2.2.1 Initial Configuration (Automatic)

Before you can work with the Secure Login Server, a wizard leads you through the initial configuration of the Secure Login Server.

## Context

This section describes the initial configuration of the Secure Login Server. The initialization wizard accesses the Secure Login Server global directory, which contains the all the PKI information you need. It generates the PKI certificates and user certificates with the respective values automatically. Nevertheless you can change individual parameter values.

For more information about the parameters, see the related link below.

## Procedure

1. Start the initial configuration using the browser URL:

`http://localhost:<port>/slac` OR `https://<host_name>:<SSL_port>/slac`

#### ❖ Example

`https://localhost:50001/slac`

#### i Note

If you want to start the initial configuration wizard from a remote computer, you have to use **https**.

2. To change a parameter, choose [Edit](#).

The details section displays the parameters. Mandatory parameters are marked by an asterisk (\*).

3. Enter the related value or choose from a list.
4. Save your changes.

If you want to undo your changes, choose [Reset](#). This command restores the original configuration.

5. To get to [User Certificate Configuration](#), choose [Next](#).
6. Enter the related parameters.
7. Choose [Finish](#) to complete the initial configuration of the PKI certificates and user certificates.

## Related Information

[Parameters for Initial Configuration \(PKI Certificates\) \[page 270\]](#)

### 6.2.2.2 Initial Configuration (Manual)

Before you can work with the Secure Login Server, a wizard leads you through manual steps for the initial configuration of the Secure Login Server.

## Context

The manual configuration mode allows you to change values for the root CA, user CA, SAP CA, SSL CA, and the user certificate configuration. You can also generate an entry by importing a file.

## Procedure

1. If you want to enter the values for the PKI and user certificates yourself, choose the [Manual](#) radio button.
2. (Optional) If you do not want to generate a root CA, mark the [Skip Root CA](#) checkbox. In each wizard step (except in the user CA step), you can skip the generation of each CA by marking the respective [Skip](#) field.
3. (Optional) Import an entry in a key-pair file. For more information, see the related link.
4. Enter the respective values. For more information about the parameters, see the related link below.
5. To get to [User Certificate Configuration](#), choose [Next](#).
6. Enter the related parameter. For more information, see the related link.
7. To complete the initial configuration, choose [Finish](#).

## Related Information

[Parameters for Initial Configuration \(PKI Certificates\) \[page 270\]](#)

[Importing Certificate Entries from a File \[page 179\]](#)

[Parameters for Certificate Configuration \[page 297\]](#)

### 6.2.2.3 Transferring PKI Information to Secure Login Server

For migration purposes, you must make sure that the PKI information of Secure Login Server 1.0 is available for your migrated Secure Login Server 2.0 or higher.

#### Context

If you want to use the automatic initial configuration of Secure Login Server during the migration of Secure Login Server 2.0 or higher from 1.0, you must make sure that the PKI information of Secure Login Server 1.0 is available for use. The initialization wizard of the initial configuration accesses the global directory, which contains all the PKI information you need. It generates the PKI certificates and user certificates with the respective values automatically. This is the reason why you must transfer the PKI information. Proceed as follows:

You must copy the entire directory and its content from the AS Java environment of your Secure Login Server 1.0. Simply copy it and insert it accordingly into the environment where your AS Java with Secure Login Server 2.0 is located.

#### Procedure

1. In the Application Server Java, go to the following directory:

```
/usr/sap/<SID>/SYS/global/SecureLoginServer
```

2. Copy the whole directory to a directory with the corresponding name in the AS Java where your Secure Login Server 2.0 is located.

The initial configuration wizard is now able to access your PKI information automatically.

3. Start the initial configuration. For more information, see related link.

## Related Information

[Initial Configuration Wizard \[page 174\]](#)

## 6.2.2.4 Importing Certificate Entries from a File

You can import entries for the root CA and/or the user CA during certificate management.

### Context

You want to import entries and parameters for the root CA or the user CA from a key-pair file using the initialization wizard for the generation of PKI and user certificates.

#### i Note

If you want to migrate from Secure Login Server 1.0 to the current version, we recommend that you migrate the PKI.

### Procedure

1. Choose [Import](#)

The dialog box [Import Certificate](#) appears. All fields are marked as mandatory.

2. Select the file type in the [Entry Type](#) field. The options [PSE Key Pair](#) and [PKCS#12 Key Pair](#) are available. You can only import files with the file extensions `pse` or `p12`.

#### i Note

If you are migrating the Secure Login Server, import the PSE file with the respective PKI. Since this file is encrypted, you are prompted to enter a password.

3. Enter the path of the entry file in the next field or browse to the file with [Browse...](#)
4. (If applicable) If the entry is decrypted and protected by a password, enter the password to decrypt the file.
5. To complete the import, choose [Save](#).

## 6.3 Administration

This topic contains administration tasks such as starting Secure Login Administration Console, password management, and stopping and starting Secure Login Server.

## 6.3.1 Starting the Secure Login Administration Console

This section describes how you start the Secure Login Administration Console.

### Context

To open the administration console, use a web browser.

#### Note

You find the https port in the SSL setting of the SAP NetWeaver configuration. The port number is usually 50001.

### Procedure

1. Open the Secure Login Administration Console.

```
https://<host_name>:<port>/webdynpro/resources/sap.com/securelogin.ui/Main
```

Shortcut:

```
https://<host>:<port>/slac
```

#### Example

```
https://example.com:50001/webdynpro/resources/sap.com/securelogin.ui/Main
```

2. Enter your administration user name and the password. The Secure Login Administration Console opens.

## 6.3.2 Changing Password

This section describes how to change the administration password of the Secure Login Administration Console.

### Context

Since the Secure Login Administration Console runs within SAP NetWeaver, you must change the administration password in SAP NetWeaver.

## 6.3.3 Stopping and Starting Secure Login Server with Telnet

You can start and stop Secure Login Server with Telnet means.

### Procedure

1. Start a Telnet session.

```
c:\telnet localhost 5$(DIR_INSTANCE)08
```

#### ❖ Example

```
c:\telnet localhost 50008
```

2. Stop Secure Login Server.

```
stop_app sap.com/securelogin.ui
```

3. Start Secure Login Server.

```
start_app sap.com/securelogin.ui
```

## 6.3.4 Stopping and Starting Secure Login Server Using SAP Management Console

You can also monitor Secure Login Server using SAP Management Console

### Context

Secure Login Server has the following AS Java components in the SAP Management Console:

- sap.com/SecureLoginServer
- sap.com/securelogin.ui
- sap.com/securelogin.ui.alias
- sap.com/securelogin.umep

### Procedure

1. Start the SAP Management Console.
2. Choose [AS Java Components](#).
3. Filter the applications for Secure Login Server by entering the names of the components. For example, enter the following in the [Name](#) column:



[sap.com/\\*ecure\\*](http://sap.com/*ecure*)

This displays the AS Java components of Secure Login Server.

4. Choose ► **Action** ► **Stop** ► or ► **Action** ► **Start** ► for stopping and starting.

## 6.4 Secure Login Web Client

Secure Login Web Client is a feature of the Secure Login Server that is a Web-based solution for the authentication of users in Web browsers (in portal scenarios) on a variety of platforms and for launching SAP GUI with SNC.

You can use the Secure Login Web Client to start an SAP GUI with a connection type you configure as post authentication action without using a `saplogon.ini` configuration file. The Secure Login Web Client provides short-term certificates to employees. You also use it for authentication against SAP Netweaver Application Server. This means that the client is no longer limited to Microsoft Windows, but Mac OS X based client systems can be used as well.

### Note

To run Secure Login Web Client, your browser needs a Java Runtime Environment. See the related link to the Product Availability Matrix for an overview of the supported operating systems and browsers.

The following differences between Secure Login Client and Secure Login Web Client exist:

- With Secure Login Client the required security library is available. With Secure Login Web Client the security library needs to be downloaded in a Web browser application.
- With Secure Login Client, the authentication process and secure communication can be triggered on demand (for example, in SAP GUI). The Secure Login Web Client triggers an authentication process and secure communication. After the authentication process, the Secure Login Web Client starts the SAP GUI. As post authentication action, you can redirect to another web page which needs secure authentication, for example, SAP Enterprise Portal. Moreover, the Secure Login Web Client can reuse existing security browser sessions, for example, convert already existing browser sessions for using SSL client authentication with X.509 certificates or start SAP GUI without any user interaction.

The following main features are available:

- Browser-based authentication (including support of all authentication servers)
- Support for SAP GUI for Microsoft Windows and SAP GUI for Java. For more information, see the related link.
- Certificate store support for Microsoft Internet Explorer and Mozilla Firefox browser on Microsoft Windows
- Support for MAC OS X Keychain.
- URL redirect X.509 authentication support to SAP application server
- Localization and customization of HTML pages and applet messages

## Related Information

[Configuring Secure Login Web Client Connections to SAP GUI \[page 80\]](#)

[Parameters for Secure Login Web Client Configuration \[page 286\]](#)

<http://support.sap.com/pam>

## 6.4.1 Enabling SAP GUI to Use Credentials with Secure Login Web Client

You want to enable the Secure Login Web Client to perform authentication and create local credentials that are used by SAP GUI on Microsoft Windows platforms. To enable Secure Login Web Client to make an SNC connection to SAP GUI, you can use multiple connection modes.

- Secure Login Client is not installed on your Microsoft Windows client. Secure Login Web Client copies the SNC libraries from Secure Login Server into the following path:  
`%LOCALAPPDATA%\sapsnc\` (can be changed in [Platform Binaries Download Path](#) in client authorization profile with [Secure Login Web Client Settings](#)).
- Secure Login Client is installed on your Microsoft Windows client with the [Secure Login Server Support](#) option.
  - You have activated [Web Adapter Mode](#) in the [Client Behavior](#) section. Secure Login Web Client uses the Secure Login Client installation path for the SNC connection.
  - You have not activated [Web Adapter Mode](#) in the [Client Behavior](#) section. In this case, the Secure Login Web Client copies the SNC libraries from Secure Login Server into the following path:  
`%LOCALAPPDATA%\sapsnc\`

## 6.4.2 Security Features of Secure Login Web Client

The following features are designed to improve security of the Secure Login Web Client:

- Forced use of HTTPS
- SAP-signed Secure Login Web Client JAR package to protect SNC libraries
- PKI check before storing in Microsoft Certificate store (for Microsoft Windows only)
- Removal of certificates by users

### Related Information

[Forced Use of HTTPS \[page 184\]](#)

[SAP-Signed Secure Login Web Client JAR Package to Protect SNC Libraries \[page 185\]](#)

[PKI Check before Storing in a Client Certificate Store \[page 185\]](#)

[Removing Certificates of the Secure Login Web Client \[page 186\]](#)

## 6.4.2.1 Forced Use of HTTPS

It is mandatory to use the HTTPS protocol. With HTTPS, data and passwords are transported in a secured way.

The trust relationship is established between the trust store of the browser and the SAP NetWeaver Key Storage. If someone tries to bypass HTTPS, the connection is terminated, and an error occurs.

### **i** Note

The Secure Login Web Client needs an SSL connection with the Secure Login Server. When communicating with the Secure Login Server, it must use server authentication without client authentication. You can disable client authentication in the ► [SAP NetWeaver Administrator](#) ► [Configuration](#) ► [SSL](#) ► [SSL Access Points](#) ► [Client Authentication Mode](#) column by setting the value *Do Not Request*.

If SSL is not enabled in the clients, they get a browser message saying that the Java security settings block this application from running. To avoid trust warnings on the clients' browsers, enable SSL on the clients, you must export the SSL CA root in the SAP NetWeaver Administrator. In a Microsoft Windows environment, use utilities of the domain controller to distribute the SSL CAs to your clients.

## Related Information

[Importing CAs or Certificates into the SAP NetWeaver Key Storage \[page 184\]](#)

### 6.4.2.1.1 Importing CAs or Certificates into the SAP NetWeaver Key Storage

## Context

To establish a trust relationship with the SAP Netweaver Application Server, you import your CA certificate of the LDAP server into the Key Storage of SAP Netweaver Application Server. Take the following steps:

## Procedure

1. Start SAP NetWeaver Administrator.
2. Go to the [Configuration](#) tab.
3. Choose [Views](#) in [Certificates and Keys](#).
4. Select [Key Storage](#).

5. Select the Key Storage view `TrustedCAs`.

You display the details of the `TrustedCAs` view in the [View Entries](#) tab.

6. Choose [Import Entry](#).
7. Select the file format of your CA certificate.
8. Browse to your file.
9. To import your file, choose [Import](#).

## Results

You have now established a trust relationship by having imported CAs or certificates files.

For more information, see the SAP Help Portal under ► [SAP NetWeaver Library: Function-Oriented View](#) ► [Security](#) ► [Security](#) ► [System Security](#) ► [System Security for AS Java Only](#) ► [Using the AS Java Key Storage](#) ►.

### 6.4.2.2 SAP-Signed Secure Login Web Client JAR Package to Protect SNC Libraries

To make sure that the files on the server and on the client are not manipulated, an SHA-256 checksum is in place. It prevents a manipulation of the SNC libraries on the side of the client and of the server.

The SAP signature in the JAR file of the Secure Login Web Client applet protects the SHA-256 checksums against manipulation attempts. This makes sure that the SNC libraries are identical with those delivered in the Secure Login Server package.

During a download of a Secure Login Web Client package there is a check of the local files that verifies whether the native SNC libraries have already been downloaded even before the package is written to the hard disk. If the verification of the checksum fails, the files are deleted, and new files are downloaded from the server.

### 6.4.2.3 PKI Check before Storing in a Client Certificate Store

You must have established a trust relationship for the Secure Login Web Client.

## Context

#### i Note

This section only refers to Microsoft Windows and Mac OS operating systems.

To avoid that already valid enrolled keys and certificates are being overwritten with invalid ones from an untrustworthy Secure Login Server, the system performs a PKI check before keys and certificates are stored or overwritten in the Microsoft certificate store and in the local PSE file.

To enable a PKI check, you must set a trust anchor in the clients.

## Procedure

1. Import the root CAs from the user CA of the Secure Login Server in the trusted root Certification Authorities.
2. Distribute the trust anchors that are used by your authentication profiles, which are responsible for your clients. Use Microsoft or Mac OS utilities to import the trusted root CAs into the clients' certificate stores or login/system Keychain and to set a trust relationship.

### 6.4.2.4 Removing Certificates of the Secure Login Web Client

You have started a Secure Logon Web Client session and signed on. The Secure Login Server provides a certificate for this session. When this sessions ends, you remove the certificate.

## Context

Every time you start the Secure Login Web Client and enroll for a certificate, the Secure Login Web Client gets a certificate from the Secure Login Server. This certificate is available as long as you are running this session. You manually remove the certificate, for example from Microsoft Store, by choosing the [Sign Off](#) button, by closing your browser window, or by re-enrolling.

## Procedure

To remove the certificate for a running Secure Login Web Client session, use one of the following options:

- Choose the [Sign Off](#) button.
- Close the browser window of the Secure Login Web Client.
- Re-enroll

You have removed your certificate. Choosing [Back to Sign-On Page](#) takes you back to a Secure Login Web Client window where you can perform a new enrollment.

## 6.4.2.5 Removing Certificates in Web Clients with JavaScript Functions

These JavaScript functions enable you to remove X.509 certificates for web clients from the Microsoft Crypto Store or from the Apple OS X Keychain.

### Context

The Secure Login Server provides a JavaScript API in the default Secure Login Web Client. When the Secure Login Web Client loads, it gets the JavaScript files and makes JavaScript functions available in the browser. You can use them in your own, customized web client implementations.

You can use web clients that are integrated into your own customized HTML page with integrated Single Sign-On functions, for example, in an iView in a portal web client environment.

To support the sign-off function, you need to activate the following JavaScript functions that are provided in your own web client page.

JavaScript Functions for Removing X.509 Certificates

JavaScript Function in <code>securelogin.js</code>	Description
<code>seclogin.isSLCLogoutAvailable()</code>	This JavaScript function checks whether the sign-off feature is available. It is active in the default web client.
JavaScript section: <code>seclogin.doLogout()</code>	This JavaScript function is the implementation of sign-off. It is active in the default client with the <i>Sign Off</i> button.
<code>seclogin.startBrowserMonitor()</code>	(Optional) This JavaScript function performs a sign-off after the last browser window has been closed or when the computer is shutting down. Integrate this JavaScript function into your own web client. The JavaScript function is not active in the default web client.

#### ! Restriction

This feature is only supported on Microsoft Windows platforms with Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome.

To use the JavaScript functions, proceed as follows:

### Procedure

1. Create your own HTML page for your customized web client implementation.

2. Build your HTML page using iViews. For more information, see the [SAP NetWeaver Library: Function-Oriented View](#) > [Enterprise Portal](#) > [Portal](#) > [Managing the Portal](#) > [Creating and Editing iViews](#).
3. Implement the JavaScript function `afterCreateCredentials(okMsg.okType)`. This function becomes effective when the credentials have been successfully created. Use the following code example as a template for your own implementations. The example shows a minimum implementation. If you want, you can integrate further items, for example a [Sign Off](#) button.

#### ❁ Example

```
<HTML>
<HEAD>
<TITLE>Secure Login Web Client</TITLE>
<META content="text/javascript" http-equiv=content-script-type>
<META content= "text/html;
      charset=UTF-8" http-equiv=Content-Type>
<META http-equiv='pragma' content='no-cache'>
<!-- include JQuery and SecureLogin Core -->
<SCRIPT type= "text/javascript" src= "jquery.min.js"></script>
<!-- include Default webclient stylesheets -->
<LINK rel= "stylesheet" type= "text/css" href= "webclient.css">
<SCRIPT language= "javascript" >
    //Callback function after successful
    CredentialCreation    function afterCreateCredentials(okMsg,okType)
{
    // needed for showing success button
    seclogin.onViewChange( "SSO");
    seclogin.onStatusChange(okMsg, okType);
    // optional actions
    seclogin.startBrowserMonitor();
    // start configured post-authentication actions
    seclogin.startSAPApplication();

}
$(document).ready(function() {
    $('head').append('<script type= "text/javascript" src= "securelogin.js?
version=' + new Date().getTime() +
    "' />');

    $('#startSAP').hide();

    seclogin.initPages();
    seclogin.initContainer( "#AppletContainer");

});
</SCRIPT>
</HEAD>
<BODY class= "prtlBody urFontBaseFam urScrl">
<SPAN id= "UMELogon">
<DIV class= "urLogonData">
<FORM id= "SNCForm1" method= "POST" name= "SNCForm1" AUTOCOMPLETE= "off"
action= "/SecureLogin/login">
<TABLE class= "urLogonTable" cellSpacing= "3" cellPadding= "0" valign=
"top">
<TBODY>
<TR>
<TD colSpan= "3">
<DIV class= "urMessageArea" id= "MessageArea">
</DIV>
</TD>
</TR>
<TR>
<TD colSpan= "3">
<!-- Authentication Table -->
```

```

<TABLE cellSpacing= "3" cellPadding= "0" valign= "top" id= "PageAuth"
style= "display:
none">
<TBODY>
<TR>
<TD><LABEL class= "urLblStdNew"><NOBR>User<SPAN class=
"urLblReq">&nbsp;</SPAN></NOBR></LABEL> </TD>
<TD><INPUT style= "WIDTH: 170px" id= "un" class= "urEdfTxtEnbl" title=
"User *" name= "j_username"> </TD>
<TD width= "100%">&nbsp;</TD>
</TR>
<TR>
<TD><LABEL class= "urLblStdNew" for=logonpassfield><NOBR>Password<SPAN
class=urLblReq>&nbsp;</SPAN></NOBR></LABEL> </TD>
<TD><INPUT style= "WIDTH: 170px" id= "pw" class= "urEdfTxtEnbl" title=
"Password *" value= ""
type="password "
name="j_password"> </TD>
<TD>&nbsp;</TD>
</TR>
<TR>
<TD>&nbsp;</TD>
<TD align=right><INPUT class= "urBtnStdNew" value= "Sign
On" type= "submit" name= "uidPasswordLogon" id = "logon"> </TD>
<TD>&nbsp;</TD>
</TR>
<input type= "hidden" name= "j_salt" id= "j_salt" />
</TBODY>
</TABLE>
</TABLE>
</TBODY>
</FORM>
</DIV>
</SPAN>
<DIV id= "AppletContainer">
</DIV>
</BODY>
</HTML>

```

### 6.4.3 Secure Login Security Device for Mozilla Firefox

The Secure Login security device (SecureLogin PKCS#11 module) provides the certificates of the Microsoft Certificate Store in Mozilla Firefox.

After successful user authentication, the Secure Login Web Client stores, the certificate in the Microsoft Certificate Store. The same function is provided for the Mozilla Firefox browser.



## 6.4.3.1 Installing Mozilla Firefox Security Device Manually

You can manually install a Mozilla Firefox security device for Secure Login Web Client.

### Context

Mozilla Firefox 48 and ESR 52 or higher do not accept that users install unsigned extensions/add-ons anymore. Secure Login does not intend to provide a signed Secure Login Firefox extension. The Secure Login Firefox extension only installs the Secure Login PKCS#11 as security device. You must install the security device manually using Mozilla Firefox means.

#### Note

The SecureLogin PKCS#11 module `sbuspkcs11.dll` is only available if the Secure Login Client is installed.

### Procedure

1. Open your Mozilla Firefox browser and choose **Tools > Options**.
2. In the **Advanced** section, go to the **Certificates** tab and choose the **Security Devices** button.
3. Choose **Load**.
4. Enter a name for the security module, such as **SecureLogin PKCS#11 Module**.
5. Choose **Browse...** and navigate to the respective path. .
  - (With 32-bit Firefox and 64-bit Windows)  
C:\Program Files (x86)\SAP\FrontEnd\SecureLogin\lib\
  - (With 64-bit Firefox)  
C:\Program Files\SAP\FrontEnd\SecureLogin\lib\
6. Select `sbuspkcs11.dll` and choose **OK**.

## 6.4.3.2 Uninstall Mozilla Firefox Security Device

This topic describes how you uninstall the Secure Login security device for Mozilla Firefox.

### Procedure

1. Open your Mozilla Firefox browser and choose **Tools > Options**.

2. In the *Advanced* section, go to the *Certificates* tab and choose the *Security Devices* button.
3. To uninstall, select the Secure Login security module and choose the *Unload* button.

## 6.4.4 Rebranding Secure Login Web Client

You may want to rebrand the logon user interface of Secure Login Web Client according to the needs of your company.

Many users of your company or external users use the Secure Login Web Client to log on to your company's systems. You want to change the appearance of the Secure Login Web Client so that all users immediately recognize that they are about to log on to your company's systems. For this reason, you want to rebrand the Secure Login Web Client and modify its logon user interface, for example in a way that it reflects the corporate identity of your company.

### 6.4.4.1 Configuring Secure Login Web Client for Rebranding

You configure rebranding options in a script file of SAP NetWeaver AS for Java.

#### Context

The file `webclient.html` contains all options for rebranding your logon user interface. If you want to rebrand Secure Login Web Client, take the following steps:

#### Procedure

1. Go to the following directory:

```
\usr\sap\<host_name>\<instance_name>\j2ee\cluster\apps\sap.com\SecureLoginServer\nservlet_jsp\SecureLoginServer\webclient\root
```

#### ❖ Example

```
D:\usr\sap\NJ4\J00\j2ee\cluster\apps\sap.com\SecureLoginServer\nservlet_jsp\nservlet_jsp\SecureLoginServer\webclient\root
```

2. Open `webclient.html`.
3. Make the appropriate changes in the HTML file. It makes sense to change the value in the sections surrounded by `<LABEL>` and `</LABEL>`.

### ! Restriction

Do not change the values in the parameters `id` and `name`.

4. Save your changes. You need not restart the Secure Login Server.

## 6.4.5 Export Restrictions

Export restriction according to ECCN 5D002

If you do not run Secure Login Web Client in Web Adapter mode, the Secure Login Web Client, when starting, transfers components that are required for authentication and for a secure network connection from the server to the client.

The Secure Login Web Client contains components with cryptographic features for authentication and for a secure server/client network connection. Under German export control regulations, these components are classified with ECCN 5D002. If server and client are not located in the same country a transfer takes place that requires compliance with applicable export and import control regulations.

### ⚠ Caution

If the Secure Login Server and the Secure Login Web Client are installed in different countries and if you are not using Web Adapter mode, you are obliged to make sure that you abide by the export and import regulations of the countries involved.

## 6.5 Configuration

In the following, you find information about how you can configure Secure Login Server.








### 6.5.1 Overview of Login Modules Supported by SAP Single Sign-On

This table contains the login modules, the login module names, and the location where the destinations are configured.

The following table contains an overview of the login modules that are available in SAP Single Sign-On. For some of them, you must configure destinations (in the Secure Login Administration Console or in the SAP NetWeaver Administrator).

For more information about creating and configuring destinations in Secure Login Administration Console, see the corresponding documents in the related links.

## Overview of Login Modules for SAP Single Sign-On

Login Module	Login Module Name	Destination Configured in
SPNego login module	SPNegoLoginModule	(No destination required)
LDAP login module	SecureLoginModule20LDAP	Secure Login Administration Console
RADIUS login module	SecureLoginModule20RADIUS	Secure Login Administration Console
ABAP login module	SecureLoginModule20ABAP	SAP NetWeaver Administrator
SAP NetWeaver AS for Java User Management Engine (UME).	BasicPasswordLoginModule	(No destination required)
<p>For more information on basic authentication, see <a href="#">SAP Help Portal</a> for SAP NetWeaver.  <a href="#">SAP Library: Function-Oriented View</a>  <a href="#">Security</a>  <a href="#">User Authentication and Single Sign-On</a>  <a href="#">Integration in Single Sign-On (SSO)</a>  <a href="#">Environments</a>  <a href="#">Using User ID and Password Authentication</a> </p>		
One-Time Password Authentication login module. It can be configured to support single-factor authentication or two-factor-authentication.	TOTPLginModule	(No destination required)
<p>For more information on One-Time Password Authentication, see the related link.</p>		

## Related Information

[Creating Destinations \[page 197\]](#)

[Managing Destinations \[page 214\]](#)

[One-Time Password Authentication](#)

## 6.5.2 Adding a Policy Configuration

You must first add a policy configuration, which contains login modules.

### Context

The policy configuration contains several login module stacks.

### Procedure

1. Start the SAP NetWeaver Administrator.

#### ❖ Example

```
https://<host_name>:<port>/nwa
```

2. Choose the [Configuration](#) tab.
3. Go to [Authentication and Single Sign-On](#).
4. To add a policy configuration for a login module stack (for example, for LDAP) for SAP Single Sign-On 3.0, choose [Add](#) in the [Authentication](#) tab.
5. Enter the name of the policy configuration.
6. Choose the [Create](#) button.
7. To specify all the details of the policy configuration, choose [Edit](#).
8. For choosing the relevant login module, go to the section [Details of policy configuration](#) below.
9. Choose the [Add](#) button.
10. Open the dropdown list in the [Login Module Name](#) column.

#### ❖ Example

For LDAP, select [SecureLoginModule20LDAP](#).

11. Select the respective login module for SAP Single Sign-On 3.0. You find an overview of the login modules for SAP Single Sign-On 3.0 in the related link.
12. Set a flag to make sure that the authentication proceeds down the list to the next login module if authentication is not successful.
13. Go to the section [Option of login](#) module. This section contains all the parameters that are relevant for the configuration.

#### ❖ Example

You may find the parameters [PasswordExpirationAttribute](#) and [PasswordExpirationGracePeriod](#) in the options section. The related link explains the meaning of the parameters.

14. Copy the respective values from the previous login module and paste them into the parameters of the login module for SAP Single Sign-On 2.0.

15. Enter the name of the destination. For example in the case of an LDAP and RADIUS login module, you have to configure the destination in the Secure Login Administration Console. For more information, see related link that offers an overview of the login modules.
16. Choose the *Properties* tab.
17. Enter **UserMappingMode** and type in the value **VirtualUser**. This overrides the configuration of the User Management Engine.

## Results

You have now configured the policy configuration with login modules for SAP Single Sign-On 3.0. What is still missing in this stage is the creation of an authentication profile pointing to the policy configuration and the destination configuration.

## Related Information

[Overview of Login Modules Supported by SAP Single Sign-On \[page 192\]](#)

[Parameters for the Policy Configuration \[page 281\]](#)

## 6.5.3 Creating an Authentication Profile Pointing to a Policy Configuration

An authentication profile in the Secure Login Administration Console serves as a pointer to the configuration of the login module.

## Context

At this point, create an authentication profile that points to the relevant policy configuration in the SAP NetWeaver Administrator where the configuration of the login module is located (in the *Authentication* tab of the SAP NetWeaver Administrator).

To create and configure an authentication profile pointing to a policy configuration, proceed as follows:

## Procedure

1. Open the Secure Login Administration Console.

`https://<host_name>:<port>/webdynpro/resources/sap.com/securelogin.ui/Main`

You can also use the following short command:

```
https://<host_name>:<port>/slac
```

### ❖ Example

```
https://example.com:50001/webdynpro/resources/sap.com/securelogin.ui/Main
```

2. To create an authentication profile, choose [Create](#). The wizard for configuring the new authentication profile opens.
3. Enter the authentication profile and a description.
4. Go to [Client Type](#).
5. Select the client you use. The following clients are feasible here:
  - Secure Login Client Profile
  - Secure Login Web Client Profile

### i Note

If you use a Secure Login Web Client profile, you find the client parameters in the related link.

6. In the parameter [User Authentication](#), select the name of the policy configuration.
7. Go to the [User Authentication](#) section.
8. Choose [Use Policy Configuration](#).
9. Select the name of your policy configuration in the dropdown list. For more information, see the related link.

### i Note

You can access the policy configuration in the SAP NetWeaver Administrator if you choose the link [Authentication and Single Sign-On](#).

10. Choose [Next](#) to continue. The next step is the user certificate configuration. It comprises a number of user certificate parameters. For more information, see the related link to the user certificate parameters for Secure Login Server.

### i Note

The field [CA for Issuing Certificates](#) already contains a value for the user CA. You generated the value when you imported the PKI during initial configuration. For more information, see the related link.

11. Choose [Next](#) to continue. The [Enrollment URL](#) is already available. It is displayed split up in several columns.

Consider that when Secure Login server is configured to allow only secure communication, you can only choose HTTPS protocol for the Enrollment URL. For more information, see the corresponding document in the related links.

12. (Optional) Enter the URL of your proxy. For more information, see the related link about the client configuration.

## Related Information

[Adding a Policy Configuration \[page 194\]](#)

[Initial Configuration \[page 175\]](#)

[Parameters for Client Configuration \[page 281\]](#)

[Configuring Secure Login Web Client Connections to SAP GUI \[page 80\]](#)

[Parameters for Secure Login Web Client Configuration \[page 286\]](#)

[Configuring Secure Communication \[page 223\]](#)

## 6.5.4 Creating Destinations

LDAP and RADIUS login modules require destinations in the Secure Login Administration Console.

### Context

To create a destination, proceed as follows:

### Procedure

1. Open the Secure Login Administration Console.

```
https://<host_name>:<port>/webdynpro/resources/sap.com/securelogin.ui/Main
```

#### ❖ Example

```
https://example.com:50001/webdynpro/resources/sap.com/securelogin.ui/Main
```

2. Select the *Destination Management* tab.
3. Choose the *Create* button. The system prompts you to enter a destination name.
4. Enter the same destination name you specified in policy configuration. Provide a description of the destination. For more information, see the related link dealing with policy configuration.
5. Select the destination type from the list. *LDAP Destination* and *RADIUS Destination* are available.
6. Choose *Next* to continue.
7. Enter the relevant parameters. They vary depending on the destination type.
  - a. You can set optional authentication parameters in the section below.
    - (Optional, for LDAP login modules) You can set optional server authentication parameters in the section *LDAP Server Authentication (Optional)*.
    - (Optional for RADIUS login modules) If available, you can also import a server message file delivered by RSA in the *Advanced Configuration for RSA Authentication* section. The imported file fills all the parameters with values.



8. Choose *Finish* to complete the destination configuration.

## Results

You have configured a destination in Secure Login Administration Console. Enter the name of the destination in the policy configuration.

For more information about testing and managing the connection you created, see the corresponding document in the related links.

## Related Information

[Adding a Policy Configuration \[page 194\]](#)

[Managing Destinations \[page 214\]](#)

## 6.5.5 Setting the Enrollment URL for Secure Login Client

You might want to adapt the protocol of the enrollment URL in Secure Login Server.

## Context

Each authentication profile has its own enrollment URLs for communicating with the clients. If, for example you want to run Secure Login Client 1.0 clients with Secure Login Server 2.0 or higher, you must use the correct communication protocol. The enrollment URL for SAP Single Sign-On 2.0 has the following syntax:

```
<Server host:port>/SecureLoginServer/slc2/doLogin?profile=<profile uuid>
```

```
<Server host:port>/SecureLoginServer/slc1/doLogin?profile=<profile uuid>
```

`slc2` stands for the protocol for SAP Single Sign-On 2.0 and `slc1` for 1.0.

To configure the protocol in the enrollment URL, proceed as follows:

## Procedure

1. Start the Secure Login Administration Console.

```
https://<host_name>:<port>/webdynpro/resources/sap.com/securelogin.ui/Main
```

### ❖ Example

```
https://example.com:50001/webdynpro/resources/sap.com/securelogin.ui/Main
```

2. Choose the respective authentication profile.
3. Go to the [Secure Login Client Settings](#) tab.
4. Choose [Edit](#).
5. Go to the [Enrollment URL](#) section. You find the current enrollment URL split up into several parts. It consists of the [Protocol](#), [Host Name](#), [Port](#), and [Secure Login Client Version](#) columns.

If you use different clients, for example Secure Login Client 2.0 and 1.0, you must provide several enrollment URLs having different protocol versions.

6. Choose the Secure Login Client versions you want to use for your clients, for example [1.0](#).
7. Save your changes.

## 6.5.6 Configuring Actions at Policy Download

This topic describes the actions that are possible after a policy download to Secure Login Client.

### Context

Secure Login Server downloads the client policies to the clients at regular intervals. You determine certain actions that are launched after the policy download to Secure Login Client.

### Procedure

1. Start the Secure Login Administration Console.

`https://<host_name>:<port>/webdynpro/resources/sap.com/securelogin.ui/Main`

#### ❖ Example

`https://example.com:50001/webdynpro/resources/sap.com/securelogin.ui/Main`

2. Go to ► [Profile Management](#) ► [User Profile Groups](#) ►
3. Select the profile group for which you want to download the policies to Secure Login Client.

#### i Note

You find the parameters you download to the Secure Login Client in the [User Profile Group](#) tab under the respective authentication profile (including the assignment of SAP AS ABAP SNC names the client authentication is valid for). Go to the section [Information for Client Authentication Profile Windows Authentication \(SPNEGO\)](#) to see the parameters and the values.

4. Go to the [General](#) tab.
5. Choose the [Edit](#) button. For configuring the actions at policy download, use the parameters in the [Actions at Policy Download](#) section. For more information about the parameters, see related link.

6. Choose the field [Action on SAP AS ABAP Application Settings](#). This parameter refers to the profile group configuration in the Secure Login Server.
7. Choose the field [Action on Client Settings](#). This parameter refers to the profile group configuration in the Secure Login Client.
8. Save your changes.

## Related Information

[Parameters for Downloading Policies Using Profile Groups \[page 292\]](#)

## 6.5.7 Configuration of User Certificate Names

This topic describes how you change the common name or Distinguished Name that is used in a user certificate.

You want to change the common name or the Distinguished Name that is used in a user certificate, because you want to have a different name in the user certificate or because your server has special requirements for the user name. Some systems require a certain length, others special trailing or leading characters. If user names in the common name (CN) field need a fixed or minimum length, padding can be turned on. Typically this configuration is used if personnel numbers are used. SAP user IDs have a maximum length of 12 characters (AS ABAP environment) which needs to be considered by SNC X.509 certificates. The password length or value can be customized.

The following changes of the Distinguished Name are possible:

- Expanding the length of the Distinguished Name
- Shortening the Distinguished Name
- Using a completely different Distinguished Name
- Adding additional characters to the Distinguished Name
- Enriching the Distinguished Name by adding additional attributes

### i Note

You can configure all those options if you use certificate user mapping and/or user logon ID padding. Certificate user logon ID mapping and user logon ID padding enable you to use multiple attributes for the generation of the Distinguished Name.

## Related Information

[Parameters for Certificate Configuration \[page 297\]](#)

[Parameters for Certificate Attribute Configuration \[page 298\]](#)

[Parameters of User Mapping Destinations and Attributes \[page 299\]](#)

[Parameters for User Logon ID Padding \[page 300\]](#)

## 6.5.7.1 Certificate User Mapping in the Secure Login Server

This topic describes certificate user mapping.

### **i** Note

User mapping is only possible with LDAP or Active Directory server.

The aim of the Secure Login Server user mapping is to adapt logon between Windows operation systems and an SAP environment. This is implemented by the fact that the Secure Login Server issues a certificate with user information that is used by other applications. It conveys only user information, not necessarily a user name.

This means that you do not need a user-to-user mapping, but the information in the certificate makes sure that the authentication request of a certain user are accepted.

The application recognizes the information and uses it to map to a certain user.

User mapping is possible in the following applications:

- LDAP
- OpenLDAP
- User Management Engine
- Microsoft Active Directory
- ABAP login module
- SPNego login module
- RSA
- RADIUS

## Related Information

[Parameters for Destination Management Configuration \[page 308\]](#)

[\(Optional\) Configuring User Logon ID Padding in Secure Login Server \[page 202\]](#)

## 6.5.7.2 Configuring User Mapping for Secure Login Server in an Authentication Profile

User mapping for Secure Login Server only runs if you use Microsoft Active Directory or LDAP.

## Prerequisites

You have a service user in Microsoft Active Directory or LDAP.

An LDAP server or a Microsoft Active Directory Server is installed in ► [Destination Management](#) ► [Settings](#) ► [LDAP Server Authentication \(Optional\)](#) ►.

For more information, see the related link.

You have defined authentication profiles for the authentication stack you use.

You have entered the optional parameters in the section [LDAP Server Authentication \(Optional\)](#) of the [Destination Management](#).

## Procedure

## Related Information

[Parameters for LDAP Login Modules \[page 287\]](#)

[Creating Destinations \[page 197\]](#)

### 6.5.7.2.1 (Optional) Configuring User Logon ID Padding in Secure Login Server

User logon ID padding enables you to set the lengths of user names, and add padding characters. It is also transferred from the Secure Login Server to the Secure Login Client.

## Prerequisites

You have set the common name to [PADDEDNAME](#) in the certificate attribute configuration

## Context

User names in the common name (CN) field may need a fixed or minimum length. User IDs need a maximum length of 12 characters in the AS ABAP environment. In these cases, you can turn on padding. The padding length sets the minimum length of user names.

## Procedure

1. Go to [User Logon ID Padding \(Optional\)](#). This section contains the padding parameters that are passed on in the certificate when a client or a Secure Login Client authenticates.

2. Activate the checkbox [Enable User Logon ID Padding](#). This displays the user logon ID padding parameters.
3. Enter the relevant values.
4. Save your changes.

For more information about the user logon ID padding parameters, see the related link.

## Related Information

[Parameters for User Logon ID Padding \[page 300\]](#)

### 6.5.7.2.2 Configuring a Distinguished Name with Active Directory Server and SPNego Login Module

This topic describes the configuration of Distinguished Names for users in different trusted domains.

## Context

You want to use Secure Login Client, Secure Login Server, and the SPNego login module for certificate enrollment. The users are located in different trusted Microsoft Active Directory domains.

#### Caution

Since the user IDs may be identical in the subdomains, the Secure Login Server must ensure that non-ambiguous certificates are issued. Thus it adds the domain components to the subject names.

You can use the field [Appendix Subject Name](#) in the [Certificate Attribute Configuration](#) section of [Profile Management](#) > [Certificate Configuration](#) for this. It allows you to customize the Distinguished Name of a certificate.

Use one of the following variables for the [Common Name](#) field:

Variable	Description
<a href="#">(AUTH:USERID)</a>	User name only
<a href="#">(AUTH:UPN)</a>	User principal name
<a href="#">(AUTH:DCS)</a>	All domain components are displayed.

#### Prerequisites

- You use the SPNego login module in the Secure Login Server.
- You have a Microsoft Active Directory environment.

## Procedure

1. Go to *Profile Management*.
2. Select the relevant authentication profile.
3. Choose the *Certificate Configuration* tab.
4. Expand the *Certificate Attribute Configuration* tray.
5. Choose *Edit*.
6. Enter the values with the data as required. If there are two users in different domains, you must output the domain components in the Distinguished Name. For example, enter data for common name, organization, and country. See the following examples:

### ❖ Example

Values for Appendix Subject Name	Result
	<b>If a user smith@example.com logs on, the following Distinguished Name is used:</b>
<b>(AUTH:USERID)</b>	CN=smith
<b>(AUTH:UPN)</b>	CN=smith@example.com
<b>(AUTH:DCS)</b>	CN=smith, DC=example, DC=com"
	Display of the domain components

### ❖ Example

Variables with Output of Domain Components	Result
	<b>If there are different users called Smith in two subdomains (one in sub1.example.com and one in sub2.example.com), the following Distinguished Names are used:</b>
<i>Common Name</i> with <b>(AUTH:UPN)</b>	CN=smith@sub1.example.com
	CN=smith@sub2.example.com
<i>Common Name</i> with <b>(AUTH:USERID)</b>	CN=smith, DC=sub1, DC=example, DC=com
<i>Appendix Subject Name</i> with <b>(AUTH:DCS)</b>	CN=smith, DC=sub2, DC=example, DC=com

### ❖ Example

In addition to this, you can set any valid Distinguished Name attribute as static part of the Distinguished Name.

Values for Appendix Subject Name	Result With different users called Smith in two subdomains (sub1.example.com and sub2.example.com)
CN= (AUTH:UPN) , OU=HR, O=SAP, C=DE	CN=smith@sub1.example.com, OU=HR, O=SAP, C=DE  CN=smith@sub2.example.com, OU=HR, O=SAP, C=DE

7. Save your entries.

### i Note

Use [Appendix Subject Name](#) to configure a Relative Distinguished Name.

## 6.5.7.3 Configuring the Certificate Attributes for User Mapping in the Secure Login Server

The Secure Login Server passes the certificate attributes for user mapping on to the Secure Login Client. This topic explains the configuration.

### Context

The [Certificate Attribute Configuration](#) contains all the attributes that are transferred from the Secure Login Server to the Secure Login Client. You can use the input values, such as [AUTH:USERID](#) or directly type in what you want to include in the user certificate.

### Procedure

1. Go to [Certificate Attribute Configuration](#). This section contains the certificate attributes that are passed on in the certificate when a client or a Secure Login Client authenticates or when the Secure Login Server uploads the user certificate profile.
2. Enter the mandatory common name or choose an input value, for example [AUTH:USERID](#).

If you have defined mapping attributes from an LDAP or Active Directory, you can also use these attributes, for example, [LDAP:mail](#) for an e-mail address.



3. Step through the fields and determine the elements you want to include in the user certificate.
4. Fill the fields you need.
5. Save your changes.

For more information about which parameters of SAP Single Sign-On 2.0 correspond to those in 1.0, see the related link.

## Related Information

[Parameters for Certificate Attribute Configuration \[page 298\]](#)

### 6.5.7.4 Example for User Mapping with an Application Server for ABAP

This is an example for user mapping with Secure Login Server using an LDAP user with a UME.

You have an LDAP user and want to use it in the User Management Engine (UME) of an Application Server ABAP as well. You want to add further attributes to the certificate Distinguished Name, for example, e-mail address, AUTH:UPN, or AUTH:DCS.

The user authenticates with Secure Login Server at a User Management Engine of an Application Server ABAP. The Secure Login Server connects to LDAP to get further attributes from the LDAP search base. These attributes are maintained in the Distinguished Name of the user certificate.

A user logs on to Secure Login Server with user name and password. The Secure Login Server receives the user name and password in the authentication request and identifies the user. The Secure Login Server issues a certificate that contains information about the user, for example the e-mail address.

Now the user authenticates with Secure Login Client or Secure Login Web Client at the SAP GUI. Using the User Maintenance (SU01 transaction) in the Application Server ABAP, you map the certificate Distinguished Name as SNC name. SAP GUI reads the user information (the e-mail address) that is sent with the certificate and identifies the appropriate SAP user.

#### **i** Note

For more information, see [SAP NetWeaver Library: Function-Oriented View > Security > Network and Transport Layer Security > Transport Layer Security on the AS ABAP > Secure Network Communication > Configuring SNC on AS ABAP > User Maintenance on AS ABAP](#) in the SAP Help Portal.

## 6.5.7.5 Example for Configuring a User Distinguished Name in Secure Login Server

This section contains an example for user name mapping in the Secure Login Server.

### Assumption

You have service user called Denise Smith who works in the organization BI ADM. You want to use user name mapping from an LDAP server with user name padding.

When a user authenticates, the Secure Login Server uses a certain policy configuration that determines the result variables, for example [AUTH:UPN](#), which, in the user certificate itself, generates the output `denisesmith@domain.org`.

### Example

You want to enrich the Distinguished Name by adding a number of new attributes from the LDAP server. For this purpose, you must select the LDAP search attributes you want to add, for example, `userNameMappingLDAPSearchAttributeValue=(AUTH:USERID)`. The LDAP search uses the LDAP:name with the search result `Denise Smith` (in the fourth column of the table).

You can only use user name padding if you have set [PADDEDNAME](#) in the [Common Name](#) field of the certificate attribute configuration. However, you can fix the length of the Distinguished Name in the [Padding Length](#) and [Maximum Length](#) fields.

The last row contains an example of options for a complete output in a user certificate.

Overview of User Distinguished Name Configuration

Action	Configuration	Result Variable(s)	Result Values
Authentication	PolicyConfigurations- Name="<client_authentication_profile>"	<a href="#">(AUTH:USERID)</a>	denisesmith
		<a href="#">(AUTH:UPN)</a>	denisesmith@domain.org
		<a href="#">(AUTH:DCS)</a>	DC=domain, DC=org
LDAP User Name Mapping (optional)	userNameMappingLDAP- SearchAttributeName="sA- MAccountName"	(LDAP:userPrincipal)	denisesmith@domain.org
	userNameMappingLDAP- SearchAttribute- Value="(AUTH:USERID)"	(LDAP:name)	Denise Smith

Action	Configuration	Result Variable(s)	Result Values
	userNameMappingLDAPAttributes="userPrincipal,name,email"	(LDAP:email)	denisesmith@mail.domain.org
User Name Padding (optional)	Padding For="(AUTH:USERID)"  Padding Character="0"  Padding Length=12  Maximum Length=14	(PADDEDNAME)	0denisesmith
Certificate creation	Common Name="(PADDED-NAME)"		"0denisesmith"
	Organizational Unit Name="BI ADM"		"BI ADM"
	Organizational Name=""		
	Locality=""		
	Country Name=""		
	Appendix Subject Name="(AUTH:DCS)"		"DC=domain, DC=org"
		Certificate Distinguished Name	"CN=0denisesmith, OU=BI ADM, DC=domain, DC=org"
	Subject Alternative Name (RFC822 Name)="(LDAP:email)"		"denisesmith@mail.domain.org"
	Subject Alternative Name (Principal Name)="(LDAP:userPrincipal)"		"denisesmith@domain.org"

## Result

The certificate you created with this configuration has the following Distinguished Name:

```
"CN=0denisesmith, OU=BI ADM, DC=domain, DC=org"
```

Moreover, the certificate contains the following subject alternative names (RFC822 and principal name):

```
"denisesmith@mail.domain.org"
```

"denisesmith@domain.org"

## 6.5.7.6 Testing Your User Certificate Configuration

After having configured the user certificate, we recommend that you test the configuration.

### Context

#### Note

If the current authentication profile runs with SPNego or Active Directory, you must enter the User Principal Name for testing.

### Procedure

1. Start the Secure Login Administration Console.
2. Go to the [Profile Management](#) tab.
3. Choose the authentication profile of which you want to test the certificate attribute configuration.
4. Choose [Edit](#).
5. Go to the [Certificate Attribute Configuration](#) section.
6. Enter the relevant values.

#### ❖ Example

Certificate Attribute Configuration

Parameter for Certificate Attribute Configuration	Value for Certificate Attribute Configuration
<a href="#">Common Name</a>	<a href="#">(AUTH:UPN)</a>
<a href="#">Country Name</a>	<a href="#">DE</a>
<a href="#">Organizational Name</a>	<a href="#">ARAddev</a>
<a href="#">Organizational Unit Name</a>	<a href="#">BI ADM</a>

7. Go to the [Configuration Check](#) section.
8. Enter your user name in the [User Name](#) field. If the current profile is SPNego or Active Directory, enter the User Principal Name to test. Otherwise, enter only the user ID.

#### ❖ Example

User Principal Name: `dsmith@domain.org`

User ID: `dsmith`

9. Choose [Test](#).

You get the following test output:

```
CN=dsmith@domain.org,OU=BI ADM,O=ARAddev,C=DE
```

The test output displays the common name as it appears in the certificate.

## 6.5.7.7 (Optional) Configuring the User Logon ID Mapping with Added Attributes

Here you learn how you use LDAP or Microsoft Active Directory Server attributes instead of the user name passed on by the client.

### Context

To configure the basic and optional functions for the user mapping certificate, take the following steps:

### Procedure

1. Go to [Profile Management](#).
2. Choose the [Certificate Configuration](#) tab.
3. Expand the [User Logon ID Mapping \(Optional\)](#) tray.
4. Choose the [Edit](#) button.
5. Activate the checkbox [Enable User Logon ID Mapping](#). This enables you to configure the use of an LDAP or Microsoft Active Directory Server attributes instead of the user name passed by the client. The system displays the [Mapping Destinations](#) and [Mapping Attributes](#) sections.
6. Select the respective destination names in the [Mapping Destinations](#) table. It is possible to select multiple destinations. The following destinations are available:
  - LDAP destination
  - Windows Active Directory
7. Enter a search attribute and search values for the LDAP or Active Directory database in the mandatory parameters [LDAP Search Attribute](#) and [Search Value](#).

#### ❖ Example

Use the LDAP search attribute `userPrincipalName` with search value `(AUTH:UPN)`.

Use the LDAP search attribute *sAMAccountName* with search value (*AUTH:USERID*).

The following values are available for *Search Value*:

*AUTH:USERID*

*AUTH:UPN* (available for SPNego only)

*AUTH:DCS* (available for SPNego only)

This search method finds an entire row in an LDAP or Active Directory database.

8. To search in a specific column in the LDAP or Active Directory database, go to the section *Mapping Attributes*. You may find several attributes. You can also add new attributes, for example, from LDAP.

The following attributes are available as default values. If you want to use further values, you must enter them explicitly.

*displayName*

*givenName*

*mail*

*name* (last name)

*sAMAccountName*

*sn* (first name)

*userPrincipalName*(user principal name)

The attributes you enter here add values to all the fields in the *Certificate Attribute Configuration* section below.

### Caution

If any one of the attribute values is not valid, for example, if you misspelled it, no user certificate is issued.

### Example

In the default setting, the field *Common Name* contains the values *AUTH:USERID*, *AUTH:UPN*, and *AUTH:DCS*. If you add the mapping attributes *displayName*, *mail*, and *userPrincipalName* in this sequence, you can enrich the *Common Name* field with the following values (in the following sequence):

AUTH:USERID

AUTH:UPN

AUTH:DCS (for *Appendix Subject Name* only)

LDAP:displayName

LDAP:mail

LDAP:userPrincipalName

It is clear that you can also use all other configured LDAP attributes. For more information, see the related link.

## Results

When a user logs on to a Secure Login Client, all those attributes are immediately transferred by the certificate. When an attribute is found, for example "mail", user information contains the e-mail address.

## Related Information

[Configuring the Certificate Attributes for User Mapping in the Secure Login Server \[page 205\]](#)

### 6.5.7.7.1 Restrictions of Certificate User Mapping

This section describes how to configure the use of an attribute from an LDAP or Microsoft Active Directory Server instead of the user name given by the client.

This may be useful if the SAP user names and the authenticated user names (for example, from a Microsoft Windows domain) are not the same.

#### ⚠ Caution

Do not use certificate user mapping together with a configured Distinguished Name with SPNego. For more information, see related link.

## Example

The Microsoft user name is "UserADS" and the SAP user name is "UserSAP". Without certificate user mapping the Secure Login Server would create a user certificate with the Distinguished Name `CN=UserADS`.

If the SAP user name is stored in the Microsoft Active Directory, for example, in the attribute `AUTH:USERID`, the Secure Login Server can read this attribute and create a user certificate with the Distinguished Name `CN=UserSAP`.

The advantage of having the SAP user name in Distinguished Name is easier configuration in the AS ABAP/Java Server environment (user mapping configuration).

#### ⚠ Caution

If users change their own attributes (for example, through a self-service), and these attributes are used by the user certificate (issued by the Secure Login Server), a situation may occur in which these users are able to assign additional rights to themselves. Thus these users might get rights they are not supposed to have. For this case, we recommend that you implement access restrictions for the change of user attributes.

## Example

An AS ABAP uses, for example, certificate-based logon with the users' e-mail addresses in the Distinguished Names. The string in the certificate has the following format:

```
CN=employee@company.com
```

This means that the user's e-mail address is used for the user mapping in SNC. If an administrator enables the user to change his or her own data, for example, e-mail address, first name, last name etc. through a self-service, this user now has the possibility to enter, for example, his or her manager's e-mail address (**manager@company.com**) as attribute. Since this data is usually maintained centrally, this change would also affect the Secure Login Server. If the certification user mapping feature of the Secure Login Server is configured with the e-mail address as an attribute of the certificate, the user receives a certificate with the Distinguished Name CN=manager@company.com. This user is now able to log on to the AS ABAP as his or her manager.

The prerequisite is that the SAP user name is stored in the LDAP or Microsoft Active Directory system. Certificate user mapping depends on the Secure Login Server user credential check against the authentication server.

## Related Information

[Configuring a Distinguished Name with Active Directory Server and SPNego Login Module \[page 203\]](#)

## 6.5.7.7.2 Defining an LDAP Destination

If you want to establish certificate user mapping, you must have defined an LDAP destination as a prerequisite.

## Context

You must define an LDAP destination. For more information, see related link.

Enter the optional parameters in the section [LDAP Server Authentication \(Optional\)](#) of the [Destination Management](#). Proceed as follows:

## Procedure

1. Open the Secure Login Administration Console.

```
https://<host_name>:<port>/webdynpro/resources/sap.com/securelogin.ui/Main
```

```
https://example.com:50001/webdynpro/resources/sap.com/securelogin.ui/Main
```



2. Select the [Destination Management](#) tab.
3. Go to the [Settings](#) tab.
4. Choose the [Edit](#) button.
5. Go to the [LDAP Server Authentication \(Optional\)](#) section.
6. Enter values for the parameters. You need to specify the LDAP search base DN and the service user name. Entering a password is optional.
7. Save your changes.

For more information on the parameters, see [related link](#).

8. Go through user logon ID mapping in the user certificate configuration of the authentication profile and enter the parameters you need. For more information, see the [related link](#).
9. (Optional) If you want to use user logon ID padding, enter the required values. For more information, see [related link](#).

## Related Information

[Parameters for Destination Management Configuration \[page 308\]](#)

## 6.5.8 Managing Destinations

This topic explains how you configure destination for LDAP or RADIUS login modules.

### Prerequisites

- You have accessed the Secure Login Administration Console in the following way:  
`https://<host_name>:<port>/webdynpro/resources/sap.com/securelogin.ui/Main`

#### ❖ Example

```
https://example.com:50001/webdynpro/resources/sap.com/securelogin.ui/Main
```

- You have created a destination for each domain. For more information, see the corresponding document in the [related links](#).
- You have selected a destination in the [List of Destinations](#) table.

### Context

In the Secure Login Administration Console, you can manage the destinations you created.

## Procedure

- You can test the connectivity between Secure Login Server and the system for which a destination is created by choosing the [Test Connection](#) button in the [Settings](#) tab.

You need to enter the credentials of a user available on the destination system.

- Choose the [Edit](#) button if you want to modify destination parameters such as the name, description, IP address, host name, and so on.

Optionally, if you use user logon ID mapping, you can modify the corresponding parameters. They only apply to LDAP or Microsoft Active Directory servers. For more information on destination parameters and mapping, see the corresponding documents in the related links.

If you want to perform logon ID mapping in multiple domains, see the related link.

You can also test a connection while modifying the destination parameters. In such a situation, the system first performs a validation of the values of all mandatory parameters, and the connection test is initiated only if these values are valid.

- You can copy the selected destination to a new one, or delete it if you do not need it.

## Related Information

[Parameters for Destination Management Configuration \[page 308\]](#)

[Creating Destinations \[page 197\]](#)

[LDAP User Mapping with Multiple Search Base DNs \[page 215\]](#)

### 6.5.8.1 LDAP User Mapping with Multiple Search Base DNs

In LDAP or Active Directory, there are scenarios where it is necessary to define several search base DNs for user mapping. In these cases, administrators must create one LDAP destination for each search base DN.

- Scenario with multiple domains in one LDAP server  
It is possible to define several domains, for example for several organizations of your company. If you want to search multiple domains for user names in multiple organizations, you must create a separate LDAP destination for each domain.

#### ❖ Example

You have several domains in one LDAP server and you want to execute an LDAP search in both domains. You want to set up an LDAP search for user mapping in the domains domain01 and domain02. In this case, you must create LDAP destinations for both domains.

You can now use the following search base DNs in the [LDAP Server ID Mapping mode](#) section of [Destination Management](#):

1. LDAP destination for domain01:  
[Search Base DN](#) DC=domain01, DC=com

2. LDAP destination for domain02:

*Search Base DN* DC=domain02, DC=com

- Scenario with several organizational units in the subtree of one domain

#### ❖ Example

You have several organizational units in the subnodes of only one LDAP or Active Directory domain, but you only want to include specific organizational units in your LDAP search.

```
OU=Admin  
OU=HR  
OU=Prod01  
OU=Prod02
```

You want to set up an LDAP search for user mapping in the organizational units Prod01 and Prod02, but not in Admin and HR. In this case, you must create LDAP destinations for both organizational units.

You can now use the following search base DN in the *LDAP Server ID Mapping mode* section of *Destination Management*.

1. LDAP destination for Prod01  
*Search Base DN* OU=Prod01, DC=domain, DC=com
2. LDAP destination for Prod02  
*Search Base DN* OU=Prod02, DC=domain, DC=com

## 6.5.9 Archiving Certificate Requests, Issued Certificates, and User Certificates

This topic deals with settings for archiving certificate requests, issued certificates, and user certificates in a separate folder or in the UME.

If you activate the checkbox *Archiving Folder Path*, you can log all certificate requests and the issued certificates as files on a file system, for example for later auditing. The Secure Login Server stores certificate requests (for successful and unsuccessful authentication) and the respective certificates (for successful authentication only) in the archiving directory as Base64-encoded files. The certificate requests are stored as PKCS#10 files, whereas the responses are stored as PKCS#7 files.

After having decided to use archiving of certificate requests and responses you must provide a file system with ample space.

Moreover you can also store user certificates in the user's User Management Engine (UME) entry after successful authentication. To do so, activate the *UME Propagation* checkbox.

### Exceptions

If you use the SPNego login module, the Secure Login Server does not create archive files for invalid or failed authentication attempts because the client does not receive a valid Kerberos ticket. In this case the client does not create a certificate request either.

## Prerequisites

The file system has the required space.

Example:

In an organization with 1000 employees at minimum 1000 certificate requests occur per day. This amounts to 2000 files (for requests and issued certificates) that are stored every day. A certificate request (about 0.5 KB) and the certificate (about 2.5 KB) have an overall size of about 3 KB. Employees log on and off several times during the day, so the number of files is usually considerably higher (the employees go to meetings, have breaks, or go to other buildings).

### 6.5.9.1 Configuring Archiving Certificate Requests and Issued Certificates

This configuration allows the user to specify where to store archived certificate requests and issued certificates as well as writing the user certificate to the user's UME entry after successful authentication.

## Context

You can store archived certificate requests and issued certificates either in a special directory configured by you. You can also store user certificates in the user's User Management Engine (UME) after successful authentication. Both options are available as well. If you want to use archiving, take the following steps:



## Procedure

1. Open the Secure Login Administration Console.

```
https://<host_name>:<port>/webdynpro/resources/sap.com/securelogin.ui/Main or  
https://<host>:<port>/slac
```

#### ❖ Example

```
https://example.com:50001/webdynpro/resources/sap.com/securelogin.ui/Main
```

2. Go to  [Profile Management](#) .
3. Select an authentication profile from the list.
4. Go to the [Certificate Configuration](#) tab.
5. Expand the [Certificate Archiving and Storage \(Optional\)](#) tray.
6. (Optional) Activate [Archiving Certificates](#). It is mandatory to specify an archiving directory in the next field.
  - a. Enter the path of the archiving directory according to the syntax that conforms with your operating system:

### ❖ Example

c:\cert\_archive

7. (Optional) Activate *Store Certificates in UME* to write the user certificate to the user's UME entry after successful authentication.

The URL for archiving in UME is `https://<host_name>:<port>/sbs/docs/DOC-66034`.

For more information on the User Management Engine (UME), see the SAP Help Portal under

► [Application Help](#) ► [Function-Oriented View](#) ► [Security](#) ► [Identity Management](#) ► [User Management of the Application Server Java](#) ► [User Management Engine](#) ►

8. Save your changes.

## 6.5.9.2 Structure of the Archive Files

This topic explains the structure of the archive file names.

The file names of the PKCS#10 (for certificate requests) and PKCS#7 files (for certificates) stored in the archiving are generated by the system. Among other things, they identify the authentication profile, the user, the time, and the instance of the SAP NetWeaver system.

Syntax

```
[<timestamp>] [<profile_ID>] [<user_name>] [<client_ID>_<port>]  
[<SAP_NetWeaver_instance_number>].ext
```

This is an example of an archived file for a certificate request (PKCS#10 format):

Example for a certificate request

```
[20130731152533534] [b56b62e6-10b5-9176-9b79-5a1faab4448d] [jarmstrong]  
[10.69.298.176_49633] [ABC_00].p10
```

Example for a certificate file

```
[20130731152533534] [b56b62e6-10b5-9176-9b79-5a1faab4448d] [jarmstrong]  
[10.69.298.176_49633] [ABC_00].p7c
```

The file names consist of the following elements:

File Name Element	Description
timestamp	Timestamp with year, month, day, hours, minutes, seconds, and milliseconds.  Format: <code>yyyymmddhhmmssmm</code>
profile_ID	Authentication profile ID
user_name	User name of the user who authenticated or tried to authenticate.

File Name Element	Description
client_IP	IP of the client that sends the certificate request.
port	Port of the client
SAP_NetWeaver_instance_number	Instance of the SAP NetWeaver where the Secure Login Server is installed.
ext	File extension: <ul style="list-style-type: none"> <li>• p10 Extension for PKCS#10 files for archived certificate requests.</li> <li>• p7c Extension for PKCS#7 files for archived certificates.</li> </ul>

### Note

For technical reasons, it is not possible to get the user name from an SPNego Kerberos authentication. In this case, the user name of the certificate request (in the PKCS#10 file) is always kerberos\_. However, the file name of the respective certificate (PKCS#7 file) contains the correct user name.

## 6.5.10 Adding Certification Authorities

### Prerequisites

- You are using an user account to which the `SLAC_CERT_ADMIN` role is assigned.
- You have accessed the Secure Login Administration Console using one of the following addresses:  
`http://localhost:port/slac` or `https://host_name:SSL_port/slac`  
For example, you can use the following address: `https://localhost:50001/slac`
- For external configuration, the *Secure Login JNI Library* parameter in [System Management](#) > *System Configuration* is configured .
- For external configuration, you know the path to the PSE file.

### Context

You can add new Certification Authority (CA) for PKI certificate management.

## Procedure

1. Choose ► [Certificate Management](#) ► [PKI Structure](#) ►.
2. Choose [Create New Root CA](#).

The system starts the [Certificate Management](#) wizard.

3. On the [Configuration Type](#) step, choose one of the following:
  - When using standard PKI, choose [Standard Configuration](#). The created CA would be of `ROOT` CA type.
  - When using hardware encryption device, choose [External Configuration](#). The created CA would be of `USER` CA type.
4. Enter the CA parameters.

The mandatory parameters are marked with an asterisk (\*). For more information about the parameters, see the document in the related links.

### Note

For external configuration, when you enter the parameters and go to the [Summary](#) step the system tests the connection to the specified hardware encryption device using the values you specified. In case the connection is not successful you would need to enter the correct parameter values.

5. Choose [Finish](#) to save the new root CA.

## Related Information


[Parameters for Initial Configuration \(PKI Certificates\)](#) [page 270]

## 6.5.11 Using External User Certification Authorities

You can optionally use, for example, hardware security module (HSM) boards or other PKCS#11-enabled devices as external user Certification Authorities (CAs).

## Prerequisites

### Prerequisites

- You have installed and tested the hardware security module and its software components, for example, the driver libraries.
- You have initialized the hardware security module, and, for example, generated one or more RSA keys with X.509 certificates, which are available as slot and tokens, respectively.
- You have access to information about the keys using suitable tools.
- You are using the SAP Cryptographic Library (see SAP Note [1848999](#) ). For more information, see the related link.

## Context

In this case, the external CA acts as a key store entry of the type user CA. You find an example configuration in SAP Note [1884870](#).

To configure the usage of an external CA, proceed as follows:

## Procedure

1. Start the Secure Login Administration Console.
2. Go to *System Configuration* on the *System Management* tab.
3. Choose the *Edit* button.
4. Go to the *External CA Configurations* section.
5. Enter the path to the SAP Cryptographic Library in the *Secure Login JNI Library* field. For more information, see the related link.

### ❖ Example

For SAP Cryptographic Library

```
/usr/sap/<SID>/<instance_number>/exe/libsapcrypto.so (for UNIX platforms)
```

6. Save your changes.
7. Restart the Application Server Java.
8. Start the Secure Login Administration Console.
9. Go to the *PKI Structure* section in the *Certificate Management* tab.
10. Select the CA entry you want to configure as an external CA.
11. Choose the *Create New Root CA* button.  
This starts the Certificate Management configuration wizard.
12. Choose *External Configuration* and continue.
13. Enter the relevant parameters. For more information, see the related link.
14. Choose *Finish* to complete the configuration.

## Related Information

[Installing Additional Features for Secure Login \[page 231\]](#)

[Parameters for Initial Configuration \(PKI Certificates\) \[page 270\]](#)

## 6.5.12 Using Certificate Templates

The Secure Login Server contains a number of certificate templates. Their use depends on the type of client that receives certificates from the Secure Login Server. Certificate templates are templates for client



certificates, and they contain the respective properties and tags, for example, basic constraints, key usages, and standard extensions.

## Certificate Templates for Certificate Lifecycle Management

When you create an authentication profile with the client type *Secure Login Client*, for example, the Secure Login Server uses a certificate template called *User Template* for its user certificates.

Depending on the stack, a private key with certificate (henceforth called 'key certificate') is stored in a PSE (AS ABAP) or a key storage view (AS Java). The table below displays the certificate templates that are available in the Secure Login Server, the corresponding key certificates and their purpose.

It is distinguished between a number of key certificate types, for example SSL server PSEs or SSL client PSEs. For certificate lifecycle management, you should ensure that the certificate tags in the Secure Login Server match the certificates of the respective key certificate type.

Secure Login Server contains certificate templates that correspond to the purposes of the key certificate types. You can use them when you configure authentication profiles for application server profile groups.

Each key certificate type is suitable for a special purpose. There is a certificate template that is the counterpart for these purposes in the Secure Login Server.

### ❖ Example

An SSL server PSE, for example, contains certificates for server authentication using TLS/SSL. The purpose of the PSE must correspond to the certificate configuration in the Secure Login Server. Obviously, you want to renew SSL server certificates by certificates that have the same settings and tags. In this case, the Secure Login Server should have an application server profile group that includes an application server authentication profile that corresponds to the PSE type used for your purpose. In our case, the certificate configuration of the application server authentication profile should be based on an SSL server template. The SSL server certificate template already contains all the settings and tags that are suitable for certificates of SSL server PSEs. Thus it makes sure that the renewed certificates have the appropriate structure.

Certificate Templates for Certificate Lifecycle Management

Description	PSE Type	Certificate Template
Suitable for SNC with the SAP Cryptographic Library (SAPCryptolib or CommonCryptoLib)	SNC SAPCryptolib PSE	SNC SAPCryptolib template
Can be used for server authentication using TLS/SSL	SSL server PSE	SSL server template
Suitable for client authentication using TLS/SSL	SSL client PSE	SSL client template
Uses Web service security	WS Security PSE	WS Security template

Description	PSE Type	Certificate Template
Can be used for generic encryption and/or digital signatures using S/MIME	SMIME PSE	S/MIME template
		Encryption template
		Digital signature template
Can be used for generic encryption or digital signatures using SSF	SSF PSE	Encryption template
		Digital signature template
For AS ABAP	System PSE	SAP server template

For more information about certificate templates, see the related link.

## Related Information

[List of Certificate Templates of Secure Login Server \[page 301\]](#)

## 6.5.13 Configuring Secure Communication

Secure Login Server can be configured to accept only HTTPS connections.

### Prerequisites

- You are using a user account to which the `SLAC_CERT_ADMIN` role is assigned.
- You have accessed the Secure Login Administration Console using one of the following addresses:  
`http://localhost:port/slac` or `https://host_name:SSL_port/slac`  
For example, you can use the following address: `https://localhost:50001/slac`

### Context

When creating and managing authentication profiles and profile groups, you can choose whether the clients should communicate with Secure Login Server via HTTP or HTTPS protocol. If you want to secure this communication by allowing only HTTPS, you can configure this in the Secure Login Administration Console.

## Procedure

1. Choose ► *System Management* ► *System Configuration* ►.
2. Choose *Edit* and then modify the *Use only HTTPS protocol* option as needed.
3. Save your changes.

## Results

When you make secure communication between Secure Login Clients and Secure Login Server required, this would have the following effects:

- All existing authentication profiles and profile groups that are set to use HTTP are locked immediately. They can be reconfigured to use HTTPS instead of HTTP. To avoid service downtime, contact the responsible people (those who are assigned the `SLAC_OPERATOR` role) in advance.
- When creating new authentication profiles and profile groups, you would be able to select only HTTPS as protocol for communication.

## Related Information

[Creating an Authentication Profile Pointing to a Policy Configuration \[page 195\]](#)

[Creating a Profile Group of Authentication Profiles \[page 145\]](#)

## 6.5.14 Checking the Availability of Secure Login Server Configuration

### Prerequisites

- You have accessed the Secure Login Administration Console in the following way:  
`https://<host_name>:<port>/webdynpro/resources/sap.com/securelogin.ui/Main`

#### ❖ Example

```
https://example.com:50001/webdynpro/resources/sap.com/securelogin.ui/Main
```

- You have selected ► *System Management* ► *System Check* ►.

## Context

You can check the status of the Secure Login Server and see whether the components that it needs are currently available.

## Procedure

- User Authentication

The Secure Login Administration Console checks whether the policy configuration names of all authentication profiles are available in [Authentication and Single Sign-On](#) of SAP NetWeaver Administrator. The green indicator means that the configuration is correct. If the indicator is red, you must change your configuration. If you choose this link, you access the SAP NetWeaver Administrator where you can check the configuration.

- PKI Structure

If the indicator of [PKI Structure](#) is yellow, make sure that your PKI has a user CA. If the indicator is red, check whether the user CA which is selected in client authentication profile is available. Green means that the PKI structure is available and correct.

## 6.6 Configuration Examples

This section describes some configuration examples for Secure Login Server.

### 6.6.1 Verify Authentication Server Configuration

This topic shows you how to verify the communication to the authentication server.

## Context

After successful configuration of authentication profiles, certificate management, and destinations, the Secure Login Client or Secure Login Web Client can be used to verify communication to the authentication server.

The authentication work process takes place as follows:

## Procedure

1. Start Secure Login Client or Secure Login Web Client.
2. Choose the desired client profile and enter your user name and password.
3. The responsible authentication profile for the chosen client profile is used.
4. The authentication profile are assigned to policy configurations in an authentication stack, which contains login modules. A login module establishes a connection to the authentication server. Login modules are configured in [SAP NetWeaver Administrator](#).
5. The Secure Login Server sends the user credentials to the authentication server. If the response is successful, the Secure Login Server provides a user certificate to the Secure Login Client or Secure Login Web Client.

## 6.6.2 Integrate into Existing PKI

You can use the existing PKI to create the certificates for the SSL server and the SAP NetWeaver AS.

### Context

If a Public Key Infrastructure (PKI) is available, the Secure Login Server can be integrated. You can use the existing PKI to create the certificates for the SSL server and the SAP Netweaver Application Server.

To provide X.509 user certificates, the Secure Login Server requires a User CA certificate which needs to be provided by the PKI.

The following certificate attributes are required for the user CA certificate.

Certificate Attribute	Details
Version	V3
Asymmetric Algorithm	RSA Algorithm

Certificate Attribute	Details
Key Usage	Digital Signature
	Non-Repudiation
	Key Encipherment
	Data Encipherment
	Certificate Signing
	Off-line CRL Signing
	CRL Signing
Basic Constraints	Subject Type=CA
	Path Length Constraint=None

#### **i Note**

The user CA certificate should include the complete certificate chain. This means all public certificate information of the chain should be provided.

Typically the file is provided in P12 or PSE format. Import the user CA certificate using Secure Login Administration Console.

## **Procedure**

1. Log on to the Secure Login Administration Console and import the PSE or P12 file in [Certificate Management](#), and the option [Import Certificate](#).
2. Go to [Certificate Management](#).
3. Select [USER\\_CA](#).
4. Choose the [Import Certificate](#) button.
5. To import your certificate, fill the relevant mandatory fields.
6. Choose [User CA](#) as CA type.
7. To import the certificate file, choose [Import](#).
8. Restart the Secure Login Server application.

## **6.6.3 High Availability and Failover for Secure Login Server and Secure Login Client**

You want to ensure high availability of the Secure Login Server.

For example, you want to make sure that users are able to authenticate even if an authentication server for a configured authentication method is not available.

You must make sure that the Secure Login Servers your clients are connected to continue to run. Using SAP NetWeaver AS for Java instances running in the AS Java cluster architecture you make sure that (at least some of) your Secure Login Servers are running and provide high availability for Secure Login Client. Install a Secure Login Server per Application Server Java. If an AS Java with a Secure Login Server fails, another AS Java with a Secure Login Server is still running. Thus you provide high availability. For more information, see SAP Help Portal in the SAP NetWeaver Library: Function-Oriented View under ► [Application Server](#) ► [Application Server Java](#) ► [Administering Application Server Java](#) ► [Technical System Landscape](#) ► [Architecture of AS Java](#) ► [AS Java Cluster Architecture](#) ►.

You can also ensure failover for the Secure Login Client by using a load balancer, for example SAP Web Dispatcher. For more information, see related link.

## Related Information

[Configuring Secure Login Servers as Failover Servers for High Availability \[page 228\]](#)

### 6.6.3.1 Configuring Secure Login Servers as Failover Servers for High Availability

It makes sense to configure failover connections for high availability to avoid that a client cannot authenticate.

## Context

### Use Case

You want to ensure high availability of the Secure Login Server. For example, you want to prevent that the Secure Login Client sends a certificate request and does not get a response.

### Concept

Install and run a load balancer, for example [SAP Web Dispatcher](#).

Install and run several Secure Login Servers on different AS Java servers acting as failover servers. The URLs of the Secure Login Servers that are available are listed in the [Enrollment URL](#) parameter of the client policy. This is where the Secure Login Client checks which path to use. These URLs are in the following replaced with the URL of your load balancer.

## Procedure

1. Configure your load balancer or SAP Web Dispatcher for your AS Java servers.
2. For each Secure Login Server, log on to the Secure Login Administration Console.

The ports, profile ID, and group ID must be the same on all Secure Login Servers.

3. Update Enroll URL
  - a. Choose the relevant client authentication management in ► [Profile Management](#) ► [Authentication Profile](#) ► [Secure Login Client Settings](#). ►
  - b. Choose the [Edit](#) button.
  - c. Go to the [Enrollment URL](#) section.
  - d. Edit the host name to add the name of your load balancer or SAP Web Dispatcher.
  - e. Configure the enrollment URL for Secure Login Client. For more information, see related link.
  - f. Save your entries.
4. Update your client policy download URL.
  - a. Choose the relevant User Profile Group List of the Profile Group General.
  - b. Choose the [Edit](#) button.
  - c. Edit the IP address / host name of your load balancer or SAP Web Dispatcher.
  - d. Save your entries.

## Related Information

[Setting the Enrollment URL for Secure Login Client \[page 198\]](#)

### 6.6.3.2 Configuring Login Module Stacks as Failover Servers in SAP NetWeaver

Failover servers ensure high availability of the login modules.

## Use Case

For example, you want to make sure that users are able to authenticate even if an authentication server for a configured authentication method is not available.

## Concept

Install and run authentication servers of the same type, for example two LDAP servers, in different networks acting as an authentication failover solution. The authentication logic of the Secure Login Server is handled by login modules. Several login modules of the same kind are put into authentication stacks. These login modules are configured to run with different authentication servers and have, for example, different IPs. When an authentication request comes in, the Secure Login Server tries to use all configured login modules until it gets to an authentication server that is online and returns an authentication result. If, for any reason, the login



module on top of the stack does not respond, the Secure Login Server sends its authentication request to the next login module in the stack and expects it to process the authentication request. This behavior does not depend on the flag (*SUFFICIENT*, *REQUISITE*, *OPTIONAL*, or *REQUIRED*) set for the login module (in the policy configuration of SAP NetWeaver Administrator).

For more information, see the SAP Help Portal and choose ► [Application Help](#) ► [SAP Library](#) ► [SAP NetWeaver Library](#) ► [Function-Oriented View](#) ► [Security](#) ► [User Authentication and Single Sign-On](#) ► [Authentication Infrastructure](#) ► [Authentication on the AS Java](#) ► [Login Modules](#) ►.

## Limitations

SAP Single Sign-On only supports failover if you configure the authentication stacks in SAP NetWeaver Administrator using the following login modules:

- LDAP login module
- RADIUS login module
- ABAP login module

### **i** Note

Put only login modules of the same kind into the authentication stack. We do not support the use of different login modules (mixed authentication types).

# 7 Secure Login Library

The Secure Login Library is a library that provides a toolset for Secure Login.

The following utilities are available:

- `sapsslcli`  
Command line interface for managing the certificate lifecycle using operating system means. For more information, see the related link.

## 7.1 Installing Additional Features for Secure Login

The following topics explain how to install the additional features for Secure Login.

### Context

For more information, see the related links.

### Procedure

1. Open a browser and go to the SAP Software Download Center.
2. Choose ► [Software Downloads](#) ► [Support Packages and Patches](#) ► [Software Downloads](#) ► [By Category](#) ► [SAP NetWeaver and complementary products](#) ► [SAP SINGLE SIGN-ON](#) ► [Installation](#) ►.
3. Choose the respective file and add it to the download basket.

### Related Information

[Certificate Lifecycle Management Using the Secure Login Server \[page 57\]](#)

## 8 SAP Cryptographic Library

The SAP Cryptographic Library is a cryptographic library for an AS ABAP system. It supports both X.509 and Kerberos technology.

### i Note

The SAP Cryptographic Library is the default cryptographic library that comes with the SAP Netweaver Application Server. For more information, see SAP Note [1848999](#). You can optionally download the SAP Cryptographic Library from the SAP Service Marketplace under ► [Software Downloads](#) ► [Browse our Download Catalog](#) ► [SAP Cryptographic Software](#) ►.

### 8.1 SAP Cryptographic Library for Secure Login

The SAP Cryptographic Library (CommonCryptoLib) is the default cryptographic library for a newly-installed SAP Single Sign-On 2.0 SP03 or higher.

The SAP Cryptographic Library comes with the kernel of Application Server ABAP. For more information, see SAP Note [1848999](#). You can also download it from the SAP Service Marketplace (see related link).

After a new installation, SAP Single Sign-On uses the SAP Cryptographic Library. The relevant profile parameter of the instance of the Application Server ABAP points to the path of the SAP Cryptographic Library.

### Overview

The SAP Cryptographic Library enables you to use a number of functions, such as revocation check, configuration of the SNC communication protocol parameters, and/or support for a PKCS#11-based hardware security module.

### Installation Details

By default, the SAP Cryptographic Library is installed in the following path:

`$(DIR_EXECUTABLE) or $(DIR_CT_RUN)`

The installation folder contains the following files:

- `$(FT_DLL_PREFIX)sapcrypto $(FT_DLL)`
- `$(FT_DLL_PREFIX)sapcrypto $(FT_DLL) .pdb` (for Microsoft Windows platforms only)

- \$(FT\_DLL\_PREFIX)slcryptokernel \$(FT\_DLL)
- \$(FT\_DLL\_PREFIX)slcryptokernel \$(FT\_DLL).sha256
- sapgenpse\$(FT\_EXE)
- sapgenpse\$(FT\_EXE).pdb (for Microsoft Windows platforms only)
- sapcrypto.lst

## Configuration of Secure Login Client

By default, Secure Login Client 2.0 SP 03 or higher works with the SAP Cryptographic Library. For this reason, the Secure Login Client installation package comes without the configuration file `gss.xml` in `C:\Program Files (x86)\SAP\FrontEnd\SecureLogin\etc`

## Related Information

<https://support.sap.com/swdc> 


### 8.1.1 Configurable Features of SAP Cryptographic Library

The SAP Cryptographic Library supports multiple features for secure communication, authentication, and single-sign-on.

Among other things, the SAP Cryptographic Library supports the following features:

- SNC for Kerberos and X.509 certificate authentication (see the related link)
- SPNego for ABAP
- Keytab maintenance for Kerberos authentication (see the related link)
- Various SNC communication protocols, certificate revocation lists, and trace of the cryptographic library  
You configure the SNC communication. There is a certificate revocation tool, and the file `sectrace.ini` is required for the trace configuration.

Overview of Configurable Features

Feature	Required File	Information
Certificate revocation lists	<code>sapgenpse get_crl</code>	We recommend that you use this tool to manage certificate revocation lists. It is shipped with the SAP Cryptographic Library.
Trace of the SAP Cryptographic Library	<code>sectrace.ini</code>	A template for this file is available in SAP Note <a href="#">1996839</a>  .

## Related Information

[SNC X.509 Configuration \[page 24\]](#)

[SNC Kerberos Configuration \[page 27\]](#)

[Using Certificate Revocation Lists \[page 244\]](#)

[Configuring Tracing for the Cryptographic Library \[page 248\]](#)

## 8.2 Downloading the Installation Package

This section tells you where you find the additional features for the SAP Cryptographic Library.

### Context

You can also download the installation package of the SAP Cryptographic Library (CommonCryptoLib 8.5 or higher) software from the SAP Software Download Center. It is available for the several operating systems. For more information, see the related link.

### Procedure

1. Open a browser and go to the SAP Software Download Center.
2. Choose ► [Software Downloads](#) ► [By Category](#) ► [SAP Cryptographic Software](#) ► [SAPCRYPTOLIB](#) ► [COMMONCRYPTOLIB 8](#) ►.
3. Choose the respective operating system in the [DOWNLOADS](#) tab.
4. Choose the newest SAR file and add it to the download basket.

## Related Information

<https://support.sap.com/swdc> 

<http://support.sap.com/pam> 

[Secure Login Client Installation \[page 132\]](#)

## 8.3 Standard and FIPS 140-2 Certified Crypto Kernel of the SAP Cryptographic Library

The SAP Cryptographic Library supports the FIPS 140-2 security standard.

### Purpose

When in the United States or Canada a government department wants to use crypto software in their computer systems, this software needs to be tested and validated against the FIPS security standard. This standard contains special security requirements regarding the design and implementation of cryptographic modules. SAP supports the FIPS 140-2 standard in the SAP Cryptographic Library.

#### i Note

SAP is pursuing FIPS 140-2, security level 1 certification for the default SAP Cryptographic Library (which comes with Application Server ABAP). FIPS 140-2 certification ensures that the cryptographic module of the SAP Cryptographic Library is designed, tested, and implemented correctly and indeed protects sensitive data from unauthorized access.

### Implementation

The package of the SAP Cryptographic Library comes with a standard crypto kernel and with a crypto kernel that is certified according to the FIPS 140-2 standard. The crypto kernel is a library with different cryptographic algorithms. If you are obliged to use a FIPS-certified crypto kernel, for example, to comply with legal standards and guidelines, you use the cryptographic module with the certified crypto kernel. The crypto kernel is included in the SAR file of the installation package. For more information, see the related link. SAP Note [2117112](#).

#### i Note

Patches and extensions of the SAP Cryptographic Library, for example, adding a new encryption algorithm, are only implemented in the library with the standard crypto kernel. The library with the FIPS-certified crypto kernel remains unchanged for the time being. Patches and extensions of the library with the FIPS-certified crypto kernel are only available after the completion of an elaborate FIPS certification process. Keep in mind that you might have to wait some time for the release of the FIPS-certified library that includes the patches and extensions you want to use (see SAP Note [2117112](#)).

After the installation, the crypto kernel is located in the `$(DIR_EXECUTABLE)` or `$(DIR_CT_RUN)` directory and consists of the following files:

For Windows operating systems

- `slcryptokernel.dll`
- `slcryptokernel.dll.sha256`

For UNIX platforms

- libslcryptokernel.so
- libslcryptokernel.so.sha256
- libslcryptokernel.sl (for HP-UX on PA-RISC)
- libslcryptokernel.sl.sha256 (for HP-UX)

For more information on how to activate the FIPS-certified crypto kernel in an Application Server ABAP and SAP HANA, see SAP Note [2180024](#).

## 8.3.1 Using the FIPS 140-2 Certified Secure Login Crypto Kernel

This topic shows how you can use the FIPS 140-2 security standard.

### Procedure

1. You are already running the SAP Cryptographic Library, or you must install it as described in the related link.

After the installation, you find the standard crypto kernel files in the standard \$(DIR\_EXECUTABLE) directory.

2. To use the certified crypto kernel files, set the respective profile parameter in Application Server ABAP and SAP HANA. For more information, see [2180024](#).
3. Restart your AS ABAP.
4. To display details of the crypto kernel files that are used by the SAP Cryptographic Library, use the following command:

```
sapgenpse cryptinfo
```

Result:

The command displays the following details of the crypto kernel:

- Version
- Cryptographic algorithms
- Certification status (FIPS)

#### ❖ Example

```
C:\_work\src\3.0>sapgenpse cryptinfo
```

#### ⇐ Output Code

```
Activate FIPS 140-2 mode with crypto kernel version 8.4.47.0
Properties of SAP CommonCryptoLib Crypto Kernel:
FIPS 140-2                = YES
API-VERSION               = 2
VERSION                   = 8.4.47
FILE-VERSION              = 8.4.47.0
```

```

SELFTEST = OK (run in library initialization)
BINARY-FILE = C:\sec\tmpfips\slcryptokernel.dll
CPU-FEATURES-SUPPORTED = AES-NI, CLMUL, SSE3, SSSE3
CPU-FEATURES-ACTIVE = AES-NI, CLMUL, SSE3, SSSE3
HASH-ALGORITHMS =
MD5, SHA1, SHA224, SHA256, SHA384, SHA512, RIPEMD128, RIPEMD160
CHECKSUM-ALGORITHMS = MD2, MD4, CRC32
ENCRYPTION-ALGORITHMS =
RSA, ELGAMAL, AES128, AES192, AES256, DES, TDES2KEY, TDES3KEY, IDEA, RC2, RC4, RC5_32
ENCRYPTION-MODES = ECB, CBC, CFB*8, OFB*8, CTR, CTSECB, CTSCBC, GCM
PADDING-MODES = PKCS1BT01, PKCS1BT02, PKCS1PSS, PKCS1OAEF, X.
923, PEM, B1, XML, SSL
KEYEDHASH-ALGORITHMS = HMAC
SIG-ALGORITHMS = RSA, DSA, ECDSA
KEYEXCHANGE-ALGORITHMS = DH, ECDH
ELLIPTIC-CURVES = P-192, P-224, P-256, P-384, P-521
RANDOM-ALGORITHMS = CTR_DRBG

```

## Related Information

[Downloading the Installation Package \[page 234\]](#)

## 8.4 Configuration for the AS ABAP

You perform the secure network communication (SNC) configuration for the SAP NetWeaver server system using the default profile. Use transaction RZ10 to maintain the SNC profile parameters.

The SAP Cryptographic Library can be configured to accept user authentications based on Kerberos tokens and X.509 certificates. You can use both authentication mechanisms in parallel.

### Configuration Using Transaction SNCWIZARD

The SAP Single Sign-On configuration wizard (transaction SNCWIZARD) in the SAP GUI allows you to easily configure the Application Server ABAP for SAP Single Sign-On 2.0 SP03 or higher. It enables you to set up a default configuration for SNC and SPNego on your Application Server ABAP.

The configuration wizard is available with SAP NetWeaver 7.0 EHP3 SP15, SAP NetWeaver 7.3 EHP1 SP15, and SAP NetWeaver 7.4 SP08 or higher. For more information on the availability of the SAP Single Sign-On configuration wizard, see the SAP Help Portal under the SAP NetWeaver version, the support package stack number in ► [SAP NetWeaver](#) ► [What's New - Release Notes](#) ► [English](#) ► [Support Package Stack](#) ► [Security](#) ► [SAP Single Sign-On Wizard for SNC and SPNego \(New\)](#) ►, and the SAP Note [2304831](#) ►.



## Manual Configuration of SNC and SPNego

You can create or import X.509 certificates in the Trust Manager using transaction `STRUST`. If your release of the Application Server ABAP does not provide the transaction `SNCWIZARD`, and if you want to configure the SAP Cryptographic Library for Kerberos, you can perform a manual configuration using a command line tool. For more information, see the related links.

## Checking the SNC and SPNego Parameters

You can see your current SNC and SPNego configuration in *SNC Configuration* (transaction `SNCCONFIG`) of the kernel default profile and of the instance profile. For a complete description of the SNC interface and parameters, see the SAP SNC manual <http://help.sap.com>

### Note

If you want to manage your PSEs in the trust manager, you must use the SAP Cryptographic Library. The SAP Cryptographic Library is delivered with AS ABAP. For more information, see SAP Note [1848999](#). If you are not running an AS ABAP, download SAPCRYPTOLIB from the SAP Service Marketplace. Go to <https://support.sap.com/swdc>, choose *Search for Software*, and look for the relevant download package.

### Caution

If you are using AS ABAP 7.0, you need to set the environment variable `<SECUDIR>` to `$(DIR_INSTANCE) / sec`. Otherwise AS ABAP 7.0 does not start.

## Related Information

[SNC X.509 Configuration \[page 24\]](#)

[SNC Kerberos Configuration \[page 27\]](#)

## 8.4.1 Using the Single Sign-On Wizard to Configure SNC and SPNego

This wizard helps you to configure SAP Single Sign-On for secure network communication (SNC) and SPNego in the default profile. It provides a default SNC and SPNego configuration for your Application Server ABAP and writes it into the configuration file `DEFAULT.PFL`.

### Prerequisites

- The SAP Cryptographic Library (CommonCryptoLib) is the default cryptographic library (see SAP Note [1848999](#)) of your Application Server ABAP.
- You have already configured service accounts in your Active Directory server for which you want to configure SNC with Kerberos or SPNego.

### Context

If required, you can manually change the default settings made by the wizard in transaction `RZ10`.

The SAP Single Sign-On wizard (transaction `SNCWIZARD`) assists you with the following changes:

- Defines the SNC identity. The default value is `p:CN=<system_ID>`.
- Sets the profile parameters for SNC and SPNego in the default profile.
- Maintains Kerberos and X.509 credentials.
- Creates an SNC PSE if it does not exist.

#### Note

You need to restart the server instances of your application server for the profile parameters to take effect.

### Procedure

1. Open SAP GUI.
2. To start the SAP Single Sign-On wizard, enter `SNCWIZARD`.
3. Set the SNC and SPNego profile parameters to the default values by stepping through the wizard.
4. After having changed the SNC and SPNego profile parameters, you need to restart the application server instances.
5. Start the SAP Single Sign-On wizard again. If you want to configure SNC with Kerberos or SPNego, continue to generate a keytab file. The SAP Single Sign-On wizard calls the *SPNego Configuration* (transaction code `SPNEGO`).
6. (If applicable) Maintain the Kerberos and/or X.509 credentials according to your needs.

7. Choose [Complete](#) to finish the configuration wizard.

## 8.4.2 Digital Signatures (SSF) with a Hardware Security Module

You can use X.509 certificates for digital signatures in an SAP environment. A hardware security module provides keys for encryption and digital signing that are highly secure and very fast.

For example, the signing process with 2048-bit keys is about three times faster than a software-based process for providing keys. You trigger the server-based digital signatures in SAP GUI.

The supported interface is Secure Store and Forward (SSF).

If you want to configure digital signatures (SSF) with a hardware security module, see SAP Note [1973271](#) .

### Related Topics

You can use external user Certification Authorities (CAs) with certificates and keys provided by a hardware security module. For more information, see the related link.

### Related Information

[Using External User Certification Authorities \[page 220\]](#)

## 8.5 Configuring the SAP Cryptographic Library

You can make the settings for the SAP Cryptographic Library (CommonCryptoLib 8.5.1 or higher) by using the [Edit Profiles](#) transaction (transaction code RZ10) in SAP GUI.

The SAP Cryptographic Library (CommonCryptoLib 8.5.1 or higher) comes with a CommonCryptoLib configuration file, which contains all supported parameters. The parameters have the form of ABAP profile parameters and can be set in the default profile of the Application Server ABAP using the [Edit Profiles](#) transaction (transaction code RZ10).

#### → Recommendation

We recommend that you use the default profile parameters to configure the SAP Cryptographic Library.

## Workaround

If the kernel version does not allow you to make the configuration settings directly in the kernel of the Application Server ABAP, you can use a workaround. In this workaround, the AS ABAP uses a configuration file called `DEFAULT.PFL`. You do not edit the file directly, but you can edit the parameters in a familiar way using transaction `RZ10` in SAP GUI.

In fact, you use transaction `RZ10` in SAP GUI to edit the parameters, whatever version your AS ABAP has.

### i Note

When you set the environment variable `<CCL_PROFILE>` to the path of the CommonCryptoLib configuration file, the SAP Cryptographic Library ignores all existing XML configuration files (`gss.xml`, `pkix.xml`, `base.xml`, and `ldap.xml`). Only the configuration of the default profile parameters in transaction `RZ10` is valid.

### i Note

If you have used the configuration files `gss.xml`, `pkix.xml`, `base.xml`, and `ldap.xml` in the previous release, and you want to keep this configuration, do not take any action. The SAP Cryptographic Library continues to use these settings.

Environment Variable for RZ10 Transaction

Parameter Name	Parameter Value
<code>SETENV_&lt;free_number&gt;</code>	<code>CCL_PROFILE=\$(DIR_PROFILE)/DEFAULT.PFL</code>

### ❖ Example

<code>SETENV_00</code>	<code>CCL_PROFILE=\$(DIR_PROFILE)/DEFAULT.PFL</code>
------------------------	--

## Outlook

In future, the parameters will also be default profile parameters. They will be part of the kernel of the Application Server ABAP.


## 8.5.1 Enabling Configuration of the SAP Cryptographic Library Using AS ABAP Profile Parameters

To configure in the SAP Cryptographic Library (for example, the relevant SNC PSE, the SNC cipher suites, or the certificate revocation check), set the CCL\_PROFILE variable in the default profile parameters of the Application Server ABAP.

### Context

To enable configuration in the profile parameters of the AS ABAP, proceed as follows:

### Procedure

1. Open SAP GUI.
2. Start the transaction [Edit Profiles](#) (transaction code RZ10).
3. Select the default profile.
4. Choose [Extended maintenance](#).
5. Choose [Change](#).
6. Choose  [Parameter](#).
7. Enter the following:

#### ❖ Example

**SETENV\_00** as parameter name. Use a free number.

**CCL\_PROFILE=\$(DIR\_PROFILE)/DEFAULT.PFL** as value

This value points to the configuration file **DEFAULT.PFL**.

8. Save your changes.

You can now enter the profile parameters for the SAP Cryptographic Library configuration.

## 8.5.2 Setting Profile Parameters for the SAP Cryptographic Library

We recommend that you make the settings of the SAP Cryptographic Library (CommonCryptoLib 8.5.1 or higher) in SAP GUI.

### Prerequisites

- You have set the environment variable `<SETENV _<free_number>` to the default profile of the SAP Cryptographic Library.

### Context

For more information, see the related link.

### Procedure

1. Log on to the SAP GUI of your Application Server ABAP.
2. Start the transaction [Edit Profiles](#) (transaction code RZ10).
3. Enter the relevant profile parameters and save your changes.
4. Activate the profile parameters and restart the AS ABAP.

### Related Information

[Profile Parameters for SAP Cryptographic Library \[page 318\]](#)

## 8.6 Enabling Certificate Verification

There are profile parameters that enable you to verify certificates and/or manage certificate revocation. They all start with `ccl/pkix/`. In addition to the default certificate verification profile, you basically define certificate verification profiles with their own verification behavior.

In the default certificate verification profile, you can determine that, in general, certificate verification is in place. The default certificate verification profile has no issuer. This means that the default setting is valid for certificates from all issuers unless you have configured exceptions.

In addition to this, you can switch verification on or off for named certificate verification profiles. You can further restrict the setting of the named verification profile to certificates with special issuers. It is possible to use multiple named verification profiles with different issuers.

Moreover, it is also possible to add other parameters for the certificate verification profiles. The parameters of the default verification profile are valid unless you define exceptions by using different parameters for specific named verification profiles.

The verification profiles are used in the order of the profile parameters. If no issuer matches, the default verification profile is used.

#### ❖ Example

In this example, certificate revocation check is enabled in the default verification profile for all certificates. However, the 00\_RootCA verification profile determines that no revocation check is performed for certificates issued by SAP Root CA. Moreover, there is an additional exception - the 01\_ServerCA verification profile states that a revocation check is not performed for certificates issued by SAP Server CA.

```
ccl/pkix/profile/default/revocation_check=CRL
ccl/pkix/profile/00_RootCA/issuer=CN=SAP Root CA
ccl/pkix/profile/00_RootCA/revocation_check=No
ccl/pkix/profile/01_ServerCA/issuer=CN=SAP Server CA
ccl/pkix/profile/01_ServerCA/revocation_check=No
```

## Related Information

[Profile Parameters for SAP Cryptographic Library \[page 318\]](#)

## 8.7 Using Certificate Revocation Lists

The SAP Cryptographic Library supports certificate revocation lists, which enable you to revoke certificates that have been declared invalid.

### Prerequisite

- You have enabled the use of certificate revocation lists in the respective AS ABAP profile parameters.

This enables you to make sure that revoked certificates are not accepted. The CRL issued by the Certification Authority (CA) contains the revoked certificates. The CA issues CRLs at regular intervals. They contain a list of certificates that have been declared as invalid. CAs regularly update certificate revocation lists. They must be replaced regularly by a new CRL or by a CRL that has not yet expired.

CAs place certificate revocation lists at CRL distribution points. The SAP Cryptographic Library provides a tool that enables you to regularly download new CRLs from CRL distribution points (LDAP, HTTP, or HTTPS) to the local cache. Storing CRLs in the local cache ensures fast accessing of the CRLs. You can schedule the download using a cron job. Storing CRLs in the cache improves system performance. Otherwise performance suffers when the SAP Cryptographic must download CRLs from an external CRL distribution point.

To use the CRL functions, make the appropriate settings in the profile parameters of the AS ABAP. For more information, see related link.

The local cache for the CRLs is `\%SECUDIR%\dbcrls`.

## Limitations

The SAP Cryptographic Library covers only basic functions on the server side, such as checking client certificates with CRLs, getting CRLs from a distribution point, and storing them in a local cache. The SAP Cryptographic Library has the following limitations:

- Customers cannot use the extension `IssuingDistributionPoint` in CRLs.
- No use of delta CRLs
- At present the SAP Cryptographic Library assumes that, in a given environment, all CAs provide CRLs. This means that multiple PKIs using different revocation checking policies and one PKI with CAs using different revocation checking policies are not supported.
- Usually UNIX does not come with an LDAP client. To use the CRL tool to get CRLs from LDAP, you must provide an OpenLDAP client (`libldap.*`). The SAP Cryptographic Library searches for an LDAP client in `/usr/lib` (`/usr/lib64`) folder.

### i Note

If the installed LDAP client is not found, we recommend that you create a symbolic link from `$ (DIR_EXECUTABLE) /libldap.so` (`libldap.sl` on HP-UX on PA-RISC systems) to the installed LDAP library.

- The Secure Login Client does not check CRLs.

## Related Information

[Profile Parameters for SAP Cryptographic Library \[page 318\]](#)

## 8.7.1 Downloading CRLs with the CRL Tool

The main function of the CRL tool is to enable you to download CRLs from the CRL distribution point and to make them available in the local cache `\%SECUDIR%\dbcrls`.

When the application server checks certificates, it uses the downloaded CRL. Run the CRL tool at regular intervals to ensure that the most recent CRL is located in the local cache. We recommend using a cron job to schedule the regular download.

### i Note

Make sure the server process has read authorization for the CRL (files) in the cache directory. We recommend using the same user or, in a UNIX environment, granting read authorization with the `umask` command.



To display detailed help, use `sapgenpse get_crl -H`. For more information, see the related link.

## Related Information

[CRL Tool Commands \[page 325\]](#)

## 8.7.2 Getting a CRL from a CRL Distribution Point

This topic contains a variety of command examples that show you how you can get a CRL from a distribution point.

### Context

In the following examples, you see the commands for getting a CRL from a CRL distribution point. For an overview of all commands, see the related link.

### Procedure

Use the following command to get a CRL and store it in a file:

To get a CRL from a CRL distribution point, use one of the following commands:

- Use the following command to get a CRL and store it in a file:

```
get_crl get -u <LDAP_server> -f <CRL_file>
```

Example

```
get_crl get -u ldap:///sap.example.com -f file.crl
```

- Use the following command to get a CRL and store it in a cache without a distribution point:

```
get_crl get -u <LDAP_server> store
```

Example

```
get_crl get -u ldap:///sap.example.com store
```

- Use the following command to get a CRL and store it in a cache using the same distribution point (the URL in the `store` command must be the path of the CRL distribution list).

```
get_crl get -u <LDAP_server> store -u <LDAP_server>
```

Example

```
get_crl get -u ldap:///sap.example.com -u ldap:///sap.example.com
```

- Use the following command to get a CRL and store it in a cache using a different distribution point (the URL in the `store` command must point to the CRL distribution point specified in the certificate).

```
get_crl get -u <HTTP_server> store -u <LDAP_server>
```

Example

```
get_crl get -u http://server/ store -u ldap:///sap.example.com
```

## Related Information

[CRL Tool Commands \[page 325\]](#)

### 8.7.2.1 Example: Downloading a Certificate Revocation List Using an HTTPS Connection

You want to download a certificate revocation list to the local cache of your SAP web server.

## Context

#### Note

If you are using an HTTPS connection, you must first verify the HTTPS connection to the SAP web server. To do so, you need to create a PSE. After having verified the HTTPS connection using the PSE, you can get a revocation list from the SAP web server using HTTPS.

Get the revocation list and download it to the local cache using the `get_crl` command of `sapgenpse`.

Proceed as follows:

## Procedure

1. Create a PSE to verify the HTTPS connection with the SAP web server.

```
sapgenpse gen_verify_pse -p <PSE> -x "" -a <root_CA_certificate>
```

#### ❖ Example

```
sapgenpse gen_verify_pse -p verisign.pse -x "" -a verisign.class3.root.ca.cer
```

2. Get the CRL of the SAP code signing CA and store it in local cache.

```
sapgenpse get_crl -p <PSE> -x <PSE_password> get -u <web-server_URL> store
```

#### ❖ Example

```
sapgenpse get_crl -p verisign.pse -x 123<password> get -u https://  
tcs.mysap.com/crl/crlbag.p7s store
```

## 8.8 Configuration Options

This section describes useful configuration and troubleshooting issues of the SAP Cryptographic Library.

### 8.8.1 Configuring Tracing for the Cryptographic Library

In the case of an error, you can activate tracing for the SAP Cryptographic Library or any other cryptographic library you are using.

#### Context

The `sectrace.ini` configuration file defines the location of the trace directory. For more information, see the SAP Note [1848999](#).

##### i Note

`sectrace.ini` must be located in the same directory as your cryptographic library.

If tracing is activated, several trace files are available in the trace directory. The trace directory defined in `sectrace.ini` must be a subdirectory of `DVEBMG`. You can also use environment variables (encapsulated by `%`). Thus it is, for example, possible to specify the installation directory by using `<% .BINDIR. %>`. Each process ID gets its own trace file. The name of the trace file has the following format:

```
sec-<process_ID>.trc
```

##### i Note

If the process is already known, the file name includes the process name.

##### ❖ Example

```
sec-dev_w0.trc (trace file for work process 0)
```

If a trace file `sec-*.trc` exceeds the defined file size, its content moves to a backup file called `sec-*.<number>.trc`, and `<number>` increases.

To configure tracing, proceed as follows:

#### Procedure

1. Go to the directory where the SAP Cryptographic Library is located.
2. Open the file `sectrace.ini` using a text editor and enter your configuration. For more information, see related link.

The default trace configuration has the following default settings:

- Trace level is 0 (no trace).
- The size for all trace files per process ID is 110 Mbyte.
- The maximum number of trace files per process ID is 10.

#### Caution

The maximum size of all trace files per process ID is 110 Mbytes (10 backup files and 1 trace file). Since the cryptographic library and each SAP GUI gets a new process ID, for example, when it starts up in the morning, you may get a large quantity of trace files every day. Make sure that you provide enough disk space for the trace function. We recommend that you only use trace of your cryptographic library if an error occurred and you are investigating the cause of the error. Deactivate the trace after the error was remedied.

3. Save your changes.

#### Note

You need not restart the Application Server ABAP.

## Related Information

[Tracing Secure Login Client \[page 158\]](#)

## 9 Parameter Reference

You can use the parameter reference to look up the parameters and values for Secure Login. The parameter reference is structured according to the components of Secure Login.

### 9.1 Parameter Overview for Secure Login Client

This parameter overview contains the parameters you can set for the Secure Login Client, for example, registry settings or parameters for digital signatures.

#### 9.1.1 Registry Configuration Options

This section describes further configuration options in registry for the Secure Login Client.

The configuration is either located in the user (HKEY\_CURRENT\_USER\SOFTWARE\...) or in the client workstation (HKEY\_LOCAL\_MACHINE\SOFTWARE\...).

- Common settings
- PCSC settings
- CAPI settings
- Single Sign-On settings for Kerberos-based SNC profile
- Single Sign-On settings for SPNego profile
- SNC settings

For more information, see the related links.

#### Related Information

[Common Settings \[page 251\]](#)

[PCSC Settings \[page 254\]](#)

[CAPI Settings \[page 257\]](#)

[Single Sign-On Setting for Kerberos-Based SNC Profile \[page 262\]](#)

[Single Sign-On Setting for SPNego Profile \[page 265\]](#)

[SNC Settings \[page 267\]](#)

## 9.1.1.1 Global Settings

This table contains the configuration options in the registry for the Secure Login Client.


HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\SAP\SecureLogin

Parameter	Type	Description
EnableKerberosProfile	DWORD	<p>You can enable and disable the Kerberos profile in the Secure Login Client.</p> <p>Default value is <b>1</b>.</p> <p>To enable the Kerberos profile in the user interface of the Secure Login Client, use the value to <b>1</b>. If the user is logged on to a Windows domain, the Kerberos profile displays the name of the user in the following format:</p> <p>sAMAccountName@WINDOWS2000-DOMAIN</p> <p>SNC with Kerberos and SPNEGO profiles rolled out by Secure Login Server can be used. It's not necessarily the users principal name (UPN).</p> <p>To disable the Kerberos profile, set the value to <b>0</b>. SNC with Kerberos is not available. If the user is logged in to a Windows domain, SPNEGO profiles rolled out by Secure Login Server can still be used.</p>

## 9.1.1.2 Common Settings

This table contains the common settings in the registry for the Secure Login Client.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\common] [HKEY\_CURRENT\_USER\SOFTWARE\SAP\SecureLogin\common]

Parameter	Type	Description
DisableSNCUserSelectionCache	DWORD	<p>After an SNC connection has been established successfully, the selected certificate or the Secure Login Server profile is cached and is used for further connections to the same server. This selection stays valid until the users log out.</p> <p>Default value is <b>0</b>.</p> <p>If you want to prompt users to select from multiple certificates, enter the value <b>1</b>.</p> <p>For more information, see SAP Note <a href="#">2067284</a> .</p>
<i>Locale</i>	STRING	<p>Language setting for Secure Login Client. The language is usually recognized automatically. Use this parameter for customizing.</p> <p>Possible values are:</p> <p><b>ar_SA</b> Arabic (Saudi-Arabia)</p> <p><b>de_DE</b> German, (Germany)</p> <p><b>en_US</b> English (USA)</p> <p><b>es_ES</b> Spanish (Spain)</p> <p><b>fr_FR</b> French (France)</p> <p><b>hi_IN</b> Hindi (India)</p> <p><b>it_IT</b> Italian (Italy)</p> <p><b>ja_JP</b> Japanese (Japan)</p> <p><b>kk_KZ</b> Kazakh (Kazakhstan)</p> <p><b>nl_NL</b> Dutch (Netherlands)</p> <p><b>pt_BR</b> Portuguese (Brazil)</p> <p><b>ru_RU</b> Russian (Russia)</p> <p><b>tr_TR</b> Turkish (Turkey)</p> <p><b>zh_CN</b> Simplified Chinese (China)</p>
<i>HideTrayIcon</i>	DWORD	<p>Use this option to remove the Secure Login Client tray icon.</p> <p>To display the tray icon, set the value <b>0</b>.</p> <p>To hide the tray icon, set the value <b>1</b>.</p> <p>The default setting is that the tray icon is displayed.</p>

Parameter	Type	Description
<a href="#">TrustDB</a>	STRING	<p>Use this option to define where Secure Login Client searches for trusted root certificates.</p> <p>The following values are possible:</p> <p><b>capi</b>(default)</p> <p>Get trust from Microsoft Certificate Store</p> <p><b>token</b></p> <p>Use root certificates on tokens</p> <p>Get trust from files (.crt,.p7c,...) in a single directory</p>
<a href="#">ResourcePath</a>	STRING	<p>Use this option to specify an alternate location for the language files (.res).</p> <p>The default value is <b>&lt;install_path&gt;/etc</b>.</p>
<a href="#">ShowUserPoliciesPage</a>	DWORD	<p>Use this parameter if you want to enable a client to select profiles provided by the Secure Login Server. Since this is not a default feature, you must enter this parameter manually in the registry of the client.</p> <p>To enable profile selection in a client, set the value <b>1</b>. For more information, see the related link.</p>
<a href="#">TurnOnSSHAgent</a>	DWORD	<p>You can enable and disable the Secure Login Client to run as an SSH agent using a checkbox in the <b>SSH Agent</b> tab under <b>File &gt; Options</b>. This function is a default function. You do not need to set any registry parameter for this.</p> <p>Use this registry parameter to force the user to enable the SSH agent in the Secure Login Client. If you set the value to <b>1</b>, you enable the Secure Login SSH Agent. The user of the client PC cannot disable it.</p> <p>If you set the value to <b>0</b>, you completely hide the <b>SSH Agent</b> tab from the <b>Options</b> menu of the Secure Login Client and thus disable the use of the Secure Login Client as an SSH agent.</p> <p>For more information, see the related link.</p>

## Related Information

[Downloading User-Specific Profile Groups to the Secure Login Client \[page 147\]](#)

[Using Secure Login Client as SSH Agent \[page 62\]](#)



### 9.1.1.3 PCSC Settings

PCSC settings refer to the use of smart card readers.

The options in this section allow you to select which PCSC smart card readers are used or ignored. You can specify multiple patterns by separating the patterns with `,` or `;` Wildcards (`*` and `?`) are allowed.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\common\pcsc] [HKEY\_CURRENT\_USER\SOFTWARE\SAP\SecureLogin\common\pcsc]

Parameter	Type	Description
<i>IgnoredReadersPattern</i>	STRING	<p>Use this option to disable some PCSC smart card readers.</p> <p>The default value is <b>&lt;empty&gt;</b> (do not disable any PCSC smart card reader).</p>
<i>AllowedReadersPattern</i>	STRING	<p>Use this option to use only some specified PCSC smart card readers. This option is evaluated after IgnoredReadersPattern.</p> <p>The default value is <b>*</b> (use every PCSC smart card reader)</p> <p>Important: If you use an empty string '', all readers are used (same as <b>*</b>).</p>

### 9.1.1.4 Application Policy Settings for Kerberos and Microsoft Cryptography API (CAPI) Token

You want to use the Secure Login Client with SNC application policies for native Kerberos and X.509 authentication. The application policies are not uploaded from the Secure Login Server for Kerberos or Microsoft Cryptography API authentication. In this case, you need to set a number of parameters in the Microsoft Windows registry of your clients.

You can freely choose the name of the SNC application policy. The application policy defines the servers against which the Secure Login Client can log on using the authentication methods specified in the application policy.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\applications\<SNC\_application\_policy\_name>]

Parameter	Type	Description
<i>GSSTargetName</i>	STRING	<p>Here you must specify the servers your application policy is valid for. The Secure Login Client checks all registry keys in HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\applications to determine the application policies defining the SNC servers the client can authenticate against. The application policy sets up a server ranking that depends on the character string and the number of wildcards. If a value of the SNC name contains a higher number of specific characters, it ranks higher. If it contains a higher number of wildcard, it ranks lower. The value is an application-specific PSE URI (SAP server SNC name) that is matched when a suitable profile is searched.</p> <p>You can use the wildcards <b>*</b> and <b>?</b>.</p> <p>Enter the SNC name or parts of the SNC name of your Application Servers ABAP here. The parts you enter (with or without wildcards) determine the servers the application policy is valid for. For example, if you enter <b>OU=SAP</b>, the application policy is valid for all servers where the character string 'SAP' occurs in the SNC name.</p> <div><b>i Note</b> This parameter is mandatory.</div> <p>Example:</p> <p><b>CN=SAP, OU=SAP Security, C=DE</b></p> <p><b>CN=Server*, O=Company xyz</b></p> <p>Using the value <b>*</b> means that the client profile is used for all SAP servers.</p> <div><b>i Note</b> If <i>GSSTargetName</i> is not available in the registry, the Secure Login Client uses the application policies top down (as they appear in the registry tree).</div>
<i>Token Type</i>	STRING	<p>You define the authentication type of the Secure Login Client here.</p> <p>Values:</p> <p><b>kerberos</b> for Kerberos authentication</p> <p><b>tokcapi</b> for Microsoft Cryptography API authentication</p>

Parameter	Type	Description
<a href="#">Any CAPI filter setting</a>	STRING	<p>You enter any available CAPI filter here. For more information, see the related link. The values of the common CAPI settings override these settings.</p> <p>Example for <i>CAPIFilterIssuerDN</i>:</p> <p><b>CN=SSO_CA, O=SAP-AG, C=DE</b></p> <div> <p><b>i Note</b></p> <p>This parameter is only relevant for X.509 authentication.</p> </div>
<a href="#">allowFavorite</a>	DWORD	<p>Allows the user to select the authentication profile manually in the Secure Login Client in any application policy. When you have set this parameter, the Secure Login Client uses it for all consecutive logins. The default value is <b>0</b>.</p> <p>Example 1:</p> <p>A user can select the authentication profile manually in the Secure Login Client. If this setting exists only in one application policy, you get the authentication method selection box for the Secure Login Client.</p> <p><b>1</b></p> <p>Example 2:</p> <p>A user cannot select the authentication profile manually in the Secure Login Client.</p> <p><b>0</b></p>
<a href="#">reAuthentication</a>	DWORD	<p>This parameter determines whether or not you want to use Single Sign-On. The default value is <b>0</b>.</p> <p>Example 1:</p> <p>The selected Secure Login Client profile supports Single Sign-On.</p> <p><b>0</b></p> <p>Example 2:</p> <p>The selected Secure Login Client profile does not support Single Sign-On.</p> <p><b>1</b> (or higher)</p>

## Related Information

[CAPI Settings \[page 257\]](#)

## 9.1.1.5 CAPI Settings

This table refers to the CAPI setting from third-party cryptographic service providers.

The options in these sections allow you to select which certificates from Windows built-in or third party cryptographic service providers may be used. All policies affect the usage for SNC and the listing in Secure Login Client's main windows only. If the SSH feature is turned on, all certificates that are listed and can be selected or deselected.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\common\capi] [HKEY\_CURRENT\_USER\SOFTWARE\SAP\SecureLogin\common\capi]

Parameter	Type	Description
<a href="#">CAPIProviderFilter</a>	STRING	<p>Use this option to use only certificates provided by specific cryptographic service providers (the cryptographic service provider's name must begin with this string).</p> <p>Example:</p> <p><b>TURN OFF WINDOWS CERTIFICATES</b></p> <p>As this is no existing Windows or third party CSP name, no certificate will be available for SNC.</p> <div><p><b>i Note</b></p><p>You find the cryptographic service provider names in</p><p>HKEY_LOCAL_MACHINE/ Software/Microsoft/ Cryptography/Defaults/ Provider.</p><p>Example:</p><p><b>Microsoft Enhanced Cryptographic Provider v1.0</b></p><p>Only locally installed soft tokens are available for SNC.</p><p>If a smart card running with the standard Microsoft Base Smart Card CSP or a vendor CSP is in place but shall not be used, for instance because of undesired side effects of Secure Login Client operations, one of the values above must be configured. In addition, the SSH feature must not be turned on.</p></div>
<a href="#">CAPIFilterValidOnly</a>	DWORD	<p>Use this option to use only certificates that are valid (issued in the past and not expired).</p> <p>The default is <b>0</b>.</p>

Parameter	Type	Description
<a href="#"><i>CAPIFilterIssuerDN</i></a>	STRING	<p>Use this option to use only certificates that have an issuer's Distinguished Name that contains <a href="#"><i>CAPIFilterIssuerDN</i></a>. To specify the certificates of a certain server, enter the whole Distinguished Name or only a part of it. You cannot use wildcards.</p> <p>Example:</p> <p><b>CN=My Companies CA</b></p>
<a href="#"><i>CAPIFilterSubjectDN</i></a>	STRING	<p>Use this option to use only certificates that have a subject Distinguished Name that contains <a href="#"><i>CAPIFilterSubjectDN</i></a>. To specify the certificates of a certain server, enter the whole Distinguished Name or only a part of it. You cannot use wildcards.</p> <p>Example:</p> <p><b>O=My Org Unit</b></p>
<a href="#"><i>CAPIFilterExcludeIssuerDN</i></a>	STRING	<p>Use this option to disable certificates that have an issuer's Distinguished Name that contains <a href="#"><i>CAPIFilterExcludeSubjectDN</i></a>. To specify the certificates of a certain server, enter the whole Distinguished Name or only a part of it. You cannot use wildcards.</p> <p>Example:</p> <p><b>CN=Test CA</b></p>
<a href="#"><i>CAPIFilterExcludeSubjectDN</i></a>	STRING	<p>Use this option to disable certificates that have a subject Distinguished Name that contains <a href="#"><i>CAPIFilterExcludeSubjectDN</i></a>. To specify the certificates of a certain server, enter the whole Distinguished Name or only a part of it. You cannot use wildcards.</p> <p>Example:</p> <p><b>O=Testing only</b></p>

Parameter	Type	Description
<a href="#">CAPIFilterKeyUsage</a>	STRING	<p>Use this option to use only certificates that have a specific key usage.</p> <p>The <a href="#">CAPIFilterKeyUsage</a> may contain the following strings (you can specify multiple strings)</p> <p><b>+KEYUSAGE</b></p> <p>Use only certificates that have the specified key usage.</p> <p><b>-KEYUSAGE</b></p> <p>Do not use certificates that have the specified key usage.</p> <p>Where <b>KEYUSAGE</b> can be one of the following:</p> <p><b>dataEncipherment</b></p> <p>Data encipherment key usage</p> <p><b>digitalSignature</b></p> <p>Digital-Signature Key-Usage</p> <p><b>keyAgreement</b></p> <p>Key agreement key usage</p> <p><b>keyEncipherment</b></p> <p>Key encipherment key usage</p> <p><b>nonRepudiation</b></p> <p>Non-repudiation key usage</p> <p><b>cRLSign</b></p> <p>CRL signature key usage</p>

Parameter	Type	Description
<a href="#">CAPIFilterExtendedKeyUsage</a>	STRING	<p>Use this option to use only certificates that have a specific key usage.</p> <p>The syntax of this option is similar to <a href="#">CAPIFilterKeyUsage</a>.</p> <p>The <a href="#">CAPIFilterExtendedKeyUsage</a> may contain the following strings:</p> <p><b>+EXTKEYUSAGE</b></p> <p>Use only certificates that have the specified extended key usage</p> <p><b>-EXTKEYUSAGE</b></p> <p>Do not use certificates that have the specified extended key usage</p> <p>Where <b>EXTKEYUSAGE</b> can be one of the following:</p> <p><b>ServerAuthentication</b> (1.3.6.1.5.5.7.3.1)</p> <p><b>ClientAuthentication</b> (1.3.6.1.5.5.7.3.2)</p> <p><b>CodeSigning</b> (1.3.6.1.5.5.7.3.3)</p> <p><b>EmailProtection</b> (1.3.6.1.5.5.7.3.4)</p> <p><b>IpssecEndSystem</b> (1.3.6.1.5.5.7.3.5)</p> <p><b>IpssecTunnel</b> (1.3.6.1.5.5.7.3.6)</p> <p><b>IpssecUser</b> (1.3.6.1.5.5.7.3.7)</p> <p><b>TimestampSigning</b> (1.3.6.1.5.5.7.3.8)</p> <p><b>OcspSigning</b> (1.3.6.1.5.5.7.3.9)</p> <p><b>MicrosoftEfs</b> (1.3.6.1.4.1.311.10.3.4)</p> <p><b>MicrosoftEfsRecovery</b> (1.3.6.1.4.1.311.10.3.4.1)</p> <p><b>MicrosoftKeyRecovery</b> (1.3.6.1.4.1.311.10.3.11)</p> <p><b>MicrosoftDocumentSigning</b> (1.3.6.1.4.1.311.10.3.12)</p>



Parameter	Type	Description
		<b>MicrosoftSmartcardLogon</b> (1.3.6.1.4.1.311.20.2.2)
<i>inactivityTimeout</i>	DWORD	<p>Value in seconds until an automatic logout is performed (due to mouse and keyboard inactivity).</p> <p>Use this option if you want to configure that users are forced to log on for each SNC connection. If you have a CAPI token, for example a smart card or a soft token, the token is logged out after a complete buildup of the SNC connection (with one or several private key operations).</p> <div> <b>i Note</b>  It depends on the third-party cryptographic service provider you use whether the inactive timeout is available. Some cryptographic service providers do not allow log-out; some always prompt the user for a password. </div> <p>The following values are possible:</p> <p><b>ffffffff</b> (equivalent to -1)</p> <p>No single sign-on. Each SNC connection forces a new login.</p> <p><b>0</b> (default)</p> <p>Single sign-on and no timeout</p> <p>Enter a value &gt; 0.</p> <p>Seconds until an automatic logout is executed.</p>

### 9.1.1.6 Single Sign-On Setting for Kerberos-Based SNC Profile

You do not want to use single sign-on, but force users, for example, to enter their user name and password every time they log on to an Application Server ABAP using SNC.

Users must always enter their Microsoft Windows credentials before a Kerberos-based SNC session starts.

### Note

Please note that this configuration is not valid for MacOS.

### Caution

Different options are available for users to authenticate at an Application Server ABAP using SNC after having logged on to a Microsoft Windows domain.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\common\Kerberos] [HKEY\_CURRENT\_USER\SOFTWARE\SAP\SecureLogin\common\Kerberos]

Parameter	Type	Description
<a href="#">SSOMode</a>	DWORD	<p>Use this option to configure the setting of the Kerberos-based SNC profile of the Secure Login Client for SNC connection.</p> <p>Possible values:</p> <ul style="list-style-type: none"><li><b>0</b> The SNC connection uses the existing Microsoft Windows credentials. There is an automatic logon to the Secure Login Client Kerberos profile.</li><li><b>1</b> Users are prompted for user name and password once to log on to an SNC session. There is no automatic logon in the Secure Login Client profile. After the Microsoft Windows logon, the Kerberos-based SNC profile is grayed out.</li><li><b>2</b> Users are always prompted for user name and password for every logon to an SNC session (no single sign-on). There is no automatic logon in the Secure Login Client profile. After logon to Microsoft Windows, the Kerberos-based SNC profile is grayed out.</li><li><b>3</b> Users are prompted for user name and password once to log on to an SNC session. There is no automatic logon in the Secure Login Client profile. After the Microsoft Windows logon, the SPNego profile is grayed out. The session remains valid until you log off from this profile. Your user name appears in the <a href="#">User</a> field, and the cursor is in the <a href="#">Password</a> field.</li><li><b>4</b> Users are always prompted for user name and password for every logon to an SNC session (no single sign-on). There is no automatic logon in the Secure Login Client profile. After the Microsoft Windows logon, the Kerberos profile is grayed out. Your user name appears in the <a href="#">User</a> field, and the cursor is in the <a href="#">Password</a> field.</li></ul>

Parameter	Type	Description
		<p>5 If single sign-on has failed, users are prompted for user name and password to log on to an SNC session.</p>

### 9.1.1.7 Single Sign-On Setting for SPNego Profile

You do not want to use Single Sign-On, but force users, for example, to enter their user name and password at the Secure Login Client to enroll for a certificate that enables them to connect with an Application Server ABAP using SNC.

Users must always enter their Microsoft Windows credentials before an SNC session with an SPNego login module of AS Java starts.

#### Note

Please note that this configuration is not valid for MacOS.

#### Example

Users dial in using a VPN. In this case, they do not have a Kerberos token on their computer when they want to log on. They must wait until the VPN connection has been built up before they get a Kerberos token. Now they can authenticate and enroll for a certificate for an SNC connection.

#### Note

Different options are available for users to authenticate at an Application Server ABAP using SNC after having logged on to a Microsoft Windows domain.

If you use the SPNego login module for SNC authentication, you must make the following settings in the Microsoft Windows Registry.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\common\Kerberos] [HKEY\_CURRENT\_USER\SOFTWARE\SAP\SecureLogin\common\Kerberos]

Parameter	Type	Description
<a href="#">SSOMode</a>	DWORD	<p>Use this option to configure the setting of the SPNego profile of the Secure Login Client for SNC connection.</p> <p>Possible values:</p> <p><b>0</b> The SNC connection uses the existing Microsoft Windows credentials. There is an automatic logon to the Secure Login Client SPNego profile.</p> <p><b>1</b> Users are prompted for user name and password once to log on to an SNC session. There is no automatic logon in the Secure Login Client profile. After the Microsoft Windows logon, the SPNego profile is grayed out. The SNC connection remains until users logs off from their profiles.</p> <p><b>2</b> Users are prompted for user name and password once to log on to an SNC session (no single sign-on). There is no automatic logon in the Secure Login Client profile. After logon to Microsoft Windows, the SPNego profile is grayed out. The connection remains until the certificate expires. There is no auto-enrollment with the certificate.</p> <p><b>3</b> Users are prompted for user name and password once to log on to an SNC session. There is no automatic logon in the Secure Login Client profile. After the Microsoft Windows logon, the Kerberos profile is grayed out. The session remains valid until you log off from this profile. Your user name appears in the <a href="#">User</a> field, and the cursor is in the <a href="#">Password</a> field.</p> <p><b>4</b> Users are prompted for user name and password once to log on to an SNC session (no single sign-on). There is no automatic logon in the Secure Login Client profile. After logon to Microsoft Windows, the SPNego profile is grayed out. The connection remains until the</p>

Parameter	Type	Description
		certificate expires. There is no auto-enrollment with the certificate. Your user name appears in the <i>User</i> field, and the cursor is in the <i>Password</i> field.

## 9.1.1.8 SNC Settings

These SNC settings of the Secure Login Client refer to the use of session keys for multiple applications and to manual server trust.

[HKEY\_CURRENT\_USER\SOFTWARE\SAP\SecureLogin\common\snc]

Parameter	Type	Description
<i>ServerSessionKeyMode</i>	DWORD	Enables a temporary session key for a back end. If only this value is set, the session key is generated on the first connection to a back end. It is deleted when the user closes the last connection.  The default value is <b>0</b>
<i>ServerSessionKeyInvalidateOnExit</i>	STRING	The lifetime of the session key is extended until the selected processes terminates.  The default value is <b>&lt;empty&gt;</b>
<i>ServerSessionKeyReAuthAndInvalidateOnExit</i>	STRING	If the selected processes opens its first connection, a new session key is generated. This process can use the session key until the process ends. Other processes can use this session key without further authentication.

Parameter	Type	Description
<a href="#">SNCTMode</a>	DWORD	<p>This setting refers to SNC-encrypted logon.</p> <p><b>0</b>: Legacy compatibility mode (default)</p> <p><b>1</b>: Smart mode</p> <p><b>2</b>: Encryption only mode</p> <p>For information, see <a href="#">Logging on with Secure Login Client Using SNC [page 33]</a>.</p>
<a href="#">SNCTModeSmartTryKerberosFirst</a>	DWORD	If smart mode is selected, the Secure Login Client tries to get a Kerberos token before the handshake.
<a href="#">SNCTServerTrustPrompt</a>	DWORD	Allows manual server trust.

## 9.1.2 SSF Parameters for Digital Signatures

SSF user configuration parameters for digital signatures

The table in the related link contains parameter for the SSF user configuration in SAP GUI.

### Related Information

[SSF User Configuration \[page 268\]](#)

### 9.1.2.1 SSF User Configuration

The following table contains parameter for the SSF user configuration in SAP GUI.

SSF User Configuration

Parameter	Description
<a href="#">SSF-ID</a>	<p>Define the Distinguished Name of the user certificate.</p> <p>Example: <b>CN=Username, OU=SAP Security</b></p>
<a href="#">SSF-ID Part 2</a>	Define an additional Distinguished Name of the user certificate.

Parameter	Description
<a href="#">SSF Profile</a>	<p>Define the Secure Login Client profile. There are three options available.</p> <ul style="list-style-type: none"> <li>• Use Secure Login Client Profile The desired certificate is used for SSF, based on the Secure Login Client profile name. Example: <code>toksw:mem://securelogin/&lt;profile_name&gt;</code></li> <li>• Use Secure Login Client Profile and Re-authentication Adding the <code>[reauth]</code> option means that the user needs to authenticate again to the Secure Login Client profile, before a certificate is provided. Example: <code>[reauth]toksw:mem://securelogin/&lt;profile_name&gt;</code></li> <li>• In both cases and if the Secure Login Client profile was added manually by entering a Secure Login Server in <a href="#">File</a> <a href="#">Options</a> <a href="#">Policy Groups</a>, you must modify the configuration in the following way: Example: <code>toksw:mem://securelogin/user/&lt;profile_name&gt;</code> or <code>[reauth]toksw:mem://securelogin/user/&lt;profile_name&gt;</code></li> </ul> <p>You can also use a profile for smart cards. Enter the SSF profile with the following syntax:</p> <pre>tokcapi:&lt;token_ID&gt;&gt;</pre> <p>Example:</p> <pre>tokcapi:2B15-3774-844B #1 nFast PCI device, bus 6, slot 0</pre> <p>You can also use a profile for soft token certificates, for example for Microsoft Store. You find the CAPI ID of the Microsoft Enhanced Cryptographic Provider in the Secure Login Client trace. Enter the SSF profile with the following syntax:</p> <pre>tokcapi:*(*)</pre>
<a href="#">Destination</a>	<p>The RFC destination (logical destination) where the SSF RFC server program has been defined.</p> <p>Enter the value <code>SAP_SSFATGUI</code> (SSF for digital signatures on the front ends).</p>

For more information, see the SAP NetWeaver Library under [Function-Oriented View](#) [Security](#) [Digital Signatures and Encryption](#).



## 9.2 Parameter Overview for Secure Login Server

This parameter section gives you an overview of the parameters of Secure Login Server, the central component of Secure Login. It includes parameters for the client policies, user certificates, or user mapping.

### 9.2.1 Parameters for Initial Configuration (PKI Certificates)

This topic contains the parameters for the configuration of the PKI certificates.

#### Parameters for Standard Configuration

During the initial configuration, the initialization wizard steps through these parameters. You can also set these parameters manually if you choose [Manual](#) in the initialization wizard. This section contains an overview of the parameters and values of the PKI certificate management.

Parameters for PKI Certificate Management



Parameter	Description	Example
<i>Entry Name (mandatory)</i>	Enter the name of the Certification Authority	<b>Root CA</b>
<i>Key Length (mandatory)</i>	Select the encryption key length for the server (1024, 1536, 2048, 3072, or 4096 bits).	<b>2048</b>
<i>Valid From (mandatory)</i>	Enter the start date for the validity of this certificate.	<b>11/29/2013</b>
<i>Valid To (mandatory)</i>	Enter the end date for the validity of this certificate.	<b>04/25/2014</b>
<i>Country Name</i>	Enter the country abbreviation in this field (C)	<b>DE</b>
<i>Organization Name</i>	Enter the company name in this field (O)	<b>Company xyz</b>
<i>Locality Name</i>	Enter the regional information in this field (L).	<b>Walldorf</b>
<i>Organization Unit Name</i>	Enter the company name in this field (OU)	<b>SAP Security Department</b>

Parameter	Description	Example
<i>Common Name (mandatory)</i>	Enter the common name of the certificate (CN).	<b>Root CA SAP Security</b>
<i>Subject Alternative Name (DNS)</i>	Enter the subject alternative names in this field.  Enter the alternative name in this field. Typically this is the Fully Qualified Domain Name (FQDN).	<b>ServerName@FQDN.local</b>

## Parameters for External Configuration

If you want to use, for example, hardware security module (HSM) boards or other PKCS#11-enabled devices as external user Certification Authorities (CAs), you must set these parameters.

Parameters for PKI Certificate Management

Parameter	Description	Example
<i>Entry Name (mandatory)</i>	Enter the name of the Certification Authority	<b>User CA</b>
<i>Description</i>	Enter a description, for example, of the hardware security token.	<b>HSM token number 12</b>
<i>Key ID (mandatory)</i>	HSM token key identifier	<div>  <b>Example</b>  CA8E7B48B22531680AB4920C7D  820999D739166 </div> 9
<i>PIN</i>	Password or PIN for the PSE file you specify in <i>Token URI</i>	<b>mypassword</b> or <b>myPIN</b>
<i>Token URI (mandatory)</i>	The token URI contains the token type, the location of the middleware, and the name of the slot.	<div>  <b>Example</b>  <b>tokp11:/usr/local/  pkcs11driver/  driverpkcs11.so#HSM  Reader</b> </div>

## Related Information

[Initial Configuration \(Automatic\) \[page 176\]](#)

[Adding Certification Authorities \[page 219\]](#)


[Setting the AS ABAP Profile Parameters \[page 74\]](#)

## 9.2.2 Parameters for Signing Certificate Requests

This section describes the parameters located in the Secure Login Administration Console for signing a certificate request in the Certification Authority of the Secure Login Server PKI.

### Signing a Certificate Request of an SAP Application Server by a Secure Login Server CA

As an example scenario, a PSE or P12 file could be generated on the SAP application server side. On the SAP application server, a base64-encoded certificate request (PKCS#10) is created, copied to the Secure Login Server, and signed by the Secure Login Server CA.

An administrator logs on to an Application Server ABAP and starts the trust manager (transaction `STRUST`). After having selected the PSE, the administrator creates a certificate request using [Edit](#) [Create Certificate Request](#) . The trust manager displays the base64-encoded certificate request. The administrator selects it and copies it to the clipboard.

After having opened the Secure Login Administration Console, the administrator goes to the [Sign Certificate Requests](#) section of the [Certificate Management](#) tab and pastes the base64-encoded certificate request from the clipboard into the relevant field. To see the detail of the certificate request, he displays the certificate request using [Show Certificate Request](#) and enters the certificate validity. He chooses the issuer and the signature algorithm, and finally signs the certificate using the [Sign](#) button. The Secure Login Server CA signs the certificate request and creates a certificate response (PKCS#7). The certificate response can be returned to the Application Server ABAP.

## Parameters

You access the certificate signing function in the [Sign Certificate Requests](#) section of the [Certificate Management](#) tab of the Secure Login Administration Console.

### i Note

Entries marked with \* are mandatory.

## Parameters for Signing Certificate Requests

Option	Details
Base64 Encoded Certificate Request (PKCS #10) *	<p>The content of the certificate request in base64 encoding format.</p> <p>Use the option <a href="#">Select a File to Insert</a> to import a certificate request file. Use the button <a href="#">Read Content</a> to import.</p> <p>Another option is to copy and paste the content of the certificate request to the <a href="#">Base64-Encoded Certificate Request (PKCS#10)</a> field.</p> <p>The <a href="#">Show Certificate Request</a> button displays the content of the certificate request.</p> <p>The <a href="#">Reset</a> button enables you to clear the fields <a href="#">Base64-Encoded Certificate Request (PKCS#10)</a>, <a href="#">Certificate Request</a>, and <a href="#">Base64-Encoded Certificate Response (PKCS #7)</a>. Thus, you can also use it to undo the signing of certificates that have been signed already.</p>
Validity Period of Certificate (Months)*	Define the period of time for which the certificate is valid.
Certificate Template	If needed, select the desired certificate template. The default certificate template is used for the SAP environment.
Issuer*	Choose the desired CA certificate. The certificate request should be signed.
Signature Algorithm*	<p>Choose the signature algorithm you want to use. The default value is <a href="#">sha265WithRSAEncryption</a>.</p> <p>If you choose the <a href="#">Sign Certificate</a> button, you sign a certificate at the selected CA using the certificate request and the parameters.</p>
Base64-Encoded Certificate Response (PKCS#7)	This field displays the signed certificate response.
Certificate Encoding Type	<p>Select <a href="#">PEM</a> or <a href="#">DER</a> encoding type. A certificate response should be generated.</p> <p>Using the <a href="#">Download</a> function, you can save or open the certificate for further use.</p>

## 9.2.3 Secure Login Client Policy and Profiles

This section contains detailed information about the client policy and client profiles for Secure Login Client. The client policy is installed together with Secure Login Client on the client computer. Using the client policy configuration the client profiles can be downloaded from Secure Login Server.

## 9.2.3.1 Client Policy

Information about client policy parameters for the Secure Login Client.

These parameters are defined in the file `ProfileDownloadPolicy<profile_group_name>.reg`.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\System]

Parameter	Type	Description
<i>PolicyURL</i>	STRING	<p>Network resource from which the latest Secure Login Client profiles can be downloaded.</p> <p>The client policy is included in the file <code>GroupClientPolicy.xml</code>. Among other things, it contains the client policy name, the profile names, and the relevant enrollment URLs. You can also use IPv6 and IPv4 addresses to specify the network resource.</p>
<i>PolicyTTL</i>	DWORD	<p>The lifetime in minutes for verifying (updating) a new client policy on the Secure Login Server.</p> <p>The default is 0 minutes (hexadecimal value: <b>0</b>).</p> <p>By default, the Secure Login Client verifies during system startup of the client PC.</p>
<i>NetworkTimeout</i>	DWORD	<p>Network timeout in seconds before the connection is closed if the Secure Login Server does not respond. The default is 45 seconds (hexadecimal value: <b>2d</b>).</p>
<i>DisableUpdatePolicyOnStartup</i>	DWORD	<p>By default, the Secure Login Client verifies a new client policy during system startup of the client PC.</p> <p>You can use this parameter to disable this feature.</p> <p><b>1</b></p> <p>Disable automatic policy download.</p> <p><b>0</b></p> <p>Enable automatically policy download. Default value is <b>0</b>.</p>
<i>proxyIsPACURL</i>	DWORD	<p>You can configure the use of a proxy server using a proxy auto-config (PAC) URL for Secure Login Client policy download.</p> <p>If you want to use a proxy auto-config (PAC) file, set this parameter to <b>1</b>. In this case, <i>httpProxyURL</i> must have a valid URL.</p> <p>Default value is <b>0</b>.</p>

Parameter	Type	Description
<a href="#"><i>httpProxyURL</i></a>	STRING	<p>HTTP proxy to be used for a proxy auto-config (PAC) URL for Secure Login Client policy download. Only HTTP proxies without authentication and without SSL to proxy are supported.</p> <p>You can only use this proxy auto-config (PAC) URL if you set <a href="#"><i>proxyIsPACURL</i></a> to <b>1</b>.</p> <p><b><code>http://example.address.com:8888/wpad.dat</code></b></p>
<a href="#"><i>useWindowsHttpProxy</i></a>	DWORD	<p>You can only use this parameter if <a href="#"><i>httpProxyURL</i></a> is set to <b>AUTO</b>.</p> <p>If you use the value <b>1</b>, the Secure Login Server generates the configuration for automatically using the proxy settings of Microsoft Internet Explorer for the Secure Login Clients. The configuration flag is distributed with the policy download mechanism.</p> <p>For more information, see <a href="#">Automatically Using the Proxy Configuration of Microsoft Internet Explorer for Secure Login Client [page 154]</a>.</p>
<a href="#"><i>showErrorMsg</i></a>	DWORD	<p>Users get an error message whenever their authentication failed.</p> <p>Default value is <b>1</b>.</p>
<a href="#"><i>showSuccessMsg</i></a>	DWORD	<p>Users get a success message whenever their authentication was successful.</p> <p>Default value is <b>0</b>.</p>

## 9.2.3.2 Applications and Profiles

The policy downloader and/or the profile groups provide the Applications and Profiles configuration to the Secure Login Client using `ProfileGroup_<profile_group_name>.reg` and `ProfileDownloadPolicy_<profile_group_name>.reg`.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\applications\<Application Name>]

Parameter	Type	Description
<i>GssTargetName</i>	STRING	<p>Application-specific PSE URI (SAP server SNC name) that is matched when a suitable profile is searched. You can use the wildcards <b>*</b> and <b>?</b>.</p> <p>Example:</p> <p><b>CN=SAP, OU=SAP Security, C=DE</b></p> <p><b>CN=Server*, O=Company xyz</b></p> <p>Using the value <b>*</b> means that the client profile is used for all SAP servers.</p>
<i>profile</i>	STRING	<p>The name of the client profile to be used for the desired application.</p>
<i>allowFavorite</i>	DWORD	<p>Allow the user to select the authentication profile manually in Secure Login Client.</p> <p><b>0</b></p> <p>User cannot select the authentication profile manually in Secure Login Client.</p> <p><b>1</b></p> <p>User can select authentication profile manually in Secure Login Client.</p> <p>The default value is <b>1</b>.</p>
<i>reAuthentication</i>	DWORD	<p>Use single sign-on to log on to the Application Server ABAP.</p> <p><b>0</b></p> <p>Single sign-on is not available to log on to the Application Server ABAP. Users must enter their user names and passwords to log on.</p> <p><b>1</b></p> <p>The default value is <b>0</b>.</p>

In addition, it is possible to download the configuration using the `ProfileGroup<profile_group_name>.reg` file.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\profiles\<Profile Name>]

Parameter	Type	Description
<i>profileName</i>	STRING	The name of the client profile to be used for the desired application.
<i>pseType</i>	STRING	<p>Authentication type.</p> <p><b>promptedlogin</b></p> <p>Using this profile, the user will be requested to enter the user credentials.</p> <p><b>windowslogin</b></p> <p>Using this profile, the user credentials will be provided automatically (only available for Microsoft Windows authentication).</p> <p>Default value is <b>windowslogin</b>.</p> <p>In a client authentication profile for RFID tokens, this parameter defines the RFID reader type of the kiosk PCs.</p> <p><b>rfidpcsc</b></p> <p>This profile enables kiosk PCs to use RFID readers with the reader type PC/SC.</p> <p><b>rfidwaveid</b></p> <p>This profile enables kiosk PCs to use RFID readers with the reader type Wave ID.</p> <p><b>webadapter</b></p> <p>This profile enables users to get certificate information from the JavaScript Web Client.</p> <p><b>localSecurityHub</b></p> <p>This profile provides a TLS-protected communication channel with your browser.</p>



Parameter	Type	Description
<a href="#">enrollURL0</a>	STRING	<p>Secure Login Server URL that is used for user authentication and certificate request of the Secure Login Client. The enrollment URL depends on the configuration of the authentication profile. You can also use IPv6 and IPv4 addresses to specify the Secure Login Server.</p> <p><b><code>https://&lt;server&gt;:port/SecureLoginServer/slc(x)/doLogin?profile=&lt;profile_ID&gt;</code></b></p> <p>You can configure a path for a Secure Login Client 1.0 or for a Secure Login Client 2.0. Use <b><code>slc1</code></b> for Secure Login Client 1.0 and <b><code>slc2</code></b> for Secure Login Client 2.0.</p> <p>Example for Secure Login Client 2.0</p> <p><b><code>https://example.address.com:50201/SecureLoginServer/slc2/doLogin?profile=6506265a-3c5f-4fd1-88fd-5e962f92fe6c</code></b></p> <p>Use the <a href="#">Add</a> button to configure further Enroll URLs. This is the failover configuration for the Secure Login Client. If the first Enroll URL cannot be established, the Secure Login Client tries the next Enroll URL, defined here.</p>
<a href="#">httpProxyURL</a>	STRING	<p>HTTP proxy to be used with enrollment URLs. Only HTTP proxies without authentication and without SSL to proxy are supported.</p> <p>Example:</p> <p><b><code>http://example.address.com:8888</code></b></p>
<a href="#">reAuthentication</a>	DWORD	<p>This parameter defines how many login attempts are permitted with the Secure Login Client login form before it is closed again.</p> <p>Example with value 4:</p> <p>The Secure Login Client offers the login form 4 times (for example, wrong credential information), before the login form will be closed.</p> <p>Default value is <b><code>0</code></b>.</p> <p>The login form will never be closed. User needs to use the button <a href="#">Cancel</a> to close the login form.</p>
<a href="#">gracePeriod</a>	DWORD	<p>Value in seconds when an enrollment is to be carried out before the certificate expires. Default value is <b><code>0</code></b>.</p> <p>Value: <b><code>-1</code></b></p> <p>An expiration of a certificate does not trigger an automatic re-enrollment.</p>

Parameter	Type	Description
<i>inactivityTimeout</i>	DWORD	<p>Value in seconds until an automatic logout is performed (due to mouse and keyboard inactivity).</p> <p>Value: <b>-1</b></p> <p>No Single Sign-On (SSO). Each SNC connection forces a new login.</p> <p>Value: <b>0</b></p> <p>No timeout. SSO without constraints.</p> <p>The default value is <b>0</b>.</p> <p>Enter a value &gt; 0.</p> <p>Seconds until an automatic logout is executed.</p>
<i>autoReenrollTries</i>	DWORD	<p>The number of failed authentications in a row after which automatic re-enrollment is stopped.</p> <p>User name and password caching can be turned on to provide the automatic re-enrollment of certificates that are going to expire. Possible values:</p> <p><b>0</b>: Turn off</p> <p>Do not re-enroll automatically; do not cache user name and password. A re-enrollment must always be performed manually by the user.</p> <p>Value &gt;0 (n): Turn on with n tries to succeed:</p> <p>Try to re-enroll a maximum of n times before either a new certificate is received or the user name and password cache are cleared. The error counter is reset on success.</p> <p>The default value is <b>0</b>.</p>
<i>autoEnroll</i>	DWORD	<p>A user automatically gets an X.509 certificate when the Secure Login Client starts.</p> <p><b>0</b>: Turn off</p> <p><b>1</b>: Automatic provisioning of user certificates</p> <p>If <i>pseType</i> is set to <b>windowslogin</b>, user credentials are provided automatically (only applies for Microsoft Windows authentication).</p> <p>If <i>pseType</i> is set to <b>promptedlogin</b>, the system prompts the users to enter their credentials.</p>
<i>keySize</i>	DWORD	<p>RSA Key Length. The default value is <b>1024</b> (hexadecimal value: <b>400</b>).</p>
<i>UniqueClientID</i>	STRING	<p>Custom-defined string; will be displayed in the instance log or can be used for network filtering issues.</p>

Parameter	Type	Description
<i>networkTimeout</i>	DWORD	Network timeout (in seconds) before the connection is closed if the server does not respond The default value is <b>45</b> (hexadecimal value: <b>2d</b> ).
<i>sslHostCommonNameCheck</i>	DWORD	<p>This applies to the SSL server certificate – this checks if the peer host name is given in the <i>Common Name</i> (CN) field of the SSL Server certificate.</p> <p><b>1</b></p> <p>Verify the SSL server host name with the <i>Common Name</i> (CN) field of the SSL server certificate.</p> <p><b>0</b></p> <p>Do not verify SSL server host name with the <i>Common Name</i>(CN) field of the SSL Server certificate.</p> <p>The default value is <b>0</b>.</p>
<i>sslHostAlternativeNameCheck</i>	DWORD	<p>This applies to the SSL server certificate – this checks whether the peer host name is given in its <i>Subject Alternative Name</i> attribute of the certificate.</p> <p><b>1</b></p> <p>Verify the SSL server host name with the <i>Subject Alternative Name</i> attribute of the SSL Server certificate.</p> <p><b>0</b></p> <p>Do not verify the SSL server host name with the <i>Subject Alternative Name</i> attribute of the SSL server certificate.</p> <p>Default value is <b>1</b>.</p>
<i>sslHostExtensionCheck</i>	DWORD	<p>This applies to the SSL server certificate – this checks if the extended key usage <i>ServerAuthentication</i> is defined.</p> <p><b>1</b></p> <p>Verify whether the extended key usage ServerAuthentication is defined in the SSL Server certificate.</p> <p><b>0</b></p> <p>Do not verify whether the extended key usage ServerAuthentication is defined in the SSL Server certificate.</p> <p>The default value is <b>0</b>.</p>
<i>newPinType</i>	STRING	Message text value is used for messages (change PIN/password) to the Secure Login Client and Secure Login Web Client. Available values are <b>pin</b> and <b>password</b> .

## 9.2.4 Parameters for the Policy Configuration

The policy configuration allows you to set parameters for the login modules.

The following topics contain an overview of the policy configuration parameter. You can set them in the SAP NetWeaver Administrator under *Authentication and Single Sign-On*. You can set parameters for the following login module parameters:

- SPNego login module
- LDAP login module
- RADIUS login module
- ABAP login module

### Related Information

[Parameters for LDAP Login Modules \[page 287\]](#)

[Parameters for RADIUS Login Modules \[page 289\]](#)

[Parameters for ABAP Login Modules \[page 291\]](#)

### 9.2.4.1 Parameters for Client Configuration

This topic contains the parameters for authentication profiles.

During the configuration of the authentication profile, you come to a step where you configure the client configuration.

#### **i** Note

The fields with the asterisk (\*) are mandatory fields.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\profiles\<authentication\_profile\_name>]

Parameters	Details
<a href="#">Auto-enroll</a>	<p>A user automatically gets an X.509 certificate when the Secure Login Client starts.</p> <p><b>False: Turn off</b></p> <p><b>True: Automatic provisioning of user certificates</b></p> <p>If <i>pseType</i> is set to <i>windowslogin</i>, user credentials are provided automatically (only applies for Microsoft Windows authentication with SPNegoLoginModule AA).</p> <p>If <i>pseType</i> is set to <i>promptedlogin</i>, the system prompts the users to enter their credentials. This applies for the following login modules: SecureLoginModuleLDAP, SecureLoginModuleSAP, SecureLoginModuleRADIUS, and BasicPasswordLoginModule. If these login modules are initially set, the default is <i>promptedlogin</i>.</p>
<a href="#">Automatic Re-enroll Attempts</a>	<p>The number of successive failed authentications after which automatic re-enrollment is stopped. You can activate the user name and password caching to ensure the automatic re-enrollment of certificates that are going to expire. Possible values:</p> <p><b>0</b>: Turn off:</p> <p>Does not re-enroll automatically, does not cache user name and password. A re-enrollment must always be performed manually by the user.</p> <p><b>&gt;0 (n)</b>: Turn on with n tries to succeed:</p> <p>Tries to re-enroll a maximum of n times before either a new certificate is received or the user name and password cache are cleared. The error counter is reset on success.</p> <p>The default value is <b>0</b>.</p>

Parameters	Details
<i>Enrollment URL</i>	<p>Secure Login Server URL that is used for user authentication and certificate request. Enroll URL depends on the configuration of the authentication profile.</p> <pre>https://&lt;host_name&gt;:&lt;port&gt;/ SecureLoginServer/&lt;protocol_version&gt;/ doLogin?profile=&lt;profile_ID&gt;</pre> <p>Enrollment URL defined in a authentication profile &lt;profile_ID&gt; of the Secure Login Server.</p> <p>To configure further enrollment URLs, use the <b>Add</b> button. This is the failover configuration for the Secure Login Client. If the Secure Login Client establishes a connection to the first enrollment URL, it tries the next enrollment URL, defined here.</p>
<i>Grace Period (Seconds)</i>	<p>Integer value in seconds for the time in which an enrollment is to be carried out before the certificate expires. <b>-1</b> means that you disable automatic re-enrollment.</p> <p>The default value is <b>0</b></p>
<i>HTTP Proxy URL</i>	<p>HTTP proxy to be used with enrollment URLs. Only HTTP proxies without authentication and without SSL to proxy are supported.</p> <p>Example: <code>http://example.address.com:8888</code></p> <p>If you want to use the proxy server settings configured in Microsoft Internet Explorer, set the parameter <b>AUTO</b>. In this case, the Secure Login Client uses the proxy server settings from the Internet connection settings of Microsoft Internet Explorer. For more information, see <a href="#">Automatically Using the Proxy Configuration of Microsoft Internet Explorer for Secure Login Client</a> [page 154].</p>

Parameters	Details
<i>Inactivity Timeout (Seconds)</i>	<p>Value in seconds until an automatic logout is performed (due to mouse and keyboard inactivity). Possible values:</p> <p>Value <b>-1</b></p> <p>No Single Sign-On (SSO). Each SNC connection forces a new login.</p> <p>Value <b>0</b></p> <p>No timeout. SSO without constraints.</p> <p>The default value is <b>0</b>.</p> <p>Value <b>n</b></p> <p>Seconds until an automatic logout takes place.</p>
<i>Network Timeout (Seconds)</i>	<p>Network timeout (in seconds) before the connection is closed if the server does not respond</p> <p>The default value is <b>45</b></p>
<i>New PIN/Password Response Text</i>	<p>Message text value used for messages (change PIN/password) to the Secure Login Client and Secure Login Web Client.</p> <p>Available values are <b>pin</b> and <b>password</b>.</p>
<i>Policy Configuration Name</i>	
<i>Profile Type</i>	<p>If you are using kiosk PCs as clients with RFID identification, this parameter defines the RFID reader type.</p> <p>Available values are <b>RFID (PCSC based)</b> or <b>RFID (WaveID based)</b>.</p>
<i>Re-authentication</i>	<p>This parameter defines how many logon attempts are permitted with the Secure Login Client logon form before it is closed again.</p> <p>Example with the value <b>4</b>:</p> <p>The Secure Login Client offers the logon form 4 times (the logons fail, for example, due to wrong credential information) before the logon form is closed.</p> <p>The default value is <b>0</b>.</p> <p>With this value, the logon form is never closed. The user needs to use the <b>Cancel</b> button to close the logon form.</p>
<i>Show Error Message</i>	<p>The default value is <b>true</b>. Error messages are displayed in the client.</p>

Parameters	Details
<a href="#">Show Success Message</a>	The default value is <b>true</b> . Success messages are displayed.
<a href="#">SSL Host Alternative Name Check</a>	<p>This applies to the SSL server certificate – this checks if the peer host name is given in the <a href="#">Subject Alternative Name</a> attribute of the certificate.</p> <p><b>True</b></p> <p>Verifies the SSL server host name with the <a href="#">Subject Alternative Name</a> attribute of the SSL Server certificate.</p> <p><b>False</b></p> <p>Does not verify the SSL server host name with the <a href="#">Subject Alternative Name</a> attribute of the SSL Server certificate.</p> <p>The default value is <b>False</b></p>
<a href="#">SSL Host Common Name Check</a>	<p>This applies to the SSL Server certificate – this checks if the peer host name is given in the <a href="#">Common Name</a> (CN) field of the SSL Server certificate.</p> <p><b>True</b></p> <p>Verifies the SSL server host name with the <a href="#">Common Name</a> (CN) field of the SSL Server certificate.</p> <p><b>False</b></p> <p>Does not verify the SSL server host name with the <a href="#">Common Name</a> (CN) field of the SSL Server certificate.</p> <p>The default value is <b>False</b></p>
<a href="#">SSL Host Extension Name Check</a>	<p>This applies to the SSL server certificate – this specifies whether the system checks if the extended key usage <a href="#">ServerAuthentication</a> is defined.</p> <p><b>True</b></p> <p>Verify if the extended key usage ServerAuthentication is defined in the SSL server certificate.</p> <p><b>False</b></p> <p>Does not verify if the extended key usage ServerAuthentication is defined in the SSL Server certificate.</p> <p>The default value is <b>False</b></p>



## 9.2.4.2 Parameters for Secure Login Web Client Configuration

This topic contains the Secure Login Web Client configuration parameters.

During the configuration of the authentication profile, you come to a step where you configure the Secure Login Web Client configuration.

### Note

The fields with the asterisk (\*) are mandatory fields.

Secure Login Web Client Configuration

Parameters	Description
<i>Post Authentication Actions</i>	
<i>Actions</i>	<p>The action to be performed by the Secure Login Web Client after successful user authentication. The following options are available:</p> <ul style="list-style-type: none"><li>• <i>No Action</i> After successful user authentication, no action is performed.</li><li>• <i>Redirect to URL</i> Enter a URL for certificate-based login. After successful user authentication, this URL is called. You can use this URL to configure a location where SSL client based authentication with the enrolled X.509 certificate is required, for example, in the SAP Enterprise Portal.</li><li>• <i>Log On to ABAP System</i> After successful authentication, the user logs on to an ABAP system.</li><li>• <i>Log On to ABAP Message Server</i> Having chosen this action, you need not address a field in SAP GUI or an INI file that contains the configuration for SAP GUI. Leave the <i>SAP GUI Description</i> field empty.</li><li>• <i>Redirect to URL and Log On to ABAP Message Server</i></li><li>• <i>Redirect to URL and Log On to ABAP Message Server</i></li><li>• <i>Launch SAP Logon Pad</i> After successful authentication, the SAP Logon pad is started automatically.</li><li>• <i>Redirect to URL and Launch SAP Logon Pad</i></li></ul> <p>For more information on connection types for starting SAP GUI, see <a href="#">Configuring Secure Login Web Client Connections to SAP GUI [page 80]</a>.</p>
<i>Web Client URL</i>	
<i>IP Address/Host Name</i>	IP address or host name of Secure Login Server which is used to generate to Web Client URL.
<i>Port</i>	Port of Secure Login Server for the Web Client URL.

Parameters	Description
<i>URL</i>	This URL is made up of the IP address/host name and of the port
<i>Client Behavior</i>	
<i>Web Adapter Mode (requires Secure Login Client installation)</i>	<p>Activate this checkbox to reuse an already existing installation of the Secure Login Client at the start of a Secure Login Web Client. If Web adapter mode is active, the Secure Login Server download only <code>slwc.exe</code>.</p> <div> <p><b>i Note</b></p> <p>You have installed a Secure Login Client and activated <a href="#">Secure Login Server Support</a> during the installation procedure. This feature is only available on Microsoft Windows.</p> </div>
<i>Platform Binaries Download Path</i>	
<i>Microsoft Windows</i>	<p>Enter the download location for the security libraries. By default, the location of the Secure Login Web Client files depends on the operating system.</p> <p>Default:</p> <p>For Microsoft Windows XP:</p> <p><b>%APPDATA%</b></p> <p>For Microsoft Windows Vista/7 or higher:</p> <p><b>%LOCALAPPDATA%</b></p> <p>Example for Microsoft Windows XP:</p> <p>%USERPROFILE%\%APPDATA%\sapsnc</p> <p>Example for Microsoft Windows Vista/7:</p> <p>%USERPROFILE%\%LOCALAPPDATA%\sapsnc</p>
<i>OS X</i>	<p>Default:</p> <p>\$HOME/sapsnc</p> <p>Example:</p> <p>\$HOME/.sap_webclient/sapsnc</p>

### 9.2.4.3 Parameters for LDAP Login Modules

This table contains an overview of the parameters you can set for LDAP login modules.

You set these parameters when you create a destination for an LDAP login module. For more information on destination management, see related link.

## Parameters for LDAP Login Modules

Parameters	Details
In <i>Options of login module</i> of the SAP NetWeaver Administrator	
<i>LdapDestination</i>	Enter the exact name of the LDAP destination.
<i>LdapServerType</i>	<p>You use this parameter if you want to send messages from LDAP to the Secure Login Client. Enter the value for the LDAP server you are using. SAP NetWeaver Single-Sign-On supports Active Directory (default) and Oracle Directory Server.</p> <p>Values for LDAP servers:</p> <p><b>AD</b> (default) for Active Directory</p> <p><b>ODSEE</b> for Oracle Directory Server</p> <p>For more information, see the related link.</p>
<i>MappingMode</i>	<p>This parameter is only valid if you are using Active Directory. It contains options that determine to which format the user logon ID is mapped. By default, the user logon ID is mapped to the user principal name (UPN). For more information, see SAP Note <a href="#">2058282</a>.</p> <p>The default is no value.</p> <p>Values:</p> <p><b>&lt;none&gt;</b> or <b>DEFAULT</b></p> <p>Mapping with the user principal name</p> <div><p>❖ Example</p><p>The user name j.doe is mapped to UPN</p><p>j.doe@DOMAIN.COM</p></div> <p><b>LogonID</b></p> <p>Mapping with the user logon ID</p> <div><p>❖ Example</p><p>The user name j.doe is mapped to the user logon ID</p><p>j.doe</p></div>

Parameters	Details
<a href="#"><i>PasswordExpirationAttribute</i></a>	<p>LDAP attribute that contains the expiration date of the user password for the Secure Login Client. Secure Login Server can process one of the following formats:</p> <p>Generalized time formats:</p> <p><b>20120630181530Z</b>= 30. June 2012 18:15:30 (UTC)</p> <p><b>20120630191530+0100Z</b>= 30. June 2012 20:15:30 (CET)</p> <p><b>20120630181530 . 0Z</b>= 30. June 2012 18:15:30 (UTC)</p> <p><b>20120630191530 . 0+0100Z</b>= 30. June 2012 20:15:30 (CET)</p> <p>MS Gregorian calendar time format (100-nanosecond intervals since 1. January 1601 (UTC))</p> <p><b>1298555373000000000</b>= 30. June 2012 18:15:30 (UTC)</p> <p>Netscape Password Expiring time format (seconds until password expires)</p> <p><b>864000</b>= 10 days from current date until password expires</p> <p>If a password expiration warning message is configured, the <a href="#"><i>LdapBaseDN</i></a> property must be given in complete DN form (UPN on Microsoft Active Directory) in the configuration of the LDAP destination.</p> <p>The <a href="#"><i>PasswordExpirationAttribute</i></a> value is used for the password expiration warning message only. By default no value is defined.</p>
<a href="#"><i>PasswordExpirationGracePeriod</i></a>	<p>The interval (in days) for a password expiration warning message to be sent to the Secure Login Client prior to a password expiring.</p>

## Related Information

[Creating Destinations \[page 197\]](#)

[Enabling the Display of LDAP Messages in Secure Login Client \[page 159\]](#)

## 9.2.4.4 Parameters for RADIUS Login Modules

This table contains an overview of the parameters you can set for RADIUS login modules

You set these parameter when you create a destination for a RADIUS login module.

## Parameters in SAP NetWeaver Administrator

Parameters	Details
<a href="#">RadiusDestination</a>	Enter the exact name of your RADIUS destination.

## Parameters in the Secure Login Administration Console

Parameters	Details
<a href="#">Authentication Method*</a>	<p>Authentication method for the RADIUS server. Possible values are:</p> <p><a href="#">PAP</a></p> <p><a href="#">CHAP</a></p> <p><a href="#">MSCHAP</a></p> <p>The default value is <a href="#">PAP</a>.</p>
<a href="#">IP Address/Host Name*</a>	Host address of the RADIUS server (used for user authentication).
<a href="#">Port*</a>	The port number used by the RADIUS server for authentication requests. Typical values are <b>1645</b> or <b>1812</b> . The default value is <b>1645</b> .
<a href="#">Timeout (Milliseconds)*</a>	Period of time the Secure Login Server waits for a response before trying the next RADIUS Server (in milliseconds). The default value is <b>5000</b> milliseconds.
<a href="#">Shared Secret*</a>	A Shared Secret is used to encrypt the user password. This Shared Secret also needs to be defined in the RADIUS Server. Paste your Shared Secret into this field.
<a href="#">Confirm Shared Secret*</a>	Paste your Shared Secret again for confirmation.

## Advanced Configuration for RSA Authentication

<a href="#">Import Server Message File:</a>	<div> <b>i Note</b>            If you import a RADIUS Server message file, the following parameters are filled automatically.         </div>
<a href="#">ExtInputMustChoose_C:</a>	Enter a new PIN having n alphanumeric characters:
<a href="#">ExtInputMustChoose_C_C:</a>	Enter a new PIN having from n to n alphanumeric characters:
<a href="#">ExtInputMustChoose_D:</a>	Enter a new PIN having n digits:
<a href="#">ExtInputMustChoose_D_D:</a>	Enter a new PIN having from n to n digits:

Parameters	Details
<i>ExtInputNextCode:</i>	Wait for token to change, then enter the new tokencode:
<i>ExtInputReenterPin:</i>	Please re-enter new PIN:
<i>ExtOutputChange:</i>	PIN Accepted. Wait for token code to change, then enter the new passcode:
<i>ExtOutputReject:</i>	PIN rejected. Please try again.

## 9.2.4.5 Parameters for ABAP Login Modules

This table contains an overview of the parameters you can set for ABAP login modules.

You can set the following parameters when you configure the destination for an ABAP login module. In this case the destination is already available in the SAP NetWeaver Administrator.

Options of login module

Parameters	Details
<i>Destination</i>	The destination is already available in the SAP NetWeaver Administrator.
<i>maxNbrConnections</i>	Maximum number of connections.
<i>PasswordAlphanumeric</i>	<p>This parameter is part of the password policy for the client-side policy consistency check. Possible values:</p> <p><b>true</b></p> <p>The password can contain only alphanumeric characters (A-Z, a-z, 0-9).</p> <p><b>false</b></p> <p>The password can contain alphanumeric and special characters (such as !\$%&amp;).</p> <p>This parameter must be consistent with the SAP password policy.</p> <p>The default value is <b>true</b>.</p>

Parameters	Details
<a href="#"><i>PasswordMax</i></a>	<p>This parameter is part of the password policy for the client-side policy consistency check, specifically the maximum number of characters in the password to be used.</p> <p>This parameter must be consistent with the SAP password policy.</p> <p>The default value is <b>30</b>.</p>
<a href="#"><i>PasswordMin</i></a>	<p>This parameter is part of the password policy for the client-side policy consistency check, specifically the minimum number of characters in the password to be used.</p> <p>This parameter must be consistent with the SAP password policy.</p> <p>The default value is <b>1</b>.</p>
<a href="#"><i>SAPTimeout</i></a>	<p>Timeout for login</p> <p>Maximum number of connections until authentication is blocked</p>

## 9.2.4.6 Parameters for Downloading Policies Using Profile Groups

When you create a profile group from the authentication profiles, you can specify some properties, such as protocol, host name, policy update interval, timeout, and actions after policy download.

You can determine the parameters used by a policy update from the Secure Login Server to the Secure Login Client. The parameters define the download mode of the registry files

`ProfileGroup_<profile_group_name>.reg` and  
`ProfileDownloadPolicy_<profile_group_name>.reg`.

### **i** Note

The fields with the asterisk (\*) are mandatory fields.

Parameters for Downloading Policies Using Profile Groups

Parameters	Details
<a href="#"><i>Group Name:</i>*</a>	The profile group name appears here.
<a href="#"><i>Description:</i></a>	
<a href="#"><i>Protocol:</i>*</a>	Default is <a href="#">https</a> . For security reasons, we recommend to use https.

Parameters	Details
<i>IP Address/Host Name:*</i>	<p>Default is <i>&lt;host_name&gt;</i>. The current host name appears. You can also use the IP address or the computer name.</p> <p>Example:</p> <p>vmx6032</p>
<i>Port:*</i>	<p>Default is <i>50,001</i>. The port that is currently configured in the SAP NetWeaver Administrator appears automatically. If you use http, choose <i>50,000</i>.</p>
<i>Policy Update Interval (Minutes):*</i>	<p>Lifetime in minutes for verifying (update) a new client policy.</p> <p>Default is <b>0</b> minutes.</p> <p>By default, the Secure Login Client verifies a new client policy during the system startup of the client PC.</p>
<i>Network Timeout (Seconds):*</i>	<p>Network timeout in seconds before the connection is closed if the server does not respond.</p> <p>The default value is <b>45</b> seconds.</p>
<i>Update Policy on Startup (Default:Yes):</i>	<p>By default the Secure Login Client verifies during a new client policy during the system startup of the client PC.</p> <p>You can use this parameter, to disable this feature.</p> <p><b>Yes</b></p> <p>Secure Login Client updates the client policy at startup.</p> <p><b>No</b></p> <p>Secure Login Client does not update the client policy at startup.</p> <p>Default value is <b>Yes</b>.</p>
<i>Actions at Policy Download</i>	



## Parameters

## Details

### *Actions on SAP AS ABAP Application Settings:*

Existing profiles are handled as configured by action.

#### *Clean*

Deletes all existing profiles in the selected policy key before the given ones are written.

#### *Replace*

Replaces any existing profiles of the same name in the selected policy key with a given one.

#### *Keep*

Keeps any existing profiles of the same name in the selected policy. Does not overwrite the given one (default).

### **i Note**

In a migration setup from SAP NetWeaver Single Sign-On 1.0 to 2.0, it makes sense to use *Keep*. The Secure Login Server keeps the profile group configuration of the Secure Login Server 1.0 for fallback purposes.

The default value is *Clean*.

### *Action on Client Settings:*

Existing profiles are handled as configured by action.

#### *Clean*

Deletes all existing profiles in the selected policy key before the given ones are written.

#### *Replace*

Replaces any existing profiles of the same name in the selected policy key with a given one.

#### *Keep*

Keeps any existing profiles of the same name in the selected policy. Does not overwrite the given one (default).

The default value is *Clean*.

### **i Note**

In a migration setup from SAP NetWeaver Single Sign-On 1.0 to 2.0, it makes sense to use *Keep*. The Secure Login Server keeps the profile group configuration of the Secure Login Server 1.0 for fallback purposes.

## 9.2.5 Parameters for User Authentication in the Authentication Profile

This section contains the parameters for user authentication of your respective clients. The range of parameters depends on the authentication profile you have selected - for example, a Secure Login Client authentication profile for LDAP or a Secure Login Web Client authentication profile for SAML 2.0.

### 9.2.5.1 Parameters for User Authentication

Depending on the chosen authentication profile, you determine how users in a Secure Login Client or Secure Login Web Client authenticate.

These tables contain the parameters for the authentication profile that you can configure in the Secure Login Administration Console.

Parameters for User Authentication (for Secure Login Client Profiles)

Parameter	Description	Example
<a href="#">Policy Configuration Name</a>	Enter the policy configuration you want to use for user authentication. The policy configuration contains the logon procedure configured, for example, in authentication stacks. Maintain the policy configurations in the SAP NetWeaver Administrator.	Policy configuration with <b>SecureLoginModule20LDAP</b> in the authentication stack
<a href="#">Link to: Authentication and Single Sign-On</a>	Using this link to the SAP NetWeaver Administrator, you can set the policy configuration in the SAP NetWeaver AS for Java.	

Parameters for User Authentication (for Secure Login Web Client Profiles)

Parameter	Description	Example
<a href="#">Reuse User Authentication Session</a>	If you set this parameter to active, the Secure Login Server checks whether the user is being logged on to the portal. In this case, the user gets a certificate from the browser right at the start of the Secure Login Web Client.	

Parameter	Description	Example
<a href="#">Use Policy Configuration</a> with <a href="#">Policy Configuration Name</a>	<p>If you choose this parameter, you can open a dropdown list and choose the policy configuration you want to use.</p> <div> <p><b>i Note</b></p> <p>If you want to set up SAML 2.0 authentication, it is mandatory that you choose the policy configuration that enables SAML 2.0 authentication and that you select <a href="#">Standard Authentication Form</a> in <a href="#">Select Authentication Form</a>.</p> <p>For more information, see the related link.</p> </div>	<p>In the case of SAML 2.0 authentication, choose a policy configuration where <a href="#">SAML2LoginModule</a> has been configured earlier.</p>
<a href="#">Select Authentication Form</a> with <a href="#">Policy Configuration Name</a>	<p>This parameter determines which authentication form the browser uses.</p> <p>The following authentication forms are possible:</p> <ul style="list-style-type: none"> <li>• <a href="#">Java Applet Web Client</a></li> <li>• <a href="#">Standard Authentication Form</a></li> <li>• <a href="#">Apple iOS SCEP</a></li> </ul> <div> <p><b>i Note</b></p> <p>If you are using SAML 2.0 authentication with Secure Login Web Client, choose <a href="#">Standard Authentication Form</a> to enable the Secure Login Server to communicate with the identity provider that provides the users' identities.</p> <p>Whenever users start the Secure Login Web Client, they can choose the identity provider that manages the users' identity information and authentication.</p> </div>	
<a href="#">Link to: Authentication and Single Sign-On</a>	<p>Using this link to the SAP NetWeaver Administrator, you can set the policy configuration in the SAP NetWeaver AS for Java.</p>	

## Related Information

[Using Secure Login Server for SAML 2.0 Authentication \[page 86\]](#)

### 9.2.6 Parameters for Certificate Configuration in the Authentication Profile

This section contains the parameters for user certificates, for example, for user user logon ID mapping with attribute configuration, archiving, etc.

For a detailed overview of the parameters, see the related links.

## Related Information

[Parameters for Certificate Configuration \[page 297\]](#)

[Parameters for Certificate Attribute Configuration \[page 298\]](#)

#### 9.2.6.1 Parameters for Certificate Configuration

This table contains the parameters for certificate configuration for the authentication profile, which you can configure in the Secure Login Administration Console.

This table contains the parameters for the authentication profile, which you can configure in the Secure Login Administration Console.

#### Note

The fields with the asterisk (\*) are mandatory fields.

Parameters for User Certificate Configuration

Parameter	Description	Example
<i>Country Name</i>	Enter the country abbreviation in this field (C)	<b>DE</b>
<i>Organizational Name</i>	Enter the company name in this field (O)	<b>Company xyz</b>
<i>Locality Name</i>	Enter the regional information in this field (L).	<b>Walldorf</b>

Parameter	Description	Example
<i>Organization Unit Name</i>	Enter the company name in this field (OU)	<b>SAP Security Department</b>
<i>Validity Period (Minutes) (mandatory)</i>	Enter the period of validity of the certificate (CN).  Default value is <b>600</b> .	<b>600</b>
<i>Validity Offset (mandatory)</i>	Time offset in minutes relative to the server system time for the certificates to start being valid. This parameter is helpful if the client and server time are not in sync.  Default value is <b>-5</b> .	<b>-5</b>
<i>Key Length (mandatory)</i>	Select the encryption key length for the server (1024, 1536, 2048, 3072, or 4096 bits).	<b>2048</b>
<i>Signature Algorithm (mandatory)</i>	Choose the signature algorithm for the protection of the certificates. You find a complete list of the signature algorithms in the related link.  Default value is <b>sha256WithRSAEncryption</b>	<b>sha256WithRSAEncryption</b>

## Related Information

[X.509 Certificates \[page 375\]](#)

### 9.2.6.2 Parameters for Certificate Attribute Configuration

These are the parameters for the certificate attributes for user mapping the Secure Login Server passes on to the Secure Login Client.

#### **i** Note

The fields with the asterisk (\*) are mandatory fields.

## Parameters for Certificate Attribute Configuration

Parameter	Description
<i>Common Name</i> *	<p>Here you enter the common name. You can also use the following values from the destination:</p> <p><b>AUTH : USERID</b></p> <p><b>AUTH : UPN</b></p> <p><b>AUTH : DCS</b></p> <p><b>PADDEDNAME</b> Use this value to enable padding of the common name or any additionally defined certificate attributes.</p> <div> <p><b>Note</b></p> <p>You define the attributes for the certificate in the destination.</p> </div>
<i>Country Name</i>	Enter the two-character country code or use the above-mentioned values.
<i>Organizational Name</i>	Enter the organizational name or use the above-mentioned values.
<i>Organizational Unit Name</i>	Enter the organizational unit name or use the above-mentioned values.
<i>Locality</i>	Enter the locality or use the above-mentioned values.
<i>Appendix Subject Name</i>	Values: <b>AUTH : DCS</b> variable or a complete Relative Distinguished Name (RDN) Example: <b>OU=SAP, CN=Demo</b>
<i>Subject Alternative Name (RFC822 Name)</i>	In this certificate attribute, the RFC822 name appears in a sequence.
<i>Subject Alternative Name</i> (Principal Name)	The principal name appears in a sequence.

## 9.2.6.3 Parameters of User Mapping Destinations and Attributes

This table contains an overview of the parameters for user mapping. Moreover, it lists the user mapping attributes.

### Note

Entries marked with \* are mandatory.

#### Parameters for User Mapping Destinations and Attributes

Parameter	Description
<i>Mapping Destinations</i>	Here you select the LDAP or Active Directory destination.
<i>Enable User Logon ID Mapping</i>	Activate this checkbox to enable user logon ID mapping. The default is not active.
<i>LDAP Search Attribute</i> *	Here you enter the LDAP search attribute with search values. Default is <i>userPrincipalName</i> .
<i>Search Value</i> *	The default LDAP search value is <i>AUTH:UPN</i> .
<i>Mapping Attributes</i>	<p>Select one or several of the following mapping attributes values:</p> <ul style="list-style-type: none"><li><i>displayName</i></li><li><i>givenName</i></li><li><i>mail</i></li><li><i>name</i></li><li><i>sAMAccountName</i></li><li><i>sn</i>(first name)</li><li><i>userPrincipalName</i></li></ul> <p>Example:</p> <p>If you add the attribute name <i>userPrincipal</i>, <i>name</i>, <i>mail</i>, the following resulting values are displayed in dropdown list for the Certificate Attribute Configuration section:</p> <p>(LDAP:userPrincipal), (LDAP:name), (LDAP:mail).</p>

## 9.2.6.4 Parameters for User Logon ID Padding

If you want to use user logon ID padding, use the following parameters.

### i Note

The fields with the asterisk (\*) are mandatory fields.

#### Parameters for User Logon ID Padding

Parameter	Details
<i>Padding for</i> *	<p>Here you enter for which user name the padding is applied.</p> <p>Default: <b>AUTH : USERID</b></p>

Parameter	Details
<i>Maximum Length</i> *	<p>Maximum number of characters that a user name in the common name (CN) field can have. If the given use name is longer, it is cut from the right side.</p> <p>Default value: <b>12</b></p> <p>Example:</p> <p>"LongUsernameSAP" is cut off to "LongUsername" with the default settings.</p>
<i>Padding Length</i> *	<p>If user names in the common name (CN) field need a fixed or minimum length, padding can be turned on. The padding length sets the minimum length of user names.</p> <p>Default value: None</p>
<i>Padding Character</i> *	<p>The padding character is used to fill user names on the left side if their size is smaller than the configured padding length (<i>Padding Length</i>).</p> <p>Default value: None</p> <p>Example:</p> <p><i>Padding Length</i>= <b>11</b> and <i>Padding Character</i> = <b>0</b>.</p> <p>The result is "ShortName" is extended to 00ShortName</p> <p>Typically this configuration is used if personnel numbers are used.</p>

## 9.2.6.5 List of Certificate Templates of Secure Login Server

This is an overview of the certificate templates that are available in the Secure Login Server.

### PKI Level 1 - Top Issuers

Field	Value
Name	Root CA Template
Description	Secure Login Server Root Certificate Authority
PKI Role	Root Certificate Authority



Field	Value
Basic Constraints	TRUE
Basic Constraints Is CA	TRUE
Basic Constraints Path Length	1
Certificate Policies OIDs	none
Key Usages	keyCertSign
Extended Key Usages	none
Standard Extensions	SubjectKeyIdentifier
Private Extensions	none

## PKI Level 2 - Intermediate Issuers

Field	Value
Name	User CA Template
Description	Generic End User Certificate Authority
PKI Role	User Certificate Authority
Basic Constraints	TRUE
Basic Constraints Is CA	TRUE
Basic Constraints Path Length	0
Certificate Policies OIDs	none
Key Usages	keyCertSign
Extended Key Usages	none
Standard Extensions	AuthorityKeyIdentifier SubjectKeyIdentifier
Private Extensions	none

Field	Value
Name	SAP CA Template

Field	Value
Description	Generic SAP Client and Server Certificate Authority
PKI Role	SAP Certificate Authority
Basic Constraints	TRUE
Basic Constraints Is CA	TRUE
Basic Constraints Path Length	0
Certificate Policies OIDs	none
Key Usages	keyCertSign
Extended Key Usages	none
Standard Extensions	AuthorityKeyIdentifier SubjectKeyIdentifier
Private Extensions	none

Field	Value
Name	SSL CA Template
Description	SSL/TLS Client and Server Certificate Authority
PKI Role	SSL/TLS Certificate Authority
Basic Constraints	TRUE
Basic Constraints Is CA	TRUE
Basic Constraints Path Length	0
Certificate Policies OIDs	none
Key Usages	keyCertSign
Extended Key Usages	none
Standard Extensions	AuthorityKeyIdentifier SubjectKeyIdentifier
Private Extensions	none

## PKI Level 3 - End Entities - Generic Roles

Field	Value
Name	User Template
Description	Generic End Users
PKI Role	End User
Basic Constraints	TRUE
Basic Constraints Is CA	FALSE
Basic Constraints Path Length	-1
Certificate Policies OIDs	none
Key Usages	digitalSignature keyAgreement keyEncipherment
Extended Key Usages	ClientAuthentication
Standard Extensions	AuthorityKeyIdentifier SubjectKeyIdentifier
Private Extensions	none

Field	Value
Name	SAP Server Template
Description	Generic SAP Servers
PKI Role	SAP Server / Application Server
Basic Constraints	TRUE
Basic Constraints Is CA	FALSE
Basic Constraints Path Length	-1
Certificate Policies OIDs	none
Key Usages	dataEncipherment digitalSignature keyEncipherment keyA- greement
Extended Key Usages	none
Standard Extensions	AuthorityKeyIdentifier SubjectKeyIdentifier
Private Extensions	none

Field	Value
Name	SSL Server Template
Description	Generic SSL Servers
PKI Role	SSLServer / Application Server
Basic Constraints	TRUE
Basic Constraints Is CA	FALSE
Basic Constraints Path Length	-1
Certificate Policies OIDs	none
Key Usages	digitalSignature keyAgreement keyEncipherment dataEncipherment
Extended Key Usages	ServerAuthentication
Standard Extensions	AuthorityKeyIdentifier SubjectKeyIdentifier
Private Extensions	none

## PKI Level 3 - End Entities - Certificate Lifecycle Management Roles

Field	Value
Name	SSL Client Template
Description	SSL/TLS Client
PKI Role	Registration Agent / Application Server
Basic Constraints	TRUE
Basic Constraints Is CA	FALSE
Basic Constraints Path Length	-1
Certificate Policies OIDs	none
Key Usages	dataEncipherment digitalSignature keyEncipherment keyAgreement
Extended Key Usages	ClientAuthentication
Standard Extensions	AuthorityKeyIdentifier SubjectKeyIdentifier

Field	Value
Private Extensions	none

Field	Value
Name	SNC SAPCryptolib Template
Description	SNC with SAPCryptolib or CommonCryptoLib
PKI Role	Application Server
Basic Constraints	TRUE
Basic Constraints Is CA	FALSE
Basic Constraints Path Length	-1
Certificate Policies OIDs	none
Key Usages	dataEncipherment digitalSignature keyEncipherment keyA- greement
Extended Key Usages	none
Standard Extensions	AuthorityKeyIdentifier SubjectKeyIdentifier
Private Extensions	none

Field	Value
Name	Encryption Template
Description	Generic Encryption only (SSF or S/MIME)
PKI Role	Application Server
Basic Constraints	TRUE
Basic Constraints Is CA	FALSE
Basic Constraints Path Length	-1
Certificate Policies OIDs	none
Key Usages	dataEncipherment keyEncipherment
Extended Key Usages	none
Standard Extensions	AuthorityKeyIdentifier SubjectKeyIdentifier

Field	Value
Private Extensions	none

Field	Value
Name	Digital Signature Template
Description	Generic Digital Signature only (SSF or S/MIME)
PKI Role	Application Server
Basic Constraints	TRUE
Basic Constraints Is CA	FALSE
Basic Constraints Path Length	-1
Certificate Policies OIDs	none
Key Usages	digitalSignature nonRepudiation
Extended Key Usages	none
Standard Extensions	AuthorityKeyIdentifier SubjectKeyIdentifier
Private Extensions	none

Field	Value
Name	S/MIME Template
Description	S/MIME Encryption and Digital Signature
PKI Role	Application Server
Basic Constraints	TRUE
Basic Constraints Is CA	FALSE
Basic Constraints Path Length	-1
Certificate Policies OIDs	none
Key Usages	dataEncipherment digitalSignature keyEncipherment non-Repudiation
Extended Key Usages	none
Standard Extensions	AuthorityKeyIdentifier SubjectKeyIdentifier

Field	Value
Private Extensions	none

Field	Value
Name	WS Security Template
Description	Web Service Security
PKI Role	Application Server
Basic Constraints	TRUE
Basic Constraints Is CA	FALSE
Basic Constraints Path Length	-1
Certificate Policies OIDs	none
Key Usages	dataEncipherment digitalSignature keyEncipherment keyA- greement
Extended Key Usages	none
Standard Extensions	AuthorityKeyIdentifier SubjectKeyIdentifier
Private Extensions	none

## 9.2.7 Parameters for Destination Management Configuration

Configure destinations if you use LDAP or RADIUS login modules or user logon ID mapping.

Here you find the parameters for the destination management. You need to configure destinations if you use LDAP or RADIUS servers. Use the optional settings in [LDAP Server Authentication \(Optional\)](#) if you use user logon ID mapping mode, for example in connection with LDAP or Microsoft Active Directory databases.

For more information, see the detailed parameter overview in the related link.

### Related Information

[Parameters for Destination Management \[page 309\]](#)

## 9.2.7.1 Parameters for Destination Management

If you are using LDAP or RADIUS servers, configure a destination per domain. If you use user logon ID mapping mode, for example in connection with LDAP or Microsoft Active Directory databases, configure the optional settings in [LDAP Server Authentication \(Optional\)](#), too.

### i Note

Parameters with \* (asterisk) are mandatory.

Parameters for Destination Management

Parameters	Details
<a href="#">IP Address/Host Name</a> *	<p>Host name or IP address of the LDAP server or Active Directory server system used to authenticate the user. Use the fully qualified domain name (FQDN) or the IP.</p> <p>Example: <code>ldapservers.demo.local</code></p> <div><h3>i Note</h3><p>We recommend that you configure secure communication.</p></div>
<a href="#">Port</a> *	<p>Enter a port for the LDAP or Microsoft Active Directory server.</p> <p>Example:</p> <p><b>389</b></p>
<a href="#">Use SSL for LDAP Access</a>	<p>To use an encrypted connection for secure communication, activate this parameter. When activated, SSL/TLS is used to communicate with the LDAP server. By default the parameter is deactivated.</p> <div><h3>i Note</h3><p>Before activating, import the server certificates into the keystore view <a href="#">Trusted CAs</a> in SAP NetWeaver Key Storage.</p></div>
<a href="#">Connection Timeout (Milliseconds)</a> *	<p>The connection timeout in milliseconds: <b>500</b> is the period of time the Secure Login Server waits for a response before trying the next LDAP or ADS server (in milliseconds). The default value is <b>500</b> milliseconds.</p>
<a href="#">Provider Language</a> *	<p>Language of the LDAP or Microsoft Active Directory Server. Default is <b>en-US</b></p>



Parameters	Details
<a href="#">Login Base DN</a>	<p>For Microsoft Active Directory:</p> <p>Enter the full domain name of the LDAP server that runs the authentication. If the client sends a user name without the domain, the system appends the domain name you entered here. If the name is already in User Principle Name (UPN) format, the system ignores this parameter.</p> <p>Example: <b>\$USERID@DOMAIN.LOCAL</b></p> <p>For LDAP servers other than Microsoft Active Directory:</p> <p>Enter the base DN of the LDAP Server (Start Search Path). There are several configuration options. Secure Login Server replaces the variable <b>\$USERID</b> with the user name for user verification with the authentication server.</p> <p>LDAP Server</p> <p>Define the search path where the user is located.</p> <p>Example:</p> <p><b>uid= \$USERID,ou=Users,dc=yourdomain,dc=SSO</b></p> <p>Microsoft Active Directory System</p> <p>Define the search path where the user is located.</p> <p>Example:</p> <p><b>\$USERID@&lt;Windows_domain&gt; cn= \$USERID,cn=Users,dc=domain,dc=com</b></p> <p>If the parameter is not configured (empty), Secure Login Client must be configured to send the Microsoft Windows UPN for user authentication.</p>
The parameters in the <a href="#">LDAP Server Authentication (optional)</a> section are only relevant if you use the user mapping service.	
<a href="#">Search Base DN</a>	<p>This parameter is only relevant for user mapping with an LDAP or Microsoft Active Directory Server. It is possible to run authentication with the server entered in <a href="#">Login Base DN</a> and user logon ID mapping with Microsoft Active Directory. When searching, the user mapping goes through all subtrees of the search base DN.</p>
<a href="#">Service User Name</a>	<p>Technical user of the back end that executes the user mapping. This parameter is only relevant for user mapping with an LDAP or Microsoft Active Directory Server.</p>
<a href="#">Password</a>	<p>This parameter is only relevant for user mapping with an LDAP or Microsoft Active Directory Server.</p>

Parameters	Details
<a href="#">Confirm Password</a>	This parameter is only relevant for user mapping with an LDAP or Microsoft Active Directory Server.

## 9.2.8 Parameters for Certificate Renewal Using Secure Login Server

If you want to automatically renew long-lived X.509 certificates with Secure Login Server means, you must set some parameters on Secure Login Server and on Application Server ABAP.

### 9.2.8.1 Parameters for Application Server Profile Groups in Authentication Profiles of Profile Management

If you want to automatically renew long-lived X.509 certificates with Secure Login Server means, you must set some parameters on Secure Login Server and on Application Server ABAP.

A wizard in Secure Login Administration Console enables you to easily create application server profile groups.

Parameter	Description
<a href="#">General</a> Tab	
<a href="#">Group Name</a>	Name of the application server profile group
<a href="#">Description</a>	Here you enter a description of the application server profile group. It makes sense to give the profile group a name that denotes the SAP systems (SIDs) the profile group stands for, for example, a set of development system belonging to your system landscape.
<a href="#">Profiles</a> Tab	

Parameter	Description
<i>Application Server Authentication Profiles</i>	<p>You can add application server authentication profiles with the following types:</p> <ul style="list-style-type: none"> <li>• <code>Registration Agent</code> Enables an administrator's enrollment with credentials</li> <li>• <code>Application</code> Each application server authentication profile of this type refers to PSEs of a certain PSE type (for example, SSL server PSEs or SSL client PSEs) that contain certificates you want to renew from time to time.</li> </ul> <div> <p><b>i Note</b></p> <p>Always add an application server profile of the profile type <code>Registration Agent</code>.</p> </div>
<i>System Identifiers</i>	<p>Enter the system IDs (SIDs) of the SAP systems for which you want to renew the certificates. It makes sense to add all system IDs, for example for all development systems. The AS ABAP can use this application server profile group for renewing certificates of all your development systems.</p>

## 9.2.8.2 Parameters for Application Server Profiles in the Profile Management

If you want to automatically renew long-lived X.509 certificates with Secure Login Server means, you must set some parameters on Secure Login Server and on Application Server ABAP.

A wizard in Secure Login Administration Console enables you to easily create application server profiles.

Parameter	Description
<i>General Tab</i>	
<i>Name</i>	Name of the application server authentication profile
<i>Profile ID</i>	This is a unique profile ID that is generated automatically.
<i>Description</i>	Here you enter a description of the application server authentication profile. It makes sense to give the profile a name that denotes the PSE type the profile stands for, for example, for certificate renewal of SSL server PSEs.

Parameter	Description
<a href="#">Type</a>	<p>Here you determine which kind of authentication profile your client has. In the context of certificate renewal, choose <a href="#">Secure Login Application Server Profile</a>.</p> <ul style="list-style-type: none"> <li>• <a href="#">Registration Agent</a> Enables an administrator's enrollment with credentials</li> <li>• <a href="#">Application</a> Each application server authentication profile of this type refers to PSEs of a certain PSE type (for example, SSL server PSEs or SSL client PSEs) that contain certificates you want to renew from time to time.</li> </ul> <div> <p><b>i Note</b></p> <p>Always add an application server authentication profile of the type <a href="#">Registration Agent</a>.</p> </div>
<a href="#">Authentication Configuration Tab</a>	
<a href="#">Use Policy Configuration</a>	<a href="#">Policy Configuration Name</a>
<a href="#">Policy Configuration Name</a>	<p>In an application server authentication profile of the type <a href="#">Application</a>, the user of Secure Login Administration Console authenticates runs on a policy configuration using a certificate-based login module.</p> <div> <p><b>i Note</b></p> <p>Always add an application server authentication profile of the type <a href="#">Registration Agent</a>.</p> </div>
<a href="#">Certificate Configuration Tab</a>	
	<p>Defines the Distinguished Name (DN) of the user certificate. Secure Login Server calculates the common name (CN) using the user credentials. You can configure the usual CN elements (see the related link).</p>
<a href="#">CA for Issuing Certificates</a>	Already contains a value for the user CA.
<a href="#">Certificate Template</a>	The certificate templates cover PSEs that belong to a special PSE type, for example SSL Server PSEs.
<a href="#">Client Configuration Tab</a>	
	You find all the parameters in the parameters for certificate configuration (see the related link).

## Related Information

[Parameters for Certificate Configuration in the Authentication Profile \[page 297\]](#)

[Parameters for Certificate Configuration \[page 297\]](#)

## 9.3 Parameter Overview for the SAP Cryptographic Library

This section contains the parameters for the SAP Cryptographic Library and, for example, parameters for SNC.

### 9.3.1 SNC Parameters for the SAP Cryptographic Library

SNC profile parameters for X.509 and Kerberos certificates and SPNego profile parameters in Application Server ABAP

In the following tables, you find an overview of the profile parameters you can use to configure the SNC and (if applicable) SPNego parameters in Application Server ABAP (transaction RZ10).

#### 9.3.1.1 SNC Parameters for X.509 Configuration

Use these parameters to configure SNC in the Application Server ABAP.

In the following, you find an overview of the profile parameters you can use to configure the SNC parameters in Application Server ABAP. To set the parameters, use the transaction `sncwizard`. To verify the configuration use `sncconfig`.

SNC Parameters for the SAP Cryptographic Library

Parameter	Value
<a href="#"><i>snc/enable</i></a>	<b>1</b> Activate SNC
	<b>0</b> Deactivate SNC
<a href="#"><i>snc/gssapi_lib</i></a>	Define the SNC library. <b>\$ (DIR_EXECUTABLE) \$ (DIR_SEP) \$ (FT_DLL_PREFIX) sapcrypto\$ (FT_DLL)</b>

Parameter	Value
<a href="#"><i>snc/identity/as</i></a>	<p>Define the SNC name of the SAP server's security token. X.509 Certificate Token</p> <p><b>p:&lt;X.509_Distinguished_Name&gt;</b></p> <p>Example:</p> <p>p:CN=ABC, OU=SAP Security</p> <p>Hint: If X.509 certificate token and Kerberos tokens are used in parallel, define the X.509 certificate distinguished name. This value is case sensitive.</p>
<a href="#"><i>snc/data_protection/max</i></a>	<b>3</b>
<a href="#"><i>snc/data_protection/min</i></a>	<b>2</b>
<a href="#"><i>snc/data_protection/use</i></a>	<b>3</b>
<a href="#"><i>snc/r3int_rfc_secure</i></a>	<b>0</b>
<a href="#"><i>snc/r3int_rfc_qop</i></a>	<b>8</b>
<a href="#"><i>snc/accept_insecure_cplic</i></a>	<b>1</b>
<a href="#"><i>snc/accept_insecure_gui</i></a>	<p><b>1</b> Accept insecure communication</p> <p>Use this value if both insecure and secure communication is to be allowed for SAP GUI.</p> <p><b>0</b> Disallow insecure communication</p> <p>Use this value only if secure communication is to be allowed only (no insecure communication) for SAP GUI.</p> <p><b>U</b> User-defined (User Management SU01)</p> <p>Use this value if insecure or secure communication for SAP GUI application is to be configured in the user management tool (SU01).</p> <p>We recommend that you set this value to <b>1</b>. If you want to enforce higher security, change this value to <b>0</b> (for all) or <b>U</b> (user dependent).</p>
<a href="#"><i>snc/accept_insecure_rfc</i></a>	<b>1</b>
<a href="#"><i>snc/permit_insecure_start</i></a>	<b>1</b>
<a href="#"><i>snc/force_login_screen</i></a>	<b>0</b>

## 9.3.1.2 SNC Parameters for Kerberos Configuration

SNC parameters for AS ABAP

SNC Parameters for the SAP Cryptographic Library

Parameter	Value
<i>spnego/enable</i>	Set to <b>1</b> .
<i>spnego/krbspnego_lib</i>	Define the Kerberos library.  <b><code>\$(DIR_EXECUTABLE) \$(DIR_SEP) \$(FT_DLL_PREFIX) sapcrypto\$(FT_DLL)</code></b>  <div><b>i Note</b> This value is identical to the value for <i>snc/gssapi_lib</i>.</div>
<i>snc/enable</i>	<b>1</b> Activate SNC  <b>0</b> Deactivate SNC
<i>snc/gssapi_lib</i>	Define the SNC library.  <b><code>\$(DIR_EXECUTABLE) \$(DIR_SEP) \$(FT_DLL_PREFIX) sapcrypto\$(FT_DLL)</code></b>
<i>snc/identity/as</i>	Define the SNC name of the SAP server's security token.  Kerberos Token  <b><code>p:CN=&lt;service_User_Principal_Name&gt;</code></b>  Example:  <code>p:CN=KerberosABC@DEMO.LOCAL</code>  Hint: If X.509 certificate token and Kerberos tokens are used in parallel, define the X.509 certificate distinguished name. This value is case-sensitive.
<i>snc/data_protection/max</i>	<b>3</b>
<i>snc/data_protection/min</i>	<b>2</b>
<i>snc/data_protection/use</i>	<b>3</b>
<i>snc/r3int_rfc_secure</i>	<b>0</b>
<i>snc/r3int_rfc_qop</i>	<b>8</b>
<i>snc/accept_insecure_cplic</i>	<b>1</b>

Parameter	Value
<a href="#">snc/accept_insecure_gui</a>	<p><b>1</b> Accept insecure communication</p> <p>Use this value if both insecure and secure communication is to be allowed for SAP GUI.</p> <p><b>0</b> Disallow insecure communication</p> <p>Use this value only if secure communication is to be allowed only (no insecure communication) for SAP GUI.</p> <p><b>U</b> User-defined (User Management SU01)</p> <p>Use this value if insecure or secure communication for SAP GUI application is to be configured in the user management tool (SU01).</p> <p>We recommend that you set this value to <b>1</b>. If you want to enforce higher security, change this value to <b>0</b> (for all) or <b>U</b> (user dependent).</p>
<a href="#">snc/accept_insecure_rfc</a>	<b>1</b>
<a href="#">snc/permit_insecure_start</a>	<b>1</b>
<a href="#">snc/force_login_screen</a>	<b>0</b>


### 9.3.1.3 Profile Parameters for SPNego

SPNego profile parameters for Application Server ABAP

(If applicable) SPNego Profile Parameters for SAP Cryptographic Library

Parameter	Setting								
<a href="#">spnego/enable</a>	Set to <b>1</b> .								
<a href="#">spnego/krbspnego_lib</a>	<p>Set to the path to the Kerberos library (SAP Cryptographic Library of SAP Single Sign-On 2.0 or higher).</p> <p>Kerberos Library File Names</p> <table> <tr> <th>File Name</th><th>Operating System</th></tr> <tr> <td>sapcrypto.dll</td><td>Microsoft Windows</td></tr> <tr> <td>libsapcrypto.so</td><td>UNIX platforms</td></tr> <tr> <td>libsapcrypto.sl</td><td>HP-UX only</td></tr> </table>	File Name	Operating System	sapcrypto.dll	Microsoft Windows	libsapcrypto.so	UNIX platforms	libsapcrypto.sl	HP-UX only
File Name	Operating System								
sapcrypto.dll	Microsoft Windows								
libsapcrypto.so	UNIX platforms								
libsapcrypto.sl	HP-UX only								



Parameter	Setting
<a href="#">spnego/construct_SNC_name</a>	<p>If you use a Kerberos-based SNC product that is not SAP Single Sign-On, use this parameter to determine the format for the translation of Kerberos user name to SNC name. Default value is <b>111</b>.</p> <p>For more information, see <a href="#">SAP Note 1819808 - SPNego: Collective Corrections</a> .</p> <div> <p><b>i Note</b></p> <p>Changing this dynamic profile parameter does not require a restart.</p> </div>

### 9.3.1.4 Profile Parameters for SAP Cryptographic Library

Use the AS ABAP profile parameters of the default profile to configure the SAP Cryptographic Library. Open the SAP GUI and start transaction [Edit Profiles](#) (transaction code RZ10).

Profile parameters for the SAP Cryptographic Library

Parameter	Values	Description
<a href="#">ccl/snc/pse_x509</a>	<b>&lt;PSE_file_name&gt;</b>	<p>SNC PSE name</p> <p>By default, the AS ABAP uses the server SNC name and searches for the SNC PSE in the credentials. If this value is set, the PSE file is named directly.</p>
<a href="#">ccl/snc/pse_kerb</a>	<b>&lt;PSE_file_name&gt;</b>	<p>SNC PSE name for keytab</p> <p>By default, the AS ABAP uses the server SNC name and searches for the SNC PSE in the credentials. If this value is set, the PSE file is named directly.</p>
Creation of client SNC name		

Parameter	Values	Description
<a href="#">ccl/snc/server_partner_name_x509</a>	<b>Subject</b> (default) <b>UserPrincipalName</b> <b>PrincipalOnly</b> <b>UserPrincipalNameOrSubject</b> <b>PrincipalOnlyOrSubject</b>	<p>X.509 name source</p> <p>This profile parameter is only valid if the client authenticates with a certificate. The parameter specifies the part of the client certificate, which is used as client SNC name. You can also use the User Principal Name (SubjectAltName extension) with or without the domain part. If you specify one of the *OrSubject values, the subject name is used as a fallback if the AS ABAP does not find the User Principal Name in the certificate. The prerequisite for using the other values is that the User Principal Name must be available in all client certificates. Otherwise the authentication fails.</p>
<a href="#">ccl/snc/server_partner_name_kerb</a>	<b>UserPrincipalName</b> (default) <b>PrincipalOnly</b>	<p>Kerberos name source</p> <p>This profile parameter is only valid if the client authenticates with Kerberos. The parameter specifies whether the complete User Principal Name is used as SNC name. You can also use the principal part of it.</p> <div> <p>❖ Example</p> <ul style="list-style-type: none"> <li>• p:CN=&lt;principal&gt;@&lt;domain&gt;</li> <li>• p:CN=&lt;principal&gt;</li> </ul> </div>
<a href="#">ccl/snc/partner_case_x509</a>	<b>none</b> (default) <b>lower</b> <b>upper</b>	<p>X.509 uppercase/lowercase conversion</p> <p>If the client certificate subject name is used as client SNC name, this profile parameter specifies whether the name is converted into lowercase or uppercase.</p>

Parameter	Values	Description
<a href="#">ccl/snc/partner_case_upn</a>	<b>upper</b> (default) <b>lower</b> <b>lowerPrincipal</b> <b>upperDomain</b> <b>lowerPrincipalUpperDomain</b>	<p>Kerberos uppercase/lowercase conversion</p> <p>If the client's User Principal Name (from Kerberos or the User Principal Name in the certificate) is used as client SNC name, this profile parameter specifies whether the name is converted into lowercase or uppercase.</p>
SNC cipher suites		
<a href="#">ccl/snc/client_protocol</a>	<b>ALL</b> (default) <b>1993</b> <b>2010_1_0</b> <b>2010_1_1</b>	<p>SNC client protocol</p> <p>List the keywords separated by a colon.</p>
<a href="#">ccl/snc/client_cipher_suites</a>	<b>HIGH:MEDIUM</b> (default) <b>HIGH</b> <b>MEDIUM</b>	<p>SNC cipher suites for the client</p> <p>This parameter specifies which algorithms are allowed in the SNC client according to their strength.</p> <p>List the keywords separated by a colon.</p> <ul style="list-style-type: none"> <li><b>HIGH</b> All with hash algorithms except for SHA-1/RIPEMD160</li> <li><b>MEDIUM</b> All with SHA-1/RIPEMD160 hash algorithm</li> </ul>
<div> <b>i Note</b>  It is not possible to use the cipher suites defined in the SNC cipher suites in the server because the 1993 and 2010_1_0 protocol does not support them. </div>		
<a href="#">ccl/snc/server_protocol</a>	<b>ALL</b> (default) <b>1993</b> <b>2010_1_0</b> <b>2010_1_1</b>	<p>SNC server protocol</p> <p>List the keywords separated by a colon.</p>

Parameter	Values	Description
<a href="#">ccl/snc/server_cipher_suites</a>	<p><b>HIGH:MEDIUM</b> (default)</p> <p><b>HIGH</b></p> <p><b>MEDIUM</b></p> <p><b>SNC_CL_RSA_AES256_SHA256</b>  <b>SNC_CL_RSA_AES128_SHA1</b>  <b>SNC_CL_RSA_AES128_SHA256</b>  <b>SNC_CL_RSA_AES128_RIPEMD</b>  <b>160 SNC_CL_RSA_DES3_SHA1</b>  <b>SNC_CL_RSA_DES3_RIPEMD160</b></p> <p><b>SNC_KERBEROS_AES256_SHA256</b>  <b>56</b></p> <p><b>SNC_KERBEROS_AES128_SHA256</b>  <b>56</b></p> <p><b>SNC_SR_RSA_AES256_SHA256</b>  <b>SNC_SR_RSA_AES128_SHA256</b></p> <p><b>SNC_ECDHE_P521_AES256_SHA512</b>  <b>SNC_ECDHE_P384_AES256_SHA512</b>  <b>SNC_ECDHE_P256_AES256_SHA256</b></p>	<p>SNC cipher suites for the server</p> <p>This parameter specifies which cipher suites are allowed in the SNC server. List them separately or as a group.</p> <p>List the keywords separated by a colon.</p> <ul style="list-style-type: none"> <li><b>HIGH</b> All with hash algorithms except for SHA-1/RIPEMD160</li> <li><b>MEDIUM</b> All with SHA-1/RIPEMD160 hash algorithm</li> </ul>
<a href="#">ccl/snc/server_partner_auth_mode</a>	<p><b>0</b> (default)</p> <p>Not requested</p> <p><b>1</b></p> <p>Requested</p> <p><b>2</b></p> <p>Required</p>	<p>This parameter specifies the client authentication.</p>

Parameter	Values	Description
<a href="#">ccl/snc/server_session_key_mode</a>	<b>1</b> (default)  <b>0</b>	<p>The SNC protocol defines modes where the client uses a temporary key during the handshake.</p> <ul style="list-style-type: none"> <li>The client certificate has no encryption capability (CL-RSA)</li> <li>The client uses <code>serverSessionMode</code>.</li> </ul> <p>This parameter specifies whether the server accepts the server session key mode.</p>
<a href="#">ccl/snc/server_session_key_types</a>	<b>ALL</b> (default)  <b>RSA_1024</b>  <b>ECDSA_P256</b>  <b>ECDSA_P384</b>  <b>ECDSA_P521</b>	<p>The SNC protocol defines modes where the client uses a temporary key during the handshake.</p> <p>List the keywords separated by a colon.</p> <ul style="list-style-type: none"> <li>The client certificate has no encryption capability (CL-RSA)</li> <li>The client uses <code>serverSessionMode</code>.</li> </ul> <p>This parameter specifies which temporary client key types are accepted by the server.</p> <ul style="list-style-type: none"> <li>For non-PFS: <b>RSA_1024</b></li> <li>For PFS: <b>ECDSA_P256</b>, <b>ECDSA_P384</b>, <b>ECDSA_P521</b></li> </ul>
<a href="#">ccl/snc/server_session_key_accepted_ttl</a>	<b>600</b> (default)  10 hours	<p>Accepted lifetime of the client's session key in minutes.</p> <p>Specify a minimum of 15 minutes because clients renew the session key a few minutes before the session expires, in order to avoid problems if system clocks are not in sync.</p>
<a href="#">ccl/snc/pkix_revocation_check</a>	<b>0</b> (default)  <b>1</b>	<p>Revocation check configuration for SNC.</p> <ul style="list-style-type: none"> <li><b>0</b> No revocation check</li> <li><b>1</b> Revocation check according to the PKIX configuration</li> </ul>

Parameter	Values	Description
<a href="#">ccl/ssf/pkix_revocation_check</a>	<b>0</b> (default) <b>1</b>	Revocation check configuration for SSF. <ul style="list-style-type: none"> <li><b>0</b> No revocation check</li> <li><b>1</b> Revocation check according to the PKIX configuration</li> </ul>
Name aliases		These parameters enable you to replace parts of the certificate subject name by other strings. Use these parameters to shorten long names.
<a href="#">ccl/snc/namealias/value_&lt;digit&gt;</a>	Any string	String to search for
<a href="#">ccl/snc/namealias/replacement_&lt;digit&gt;</a>	Any string	Replaces a part of the name
<a href="#">ccl/snc/nameencoding</a>	<b>T. 61</b> (default)	Name encoding in UTF8
<a href="#">ccl/snc/nameschema</a>	<b>sapcryptolib</b> (default)	Name schema according to the RFC 2256 standard
Certificate verification		These profile parameters specify a set of named profiles for certificate verification.
<a href="#">ccl/pkix/profile/&lt;name&gt;/issuer</a>	Any string	Issuer name string  If you want to verify a certificate that has an issuer name containing this string, the AS ABAP uses the parameter in this profile for the verification.
<a href="#">ccl/pkix/profile/&lt;name&gt;/accept_no_basic_constraints</a>	<b>keyCertSign</b> (default) <b>no</b>	A missing <code>basicConstraints</code> extension in a certificate is accepted if it contains the <code>keyCertSign</code> key usage.
<a href="#">ccl/pkix/profile/&lt;name&gt;/revocation_check</a>	<b>NO</b> (default) <b>CRL</b>	Use this parameter to activate revocation check using certificate revocation lists.

Parameter	Values	Description
<code>ccl/pkix/profile/&lt;name&gt;/certificate_policies</code>	<b>noCheck</b> (default)  Object identifiers of the certificate policies	<p>If you do not want to perform a certificate policy check, use the keyword <b>noCheck</b>.</p> <p>If the certificate you want to verify contains a certificate policy, you must specify it here to get a positive verification result. The policies are defined separately as object identifiers. List the object identifiers separated by a colon.</p> <div> ❖ Example  <b>1.2.360.4.5:1.3.36.1.5</b> </div>
<code>ccl/pkix/cache_directory</code>	<b>%SECUDIR%</b> (default)  Any path	<p>If you use certificate verification, use this parameter to define the folder where CRLs are stored.</p>
FIPS 140-2 Certified Crypto Kernel		
<code>ccl/fips/enable</code>	<b>0</b> (default)  <b>1</b>	<p>The FIPS 140-2 certified crypto kernel is used. For more information, see <a href="#">Standard and FIPS 140-2 Certified Crypto Kernel of the SAP Cryptographic Library [page 235]</a>.</p>

## 9.3.2 Parameters for Certificate Revocation Lists

Parameter overview for the CRL tool

The following parameter overview tables enable you to configure a tool for certification revocation lists.

## 9.3.2.1 CRL Tool Commands

This is an overview of the CRL tool commands. The main function of the CRL tool is to enable you to download CRLs. The CRL tool is a part of the `sapgenpse` command.

CRL Tool Commands

Command	Description
<code>get_crl get</code>	Downloads a CRL from a given CRL distribution point using a given URL (Web server or LDAP server).
<code>get_crl status</code>	Shows the current status of the configuration and of the module
<code>get_crl list</code>	Shows the CRLs currently located in the local cache
<code>get_crl remove</code>	Removes the CRL from the local cache
<code>get_crl show</code>	Shows the content of a CRL file
<code>get_crl store</code>	Stores a CRL in the local cache. If the certificates contain a CRL distribution point, specify its location with <code>-u</code> so that the CRL can be found during certificate verification.

If you want to know how you can use the CRL command, for example to download CRLs, see the related link.

### Related Information

[Downloading CRLs with the CRL Tool \[page 245\]](#)



# 10 Troubleshooting

This section provides information on troubleshooting related activities

In case of problems, create a CSN Message in the component BC-IAM-SSO-SL or in the related subcomponent. Refer to the SAP Note in the related link.

## → Tip

In addition, we recommend that you regularly check the SAP Notes for the component BC-IAM-SSO-SL (or for the related subcomponent). They contain information on program corrections and provide additional documentation.

Another source of troubleshooting information is the Troubleshooting Guide for SAP Single Sign-On. This is a public wiki that is maintained by SAP support staff. For more information, see the related link.

## Related Information

<http://service.sap.com/sap/support/notes/1673155>

[Troubleshooting Guide for SAP Single Sign-On](#)

## 10.1 Troubleshooting Secure Login Client

This section describes some troubleshooting issues of Secure Login Client and how to solve them.

## i Note

If you need to contact SAP support, provide the Secure Login Client trace information as described in the related link.

## Related Information

[Tracing Secure Login Client \[page 158\]](#)

## 10.1.1 Error in SNC

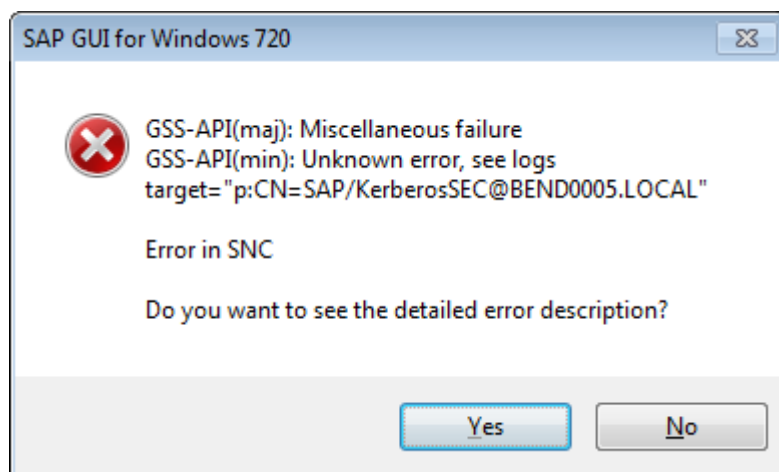
Secure Login Client SNC error

### Use Case

SAP GUI user wants to authenticate to SAP Applications Servers using Kerberos token or X.509 user certificate.

### Error Message

Miscellaneous failure. Error in SNC.



### Checklist

1. Check the certificate you are using.  
If you are using a Kerberos token, take the following steps:
  1. Verify if the user is authenticated in the Microsoft domain.
  2. Verify if Kerberos token is displayed in Secure Login Client Console.If you are using an X.509 certificate, proceed as follows:
  1. Verify if X.509 certificate is displayed in Secure Login Client Console.
2. Verify if the security token (Kerberos or certificate) is used.  
Try with the option *Use Profile for SAP Applications* if the desired profile is used.
3. Verify if SNC is enabled in SAP GUI for the desired SAP server.
4. Verify if the SNC name of the desired SAP server is configured in SAP GUI (`saplogon.ini`).  
Is the name correct? (Kerberos name / X.509 certificate name)  
Note that the SNC name is case-sensitive.

5. Verify if the environment variable SNC\_LIB is configured to use sapcrypto.dll. Example: C:\Program Files\SAP\FrontEnd\SecureLogin\lib\sapcrypto.dll

## 10.1.2 User Name Not Found

No user exists with SNC name.

### Use Case

SAP GUI user wants to authenticate to SAP server using Kerberos token or X.509 user certificate.

### Error Message

No user exists with SNC name "p:CN=WRONGSNCNAME, O=SAP, L=Walldorf, C=DE"

### Checklist

- If this message appears, the user mapping is not available or not configured correctly. Compare the user certificate distinguished name with the SNC name in SAP User Management (SU01).  
Note that SNC name is case-sensitive.

There may also be another reason for this error. For more information, see the related SAP Note

### Related Information

<https://service.sap.com/sap/support/notes/1635019> 

## 10.1.3 Invalid Security Token

During an SAP GUI authentication at an Application Server ABAP, you run into `SAP System Message S.`

### Use Case 1

SAP GUI wants to authenticate to SAP server using a Kerberos token or X.509 user certificate.

### Error Message

`SAP System Message S.`

### Checklist

- Verify if SNC is configured in the SAP ABAP server.
- If the SAP Cryptographic Library is installed on the SAP ABAP server and used for SNC, enable the trace and verify the results. For more information, see the related link.

### Use Case 2

The Secure Login Client requests a service ticket from the domain server.

### Error Message

The system displays the following error message:

`Supplied credentials not accepted by the server.`

In the trace log of the Secure Login Client, you find the error code A2600202.

### Checklist

- If the Secure Login Client does not get a service ticket from the domain server, you have to check whether the Service Principal Name used was assigned several times in the Active Directory system. To check this, you enter the following command:  
`setspn -T * -T foo -X`

## Related Information

[Configuring Tracing for the Cryptographic Library \[page 248\]](#)

### 10.1.4 Wrong SNC Library Configured

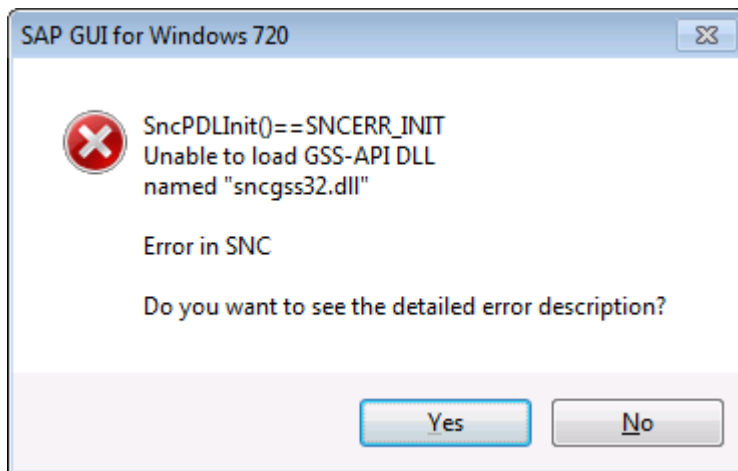
Wrong library configured in Secure Login Client

## Use Case

An SAP GUI user wants to authenticate to a SAP server using Kerberos token or X.509 user certificate.

## Error Message

Unable to load GSS-API DLL named "sncgss32.dll".



## Checklist

The wrong SNC library (in this example `sncgss32.dll`) is assigned to SAP GUI. Verify the environment variable `SNC_LIB`.

For Secure Login Client the SNC library `sapcrypto.dll` is used.

Example: `C:\Program Files\SAP\FrontEnd\SecureLogin\lib\sapcrypto.dll`

## 10.1.5 No Display of Password Expiration Warning

A user fulfills all conditions for getting a warning saying that his or her password will expire, but the Secure Login Client does not send a warning.

### Prerequisites

This error only occurs if your clients fulfill the following conditions:

- You are using Secure Login Client 2.0 with Secure Login Client protocol 1.0 in the enrollment URL.
- Your Secure Login Client is based on an authentication profile running with an LDAP login module, and you have set the following LDAP login module attributes in the SAP NetWeaver Administrator:
  - You have defined a date and time in [PasswordExpirationAttribute](#) on the [Login Module Options](#) tab of your LDAP login module. For more information, see the related links.
  - You have defined a period of time in [PasswordExpirationGracePeriod](#). During this period, you should get a warning telling you that your password is going to expire.

### Procedure

1. Open the Secure Login Administration Console.
2. Choose the authentication profile you use for LDAP.
3. Go to the [Secure Login Client Settings](#) tab.
4. Choose the [Edit](#) button.
5. Select the [Show Success Message](#) checkbox.

After you have enabled the display of success messages, your client users get warnings saying that their password will expire soon. They also get other messages, for example, success messages when they log on.

### Related Information

[Managing Destinations \[page 214\]](#)

[Parameters for Destination Management Configuration \[page 308\]](#)

## 10.1.6 SNC Error Codes in the Secure Login Client

In case of an SNC error in the client, consult the list of internal errors of the SAP Cryptographic Library's GSS module.

You find the complete list of the SNC error codes in the related link.

## Related Information

[SNC Error Codes \[page 335\]](#)

## 10.2 Troubleshooting SAP Cryptographic Library

This section provides further information about how to perform troubleshooting for the SAP Cryptographic Library.

### 10.2.1 SNC Library Not Found

The SNC library and configuration are verified when the SAP ABAP server starts.

#### Context

**Problem:** SNC library cannot be found.

#### Procedure

1. Verify SAP trace file `dev_w0`.
2. Verify if the SAP Cryptographic Library is installed correctly.  
Verify the installation described in section [Installing Additional Features for Secure Login \[page 231\]](#).
3. Verify the SNC configuration.
  - a. Log on to SAP ABAP server using SAP GUI and start transaction `RZ10`.
  - b. Choose the default profile and verify the value of the parameter `snc/gssapi_lib`.
4. Verify SNC library file access rights for the user starting the SAP server.
5. Verify the SNC library status with the command `sapgenpse`.
6. Verify whether the SAP Cryptographic Library has the same architecture as the ABAP System (32-bit or 64-bit ). On UNIX, the `file` command enables you to check whether you have a SAP Cryptographic Library with 32-bit or 64 bit. To determine the architecture, use the following command:

```
file sapgenpse
```

## Related Information

[Configuration for the AS ABAP \[page 237\]](#)

[Configuring Tracing for the Cryptographic Library \[page 248\]](#)

## 10.2.2 Credentials Not Found

The SNC library and configuration are verified when the SAP ABAP server starts.

### Context

**Problem:** Could not get credentials.

### Procedure

1. Verify SAP trace file `dev_w0`.
2. Verify if the SAP Cryptographic Library is installed correctly.  
Verify the installation described in section [Installing Additional Features for Secure Login \[page 231\]](#).
3. Verify the SNC configuration.
  - a. Log on to the AS ABAP server using SAP GUI and start transaction `RZ10`.
  - b. Choose the default profile and verify the SNC configuration.
4. Verify SNC library file access rights for the user starting the SAP server.
5. Verify if the SNC certificate was provided to the SAP Cryptographic Library PSE environment.
  - a. Start a command line shell and change to the folder of the SAP Cryptographic Library. The default path is `$ (DIR_EXECUTABLE) $ (DIR_SEP) $ (FT_DLL_PREFIX) sapcrypto$ (FT_DLL)`.
  - b. Set the environment `SECUDIR=$(DIR_INSTANCE)/sec`.
  - c. Use the command: `sapgenpse seclogin -O -l <SAP_service_user>`.

#### ❖ Example

Microsoft Windows: `sapgenpse seclogin -O -l SAPServiceABC`

Linux: `sapgenpse seclogin -O -l abcdm`

6. Enable the trace of the SAP Cryptographic Library and analyze the problem.

## Related Information

[Configuration for the AS ABAP \[page 237\]](#)



## 10.2.3 No Credentials Found at Start of Application Server ABAP

In a Microsoft Windows environment, an Application Server ABAP does not start and displays an error message saying that the credentials were not found.

### Context

Your Application Server ABAP does not start on a Microsoft Windows platform, and the following error message is displayed:

```
GSS-API(maj): No credentials were supplied
```

When you check the trace file of the SAP Cryptographic Library, you find the following message:

```
ERROR(0xA0100207) in CRYPT->credCipher(): Decryption error, invalid padding  
decrypted
```

This can happen in cases where the credentials have been created with `sapgenpse` using the following command line:

```
sapgenpse seclogin -p <server_PSE_file> -O <system_user>"
```

This command can change the spelling of the supplied system user name (-O) using Windows functions. In rare cases, the result is a wrong spelling. This is the reason why the account which is running the AS ABAP server work process cannot access the credentials of this system user.

### Procedure

Use the additional option `-N` to force `sapgenpse` to use the supplied system user name without any spelling changes for setting the credentials.

#### ❖ Example

```
sapgenpse seclogin -p <path>\SAPSNCSKERB.pse -O <system_user> -N
```

See also SAP Note [1942749](#) .

## Related Information

[Creating Keytab for Kerberos \[page 30\]](#)

### 10.2.4 No User Exists with SNC Name

**Problem:** If the error message `No user exists with SNC name ...` occurs and your login fails, a server with a default SAP Cryptographic Library configuration cannot find the SNC name in the database. For further information, see the related SAP Note.

## Related Information

<http://service.sap.com/sap/support/notes/1635019> 

### 10.2.5 Monitoring the SAP Cryptographic Library

This topic provides information about Application Server monitoring utilities you can use.

If you suspect that there might be an issue with Secure Login Server, we recommend that you use monitoring utilities provided by AS ABAP. It might help you to find a solution for your issue.

For more information, see SAP Help Portal under [▶ Function-Oriented View ▶ Solution Lifecycle Management ▶ Solution Monitoring ▶](#).

### 10.2.6 Error Occurred with sapgenpse

If errors occur with `sapgenpse`, see the following SAP Note.

<http://service.sap.com/sap/support/notes/1834979> 

### 10.2.7 SNC Error Codes

In case of an error from a calling application with the SAP Cryptographic Library, consult this list of internal errors of the GSS module.

These error codes and the corresponding error messages are sent if internal errors occur in the GSS module or if invalid input data come in from a calling application. They may occur in the client or be reported by the client

as server errors. The list of SNC error codes can also be helpful when you analyze server trace or log files. You find the complete list of error codes, error messages with description in SAP Note [1867829](#).

#### **i Note**

To analyze the problem in more detail, activate the trace function of the SAP Cryptographic Library and analyze traces. For more information, see the related link.

## **Related Information**

[Configuring Tracing for the Cryptographic Library \[page 248\]](#)

## **10.3 Troubleshooting Secure Login Server**

This section gives additional information about troubleshooting for Secure Login Server.

### **10.3.1 Secure Login Web Client Authentication Failed**

Secure Login Web Client authentication failed due to multiple tabs in your browser.

#### **Context**

You have authenticated with a Secure Login Web Client. The following error message occurs:

```
Authentication failed. Client is already authenticated as a different user.
```

The cause for this error is that you are authenticated several times if you use Secure Login Web Client in one browser window with several tabs. The browser shares the authentication information, for example, cookies and URL of the SAP Netweaver Application Server, and uses it in the additional tabs. To make sure that your Secure Login Web Client does not authenticate several times, proceed as follows:

#### **Procedure**

Make sure that you close the additional tabs of your browser.

## 10.3.2 Trust Warnings in Secure Login Web Client

Before you can authenticate with Secure Login Web Client, your browser sends trust warnings and denies access.

### Context

The Secure Login Web Client does not use SSL on its port. You must check the web client URL in the authentication profile.

### Procedure

Distribute the SSL CAs into the trusted certificate stores of your clients. Use the utilities of your operating system (Microsoft Windows and Keychain for Mac OS X are supported).

## 10.3.3 Error Codes of SAP Stacktrace Errors

This chapter describes the error codes and return codes, their meaning and possible corrections.

### 10.3.3.1 SAP Stacktrace Error Codes

This table contains the SAP stacktrack error codes.

Runtime Error Codes	Description
CALL_BACK_ENTRY_NOT_FOUND	The called function module is not released for RFC.
CALL_FUNCTION_DEST_TYPE	The type of the destination is not allowed.
CALL_FUNCTION_NO_SENDER	Current function is not called remotely.
CALL_FUNCTION_DESTINATION_NO_T	Missing communication type (1 for internal connection, 3 for ABAP) when executing an asynchronous RFC.
CALL_FUNCTION_NO_DEST	The specified destination does not exist.
CALL_FUNCTION_OPTION_OVERFLOW	Maximum length of options for the destination exceeded.

Runtime Error Codes	Description
CALL_FUNCTION_NO_LB_DEST	The specified destination (in load distribution mode) does not exist.
CALL_FUNCTION_NO_RECEIVER	Data received for unknown CPI-C connection.
CALL_FUNCTION_NOT_REMOTE	The function module being called is not flagged as being "remotely" callable.
CALL_FUNCTION_REMOTE_ERROR	While executing an RFC, an error occurred that has been logged in the calling system.
CALL_FUNCTION_SIGNON_INCOMPL	Logon data for the user is incomplete.
CALL_FUNCTION_SIGNON_INTRUDER	Logon attempt in the form of an internal call in a target system not allowed.
CALL_FUNCTION_SIGNON_INVALID	RFC from external program without valid user ID.
CALL_FUNCTION_SIGNON_REJECTED	Logon attempt in target system without valid user ID. This error code may have any of the following meanings: <ul style="list-style-type: none"> <li>• Incorrect password or invalid user ID.</li> <li>• User locked.</li> <li>• Too many logon attempts.</li> <li>• Error in authorization buffer (internal error).</li> <li>• No external user check.</li> <li>• Invalid user type.</li> <li>• Validity period of the user exceeded.</li> </ul>
CALL_FUNCTION_SINGLE_LOGIN_REJ	No authorization to log on as a trusted system. The error code may have any of the following meanings: <ul style="list-style-type: none"> <li>• Incorrect logon data for valid security ID.</li> <li>• Calling system is not a trusted system or security ID is invalid.</li> <li>• Either the user does not have RFC authorization (authorization object S_RFCACL), or a logon was performed using one of the protected users DDIC or SAP*.</li> <li>• Time stamp of the logon data is invalid.</li> </ul>
CALL_FUNCTION_SYSCALL_ONLY	RFC without valid user ID only allowed when calling a system function module. The meaning of the error codes is the same as for CALL_FUNCTION_SINGLE_LOGIN_REJ.
CALL_FUNCTION_TABINFO	Data error (info internal table) during a RFC.
CALL_FUNCTION_TABLE_NO_MEMORY	No memory available for table being imported.
CALL_FUNCTION_TASK_IN_USE	For asynchronous RFC only: task name is already being used.

Runtime Error Codes	Description
CALL_FUNCTION_TASK_YET_OPEN	For asynchronous RFC only: the specified task is already open.
CALL_FUNCTION_NO_AUTH	No RFC authorization.
CALL_RPERF_SLOGIN_AUTH_ERROR	No trusted authorization for RFC caller and trusted system.
CALL_RPERF_SLOGIN_READ_ERROR	No valid trusted entry for the calling system.
RFC_NO_AUTHORITY	No RFC authorization for user.
CALL_FUNCTION_BACK_REJECTED	Destination "BACK" is not permitted in current program.
CALL_XMLRFC_BACK_REJECTED	Destination "BACK" is not permitted in current program.
CALL_FUNCTION_DEST_SCAN	Error while evaluating RFC destination.
CALL_FUNCTION_DEST_SCAN	Error while evaluating RFC destination.
CALL_FUNCTION_CONFLICT_TAB_TYP	Type conflict while transferring table.
CALL_FUNCTION_CREATE_TABLE	No memory available for creating a local internal table.
CALL_FUNCTION_UC_STRUCT	Type conflict while transferring structure.
CALL_FUNCTION_DEEP_MISMATCH	Type conflict while transferring structure.
CALL_FUNCTION_WRONG_VALUE LENG	Invalid data type while transferring parameters.
CALL_FUNCTION_PARAMETER_TYPE	Invalid data type while transferring parameters.
CALL_FUNCTION_ILLEGAL_DATA_TYP	Invalid data type while transferring parameters.
CALL_FUNCTION_ILLEGAL_INT_LEN	Type conflict while transferring an integer.
CALL_FUNCTION_ILL_INT2 LENG	Type conflict while transferring an integer.
CALL_FUNCTION_ILL_FLOAT_FORMAT	Type conflict while transferring a floating point number.
CALL_FUNCTION_ILL_FLOAT LENG	Type conflict while transferring a floating point number.
CALL_FUNCTION_ILLEGAL_LEAVE	Invalid LEAVE statement on RFC Server.
CALL_FUNCTION_OBJECT_SIZE	Type conflict while transferring a reference.
CALL_FUNCTION_ROT_REGISTER	Type conflict while transferring a reference.

## 10.3.4 Checklist User Authentication Problem

### Context

This section describes the configuration issues to check if a user authentication is not successful.

### Procedure

1. Is verification using different user credentials?
2. Log on to Secure Login Administration Console and check the log information in [Authentication Profiles](#). Check if the user authentication is displayed. If this is not the case, there may be a problem on the Secure Login Client or Secure Login Web Client. Verify the following parameter:
  - a. Check whether the [Enrollment URL](#) parameter is configured for the desired instance. Check [Secure Login Client Settings](#) or [Secure Login Web Client Settings](#) in Secure Login Administration Console.
  - b. Copy this URL to the browser application and check if a response is displayed (ignore the responses `ERROR_ACTION` or `INTERNAL_SERVER_ERROR`).
  - c. If you are using HTTPS, the problem may relate to the certificate trust relationship. If this is the case, import the root certificate, on which the SSL server certificate depends and move it to the Microsoft Certificate Store (Computer Certificate Store).
3. Choose the tab [Certificate Management](#) and verify whether `USER_CA` is active.

## 10.3.5 Enable Fully Qualified Distinguished Name in Enrollment URL

The following topics describes how to enable a fully qualified distinguished name in an enrollment URL.

It may occur that some installations of SAP NetWeaver Application Server for Java do not automatically generate fully qualified distinguished names. This may cause an error, for example, when you download a policy configuration to the Secure Login Client or Secure Login Web Client because the policy download does not provide a fully qualified distinguished name in the enrollment URL.

## 10.3.5.1 Enable Fully Qualified Distinguished Name for SAP Net Weaver 7.0 or Higher on Microsoft Windows

How to enable fully qualified distinguished name for SAP NetWeaver 7.0 or higher on Microsoft Windows.

### Context

In the default configuration of the SAP Netweaver Application Server, the fully qualified domain is not used and cannot be changed. The steps below are only relevant for SAP NetWeaver 7.0 or higher Engine.

To enable the fully qualified distinguished name, you need to execute the following steps.

### Procedure

1. Stop the J2EE engine.
2. Go to the profile directory: `usr/sap/<SID>/SYS/profile`, open the profiles (java instance profile `<SID>_J00_your_current_host_name` and SCS profile `<SID>_SCS01_your_current_host_name`) and add the lines below:

```
SAPLOCALHOST = <current_host_name>
SAPLOCALHOSTFULL = <current_fully_qualified_distinguished_name>
icm/host_name_full = $(SAPLOCALHOSTFULL)
```

#### ❖ Example

```
SAPLOCALHOST = veisa730vmmst
SAPLOCALHOSTFULL = veisa730vmmst.dhcp.wdf.sap.corp
icm/host_name_full = $(SAPLOCALHOSTFULL)
```

3. Open the file `DEFAULT.PFL` in the profile directory. Add the entries **SAPLOCALHOSTFULL** and **SAPFQDN**. The entries **SAPFQDN** and **SAPLOCALHOSTFULL** have to be the first two entries.

```
SAPLOCALHOSTFULL = <current_fully_qualified_distinguished_name>
```

```
SAPFQDN = <current_domain>
```

#### ❖ Example

```
SAPLOCALHOSTFULL = veisa730vmmst.dhcp.wdf.sap.corp
SAPFQDN = dhcp.wdf.sap.corp
```

Modify the value of the entries `SAPDBHOST`, `j2ee/dbhost`, and `j2ee/scs/host`:

#### ❖ Example

```
SAPDBHOST = $(SAPLOCALHOST) . $(SAPFQDN)
```



```
j2ee/dbhost = $(SAPLOCALHOST) . $(SAPFQDN)
j2ee/scs/host = $(SAPLOCALHOST) . $(SAPFQDN)
```

4. Start the J2EE engine.

## 10.3.5.2 Enable Fully Qualified Distinguished Name for SAP NetWeaver 7.0 or Higher on Linux

How to enable fully qualified distinguished name for SAP NetWeaver AS for Java 7.0 or higher on Linux.

### Procedure

1. Stop the J2EE engine.
2. Go to the profile directory at `usr/sap/<SID>/SYS/profile`, open the profiles (java instance profile `<SID>_J00_your_current_hostname` and SCS profile `<SID>_SCS01_your_current_hostname`) and add the lines below:

```
SAPLOCALHOST = <current_host_name>
SAPLOCALHOSTFULL = <current_fully_qualified_distinguished_name>
icm/host_name_full = $(SAPLOCALHOSTFULL)
```

3. Go to the profile directory `/usr/sap/SL3/profile`, open the `SL3_SCS01_java67` profile, and add the lines below to the SCS profile:

```
SAPLOCALHOST = java67
SAPLOCALHOSTFULL = java67.slac185.local
icm/host_name_full = $(SAPLOCALHOSTFULL)
```

4. Go to the profile directory `/usr/sap/SL3/SYS/profile`, open the `SL3_SCS01_java67` profile, and add the lines below to the java instance profile.

```
SAPLOCALHOST = java67
SAPLOCALHOSTFULL = java67.slac185.local
icm/host_name_full = $(SAPLOCALHOSTFULL)
```

5. Open the file `DEFAULT.PFL` in the profile directory:  
Add the entries **SAPLOCALHOSTFULL** and **SAPFQDN**. The entries **SAPFQDN** and **SAPLOCALHOSTFULL** must be the first entries.

```
SAPLOCALHOSTFULL = <YOUR_CURRENT_FQDN> SAPFQDN = <YOUR_CURRENT_DOMAIN>
```

6. Go to the profile directory `/usr/sap/SL3/SYS/profile`, open the `DEFAULT.PFL` profile and add the lines below to the `DEFAULT.PFL` profile.

```
SAPLOCALHOST = java67
SAPLOCALHOSTFULL = java67.slac185.local
SAPFQDN = slac185.local
```

Modify the values as described in the following example:

#### ❁ Example

```
SAPDBHOST = $(SAPLOCALHOST) . $(SAPFQDN)
j2ee/dbhost = $(SAPLOCALHOST) . $(SAPFQDN)
j2ee/scs/host = $(SAPLOCALHOST) . $(SAPFQDN)
```

7. Make sure that the system can find the fully qualified distinguished name.

#### ❁ Example

```
10.35.168.67 java67.slac185.local
```

- a. If the system cannot find a fully qualified distinguished name, add the domain to `/etc/hosts`.
- b. Restart the SAP NetWeaver Application Server for Java.

Now when an authentication profile of Secure Login Client is created, the enrollment URL will include the fully qualified distinguished name.

The screenshot shows the 'Enrollment Configuration' step of a wizard. At the top, a progress bar indicates three steps: 1. Authentication Configuration, 2. Certificate Configuration, and 3. Enrollment Configuration (the current step). Below the progress bar are buttons for 'Previous', 'Next', 'Finish', and 'Cancel'. The main area contains an 'Enrollment URL' section with 'Add' and 'Remove' buttons. Below these is a table with columns: Protocol, Host Name, Port, and Secure Login Client Version. The table contains one entry: Protocol 'HTT...', Host Name 'java67.slac185.local', Port '50,100', and Secure Login Client Version '2.0'. Below the table is a 'Profile Type' dropdown menu set to 'Automatic Windows login'. Below that is an 'HTTP Proxy URL' text field. At the bottom, there is an 'Auto-Enroll' checkbox which is checked, and an 'Automatic Number of Re-Enroll Retries' text field set to '0'.

Protocol	Host Name	Port	Secure Login Client Version
HTT...	java67.slac185.local	50,100	2.0

## 10.3.6 Locking and Unlocking

You want to change data in the Secure Login Administration Console and you get a message saying that this data is locked by another user.

### Context

If you believe that this lock is not part of a normal change operation, you can unlock the data. This can occur, for example, if someone forgets to log out during a change operation or if their browser crashes. Proceed as follows:

## Procedure

1. Log in as an administrator to SAP NetWeaver Administrator.
2. Use the standard unlock function of SAP NetWeaver Administrator to remove the lock. For more information, see the SAP NetWeaver Library under [Function-Oriented View](#) > [Application Server](#) > [Application Server Java](#) > [Administering Application Server Java](#) > [Administration](#) > [Administration Tools](#) > [SAP NetWeaver Administrator](#) > [Problem Management](#) > [Managing Locks](#).

## 10.3.7 Secure Login Server SNC Problem

The Secure Login Server cannot establish an SNC connection to the SAP Server.

### Context

For the Secure Login Server to verify SAP user credentials, secure communication to the AS ABAP needs to be established. The communication is secured using SNC.

Problem: The Secure Login Server cannot establish an SNC connection to the AS ABAP.

## Procedure

1. Start SAP NetWeaver Administrator and verify the configuration in the [Configuration](#) tab and [Destinations](#).
2. Select the destination with the destination type RFC Destination.
3. Go to the [Destination Detail](#) section and choose [Ping Destination](#).

If the test is successful, the status line displays the following message:

```
Successfully connected to system <SID> as user <user_name>.
```

4. (If the Ping operation was successful) Proceed with step for enabling trace for the SAP Cryptographic Library.
5. (If Ping Destination failed) Verify whether the SAP Cryptographic Library is installed correctly. Verify the installation described in section [Installing Additional Features for Secure Login \[page 231\]](#).
6. Verify whether an SNC certificate was provided to the SAP Cryptographic Library PSE environment. Verify whether the security token file `SAPSNCS.pse` is available in folder `<DIR_INSTANCE>\sec`.
  - a. Start the command line shell and change to the folder `<DIR_INSTANCE>/exe/$ (DIR_EXECUTABLE)`.
  - b. Set the environment `SECUDIR = <DIR_INSTANCE>/sec`.
  - c. Use the command `sapgenpse get_my_name -p SAPSNCS.pse -x <PSE_password> -O <SAP_service_user>`.
7. Verify whether the SNC name is configured correctly.
8. Enable trace for the SAP Cryptographic Library and analyze the problem. For more information, see related link.

If the error messages `Couldn't acquire DEFAULT INITIATING credentials` is displayed, verify whether the environment variable `SECUDIR` is configured correctly for the user who is starting the SAP server. Verify the installation of the SAP Cryptographic Library in the section of the cryptographic library.

## Related Information

[Configuring Tracing for the Cryptographic Library \[page 248\]](#)

<http://service.sap.com/sap/support/notes/1834979> 

## 10.3.8 Secure Login Authentication Profile Lock and Unlock

A Secure Login authentication profile locks itself when it detects a serious problem such as authentication server failure that affects all clients. To unlock the authentication profile, use the [Unlock](#) button in the Secure Login Administration Console.

## 10.3.9 Internal Server Message

You tried to authenticate to an AS Java using a login module stack, but did not succeed. An 'Internal server message' is displayed.

A reason for this error could be an ICM timeout error. For more information, see *Internet Communication Manager (ICM)* in the SAP Library under [Administration of the Internet Communication Manager](#) [Additional Profile Parameters](#) [icm/conn\\_timeout](#).

## Related Information

[Parameters for Destination Management Configuration \[page 308\]](#)

## 10.3.10 Error Codes

Error codes and return codes for Secure Login Server

This chapter describes the error codes and return codes, their meaning and possible corrections.

## 10.3.10.1 Secure Login Web Client Error Codes

The following table provides you with an overview of the Secure Login Server error codes.

Error Code	Error Message	Description
Client Error 0x01	Problem during download or saving the native components.	<p>In most cases, this is a connection error that prevented that the native libraries were downloaded to the Secure Login Web Client or saved in the user's directory. We recommend that you switch on logging and have a look at the log file to get more information about the cause of the error.</p> <p>To remedy the error, it is generally sufficient to restart SAP GUI and your browser. Thus the configuration is newly read in.</p>
Client Error 0x02	Insecure HTTP connection to Secure Login Server is rejected.	<p>Attempted buildup of an HTTP connection instead of a (secured) HTTPS connection. For more information, see <a href="#">Forced Use of HTTPS [page 184]</a>.</p>
Client Error 0x03	Checksum error in local or remote Secure Login Web Client libraries.	<p>This error occurs when a user is working online during an update from SAP NetWeaver Single Sign-On 1.0 SP1 or SP2 to a higher support package. During an update, the native libraries must be updated. The user might lock a directory, and thus block the update process from replacing the files.</p> <p>To remedy the error, restart your browser, log off from SAP GUI, and log on again. This removes the locking mechanism.</p> <p>If the error persists, we recommend that you switch on logging and have a look at the log file to get more information about the cause of the error.</p> <div><b>⚠ Caution</b> If this error persists, the native libraries on your server system might be manipulated. In the log</div>

Error Code	Error Message	Description
		<p>file on client side, you can see which file is corrupted. Check the Secure Login Server installation for consistency.</p>
Client Error 0x04	Unknown or untrustworthy Secure Login Server user certificate issuer is rejected.	<p>PKI checking error. A root CA from the user CA of the Secure Login Server must be available in the Microsoft Trusted Root Certification Authorities.</p> <p><b>i Note</b></p> <p>This error only occurs in Microsoft Windows and Mac OS operating systems.</p> <p>If this error occurs, proceed as described in <a href="#">PKI Check before Storing in a Client Certificate Store [page 185]</a></p>
Client Error 0x05	This Platform is not supported by the web client, abort.	The Secure Login Web Client can only run in Mac OS X or Microsoft Windows, otherwise you get this error.
Client Error 0x06	Communication Error with the native SLWC agent, abort.	This error occurs if there is an inconsistency in the Secure Login Web Client components that are cached locally. This can be caused, for example, by changes being made in the file folder of the the Secure Login Web Client while the Secure Login Web Client was running. Try again or contact your IT support if the issue persists.
Client Error 0x07	Please install SAP Gui	This happens when the SAP GUI is not installed on the users' client. Users must install the SAP GUI on their systems.
Client Error 0x08	Web Client is running in Web Adapter Mode, but no Web Adapter installation is found, abort.	The administrator configured the Secure Login Web Client to run in Web Adapter mode, but the Secure Login Server Support option was not activated during the installation. Install Secure Login Client with Secure Login Server Support option.

Error Code	Error Message	Description
Client Error 0x09	Cannot load configuration for web client.	The Secure Login Web Client could not load the configuration. Contact the administrator to see what is wrong with the profile. Usually this happens if the profile was configured to use the Windows Secure Login Client, and a Secure Login Web Client accessed this profile.

## 10.3.11 Monitoring Secure Login Server

This topic provides information about Application Server monitoring utilities you can use.

If you suspect that there might be an issue with Secure Login Server, we recommend that you use monitoring utilities provided by SAP NetWeaver AS for Java. It might help you to find a solution for your issue.

For more information, see SAP Help Portal under ► [Function-Oriented View](#) ► [Solution Lifecycle Management](#) ► [Solution Monitoring](#) ►.

## 10.3.12 Logging and Tracing Secure Login Server with the Log Viewer of SAP NetWeaver Administrator

You can use the Log Viewer tool of SAP NetWeaver Administrator to log Secure Login Server.

### 10.3.12.1 Viewing Logs

With Log Viewer, you can view all log and trace messages generated in the whole SAP NetWeaver system landscape.

### Context

These log records assist you to monitor and diagnose problems.

## Procedure

In SAP NetWeaver Administrator, start Log Viewer by choosing ► *Troubleshooting* ► *Logs and Traces* ► *Log Viewer* ►. Alternatively, start it in the browser at <https://<host>:<port>/nwa/logs>.

## Related Information

[http://help.sap.com/saphelp\\_nw73ehp1/helpdata/en/47/af4560fa711503e10000000a42189c/content.htm](http://help.sap.com/saphelp_nw73ehp1/helpdata/en/47/af4560fa711503e10000000a42189c/content.htm)

### 10.3.12.2 Configuring Logging

Using Log Configuration you can configure the severities of log controllers online in the whole system or in certain system instances.

## Context

When deploying a configuration on SAP NetWeaver AS for Java, the logs are managed in AS Java's logging framework. Secure Login Server writes log messages and debug traces to the following log controllers:

Category

Category	Default Severity
Applications/Common/Security/SecureLoginServer/Authentication	INFO
Applications/Common/Security/SecureLoginServer/Certificates	INFO
Applications/SecureLoginServer/Server	INFO
Applications/Common/Security/NetweaverSSO/Certificates	INFO
Applications/Common/Security/NetweaverSSO/KeyStore	INFO
Applications/ NetweaverSSO/Server	INFO
Applications/SecureLoginServer/SLAC	INFO
System/Security/SecureLoginServer/SLAC	INFO



Location

Location	Default Location
com.sap.securelogin.* (and subnodes)	INFO

Location

Application
sap.com/SecureLoginServer
sap.com/securelogin.ui

To view log and debug entries with a lower severity, change the log configuration in the log configurator. The changes are effective immediately. There are no log objects and sub-objects. The log messages of Secure Login Server are compliant with the logging and tracing concept of SAP NetWeaver AS for Java (for example, severities INFO, WARNING, ERROR, FATAL etc.).

For more information, see related link.

## Procedure

To start log configuration, open SAP NetWeaver Administrator and choose ► [Troubleshooting Logs and Traces](#) ► [Log Configuration](#) ►. Alternatively, start it in the browser at <https://<host>:<port>/nwa/log-config>.

## Related Information

[Log Configuration with SAP NetWeaver Administrator](#)

### 10.3.12.3 Enabling Diagnostics for Authentication

You can enable diagnostics that tell you what happens in SAP Single Sign-On, for example, if Secure Login Client or Secure Login Web Client could not authenticate successfully. The diagnostic trace tool of SAP NetWeaver Administrator traces the client-server interaction.

#### Context

To enable diagnostics for client authentication issues, take the following steps:

#### Procedure

1. Start SAP NetWeaver Administrator and log on.
2. Choose ► *Go to* ► *Troubleshooting* ► *Logs and Traces* ► *Security Troubleshooting Wizard* ►
3. Choose the diagnostic type *Authentication*.
4. To start the trace, choose the *Start Diagnostics* button.
5. Repeat the user authentication in Secure Login Client or Secure Login Web Client.
6. Stop the trace by choosing the *Stop Diagnostics* button
7. Analyze the results.

# 11 List of Abbreviations

Abbreviations	Meaning
ADS	Active Directory Service
CA	Certification Authority
CAPI	Microsoft Crypto API
CSP	Cryptographic Service Provider
DN	Distinguished Name
EAR	Enterprise Application Archive
HTTP	Hyper Text Transport Protocol
HTTPS	Hyper Text Transport Protocol with Secure Socket Layer (SSL)
IAS	Internet Authentication Service (Microsoft Windows Server 2003)
JAAS	Java Authentication and Authorization Service
LDAP	Lightweight Directory Access Protocol
NPA	Network Policy and Access Services (Microsoft Windows Server 2008)
PEM	Privacy Enhanced Mail
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKCS#10	Certification Request Standard
PKCS#11	Cryptographic Token Interface Standard
PKCS#12	Personal Information Exchange Syntax Standard
PKI	Public Key Infrastructure
PSE	Personal Security Environment
RADIUS	Remote Authentication Dial-In User Service
RFC	Remote function call (SAP NetWeaver term)

Abbreviations	Meaning
RSA	Rivest, Shamir and Adleman
SAR	SAP Archive
SCA	Software Component Archive
SLAC	Secure Login Administration Console
SLC	Secure Login Client
SLS	Secure Login Server
SLWC	Secure Login Web Client
SNC	Secure Network Communication (SAP term)
SSL	Secure Socket Layer
UPN	User Principal Name
WAR	Web Archive
WAS	Web Application Server

# 12 Glossary

Glossary for Secure Login

## Answer to Reset (ATR)

A message output by a contact smart card conveying information, for example, about the communication parameters proposed by the card, the card's nature and state.

## Authentication

A process that checks whether a person is really who they are. In a multi-user or network system, authentication means the validation of a user's logon information. A user's name and password are compared against an authorized list.

## Base64 Encoding

The Base64 encoding is a three-byte to four-characters encoding based on an alphabet of 64 characters. This encoding has been introduced in PEM (RFC1421) and MIME. Other uses include HTTP Basic Authentication Headers and general binary-to-text encoding applications.

### i Note

Base64 encoding expands binary data by 33%, which is quite efficient

## Certificate

A digital identity card. A certificate typically includes:

- The public key being signed.
- A name which can refer to a person, a computer, or an organization.
- A validity period.
- The location (URL) of a revocation center.
- The digital signature of the certificate produced by the private key of the CA.

The most common certificate standard is the ITU-T X.509.

## Certification Authority (CA)

An entity which issues and verifies digital certificates for use by other parties.

## Certificate Revocation List (CRL)

A group of certificates that have been declared to be invalid. The certificate revocation list is maintained and publically released by the issuing Certification Authority (CA) and typically contains the following information:

- The certificate's serial number
- The issuing CA's Distinguished Name
- The date of revocation

## Certificate Store

Sets of security certificates belonging to user tokens or certification authorities.

## Credentials

Used to establish the identity of a party in communication. Usually they take the form of machine-readable cryptographic keys and/or passwords. Cryptographic credentials may be self-issued, or issued by a trusted third party; in many cases the only criterion for issuance is unambiguous association of the credential with a specific, real individual or other entity. Cryptographic credentials are often designed to expire after a certain period, although this is not mandatory. Credentials have a defined time to live (TTL) that is configured by a policy and managed by a Client service process.

## CRL Distribution Point

Publicly available location where a Certification Authority (CA) hosts its certificate revocation list (CRL).

## Cross-Origin Resource Sharing (CORS)

Defines a way in which a browser and server can interact to determine safely whether or not to allow the cross-origin request. It allows for more freedom and functionality than purely same-origin requests, but is more secure than simply allowing all cross-origin requests.

## Cryptographic Application Programming Interface (CAPI)

The Cryptographic Application Programming Interface (also known variously as CryptoAPI, Microsoft Cryptography API, or simply CAPI) is an application programming interface included with Microsoft Windows operating systems that provides services to enable developers to secure Windows-based applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data. Cryptographic Token Interface Standard A standardized crypto-interface for devices that contain cryptographic information or that perform cryptographic functions.

## Directory Service

Provides information in a structured format. Within a PKI: Contains information about the public key of the user of the security infrastructure, similar to a telephone book (e.g. a X.500 or LDAP directory).

## Distinguished Name (DN)

A name pattern that is used to create a globally unique identifier for a person. This name ensures that a certificate is never created for different people with the same name. The uniqueness of the certificate is additionally ensured by the name of the issuer of the certificate (that is, the Certification Authority) and the serial number. All PKI users require a unique name. Distinguished Names are defined in the ISO/ITU X.500 standard.

## Hardware Security Module (HSM)

A physical computing device that protects and manages cryptographic keys for strong authentication and provides cryptographic operations. These modules are , for example, smart cards, plug-in cards, or external security devices.

For more information, see [Adding Certification Authorities \[page 219\]](#) and [Using External User Certification Authorities \[page 220\]](#).

## Key Usage

Key usage extensions define the purpose of the public key contained in a certificate. You can use them to restrict the public key to as few or as many operations as needed. For example, if you have a key used only for signing, enable the digital signature and/or non-repudiation extensions. Alternatively, if a key is used only for key management, enable key encipherment.

## **Key Usage (extended)**

Extended key usage further refines key usage extensions. An extended key is either critical or non-critical. If the extension is critical, the certificate must be used only for the indicated purpose or purposes. If the certificate is used for another purpose, it is in violation of the CA's policy.

If the extension is non-critical, it indicates the intended purpose or purposes of the key and may be used in finding the correct key/certificate of an entity that has multiple keys/certificates. The extension is then only an informational field and does not imply that the CA restricts use of the key to the purpose indicated. Nevertheless, applications that use certificates may require that a particular purpose be indicated in order for the certificate to be acceptable.

## **Lightweight Directory Access Protocol (LDAP)**

A network protocol designed to extract information such as names and e-mail addresses from a hierarchical directory such as X.500.

## **Microsoft Windows Credentials**

A unique set of information authorizing the user to access the Microsoft Windows operating system on a computer. The credentials usually comprise a user name, a password, and a domain name (optional).

## **Login Module Stack (Authentication Stack)**

List of login modules containing authentication logic that is assigned to a component. When a user is authenticated on the J2EE Engine, the server sequentially processes the login module stack that applies to the component that the user accesses. It is possible to assign different login module stacks to different components, thus enabling pluggable authentication.

## **PKCS#11**

PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA Security. PKCS#11 is an API defining a generic interface to cryptographic tokens.

## **Personal Identification Number (PIN)**

A unique code number assigned to the authorized user.



## Personal Information Exchange Syntax Standard

Specifies a portable format for saving or transporting a user's private keys, certificates, and other secret information.

## Personal Security Environment

The PSE is a personal security area that every user requires to work with. A PSE is a security token container with security-related information. This includes the certificate and its secret private key. The PSE can be either an encrypted file or a Smart Card and is protected with a password.

## Privacy-Enhanced Mail (PEM)

The first known use of Base64 encoding for electronic data transfer was the Privacy-enhanced Electronic Mail (PEM) protocol, proposed by RFC 989 in 1987. PEM defines a "printable encoding" scheme that uses Base64 encoding to transform an arbitrary sequence of octets to a format that can be expressed in short lines of 7-bit characters, as required by transfer protocols such as SMTP.

The current version of PEM (specified in RFC 1421) uses a 64-character alphabet consisting of upper- and lower-case Roman alphabet characters (A–Z, a–z), the numerals (0–9), and the + and / symbols. The "=" symbol is also used as a special suffix code. The original specification additionally used the \* symbol to delimit encoded but unencrypted data within the output stream.

## Public FSD

Public file system device. An external storage device that uses the same file system as the operating system.

## Public Key Cryptography Standards

A collection of standards published by RSA Security Inc. for the secure exchange of information over the Internet.

## Public Key Infrastructure

Comprises the hardware, software, people, guidelines, and methods that are involved in creating, administering, saving, distributing, and revoking certificates based on asymmetric cryptography. Is often structured hierarchically.

In X.509 PKI systems, the hierarchy of certificates is always a top-down tree, with a root certificate at the top, representing a CA that does not need to be authenticated by a trusted third party.

## **Radio Frequency Identification (RFID)**

A technology that uses electronic tags to relay identifying information to an electronic reader by means of radio waves.

## **Root Certification Authority**

The highest Certification Authority in a PKI. All users of the PKI must trust it. Its certificate is signed with a private key. There can be any amount of CAs between a user certificate and the root Certification Authority. To check foreign certificates, a user requires the certificate path as well as the root certificate.

## **Root Certification**

The certificate of the root CA.

## **RSA**

An asymmetric, cryptographically procedure, developed by Rivest, Shamir, and Adleman in 1977. It is the most widely-used algorithm for encryption and authentication. Is used in many common browsers and mail tools. Security depends on the length of the key: key lengths of 1024 bits or higher are regarded as secure.

## **SECUDIR**

A directory on the server in which information is placed that goes beyond the PSE (personal security environment).

## **Secure Network Communications**

A module in the SAP NetWeaver system that deals with the communication with external, cryptographically libraries. The library is addressed using GSS API functions and provides SAP NetWeaver components with access to the security functions.

## Secure Sockets Layer

A protocol developed by Netscape Communications for setting up secure connections over insecure channels. Ensures the authorization of communication partners and the confidentiality, integrity, and authenticity of transferred data.

## Single Sign-On

A system that administrates authentication information allowing a user to logon to systems and open programs without the need to enter authentication every time (automatic authentication).

## Token

A security token (or sometimes a hardware token, authentication token or cryptographic token) may be a physical device that an authorized user of computer services is given to aid in authentication. The term may also refer to software tokens.

Smart-card-based USB tokens (which contain a Smart Card chip inside) provide the functionality of both USB tokens and Smart Cards. They enable a broad range of security solutions and provide the abilities and security of a traditional Smart Card without requiring a unique input device (Smart Card reader). From the computer operating system's point of view such a token is a USB-connected Smart Card reader with one non-removable Smart Card present.

Tokens provide access to a private key that allows performing cryptographic operations. The private key may be persistent (like a PSE file, Smart Card, and CAPI container) or non-persistent (like temporary keys provided by Secure Login).

## X.500

A standardized format for a tree-structured directory service.

## X.509

A standardized format for certificates and blocking list.

# 13 Secure Login Security Guide

The security guide provides an overview of the security-relevant information that applies to Secure Login.

## Caution

This guide does not replace the administration or operation guides that are available for productive operations.

## Target Audience

- Technology consultants
- Security consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereas the Security Guides provide information that is relevant for all life cycle phases.

## Why is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system should not result in loss of information or processing time. These demands on security apply likewise to Secure Login. To assist you in securing Secure Login, we provide this Security Guide.

## 13.1 Before You Start

Review the information provided here before you begin your security configuration.

### Fundamental Security Guides



You install components of Secure Login on host SAP NetWeaver Application Servers, either SAP NetWeaver AS for Java or AS ABAP according to the component. Therefore, the corresponding security guides also apply to Secure Login.

For more information, see the SAP NetWeaver Security Guide for your release.

### Important SAP Notes

The most important SAP Notes that apply to the security of the Secure Login component appear in the following table.

Important SAP Notes

Title	SAP Note	Comment
Release Note SAP Single Sign-On 3.0	<a href="#">2338174</a> 	The release note for SAP Single Sign-On 3.0 describes the components and features of this release.
Central note for SAP Single Sign-On 3.0	<a href="#">2300234</a> 	The central note provides product-specific information.

### Related Information

[http://help.sap.com/saphelp\\_nw73ehp1/helpdata/en/f3/780118b9cd48c7a668c60c3f8c4030/frameset.htm](http://help.sap.com/saphelp_nw73ehp1/helpdata/en/f3/780118b9cd48c7a668c60c3f8c4030/frameset.htm)

<https://service.sap.com/securitynotes> 

<http://scn.sap.com/community/security> 

<http://support.sap.com/solutionmanager> 

## 13.2 Component Overview

SAP Single Sign-On consists of its product components, but also requires or uses third-party and operating system components. You must consider all these components for a complete and integrated secure system,

which is the basis for reliable security services for the consuming of business applications and end-user systems.

#### Entities of an SAP SSO System Landscape

Entity	Description
Secure Login Client	Security client for end users. Provides security protocols and credentials to run secure sessions with SAP GUI or web applications. Supports X.509 and Kerberos security tokens.
Secure Login Server	X.509 certificate provider running on SAP NetWeaver Application Server for Java. Supports end user authentication to several SAP and third-party services.
Secure Login Web Client	Browser-embedded and zero-footprint end-user client, which comes as an integrated component of Secure Login Server.
SAP Cryptographic Library	<p>Cryptographic library and security protocol provider for Application Server ABAP (SNC), SAP RFC (SNC), and SAP NetWeaver Application Server for Java (SSL). Supports X.509 and Kerberos security tokens.</p> <p>The SAP Cryptographic Library is the default cryptographic library of the Application Server ABAP. For more information, see SAP Note <a href="#">1848999</a>.</p>
Microsoft Windows server (domain controller)	For Kerberos and SPNego based authentication using the SAP Cryptographic Library, Secure Login Client, and Secure Login Server, service users from the respective Windows domains are required.
Microsoft Windows server (Active Directory)	For LDAP-based end-user authentication, Windows domain users and their passwords are managed here.
LDAP directory server	For LDAP-based end-user authentication, classical LDAP directories can also be used.
RSA authentication server	For RADIUS-based end-user authentication, RSA SecurID tokens can be used.

## 13.3 FIPS 140-2 Crypto Kernel

The SAP Cryptographic Library supports a FIPS 140-2 compliant cryptographic kernel module, as well as an extended cryptographic kernel module.

To run the SAP Cryptographic Library in a FIPS compliant cryptography mode, you must manually copy the files from the `/fips/` subfolder to the library folder. To make sure the original files from the library folder are not used, delete them beforehand.

To check if the SAP Cryptographic Library is running in FIPS mode, run the command line utility `cryptinfo`, which prints out the FIPS compliance status and other crypto relevant information (see SAP Note [2117112](#)).

For more information on how to activate the FIPS-certified crypto kernel in an , see SAP Note [2180024](#).

## 13.4 Secure Login Client

### 13.4.1 Installation Procedures and Settings for Secure Login Client

Secure Login Client is shipped with an SAP Setup installation program. The installation can only be performed by a local or Windows domain user with sufficient permissions to install software and system components.

As Secure Login Client supports several end-user credentials or tokens, you can achieve multiple security levels and use them in parallel or role-based. Secure Login Client, Secure Login Server, and the SAP Cryptographic Library are designed to support you in increasing the security level in your organization. You can, for example, start with Kerberos and move groups of users to RSA SecurID or Smartcard later on.

The following table provides help on selecting the right mechanisms, but your decision also depends on the security policies and conditions of your infrastructure and landscape.

Security Token	Security Level	Assessment
Windows authentication (Kerberos)	Medium	<ul style="list-style-type: none"><li>+ Very high usability, very easy to roll out, infrastructure given existing Microsoft Domain</li><li>- SNC authentication only, no SSL or SSF</li></ul>
Windows authentication (SPNego to X.509)	Medium	<ul style="list-style-type: none"><li>+ Very high usability, easy to roll out, infrastructure given existing Microsoft Domain, supports SNC/SSL/SSF</li><li>+ Secure Login Server allows to generate X.509 on the fly</li></ul>
Software Certificate (X.509)	Medium	<ul style="list-style-type: none"><li>+ High usability, supports SNC/SSL/SSF</li><li>- Enterprise PKI or public trust center services required to roll-out X.509</li></ul>

Security Token	Security Level	Assessment
Password (LDAP or ABAP Basic Authentication to X.509)	Medium	+ High usability, supports SNC/SSL/SSF  + Secure Login Server allows to generate X.509 on the fly
RSA SecurID (One Time Passcodes to X.509)	High	+ Supports SNC/SSL/SSF  + Secure Login Server allows to generate X.509 on the fly  - RSA Server and SecurID token life cycle management required
Smartcard (X.509)	Very high	+ Supports SNC/SSL/SSF  - Enterprise PKI or public trust center services and smartcard life cycle management required

## 13.4.2 Initialization Procedures for Secure Login Client

Secure Login Client makes use of existing X.509 certificates from the Windows certificate store, the Kerberos tickets of the current user, or gets Secure Login Server client profiles from the Windows registry.

The client profiles may be imported into a client machine by means of Microsoft group policy objects or registry file imports into the [Policies](#) section of the host.

A more flexible way is to use Secure Login Server as a client policy server, which only requires you to register the respective group URL, which is used by the download agent component to retrieve the profiles of the group.

In any case, Secure Login Client uses the registered security settings from the profiles. It is the responsibility of Secure Login Server and its administration console to generate client profiles with the recommended and secure default protocols. To enforce HTTPS communication with Secure Login Server, SAP NetWeaver AS for Java must provide SSL ports with [server authentication](#), and should not offer plain HTTP ports if possible.

After a default installation of SAP Netweaver Application Server (SAP NetWeaver AS) Java, there is already a self-signed X.509 certificate available for SSL connections. You can use this certificate, but with the following restriction: Because it is only self-signed, it is not recognized by web browsers as a trusted certificate from a known public-key infrastructure. A technically educated administrator can ignore this, as long as the web browser offers to ignore the warning and continue with opening the connection. In this case it is crucial that the administrator compares certificate name and fingerprint on web browser side with the certificate in SAP NetWeaver AS for Java.

This way it is possible to administrate SAP NetWeaver AS for Java over an SSL encrypted channel. However, replace the self-signed certificate as soon as possible and before any end user is allowed to connect to Secure Login Server. A valid and trusted SSL server certificate can be issued by an existing in-house or external trust center or simply by Secure Login Server.



## Related Information

[http://help.sap.com/saphelp\\_nw73ehp1/helpdata/en/bc/2ee9a2d023d64eac961745ea2cb503/content.htm?frameset=/en/cd/a3937849b043509786c5b42171e5d3/frameset.htm](http://help.sap.com/saphelp_nw73ehp1/helpdata/en/bc/2ee9a2d023d64eac961745ea2cb503/content.htm?frameset=/en/cd/a3937849b043509786c5b42171e5d3/frameset.htm)  
[http://help.sap.com/saphelp\\_nw73ehp1/helpdata/en/48/7f28a10fa44cdbe10000000a42189d/content.htm?frameset=/en/22/757da81d90447696213e5863e8fdf8/frameset.htm](http://help.sap.com/saphelp_nw73ehp1/helpdata/en/48/7f28a10fa44cdbe10000000a42189d/content.htm?frameset=/en/22/757da81d90447696213e5863e8fdf8/frameset.htm)  
[Configuration \[page 192\]](#)

### 13.4.3 Configuration Procedures and Settings for Secure Login Client

Secure Login Client gets its security configuration from Secure Login Server. There are no further security related configuration properties.

### 13.4.4 Runtime Security Considerations for Secure Login Client

Turn off massive and raw data traces in productive systems. Use logging and tracing only if required, for example, during testing and troubleshooting.

## Related Information

[Tracing Secure Login Client \[page 158\]](#)

## 13.5 Secure Login Server

## 13.5.1 Installation Procedures and Settings for Secure Login Server

Secure Login Server is shipped as an application deployment package for SAP NetWeaver Application Server for Java .

### ⚠ Caution

We do not recommend using the command line-based installation tool using telnet. If you use telnet, you must run it on the local host. A telnet deployment on a remote host is highly insecure, as plain telnet sessions are not encrypted.

The recommended installation tool is Software Update Manager.

## Related Information

[Secure Login Server Installation with Software Update Manager \[page 170\]](#)

## 13.5.2 Initialization Procedures and Settings for Secure Login Server

You initialize the Secure Login Server automatically when you start the Secure Login Administration Console page the first time after a fresh deployment.

### 13.5.2.1 X.509 Certificate Identities and PKI

The initialization wizard enables you to create and configure a default set of PKI and client profile objects with recommended secure defaults.

A new X.509 certificate requires you to select the RSA key size in number of bits. The number of bits should be high enough to avoid brute force attacks against the public key. The table below lists the recommended key size, depending on the planned key life time and the PKI role of the identity.

Recommended Key Size According to Role and Lifetime

PKI Role	Key Lifetime	RSA Key Size
Root certification authority	10 years	4096 bits
Intermediate server CA	10 years	4096 bits
Intermediate user CA	5 years	2048 bits

PKI Role	Key Lifetime	RSA Key Size
SSL or SNC server	10 years	2048 bits
End user	< 1 year	2048 bits
End user short-lived	< 1 day	2048 bits

## 13.5.2.2 Authorizations and Roles

Secure Login Server deploys user management engine roles for SAP NetWeaver AS for Java that enable you to securely initialize Secure Login Server.

Only use the role [SLAC\\_SUPERADMIN](#) for initialization and emergency operations. For other administrative operations, use the other dedicated SLAC roles.

Only administrator and operator users that work with Secure Login Server Administration Console shall get SLAC roles. Normal business users do not require SLAC roles. We recommended that you do not assign SLAC roles to business users.

Pages												
Ac- tions	Profile Authentication				Destination Management		Certificate Management				System Management	
	Authentication Profile		Profile Groups		Destinations		PKI Structure		Sign Certificate Requests		System Check	
	Write	Read	Write	Read	Write	Read	Write	Read	Write	Read	Write	Read
<a href="#">SLAC_ClientMngt_All</a>	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No
<a href="#">SLAC_ClientMngt_ReadOnly</a>	No	Yes	No	Yes	No	Yes	No	No	No	No	No	No
<a href="#">SLAC_CertMngt_All</a>	No	No	No	No	No	No	Yes	Yes	No	No	No	No
<a href="#">SLAC_CertMngt_ReadOnly</a>	No	No	No	No	No	No	No	Yes	No	No	No	No

Ac- tions	Pages											
	Profile Authentication				Destination Management		Certificate Management				System Management	
	Authentication Profile		Profile Groups		Destinations		PKI Structure		Sign Certificate Requests		System Check	
	Write	Read	Write	Read	Write	Read	Write	Read	Write	Read	Write	Read
SLAC_SignCertificateReq_All	No	No	No	No	No	No	No	No	Yes	Yes	No	No
SLAC_SignCertificateReq_ReadOnly	No	No	No	No	No	No	No	No	No	Yes	No	No
SLAC_SystemCheck_All	No	No	No	No	No	No	No	No	No	No	Yes	Yes
SLAC_SystemCheck_ReadOnly	No	No	No	No	No	No	No	No	No	No	No	Yes
Actions	Roles											
	SLAC_CERT_ADMIN	SLAC_CERT_READONLY	SLAC_OPERATOR	SLAC_OPERATOR_READONLY	SLAC_SUPERADMIN	SLAC_SUPPORTER						
SLAC_ClientMngt_All	Yes	No	Yes	No	Yes	No						
SLAC_ClientMngt_ReadOnly	No	No	No	No	Yes	No						
SLAC_CertMngt_All	Yes	No	No	No	Yes	No						
SLAC_CertMngt_ReadOnly	No	Yes	No	No	No	Yes						
SLAC_SignCertificateReq_All	Yes	No	No	No	Yes	No						

Actions	Roles					
	<a href="#">SLAC_CERT_A DMIN</a>	<a href="#">SLAC_CERT_RE ADONLY</a>	<a href="#">SLAC_OPERAT OR</a>	<a href="#">SLAC_OPERAT OR_READONLY</a>	<a href="#">SLAC_SUPERA DMIN</a>	<a href="#">SLAC_SUPPOR TER</a>
<a href="#">SLAC_SignCert Req_ReadOnly</a>	No	Yes	No	No	No	Yes
<a href="#">SLAC_SystemC heck_All</a>	No	No	Yes	No	Yes	No
<a href="#">SLAC_SystemC heck_ReadOnly</a>	No	No	No	Yes	No	Yes

## 13.5.3 Configuration Procedures and Settings for Secure Login Server

Use the Secure Login Administration Console to change the security configuration of the Secure Login Server.

### 13.5.3.1 Secure Connections

For new or changed authentication profiles, we strongly recommend the default protocol HTTPS. Otherwise, you send user passwords in clear text over the network.

Also configure external authentication back-end systems connected to Secure Login Server as destinations (ABAP/RFC, Active Directory/LDAP, RADIUS/RSA) to allow a secure communication. How to do configure secure communication depends on the respective protocol and back-end product. Protect RFC connections to AS ABAP servers with SNC, LDAP with SSL, and RADIUS with Challenge-Handshake Authentication Protocol (CHAP) and a shared secret for session key agreement.

### 13.5.3.2 X.509 Certificate Identity Export

Exporting an X.509 certificate identity in [Certificate Management](#) to a PSE or PKCS#12 file requires you to enter a new password, which protects the key file against unauthorized access. Secure Login Server implements a built-in medium-strength password policy to avoid weak passwords:

- 12 character minimum length
- 2 or more lowercase letters
- 2 or more uppercase letters or Unicode letters
- 2 or more digits
- 2 or more special characters

### → Tip

We recommended that you choose a stronger password than this policy enforces, for example, more characters.

You can also manage and export the same X.509 certificate identities in SAP NetWeaver Administrator, but without the recommended password policy. We strongly recommended that you only use Secure Login Administration Console for such operations.

A new X.509 certificate requires you to select the RSA key size in number of bits. The number of bits should be high enough to avoid brute force attacks against the public key. The table below lists the recommended key size, depending on the planned key life time and the PKI role of the identity.

Recommended Key Size According to Role and Lifetime

PKI Role	Key Lifetime	RSA Key Size
Root certification authority	10 years	4096 bits
Intermediate server CA	10 years	4096 bits
Intermediate user CA	5 years	2048 bits
SSL or SNC server	10 years	2048 bits
End user	< 1 year	2048 bits
End user short-lived	< 1 day	2048 bits

This is to be considered for new PKI instances and issued server certificates in [Certificate Management](#), as well as for [Authentication Profiles](#).

An X.509 certificate identity may also be imported from a PSE or PKCS#12 key file.

If a PSE or PKCS#12 transport password seems to be weaker than the built-in policy, we recommended that you delete the PSE or PKCS#12 file or move it to a protected folder after the import operation succeeded.

If the imported X.509 certificate has a shorter key size than recommended for the desired PKI role, consider contacting the originator of the key and ask for a larger one.

Do not write on paper or print out any password unless you really need to. If you do, keep such paper or file copy in a secure place that can be locked or encrypted.

Do not copy and distribute PSE or PKCS#12 files unless you really need to. However, we recommended that you have a secure backup of such files, also in a secure place that can be locked or encrypted.

## Related Information

[https://www.bundesnetzagentur.de/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/algorithmen\\_node.html](https://www.bundesnetzagentur.de/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/algorithmen_node.html) 📄

### 13.5.3.3 X.509 Root Certificate Life Cycle

The X.509 certificates of the one-and-only or all existing root Certification Authorities must be present and trusted in all participating components, in other words. all servers and clients with Secure Login or other X.509 enabled applications.

While all other X.509 certificates like intermediate CAs and user or server certificates can be replaced without manual re-distribution to other systems, the replacement of root CA certificates is quite complex and expensive in terms of administrative efforts. On the other hand, such replacement is needed whenever a root CA certificate expires.

To make sure that your X.509 enabled landscape does not stop working because of an expired root CA, make sure to follow these recommendations:

- Issue root CA certificates with a feasible life time. Choose the longest validity associated to the recommended RSA key size.
- Monitor all root CA certificates regularly, for example, once a month, to make sure you notice an upcoming expiration.
- Define and plan overlapping root CA validities: Create a new root CA long enough before the old ones expire, create all respective intermediate CAs and server certificates, create all authentication profiles. Roll out the new root CA certificate in time to make sure it is available and trusted everywhere before the old one expires. Once this is done, migrate server certificates first, then all authentication profiles.
- Do not delete any root or intermediate or server certificate, or authentication profile, before you can make sure the new PKI is running in the whole landscape.

### 13.5.3.4 Storing the Private Key of the Root CA

Although SAP NetWeaver AS for Java and Secure Login Server can store the private RSA key of the root CA, it is a best practice to move away the Root CA key unless another Intermediate CA is issued.

#### Procedure

1. Export the key with a very strong password.
2. Store this key file (PKCS#12) on two separate CDs or USB drives.
3. Put the keys in a safe and separate places with physical locks.
4. Delete the private RSA key (not the X.509 certificate!) in the Key Storage of SAP NetWeaver AS for Java.
5. Import the key file into the Key Storage of SAP NetWeaver AS for Java if needed, but do not forget to repeat the previous step when finished.

## 13.5.4 Runtime Security Considerations for Secure Login Server

### Logging and Tracing

Turn off massive and raw data traces in productive systems. Use logging and tracing only if required, for example, during testing and troubleshooting.

Secure Login Server uses the standard APIs of SAP NetWeaver AS for Java for logging and tracing. Filter for the application `com.sap.securelogin.ui`.

For more information, see *SAP NetWeaver AS for Java Security Guide* for your respective release: [http://help.sap.com/nw\\_platform](http://help.sap.com/nw_platform).

For more information about HTTP raw data traces, see [SAP Note 724719 - How to enable HTTP tracing in the SAP J2ee Engine 6.40/7.0](#).

### Backup and Recovery

Secure Login Server relies on the backup and recovery mechanisms of SAP NetWeaver AS for Java and its database.

For more information, see the security guides relevant for your release: [http://help.sap.com/nw\\_platform](http://help.sap.com/nw_platform).

### Virus Protection

We recommend you protect the host SAP NetWeaver Application Server for Java with the virus scan interface. If the virus scan profile `webdynpro_FileUpload` is active, you make sure that uploaded files are scanned for viruses. For more information, see the virus scan interface documentation for your SAP NetWeaver release.

## 13.5.5 Secure Login Web Client

Secure Login Web Client is integrated into Secure Login Server, and does not require its own installation, initialization, or configuration.

The Java Applet of Secure Login Web Client is digitally signed by SAP AG and automatically verified by the web browser.

All security relevant profiles and configuration properties come from Secure Login Server and the Secure Login Administration Console.



Additionally, Secure Login Web Client enforces HTTPS communication and refuses any plain HTTP URL to servers. The X.509 end user certificate it receives must also come from a locally trusted PKI: On Windows and Mac OS X, the Root Certification Authority of the PKI must be available and trusted in the respective system stores, for example, Windows Certificate Store or Apple Keychain.

Turn off massive and raw data traces in productive systems. Use logging and tracing only if required, for example, during testing and troubleshooting.

## 13.6 SAP Cryptographic Library

### 13.6.1 Installation Procedures and Settings for the SAP Cryptographic Library

In a new installation, Secure Login is using the SAP Cryptographic Library, the default cryptographic library of SAP NetWeaver AS.

For more information, see SAP Note [1848999](#) .

You can also download the SAP Cryptographic Library as platform SAP CAR archives without an installation program. The installation depends on respective platform and operating system. For more information, see the product guide.

Limit file permissions of installation folders, library and command line utility files, as well as of configuration XML files to the minimum set that is required by the application server processes.

The minimal configuration runs with built-in defaults.

#### 13.6.1.1 INTEL AES-NI Support

The SAP Cryptographic Library is shipped with AES Native Interface support for several INTEL CPUs (Windows and Linux OS only).

This hardware accelerated AES encryption does not affect the level of security, but increases the speed of encryption operations. To find out if a respective host supports AES-NI, run the command line utility `cryptinfo`. The utility displays the AES-NI status and other crypto relevant information.

## 13.6.2 Initialization Procedures for the SAP Cryptographic Library

The SAP Cryptographic Library requires a Personal Security Environment file (PSE), which contains either an X.509 certificate identity with PKI trust anchors, or one or more Kerberos keytab identities, or both. Both types allow local generation by a command line utility or import from existing key stores.

### 13.6.2.1 File Permissions of Key Files

Store any kind of key files (PSE or PKCS#12) with limited file permissions.

Only allow privileged administrators, who must be able to read and write, and application processes that must be able to read such key files to do so. Use the file permissions of the respective operating systems to grant minimum access only.

The command line utilities shipped with the SAP Cryptographic Library set such minimum file permissions if possible. We recommended that you check these automatically generated permissions after write operations.

### 13.6.2.2 X.509 Certificates

You can generate a new PSE file and an X.509 certificate identity with the command line utility `sapgenpse`.

Generating a new PSE and exporting an X.509 certificate key from a PSE requires you to enter a new password and encryption, which protects the key file against unauthorized access. `sapgenpse` implements a built-in medium-strength password policy to avoid weak passwords:

- 8 character minimum length
- 1 or more lowercase letters
- 1 or more uppercase letters
- 1 or more digits
- 1 or more special characters

SAP Single Sign-On supports the following signature algorithms. For more information, see the SAP Notes [1943240](#) and [206194](#).

- sha1WithRSAEncryption
- sha256WithRSAEncryption (recommended)
- sha384WithRSAEncryption
- sha512WithRSAEncryption
- sha1WithRSAPSS
- sha256WithRSAPSS
- sha512WithRSAPSS

#### → Tip

We recommended that you choose a stronger password than this policy enforces, for example, more characters. Use the recommended signature algorithm to protect the key.

A new X.509 certificate requires an RSA key size of a specific number of bits. The number of bits should be high enough to avoid brute force attacks against the public key. The table below lists the recommended key size and signature algorithm, depending on the planned key life time and the PKI role of the identity.

Recommended Key Size and Signature Algorithm According to Role and Lifetime

PKI Role	Key Lifetime	RSA Key Size	Recommended Signature Algorithm
Root certification authority	10 years	4096 bits	sha256WithRSAEncryption
Intermediate server CA	10 years	4096 bits	sha256WithRSAEncryption
Intermediate user CA	5 years	2048 bits	sha256WithRSAEncryption
SSL or SNC server	10 years	2048 bits	sha256WithRSAEncryption
End user	< 1 year	2048 bits	sha256WithRSAEncryption
End user short-lived	< 1 day	2048 bits	sha256WithRSAEncryption

An X.509 certificate identity may also be imported from a PKCS#12 key file. In this case, the PKCS#12 transport password is only used to read from the file. It does not replace the password of the PSE.

If a PKCS#12 transport password seems to be weaker than the password of the PSE, we recommended that you delete the PKCS#12 file or move it to a protected folder after the import operation succeeded.

If the imported X.509 certificate has a shorter key size than recommended for the desired PKI role, consider contacting the originator of the key and ask for a larger one.

Do not write on paper or print out any password unless you really need to. If you do, keep such paper or file copy in a secure place that can be locked or encrypted.

Do not copy and distribute PSE or PKCS#12 files unless you really need to. However, we recommended that you have a secure backup of such files, also in a secure place that can be locked or encrypted.

### 13.6.2.3 STRUST Managed PSEs and X.509 Certificates

A PSE file with X.509 certificate identity can also come from AS ABAP and its STRUST transaction. In this case, keyfile and password are generated and managed by STRUST, which uses the underlying SAPCRYPTOLIB version 5.5.

### 13.6.2.4 Kerberos Keytabs

You can generate a new PSE file and one or more Kerberos keytab identities with the command line utility `sapgenpse`.

Generating a new PSE for Kerberos keytab identities requires you to enter a new password and encryption, which protects the key file against unauthorized access. `sapgenpse` implements a built-in medium-strength password policy to avoid weak passwords:

- 8 character minimum length
- 1 or more lowercase letters
- 1 or more uppercase letters
- 1 or more digits
- 1 or more special characters

SAP Single Sign-On supports the following encryption algorithms for authentication at an AS ABAP with Kerberos and SNC:

- AES256 (recommended)
- AES128 (recommended)
- DES
- RC4

#### → Tip

We recommend that you choose a stronger password than this policy enforces, for example, more characters. Use the recommended encryption algorithm to protect the keytab.

A single keytab identity represents the service account created on a Windows domain controller, and consists of the service principal name and the service account password. Both must be exactly the same on Windows domain controller side and in the respective command line of `sapgenpse`.

As the SAP Cryptographic Library works in a so-called offline Kerberos verification mode, there is no technical communication between AS ABAP and Windows DC. The configuration is also done manually and offline.

This includes that the primary instance where to enter a new service account password is the Windows domain controller, which should have its own password policy configuration in place. If such password is weaker than recommended, consider contacting the administrator of the account and ask for a better password.

The second option to get a Kerberos keytab identity into a PSE file is to import it from a keytab file. This requires you to export the keytab on the Windows domain controller side.

We do not recommend this option, because the Windows domain controller does not provide a secure way to store and transport keytab files. It should only be considered if the service account passwords must not be shared between two administrators, and if there is a secure way to exchange such unprotected keytab files in a secure way, for example, through a protected file system.

## 13.6.2.5 Single Sign-On Credentials

To allow unattended server restart (for example, no need for entering PSE passwords at restart), the SAP Cryptographic Library enables you to enter the PSE password once on a server, and store it in the credentials file (`cred_v2`) of the PSE.

This SSO credentials mechanism is not highly secure on most platforms, and requires a protected operating system by standard means like firewalls, recommended application server and OS patches, and minimal file permissions of the folder containing PSE and `cred_v2` files. This minimizes the risk of stolen PSE and `cred_v2` files.

On Windows platforms, SSO credentials generated by `sapgenpse.exe` are protected with the data protection key of the host (Windows Data Protection API). In this case, PSE and `cred_v2` files cannot be used on any other system.

## 13.6.2.6 AS ABAP Default Profile (SNC)

The SAP Cryptographic Library can be used by AS ABAP to act as a protocol provider for SNC. The respective configuration is done in the ABAP default profile, which is a text property file that is either edited manually or by ABAP transaction `RZ10`.

It is important to understand how to configure SNC for AS ABAP server and its users and services. Otherwise, SNC is not enforced and insecure and password-based logon is still possible, or SNC is turned on too early which may lead to a lock-out of all users including administrators. In the latter case, only local OS level access to the default profile and command line allow you to repair and restart the server again.

For more information, see the documentation for SNC.

### Related Information

[http://help.sap.com/saphelp\\_nw73ehp1/helpdata/en/e6/56f466e99a11d1a5b00000e835363f/content.htm?frameset=/en/e6/56f466e99a11d1a5b00000e835363f/frameset.htm](http://help.sap.com/saphelp_nw73ehp1/helpdata/en/e6/56f466e99a11d1a5b00000e835363f/content.htm?frameset=/en/e6/56f466e99a11d1a5b00000e835363f/frameset.htm)

## 13.6.3 Configuration Procedures and Settings for the SAP Cryptographic Library

The SAP Cryptographic Library comes with a strong default configuration. However, there are several properties that can be used to fine-tune the security protocols and the cryptographic algorithms they use.

Any changes in the kernel profile parameters of Application Server ABAP (or in the legacy XML configuration files) should be cross-checked and tested before applied to a production system. See the administration guide for details.

All X.509 certificate or Kerberos keytab based operations are similar to the initialization, see the respective recommendations.

## 13.6.4 Runtime Security Considerations for the SAP Cryptographic Library

Turn off massive and raw data traces in productive systems. Use logging and tracing only if required, for example, during testing and trouble shooting.

### Related Information

[Configuring Tracing for the Cryptographic Library \[page 248\]](#)

## 13.7 Microsoft Windows Server Domain Controller

In addition to the security guidelines provided by Microsoft, we have a few additional recommendation for the secure operation of this product.

We recommended that you use a strong password policy for all accounts, especially for business users and service accounts used for Kerberos-based authentication.

Grant minimum account privileges to service accounts that you created for the SAP Cryptographic Library and Kerberos keytab identities. The only required privilege is membership in the Windows Domain. No other permissions or memberships should be assigned unless there is an urgent need for it.

We recommend a regular password change policy for business user and service accounts used for Kerberos-based authentication.

Before you change the password of your Kerberos service account, add another keytab entry for its SPN in the PSE of your AS ABAP or SAP NetWeaver AS for Java SPNego configuration to make sure there is no interruption in your Kerberos authentication.

## 13.8 Microsoft Windows Server Active Directory

In addition to the security guidelines provided by Microsoft, we have a few additional recommendation for the secure operation of this product.

Provide SSL protected LDAP communication for clients that send passwords for authentication.

We recommend a regular password change policy for business user and service accounts used for LDAP-based authentication.

## 13.9 LDAP Directory Server

In addition to the security guidelines provided by the LDAP vendor, we have a few additional recommendation for the secure operation of this product.

Provide SSL protected LDAP communication for clients that send passwords for authentication.

We recommend a regular password change policy for business user accounts used for LDAP-based authentication.

## 13.10 RSA Authentication Server

In addition to the security guidelines provided by the RSA, we have a few additional recommendation for the secure operation of this product.

Secure Login Server and RSA Authentication Server communicate over the RADIUS protocol. The protocol makes use of a shared secret that is required during session key agreement. Such shared secrets should meet the same password strength recommendations as for key files:

- 8 characters minimum length
- 1 or more lowercase letters
- 1 or more uppercase letters
- 1 or more digits
- 1 or more special characters

If such a password is weaker than recommended, consider contacting the administrator of the account and ask for a better one.



Use the recommended RSA SecurID token maintenance options from the vendor guides.

# Important Disclaimers and Legal Information

## Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

## Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

## Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

## Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

## Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.



© 2020 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.