Secure Login for SAP Single Sign-On Implementation Guide
Content

1 What Is Secure Login? ................................................................. 8
  1.1 System Overview ............................................................ 8
    Cryptographic Library for SAP Single Sign-On 2.0 SP03 or Higher ... 9
    Clients for Authentication ................................................. 10
    Environment Using Secure Login Client and Secure Login Server ... 11
    Environment Using Secure Login Client ................................ 14
  1.2 System Overview with Secure Login Server ......................... 17
  1.3 Authentication Profiles .................................................... 18
  1.4 PKI Structure ................................................................. 18
    Out-of-the-Box PKI Login Server ....................................... 18
    PKI Integration ............................................................... 19
  1.5 Secure Communication ................................................... 21
  1.6 Policy Server Overview .................................................. 22
  1.7 Digital Signing with Secure Store and Forward (SSF) ............... 22

2 Secure Login Client ............................................................... 24
  2.1 Secure Login Client Installation ......................................... 24
    Unattended Installation with SAPSetup Installation Server .......... 26
    Uninstalling Secure Login Client ....................................... 27
  2.2 Updating the Secure Login Client to the Current Support Package 29
  2.3 Adding Root Certificates during Installation ......................... 30
    Option 1: Installing Root CA Certificates on a Windows Client .... 31
    Option 2: Distributing Root CA Certificates on Microsoft Domain Server ... 32
    Option 3: Distribute Secure Login Server Root CA Certificates Using Microsoft Group Policies ... 32
  2.4 Downloading Policies to the Secure Login Client .................. 34
    Downloading Policies to Secure Login Client Using Profile Groups 34
    Downloading Policies to Secure Login Client Using the Policy Download Agent ... 35
    Creating a Profile Group of Authentication Profiles ................... 37
  2.5 Getting User-Specific Profiles for Certificate Enrollment ........ 38
    Configuring User-Specific Profile Download in Secure Login Client ... 39
    Downloading User-Specific Profile Groups to the Secure Login Client ... 40
  2.6 Configuration Options .................................................... 41
    Enable SNC in SAP GUI ................................................... 41
    User Mapping ................................................................... 44
    Overview of Registry Configuration Options ............................ 47
    Automatically Using the Proxy Configuration of Microsoft Internet Explorer for Secure Login Client ... 47
Using the Single Sign-On Wizard to Configure SNC and SPNego ........................................ 97
SNC X.509 Configuration ............................................................................................................ 98
SNC Kerberos Configuration ...................................................................................................... 101
X.509 and Kerberos Authentication ........................................................................................... 108
Kerberos Authentication for HTML-Based User Interfaces Using SAP NetWeaver AS for ABAP with SPNego ................................................................. 111
SNC Communication Protocol Parameters .............................................................................. 119
Use Case for Defining a Symmetric Algorithm ......................................................................... 123
User SNC Name Mapping ......................................................................................................... 125
Using Certificate Revocation Lists ........................................................................................... 129
Digital Signatures (SSF) with a Hardware Security Module ...................................................... 135

X.509 and Kerberos Authentication ......................................................................................... 108

4.6 Configuration Options ........................................................................................................ 135

Configuring Tracing for the Cryptographic Library ................................................................. 135

5 Secure Login Server .............................................................................................................. 138

5.1 Installation and Installation File Names ............................................................................. 138

Prerequisites for Installing Secure Login Server ...................................................................... 139
Authentication Servers Supported by Secure Login Server ....................................................... 139
Installing Secure Login Library (Optional) .............................................................................. 140
Secure Login Server Installation with Software Update Manager ............................................... 143
Secure Login Server Installation with Telnet ............................................................................ 144
Secure Login Server Uninstallation ........................................................................................... 146

5.2 Initial Configuration Wizard ............................................................................................... 147

Prerequisites for Running the Initial Configuration Wizard ....................................................... 147
Initial Configuration .................................................................................................................. 148

5.3 Administration .................................................................................................................. 152

Starting the Secure Login Administration Console ................................................................. 152
Changing Password .................................................................................................................. 153
Stopping and Starting Secure Login Server with Telnet .......................................................... 153
Stopping and Starting Secure Login Server Using SAP Management Console ......................... 153

5.4 Secure Login Web Client ..................................................................................................... 154

Configuring Secure Login Web Client Connections to SAP GUI ........................................... 155
Using Secure Login Client in Web Adapter Mode ..................................................................... 160
Enabling SAP GUI to Use Credentials with Secure Login Web Client .................................... 161
Security Features of Secure Login Web Client ......................................................................... 161
Mozilla Firefox Plug-In for Storing Secure Login User Certificates ......................................... 168
Rebranding Secure Login Web Client ....................................................................................... 170
Export Restrictions .................................................................................................................. 171

5.5 Using Secure Login Server for SAML 2.0 Authentication .................................................. 171

Configuring SAML 2.0 Authentication in the Secure Login Server ........................................ 172

5.6 Certificate Lifecycle Management Using Secure Login Server .......................................... 173

PSE Infrastructure Involved in Certificate Renewal Using Secure Login Server ....................... 174
Prerequisites for Certificate Renewal Using Secure Login Server ........................................ 175
Configuring Certificate Lifecycle Management in the AS ABAP Using Secure Login Server ........................................ 175
Preparing a Certificate Renewal at Regular Intervals ........................................ 179

5.7 Issuing Certificates for iOS Devices ........................................................................ 182
Configuring an Authentication Profile for iOS Devices ........................................ 183

5.8 Configuration ........................................................................................................ 184
Overview of Login Modules Supported by SAP Single Sign-On 2.0 ....................... 184
Adding a Policy Configuration ....................................................................................... 185
Creating an Authentication Profile Pointing to a Policy Configuration .................. 187
Creating Destinations ................................................................................................. 189
Setting the Enrollment URL for Secure Login Client ............................................... 190
Configuring Actions at Policy Download .................................................................... 191
Configuration of User Certificate Names .................................................................... 192
Managing Destinations ............................................................................................... 206
Archiving Certificate Requests, Issued Certificates, and User Certificates ......... 208
Adding Certification Authorities ................................................................................. 211
Using External User Certification Authorities ......................................................... 212
Configuring Secure Communication ........................................................................... 214
Checking the Availability of Secure Login Server Configuration ......................... 215

5.9 Configuration Examples ........................................................................................ 216
Verify Authentication Server Configuration .............................................................. 216
Integrate into Existing PKI ......................................................................................... 216
High Availability and Failover for Secure Login Server and Secure Login Client .... 218
Kerberos Authentication with SPNego ...................................................................... 220
LDAP User Authentication ......................................................................................... 224
User Authentication against SAP NetWeaver Application Server for ABAP ........ 226
RADIUS User Authentication ...................................................................................... 228
Identification Using RFID Tokens ............................................................................. 230

6 Parameter Reference .................................................................................................. 241

6.1 Parameter Overview for Secure Login Client ......................................................... 241
Registry Configuration Options ................................................................................. 241
SSF Parameters for Digital Signatures ...................................................................... 256

6.2 Parameter Overview for Secure Login Server ........................................................ 257
Parameters for Initial Configuration (PKI Certificates) .......................................... 258
Parameters for Signing Certificate Requests ............................................................... 260
Secure Login Client Policy and Profiles .................................................................... 261
Parameters for the Policy Configuration ..................................................................... 269
Parameters for User Authentication in the Authentication Profile ......................... 283
Parameters for Certificate Configuration in the Authentication Profile ................. 285
Parameters for Destination Management Configuration ........................................... 289
Parameters for Certificate Renewal Using Secure Login Server ............................ 292
6.3 Parameter Overview for Secure Login Library ........................................ 295
Parameters for Certificate Revocation Lists ........................................ 295
Communication and Protocol Parameters (Server and Client) ............ 298
6.4 Parameter Overview for the SAP Cryptographic Library ..................... 303
SNC Parameters for the SAP Cryptographic Library ............................. 303

7 Troubleshooting ................................................................. 308
7.1 Troubleshooting Secure Login Client .............................................. 308
Error in SNC ........................................................................ 309
User Name Not Found ............................................................ 310
Invalid Security Token ................................................................ 311
Wrong SNC Library Configured ............................................... 312
No Display of Password Expiration Warning .................................. 313
SNC Error Codes in the Secure Login Client .................................... 313

7.2 Troubleshooting Secure Login Library ............................................. 314
SNC Library Not Found ................................................................ 314
Credentials Not Found ............................................................. 315
No Credentials Found at Start of Application Server ABAP ............... 316
No User Exists with SNC Name .................................................. 317
Monitoring the Secure Login Library or the SAP Cryptographic Library 317
Error Occurred with sapgenpse ................................................... 317
SNC Error Codes .................................................................... 317

7.3 Troubleshooting Secure Login Server .............................................. 318
Secure Login Web Client Authentication Failed ................................ 318
Trust Warnings in Secure Login Web Client .................................... 319
Error Codes of SAP Stacktrace Errors .......................................... 319
Checklist User Authentication Problem ........................................... 322
Enable Fully Qualified Distinguished Name in Enrollment URL ........ 322
Locking and Unlocking ................................................................ 325
Secure Login Server SNC Problem ............................................. 326
Secure Login Authentication Profile Lock and Unlock ....................... 327
Internal Server Message ............................................................ 327
Error Codes ............................................................................ 327
Monitoring Secure Login Server .................................................. 330
Logging and Tracing Secure Login Server with the Log Viewer of SAP NetWeaver Administrator .................................................. 330

8 List of Abbreviations .................................................................. 334

9 Glossary ................................................................................. 336

10 Secure Login Security Guide ...................................................... 343
10.1 Before You Start ...................................................................... 343
10.2 Component Overview. ........................................................... 344
10.3 FIPS 140-2 Crypto Kernel. .................................................. 345
10.4 Secure Login Library. ........................................................... 346
  Installation Procedures and Settings for Secure Login Library. .......... 346
  Initialization Procedures for Secure Login Library. ......................... 346
  Configuration Procedures and Settings for Secure Login Library. ......... 350
  Runtime Security Considerations for Secure Login Library. ............... 351
10.5 Secure Login Client. .............................................................. 351
  Installation Procedures and Settings for Secure Login Client. ............ 351
  Initialization Procedures for Secure Login Client. .......................... 352
  Configuration Procedures and Settings for Secure Login Client. ......... 353
  Runtime Security Considerations for Secure Login Client. ............... 353
10.6 Secure Login Server. .............................................................. 353
  Installation Procedures and Settings for Secure Login Server. ............ 354
  Initialization Procedures and Settings for Secure Login Server. .......... 354
  Configuration Procedures and Settings for Secure Login Server. ......... 357
  Runtime Security Considerations for Secure Login Server. ............... 360
  Secure Login Web Client. .......................................................... 360
10.7 Microsoft Windows Server Domain Controller. .......................... 361
10.8 Microsoft Windows Server Active Directory. ............................ 361
10.9 LDAP Directory Server. .......................................................... 361
10.10 RSA Authentication Server. ................................................... 362
What Is 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 1912175.

- SAP GUI and SAP NetWeaver platform with Secure Network Communications (SNC)
- HTML-based user interfaces and SAP NetWeaver platform 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 NetWeaver Application Server
- 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 EP (and other HTTPS-enabled Web applications) with SSL.

1.1 System Overview

Secure Login consists of several components (Secure Login Server, Secure Login Client, NWSSO for CommonCryptoLib 2.0, 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 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 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.

- **NWSSO for CommonCryptoLib 2.0**
  NWSSO for CommonCryptoLib 2.0 enables you to use the full scope of functions of the SAP Cryptographic Library, which is the default cryptographic library of the SAP NetWeaver Application Server for ABAP (see the related link). A new installation of SAP Single Sign-On 2.0 SP03 or higher uses this cryptographic library. 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 Library**
  Cryptographic library for an SAP NetWeaver Application Server for ABAP.

**Note**
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 79]
- Identification Using RFID Tokens [page 230]

**1.1.1 Cryptographic Library for SAP Single Sign-On 2.0 SP03 or Higher**

SAP Single Sign-On can run with the following cryptographic libraries provided by SAP:

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

- **Secure Login Library (SLL)**, which is an optional component of SAP Single Sign-On.

**Note**
If you are running SAP Single Sign-On with Secure Login Library, simply upgrade your Secure Login Library to 2.0 SP03. In this case, you continue using your existing configuration. The instance profile parameter containing the path to Secure Login Library remains unchanged.

As of release 2.0 SP03, a newly installed SAP Single Sign-On uses the SAP Cryptographic Library as the default cryptographic library for SNC and SPNego for ABAP.
1.1.2 Clients for Authentication

Secure Login runs with the following clients for authentication:

1.1.2.1 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.
1.1.2.2 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 154]

1.1.3 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.

Main System Components with Secure Login Server - Manually Requesting an X.509 User Certificate

![Diagram showing Secure Login system components and their interactions.](image)
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).

1.1.3.1 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
- RSE SecurID token
- LDAP
- ABAP-based logon
- SAP NetWeaver AS for Java User Management Engine
- SAP NetWeaver AS for Java SPNego
1.1.3.2 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.
1.1.4 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.
1.1.4.1 Authentication Methods without Secure Login Server

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

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication with X.509 certificates</td>
<td>The certificate provider sends the X.509 certificates through secure network communication (SNC). The following certificate providers work with X.509 certificates:</td>
</tr>
<tr>
<td></td>
<td>• Smart card and USB tokens with an existing PKI certificate</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Crypto Store (Certificate Store)</td>
</tr>
<tr>
<td></td>
<td>In SNC the Secure Login Client can perform authentication with encryption and digital signing certificates. The Secure Login Client supports RSA and DSA keys.</td>
</tr>
<tr>
<td>Authentication with Kerberos tokens</td>
<td>For more information about the authentication with a Kerberos token, see the related link.</td>
</tr>
</tbody>
</table>

Related Information

Workflow with Kerberos Token without Secure Login Server [page 17]
1.1.4.2 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.
1.1.4.3 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.

1.2 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.

1.3 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.

1.4 PKI Structure

You can integrate the PKI in different ways.

There are different integration scenarios available for Secure Login Server.

1.4.1 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.
1.4.2 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.
What Is Secure Login?
1.5 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.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Security Protocol / Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP GUI</td>
<td>SAP NetWeaver</td>
<td>DIAG/RFC (SNC)</td>
</tr>
<tr>
<td>Business Explorer</td>
<td>SAP NetWeaver</td>
<td>DIAG/RFC (SNC)</td>
</tr>
<tr>
<td>Business Client</td>
<td>SAP NetWeaver</td>
<td>DIAG/RFC (SNC)</td>
</tr>
<tr>
<td>Web GUI</td>
<td>SAP NetWeaver</td>
<td>DIAG/RFC (SNC), HTTPS</td>
</tr>
<tr>
<td>Secure Login Client</td>
<td>Secure Login Server</td>
<td>HTTPS (SSL)</td>
</tr>
<tr>
<td>Secure Login Server</td>
<td>LDAP server</td>
<td>HTTPS (SSL)</td>
</tr>
<tr>
<td>Secure Login Server</td>
<td>SAP NetWeaver</td>
<td>RFC (SNC)</td>
</tr>
<tr>
<td>Secure Login Server</td>
<td>RADIUS server</td>
<td>RADIUS (shared secret)</td>
</tr>
</tbody>
</table>
1.6 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 show an example for dependencies of application contexts and profiles:

<table>
<thead>
<tr>
<th>Dependencies of Application Contexts and Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Contexts</strong></td>
</tr>
<tr>
<td>Application A.1</td>
</tr>
<tr>
<td>Application A.2</td>
</tr>
<tr>
<td>Application A.3</td>
</tr>
<tr>
<td>Application A.4</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Profiles and Related Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profiles and Related Settings</strong></td>
</tr>
<tr>
<td>Profile P.x</td>
</tr>
<tr>
<td>Profile P.y</td>
</tr>
<tr>
<td>Default Profile P.z</td>
</tr>
</tbody>
</table>

1.7 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 57]
Digital Signatures (SSF) with a Hardware Security Module [page 135]
2 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.

2.1 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 SAP Service Marketplace, go to https://support.sap.com/swdc.

   **Note**

   You find the most recent installation package in Support Packages and Patches > Comprised Software Component Versions.

3. Download the installation package SAPSetupSLC.exe.
4. 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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SAP Secure Login Client</strong></td>
<td>This option installs the basic components of Secure Login Client. This feature is mandatory.</td>
</tr>
<tr>
<td><strong>Start during Microsoft Windows login</strong></td>
<td>Option for an installation under Citrix XenApp, see related link.</td>
</tr>
<tr>
<td><strong>Secure Login Server Support</strong></td>
<td>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 Secure Login Server Support, it comes together with the options Crypto &amp; Certificate Store Providers, Policy Download Agent, 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.</td>
</tr>
<tr>
<td><strong>Kerberos Single Sign-On</strong></td>
<td>This feature installs the Kerberos authentication support. To hide the Kerberos profile, do not install this feature.</td>
</tr>
</tbody>
</table>

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 67]
- Option 1: Installing Root CA Certificates on a Windows Client [page 31]
2.1.1 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.

**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

2. Use the method that suits you best to distribute Secure Login Client to the client workstations.

2.1.2 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

2.1.2.1 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.

2.1.2.2 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.

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 24]
http://service.sap.com/sitoolset

2.1.2.3 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

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.

2.2 Updating the Secure Login Client to the Current Support Package

To update the Secure Login Client 2.0 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


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 2.0 Support Package 1, and the patch level are displayed.

Related Information

Secure Login Client Installation [page 24]
2.3 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

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 .crt.
   
   The dialog box displays the file name, type, size, and the download link.

   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.
2.3.1 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
2.3.2 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`.

2.3.3 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 33]
- Distributing Root CA Certificates Using Microsoft Group Policies with Microsoft Windows Server 2003/2003 R2 [page 33]
2.3.3.1 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 $Edit...$
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`.

2.3.3.2 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.
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`.

2.4 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.

2.4.1 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 2.0. 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 37]
- Enable Fully Qualified Distinguished Name in Enrollment URL [page 322]

### 2.4.2 Downloading Policies to Secure Login Client Using the Policy Download Agent

Secure Login Client gets the client authentication policies from the Secure Login Server 2.0 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 37]
Enable Fully Qualified Distinguished Name in Enrollment URL [page 322]
Option 1: Installing Root CA Certificates on a Windows Client [page 31]
Client Policy [page 262]

2.4.2.1 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.

2.4.2.2 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.

2.4.2.3 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 24]

2.4.3 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 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.
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 269]
- Parameters for Downloading Policies Using Profile Groups [page 280]
- Configuring Secure Communication [page 214]

### 2.5 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.
2.5.1 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

<table>
<thead>
<tr>
<th>Server</th>
<th>Secure Login Server 2.0 SP03 or higher on an SAP Application Server Java</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Secure Login Client 2.0 SP03 or higher (running on a Windows platform)</td>
</tr>
<tr>
<td></td>
<td>SAP GUI</td>
</tr>
</tbody>
</table>

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.
2.5.2 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 280]
2.6 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.

2.6.1 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 SAP NetWeaver Application Server for ABAP.

2.6.1.1 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 244]
2.6.1.2 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 244]
2.6.2 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.

2.6.2.1 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.

Note

Note that the definition of the SNC name is case-sensitive.

Note

You can enable only certain administrators to change the SNC name in SU01 by implementing the SAP Note 1882254.

2.6.2.1.1 Kerberos Example

In this example, the SNC name p:CN=MICROSOFTUSER@DEMO.LOCAL belongs to the user ”SAPUSER”. 

Secure Login Client
2.6.2.1.2 X.509 Certificate Example

In this example the SNC name p:CN=SAPUSER, OU=SAP Security belongs to the user "SAPUSER".

**Note**

For more information about how to perform user mapping, see the Secure Login Library Installation, Configuration and Administration Guide.
2.6.2.2  Set External Security Name for All Users

You can use transaction SNC1 (report RSUSR300) to configure the SNC name in batch mode.

**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.

2.6.2.2.1  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
```

2.6.2.2.2  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
```
2.6.3 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 242]
Application Policy Settings for Kerberos and Microsoft Cryptography API (CAPI) Token [page 244]
CAPI Settings [page 247]
Single Sign-On Setting for Kerberos-Based SNC Profile [page 251]
Single Sign-On Setting for SPNego Profile [page 254]

2.6.4 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

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 48]

2.6.4.1 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 269]
Downloading Policies to Secure Login Client Using the Policy Download Agent [page 35]

2.6.4.2 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 262]

2.6.5 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.

  ![Registry Key Example](image)

- 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 244]

### 2.6.6 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 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 SAP NetWeaver Application Server for ABAP and Java.
• You have installed Secure Login Server 2.0 on an AS Java.
• You are using SAP Cryptographic Library, or you have installed Secure Login Library 2.0 on an AS ABAP.
• You have configured Secure Login Server profiles.

Related Information

Secure Login Client Installation [page 24]

2.6.6.1 API Methods for Profile Enrollment

The front-end control slsax.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)
```

<table>
<thead>
<tr>
<th>Return Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>The relevant profile exists and is enrolled.</td>
</tr>
<tr>
<td>false</td>
<td>All other situations</td>
</tr>
</tbody>
</table>

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)
```

<table>
<thead>
<tr>
<th>Return Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>The relevant profile exists and is enrolled.</td>
</tr>
<tr>
<td>false</td>
<td>All other situations</td>
</tr>
</tbody>
</table>

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 54)
2.6.6.2 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
<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.
2.6.7 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...

ℹ️ 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.

2.6.7.1 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.
2.6.8 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.

2.6.9 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.

2.6.9.1 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 SSO1 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]

  \textbf{Example}

  \texttt{CN=Smartcard User, OU=SAP Security}

  In the \textit{SSF Profile} field, enter the token ID.

  \textbf{Example}

  \texttt{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.

  \textbf{Example}

  \texttt{CN=Username, OU=SAP Security}

  In the \textit{SSF Profile} field, enter the Secure Login Client profile configuration.

  Syntax:

  \texttt{toksw:mem://securelogin/<profile\_name>}

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

6. In parameter \textit{Input data}, enter the file to be signed.

  \textbf{Example}

  \texttt{c:\temp\ToBeSigned.txt}

7. In the parameter \textit{Output data}, enter the path and file name for the signed file.

  \textbf{Example}

  \texttt{c:\temp\IsSigned.txt}

8. Execute the program and choose the \textit{Sign} button.

   The system prompts you for a password, which is not required. Choose the green OK button. The file should be signed. You get the following output:
Related Information

SSF Parameters for Digital Signatures [page 256]

2.6.9.2 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 256]

2.6.9.3 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.

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
SNC Kerberos Configuration [page 101]
Tracing Secure Login Client [page 62]

2.6.10 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.

<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Trace Level**  | Set the trace level. The following trace levels are available:  
|                  |   ○ Deactivated (no tracing)  
|                  |   ○ Errors only  
|                  |   ○ Errors and Warnings  
|                  |   ○ Errors, Warnings, and Information  
|                  |   ○ Developer Traces (in the case of issues that must be solved by support staff)                                                        |
| **Location**     | Path of the trace files                                                                                                                                 |
| **Delete All Traces** | This function enables you to delete all trace files at once. You cannot delete traces that are currently in use.                           |
| **Open Trace Folder** | If you choose this, Microsoft Windows Explorer opens, showing the folder where your client traces are located.                             |

4. Choose **OK** or **Apply**.

### 2.6.11 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.

**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 configuration.
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 275]

2.6.12 SAP NetWeaver Business Client with Secure Login Client

Integration of Secure Login Client in SAP NetWeaver 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.
You are using on-demand short-term certificates from Secure Login Server.
You can integrate Secure Login Client in SAP NetWeaver Business Client. This means that you can log on to SAP NetWeaver Business Client using the secure login features of SAP Single Sign-On 2.0.

For more information about the configuration of SAP NetWeaver 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 ➔
2.6.12.1 Integrating Secure Login Client into SAP NetWeaver 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 attributes to the admin options file. To add attributes to the admin options file, proceed as follows:

Procedure

1. Access the NwbcOptions.xml file under %PROGRAMDATA%\SAP\NWBC\.
2. Modify your runtime connections with the attribute <UseSecureLoginClient>.

Example

```xml
<RuntimeConnection>
  <Name>Test</Name>
  <Url></Url>
  <Type>R3</Type>
  <Client>111</Client>
  <Comment></Comment>
  <User> </User>
  <UseSecureLoginClient>True</UseSecureLoginClient>
</RuntimeConnection>
```

If Secure Login Client is installed on your workstation, this setting is immediately valid.

3. **Note**

   This step is optional. It allows the user to activate or deactivate the usage of the feature for each connection using the user interface.

To activate the appearance of the Secure Login Client attribute in the users systems dialog, add the following option to your admin options file:

Example

```xml
<SINGLEOPTIONS>
  <ShowSecureLoginClientAttribute>True</ShowSecureLoginClientAttribute>
</SINGLEOPTIONS>
```

The user sees the attribute **Use Secure Login Client** on the user interface. When the user tries to connect against a system where the **Use Secure Login Client** attribute is set, SAP NetWeaver Business Client triggers
Secure Login Client to create an X.509 Certificate. It may occur that Secure Login Client opens a popup where users can enter credentials to identify themselves (secure token, RSA). After finishing the Secure Login Client process, SAP NetWeaver Business Client continues the logon process and takes over this certificate.

2.7 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.

Related Information

http://support.sap.com/pam

2.7.1 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.

2.7.2 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.
2.7.2.1 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`:

   ```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).

   ```text
   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.
2.7.3 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.

2.8 Secure Login Client for OS X

You can run Secure Login Client on Mac client computers with the OS X operating system. These Mac clients can use Secure Login Client to authenticate against an SAP GUI using SNC.

SAP Single Sign-On 2.0 SP03 has a software component which allows you to use SAP GUI with SNC on a Mac client with OS X 10.7 or higher. The clients can use either Kerberos-based authentication or, after you made the respective configuration, X.509 certificates for single sign-on with SNC.

⚠️ Restriction

A Mac client cannot use both authentication methods, Kerberos and X.509 certificates, at the same time.

If you want to authenticate to several SAP GUIs and some have SAP GUI connections with X.509 certificates and others support the Kerberos authentication method, you must switch your certificates in your Mac client depending on the authentication method used by the respective SAP GUI connection.

Secure Login Client for OS X does not support Server Login Server profiles.

The Mac clients must belong to a Microsoft Active Directory domain. By default, the Secure Login Client for OS X uses Kerberos for authenticating against an SAP GUI connection.

Prerequisites

<table>
<thead>
<tr>
<th>Application Server ABAP (server)</th>
<th>You have installed Secure Login Library or the SAP Cryptographic Library.</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS X client</td>
<td>• OS X 10.7 or higher</td>
</tr>
<tr>
<td></td>
<td>• SAP GUI for Java</td>
</tr>
<tr>
<td>(If applicable) For Kerberos as authentication mode for SNC</td>
<td>The Mac client is running OS X 10.7 or higher. The user and the computer must belong to a Microsoft Active Directory domain.</td>
</tr>
</tbody>
</table>
2.8.1 Installing Secure Login Client on a Mac Client

The installation of Secure Login Client on an OS X client uses the default OS X installation procedure.

**Procedure**

1. Download the PKG file of the Secure Login Client from the SAP Service Marketplace.
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. By default, 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.

2.8.2 Uninstalling Secure Login Client from a Mac Client

We recommend that you uninstall Secure Login Client from your Mac client by using a dedicated uninstall script.

**Context**

The uninstall script `uninstall.sh` uninstalls Secure Login Client completely.

**Procedure**

1. Open the Terminal application in
   - *Applications* > *Utilities*
2. Go to the Secure Login Client folder where the uninstall script is located. Use the following command:
   
   ```bash
   cd /Application/SecureLoginClient.app
   ```
3. Run the uninstall script.
   - `sudo ./uninstall.sh`
   - You have completely uninstalled Secure Login Client without having left any remains on your Mac client.
2.8.2.1 Cleaning Up after Removal of Secure Login Client on OS X

You have removed Secure Login Client from a Mac client without having used the recommended method (see the related link). As a consequence, you must manually clean up all remains of Secure Login Client.

Context

You have removed Secure Login Client, for example, by moving the application into the trash. The following items remain and must be removed:

- The file launchd.conf in the /etc folder still has some rows referring to the already uninstalled cryptographic library of Secure Login Library.

```
setenv SNC_LIB /Applications/SecureLoginClient.app/Contents/MacOS/lib//libsapcrypto.dylib
setenv SNC_LIB_64 /Applications/SecureLoginClient.app/Contents/MacOS/lib//libsapcrypto.dylib
setenv SSF_LIBRARY_PATH /Applications/SecureLoginClient.app/Contents/MacOS/lib/libsapcrypto.dylib
setenv SSF_LIBRARY_PATH_64 /Applications/SecureLoginClient.app/Contents/MacOS/lib//libsapcrypto.dylib
```

- The SAP Secure Login Client preference pane

Procedure

1. Open the file launchd.conf and remove the respective rows.
2. Open the system preferences and remove the SAP Secure Login Client preference pane.

Related Information

Uninstalling Secure Login Client from a Mac Client [page 70]
2.8.3 Configuring Secure Login Client on a Mac Client

By default, Secure Login Client uses Kerberos to authentication at an SAP GUI with an SNC connection. Nevertheless you can also configure your Mac client to use X.509 certificates.

Context

- Kerberos is the default authentication mode of your Mac client for logging on to an SAP GUI. You need not do anything because Kerberos is already available after the installation. Since your Mac client belongs to Microsoft Active Directory, Kerberos-based authentication mode is supported (see the related link).
- If you want to use X.509 certificates as authentication mode for the SAP GUI with SNC, you must configure it in the OS X System Preference Pane.

Procedure

1. Open the Secure Login Client in your Applications folder or in the System Preferences window.
2. In the parameter Select your SSO method of the Single Sign-On section, switch to Use your selected certificate.
3. Go to the parameter Select your certificate and choose the certificate you want to use for certificate-based authentication to SAP GUI with an SNC connection.

Note

Another option is configuring authentication with X.509 certificates in the Keychain view of OS X. You find the preferred certificate as a Secure Login identity preference.

Caution

Do not switch certificates in the Secure Login preference pane while changing the settings in the Secure Login Identity Preference of the OS X Keychain. You risk getting an inconsistent configuration.

Related Information

Secure Login Client for OS X [page 69]
3 NWSSO for CommonCryptoLib 2.0

A new installation of SAP Single Sign-On 2.0 SP03 or higher uses the SAP Cryptographic Library, which is the default cryptographic library of the SAP NetWeaver Application Server.

The optional component NWSSO for CommonCryptoLib 2.0 enables you to use the following functions in conjunction with the SAP Cryptographic Library (see the related link):

- Revocation check with certificate revocation lists (CRLs)
- Hardware security module (HSM) support together with a Secure Login Server, or for digital signing with SSF using the PKCS#11 interface of this device.

The configuration files for CRL checking, for the configuration of the SNC communication protocol parameters, and for traces of the SAP Cryptographic Library are available in the SAP Note 1996839.

Related Information

SAP Cryptographic Library for Secure Login [page 79]

3.1 Installing NWSSO for CommonCryptoLib 2.0

NWSSO for CommonCryptoLib 2.0 is an optional component of SAP Single Sign-On.

NWSSO for CommonCryptoLib 2.0 enables you to use a number of functions with the SAP Cryptographic Library (CommonCryptoLib). For more information, see SAP Note 1848999 and the related link).

You can install NWSSO for CommonCryptoLib 2.0 on an SAP NetWeaver AS for ABAP or AS Java.

Related Information

SAP Cryptographic Library for Secure Login [page 79]
3.1.1 Installing NWSSO for CommonCryptoLib 2.0 with an Application Server ABAP

With SAP Single Sign-On running with an AS ABAP, this component enables you to use CRL checking and PKCS#11-based hardware security module support.

**Context**

To install NWSSO for CommonCryptoLib 2.0 with an Application Server ABAP:

**Procedure**

1. To download the SAR file of NWSSO for CommonCryptoLib 2.0 for the desired platform, go to the SAP Service Marketplace.


3. Extract the NWSSOCCL<support_package_number>_<patch_level>-<ID>.SAR file to the source directory DIR_CT_RUN.

   **Note**

   To determine the relevant directory, use the SAP Directories transaction (AL11).

4. If you want to use CRL checking, you need additional configuration files. They are available in SAP Note 1996839.
   a. Download the XML files base.xml, pkix.xml, and ldap.xml to DIR_CT_RUN.
   b. Edit the XML files as described in Configuring the CRL Tool [page 132].

5. If, in exceptional cases, you want to configure SNC communication protocol parameters, perform these steps:
   a. Copy the XML file gss.xml to the source directory DIR_CT_RUN.
   b. Edit the file gss.xml as described in SNC Communication Protocol Parameters [page 119].

6. Edit the nwssocl.lst file that is located in the source directory DIR_CT_RUN to add only the file names of the XML files (base.xml, pkix.xml, and/or ldap.xml) that you modified a previous step.

   The template of nwssocl.lst already contains the entries that allow you to use additional functions (see SAP Note 1973271).

   For more information, see the related link.

7. Deploy the files listed in nwssocl.lst from the source directory DIR_CT_RUN to other instances using the Execute_<xx> profile parameters. Use transaction RZ10 in the current instance profile to do this. The Execute_<xx> profile parameter enables you to launch a command at operating system level. For more information, see the SAP Help Portal in Configuration in the CCMS > Profiles > Saving and Importing Profiles.
After Installation ➤ General Information About Profiles ➤ Starting SAP Services by Making an Entry in the Instance Profile.

Choose the next free number of the `Execute _<xx>` command, for example 05, and enter a new line.

Example

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute_05</td>
<td><code>immediate $(DIR_CT_RUN)$(DIR_SEP)sapcpe$(FT_EXE) pf=$(_PF) list:$(DIR_CT_RUN)/nwssoccl.lst</code></td>
</tr>
</tbody>
</table>

8. Save your changes.
9. Restart the Application Server ABAP.

Related Information

Examples for Editing `nwssoccl.lst` [Page 76]

3.1.2 Installing NWSSO for CommonCryptoLib 2.0 with an Application Server Java

With SAP Single Sign-On running with an AS Java, this component enables you to use a hardware security module with a PKCS#11 interface.

Context

Before installation, you need to fulfill the following prerequisites:

- You have installed Secure Login Server.
- A hardware security module for digitally signing certificate requests is available, and you have installed the relevant client software with PKCS#11 support. For more information, see SAP Note [1884870](https://launchpad.support.sap.com.sap) and the related link.

Take the following steps to install NWSSO for CommonCryptoLib 2.0 with an Application Server Java.
Procedure

1. To download the SAR file of NWSSO for CommonCryptoLib 2.0 for the desired platform, go to the SAP Service Marketplace.


3. Extract the NWSSOCCL<support_package_number>_ <patch_level>-<ID>.SAR file to the source directory DIR_CT_RUN.

4. Edit the instance profile file <SID>_J<instance_number>_<host_name>), which is usually located in /usr/sap/<SID>/SYS/profile/.

5. Deploy the files listed in nwssoccl.lst from the source directory DIR_CT_RUN to other instances using the Execute_<xx> command in the profile file. Check the Execute_<xx> parameters.

   Choose the next free number of the Execute_<xx> command, for example 05, and enter a new line.

   **Example**

   ```
   Execute_05 = immediate $(DIR CT_RUN)$(DIR_SEP)sapcpe$(FT_EXE) pf=$(PF) list:$(DIR_CT_RUN)/nwssoccl.lst
   ```

6. Save your changes.

7. Restart the Application Server Java.

Related Information

Using External User Certification Authorities [page 212]

3.1.3 Examples for Editing nwssoccl.lst

The nwssoccl.lst template file, which is located in the source directory DIR_CT_RUN, enables PKCS#11-based hardware security module support. You can edit the template file and add the file names of the XML configuration files that you want to use for CRL checking.

Overview

The template of nwssoccl.lst enables the functions for CRL checking and for PKCS#11 support for hardware security modules. The template like looks this:

For UNIX platforms

```
--- nwssoccl.lst ---
```
crl
libsapnwsso.so

For Microsoft Windows

--- nwssoccl.lst ---
crl.exe
crl.pdb
sapnwsso.dll
sapnwsso.pdb

After you add the relevant XML file names, deploy the files listed in nwssoccl.lst to other instances.

The nwssoccl.lst file can contain the following file names:

<table>
<thead>
<tr>
<th>File Names (UNIX/Microsoft Windows)</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crl/crl.exe with crl.pdb</td>
<td>Default</td>
<td>File name enabling CRL checking</td>
</tr>
<tr>
<td>libsapnwsso.so/sapnwsso.dll with sapnwsso.pdb</td>
<td>Default</td>
<td>Library file name enabling PKCS#11-based hardware security module support</td>
</tr>
<tr>
<td>base.xml</td>
<td>For CRL function only</td>
<td>Configuration file name for CRL checking</td>
</tr>
<tr>
<td>pkix.xml</td>
<td>For CRL function only</td>
<td>Configuration file name for CRL checking</td>
</tr>
<tr>
<td>ldap.xml</td>
<td>For CRL function only</td>
<td>Configuration file name for CRL checking</td>
</tr>
<tr>
<td>gss.xml</td>
<td>For CRL function only</td>
<td>Configuration file name for the SNC communication protocol parameters</td>
</tr>
</tbody>
</table>

### Example for CRL Checking

If you want to use CRL checking with the XML configuration files, enter the file names for base.xml, pkix.xml, and ldap.xml. (PKCS#11-based hardware security modules are also supported.)

**Example**

For Unix/Linux platforms

--- nwssoccl.lst ---
crl
libsapnwsso.so
base.xml
pkix.xml
ldap.xml
### Example for PKCS#11-Based Hardware Security Module Support

If you want to use PKCS#11-based hardware security module support, you can enter the file name for the library file. This is not mandatory.

#### Example

- **For Unix/Linux platforms**

  ```
  --- nwssoccl.lst ---
  crl
  libsapnwsso.so
  ```

- **For Microsoft Windows**

  ```
  --- nwssoccl.lst ---
  crl.exe
  crl.pdb
  sapnwsso.dll
  sapnwsso.pdb
  base.xml
  pkix.xml
  ldap.xml
  ```
4 Secure Login Library

The Secure Login Library provides a cryptographic library for an SAP NetWeaver AS for ABAP system. It supports both X.509 and Kerberos technology.

**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](#).

If, for any reason, you want to use Secure Login Library instead of the default SAP Cryptographic Library, download Secure Login Library from the SAP Service Marketplace. For more information, see the related link.

**Related Information**

[Downloading Secure Login Library](#) [page 84]

4.1 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 SAP NetWeaver Application Server for 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 SAP NetWeaver Application Server for ABAP points to the path of the SAP Cryptographic Library.

**Overview**

The SAP Cryptographic Library and the Secure Login Library provide the same functions, but they are located in different places. The Secure Login Library comes with configuration files, while the SAP Cryptographic Library is delivered as is.

The component NWSSO for CommonCryptoLib 2.0 is a component that enables you to use a number of functions in conjunction with the SAP Cryptographic Library, such as revocation check, configuration of the SNC.
communication protocol parameters, and/or support for a PKCS#11-based hardware security module. For more information, see the related link.

Revocation check and the configuration of the SNC communication protocol parameters with the SAP Cryptographic Library require additional configuration files. You can download them from SAP Note 1996839.

The certificates and Kerberos keytab files are also managed differently (see the related link). The differences mentioned above can have an impact on the Secure Login Client and the Secure Login Server.

If you are using the SAP Cryptographic Library as a replacement for Secure Login Library, this affects the following connections:

- AS ABAP connection to SAP GUI using an SNC connection
- AS ABAP connection to RFC clients using an SNC connection
- Connections with SPNego for ABAP
- Server-to-server connections
  - AS ABAP to AS ABAP
  - AS Java to AS ABAP

### 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 the Library

The configuration files, for example for SNC, are not part of the installation of the SAP Cryptographic Library. However, the optional component NWSSO for CommonCryptoLib 2.0 offers templates for the configuration files (see SAP Note 1996839).
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

NWSSO for CommonCryptoLib 2.0 [page 73]

4.1.1 Configurable Features of SAP Cryptographic Library

The SAP Cryptographic Library supports all configurable features of the Secure Login Library.

If you want to use these features, adapt the configuration in the same way as in the Secure Login Library and provide the relevant configuration files in the place where the SAP Cryptographic Library is used.

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 in an XML file. The certificate revocation tool is configured in a set of XML files, and the file `sectrace.ini` is required for the trace configuration. For more information, see the related links.

Overview of Configuration Files

<table>
<thead>
<tr>
<th>Feature</th>
<th>Required File</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNC communication protocol</td>
<td>gss.xml</td>
<td>A template for this file is available in SAP Note 1996839.</td>
</tr>
<tr>
<td>Certificate revocation lists</td>
<td>crl.exe</td>
<td>The file for the CRL tool is included in the component NWSSO for Common-CryptoLib 2.0.</td>
</tr>
<tr>
<td></td>
<td>pkix.xml, base.xml, and ldap.xml</td>
<td>Templates for these files are available in SAP Note 1996839.</td>
</tr>
<tr>
<td>Trace of the SAP Cryptographic Library</td>
<td>sectrace.ini</td>
<td>A template for this file is available in SAP Note 1996839.</td>
</tr>
</tbody>
</table>
4.1.2 Compatibility of SAP Cryptographic Library and Secure Login Library

The SAP Cryptographic Library (CommonCryptoLib) supports the same features as the Secure Login Library. However, there are some differences concerning the compatibility of these libraries.

SAP Cryptographic Library Delivered Without Configuration Files

The configuration files base.xml, gss.xml, ldap.xml, pkix.xml, sectrace.ini, and crl.exe are not part of the delivery package. They are used to configure certificate revocation list checking, SNC communication modes, or certificate policy checking. The SAP Cryptographic Library supports these configuration files although they are not included in the delivery package. For more information, see the related link.

Different SNC Name Keywords for X.509 Certificates

The SAP Cryptographic Library and the Secure Login Library use different name schemas. This means that a few keywords for the SNC name are not identical. They are displayed in a different way.

You will only encounter compatibility issues if you are using the following keywords in SNC names:

- BUSINESSCATEGORY
- DESCRIPTION
- GIVENNAME
- SERIALNUMBER
- SN
- ST
- STREET
- TITLE

This means that you must change the SNC names when you migrate from the Secure Login Library to the SAP Cryptographic Library. For more information, see SAP Note 1996852.
Caution

If you are running Secure Login Clients 1.0 and/or 2.0 SP02 or lower and/or RFC clients, and if you have the keyword issue in the SNC name, you must solve it (see Client Compatibility with the SAP Cryptographic Library [page 84]). Secure Login Client 2.0 SP03 or higher can handle all kinds of keywords in the SNC name.

Handling of SNC Names with Special Characters

The SAP Cryptographic Library handles special characters in SNC names (for example @, ä, ö, or ü) in a way that differs from the Secure Login Library. The SAP Cryptographic Library uses T61 encoding while the Secure Login Library uses UTF-8 encoding.

Caution

For example, Kerberos names or e-mail addresses in X.509 certificates always include @. If you are using @ in SNC names, it is mandatory to generate the SNC names (canonical name).

Example

SNC name with a special character:

```
p:CN=Julia Müller, O=SAP-AG, C=DE
p:CN=johndoe@sap.com
```

When migrating to the SAP Cryptographic Library, you must generate the canonical names of all SNC names again. For more information, see SAP Note 1996851.

Handling of Kerberos keytabs

If you are using SNC with Kerberos authentication and are migrating from Secure Login Library 1.0, you must create or re-import the Kerberos keytab with `sapgenpse keytab`. The keytabs in `pse.zip` cannot be used or imported. Create the required credentials and restart your server. For more information, see the related link.

Related Information

- Configurable Features of SAP Cryptographic Library [page 81]
- Creating Keytab for Kerberos [page 104]
4.1.2.1 Client Compatibility with the SAP Cryptographic Library

The SAP Cryptographic Library and Secure Login Library 1.0 or 2.0 use different keywords in SNC names. These differences in the keywords can affect the SNC name in the clients.

Context

Secure Login Client 2.0 SP03 works seamlessly with the SAP Cryptographic Library. It can handle all keywords in the SNC name.

Note

With Secure Login Client 2.0 SP03 or higher, the file gss.xml is not included in the installation kit. You can nevertheless use your old (modified) configuration file. Add it during the installation.

However, Secure Login Client 2.0 SP02 or lower and 1.0, and the respective RFC clients, only support one set of keywords. If you want to run Secure Login Client 2.0 SP02 or lower and/or 1.0, solve the keyword incompatibility.

Procedure

1. (Option 1) Upgrade all clients to Secure Login Client 2.0 SP03 or higher.
2. (Option 2) Solve the keyword incompatibility (see SAP Note 1996852). Change the SNC name in each client.

4.2 Secure Login Library Installation

The following topics explain how to install Secure Login Library.

4.2.1 Downloading Secure Login Library

This section deals with the prerequisites and requirements for the installation of Secure Login Library.

You can download the SAP Single Sign-On software from the SAP Service Marketplace. Go to the SAP Support Portal of the SAP Service Marketplace and choose Software Downloads Support Package and Patches Browse our Download Catalog SAP NetWeaver and complementary products SAP NetWeaver Single Sign-On SAP NetWeaver Single Sign-On 2.0 Comprised Software Component Versions Secure Login Library 2.0 The Secure Login Library is available for the several operating systems.
4.2.2 Installing Secure Login Library on a Microsoft Windows Operating System

This topic describes the installation of Secure Login Library on a Microsoft Windows Operating System.

Context

Before starting the installation process, the Secure Login Library software SECURELOGINLIB.SAR must be available. Copy the file to the target SAP NetWeaver Application Server. Secure Login Library must be installed in a directory to which the Application Server has access at runtime. We recommend that you create this directory below the SAP NetWeaver Application Server.

Procedure

1. Create a new folder named SLL in:
   
   $(DIR_INSTANCE)\SLL

   **Example**

   D:\usr\sap\ABC\DVEBMGS00\SLL

2. Extract the file SECURELOGINLIB.SAR to the new folder with the SAPCAR command line tool.

   `sapcar -xvf <SourcePath>\SECURELOGINLIB.SAR -R $(DIR_INSTANCE)\SLL`

   **Example**

   `sapcar -xvf D:\SECURELOGINLIB.SAR -R D:\usr\sap\ABC\DVEBMGS00\SLL`

   **Note**

   Take care that your administrator has write permission for the extracted files.

3. To verify Secure Login Library, use the following command:

   `D:\usr\sap\ABC\DVEBMGS00\SLL\sapgenpse`

   This command displays status and version information of the Secure Login Library.
4.2.3 Installation on a UNIX/Linux Operating System

Context

Before starting the installation process, the Secure Login Library software SECURELOGINLIB.SAR must be available. Copy the file to the target SAP NetWeaver Application Server.

Secure Login Library must be installed in a directory to which the Application Server has access to at runtime. We recommend that you create this directory below the SAP NetWeaver Application Server.

Note

Perform the configuration steps for the Secure Login Library with the user account that will start the SAP application (for example, <SID>adm). Once configuration is complete, the <SID>adm user needs to have access rights to the Secure Login Library.

Procedure

1. Create a new folder named SLL in:

   $(DIR_INSTANCE)/SLL

   Example

   /usr/sap/ABC/DVEBMGS00/SLL

2. Extract the file SECURELOGINLIB.SAR to the new folder with the SAPCAR command line tool.

   SAPCAR -xvf <SourcePath>/SECURELOGINLIB.SAR -R $(DIR_INSTANCE)/SLL/

   Example

   SAPCAR -xvf /tmp/SECURELOGINLIB.SAR -R /usr/sap/ABC/DVEBMGS00/SLL/

3. Define File Attributes in UNIX/Linux. To use shared libraries in shell (operating system UNIX/Linux) and the crl command, you need to set the file permission attributes with the following command:

   chmod +rx $(DIR_INSTANCE)/SLL/lib*

   Example

   chmod +rx /usr/sap/ABC/DVEBMGS00/SLL/lib*
To use the shell under the operating system HP-UX with the shared libraries, you need to set an attribute with the following command:

```bash
chatr +s enable <INSTDIR>/<SID>/DVEBMS<instance_number>/SLL/crl
```

4. If you did not use the `<SID>adm` user during the installation, you must define the file owner in UNIX/Linux. Apply access rights to the user account that will start the SAP application (for example, `<SID>adm`).

```bash
chown [OWNER]:[GROUP] *
```

**Example**

```bash
chown abcadm:sapsys
```

5. Test Secure Login Library. To verify Secure Login Library, use the `sapgenpse` command (in UNIX/Linux environment test with user `<SID>adm`):

```bash
/usr/sap/ABC/DVEBMS00/SLL/sapgenpse
```

The `sapgenpse` command produces the following output with library name, platform `sapgenpse` version, file, and environment variable.

```
Usage: sapgenpse [-h] [-l <sapcryptoPath>] <command> [-h] [sub-options] ...
   -l <sapcryptoPath> Path of CommonCryptoLib (libsapcrypto.so) to be used
   -h Show help text
   <command> Command to execute
   <command> -h Show help text of named command

Loaded CommonCryptoLib from sapgenpse folder "/Disk1/sap/ABC/DVEBMGS04/SLL/libsapcrypto.so"
Platform:   linux-gcc-4.3-x86-64   (linux-gcc-4.3-x86-64)
Versions:   SAPGENPSE     2.0 SP2 (Oct 29 2013)
            FILE-Version  8.4.10.0
CommonCryptoLib (SAPCRYPTOLIB) Version 8.4.10 pl40 (2.0 SP2) (Oct 31 2013) MT-safe
USER="abcadm"
Environment variable $SECUDIR is not defined!
Fallback selection of SECUDIR through HOME:
"/home/abcadm/sec"
```

### 4.2.4 Uninstallation

This section explains how to uninstall Secure Login Library.

**Procedure**

1. Remove folder SLL. Remove the folder and its contents:

   **Microsoft Windows**
   ```
   $(DIR_INSTANCE)\SLL\ ...
   ```

   **UNIX/Linux**
   ```
   ```
2. Deactivate SNC Library Configuration. This step is optional and required only if the Secure Login Library is configured in an SAP NetWeaver instance profile parameter. If you want to deactivate SNC, define the following instance profile parameter and restart the SAP NetWeaver AS for ABAP Application Server:

```
Example
snc/enable = 0
```

For more information about the instance profile parameters see related link.

**Related Information**

*SNC Parameters for the SAP Cryptographic Library [page 303]*

### 4.3 Updating Secure Login Library from 2.0 SP03 to the Current Support Package

If you want to update Secure Login Library from version 2.0 SP03 to the current support package of release 2.0, use the software from the SAP Service Marketplace.

You can download the SAP Single Sign-On software from the SAP Service Marketplace. For more information, see the related link.

**Related Information**

[https://support.sap.com/swdc](https://support.sap.com/swdc)
[http://support.sap.com/pam](http://support.sap.com/pam)

*Downloading Secure Login Library [page 84]*
4.3.1 Downloading the Secure Login Library Software

Before you start the update process, the SAR file for Secure Login Library of Secure Login for SAP Single Sign-On 2.0 SP1 must be available.

**Context**

To get the relevant Secure Login Library installation kit, proceed as follows:

**Procedure**

1. Download the relevant Secure Login Library SAR file from the SAP Service Marketplace. This archive file contains a directory structure that lists the different platforms.
2. Choose the directory for relevant platform.
3. Extract the `SECURELOGINLIB.SAR` file that is suitable for your platform.

4.3.2 Updating Secure Login Library to the Current Support Package on a Microsoft Windows Operating System

You can update Secure Login Library from version 2.0 SP01 to the current support package of release 2.0 on a Microsoft Windows Operating System.

**Context**

Before you start the update process, the current support package of the Secure Login Library software `SECURELOGINLIB.SAR` for Secure Login of SAP Single Sign-On 2.0 must be available. You copy the file to the target SAP NetWeaver Application Server. Secure Login Library must be installed in a directory to which the Application Server has access at runtime. We recommend that this directory is located below the SAP NetWeaver Application Server.

**Procedure**

1. Stop the SAP NetWeaver Application Server.
2. Rename the `SLL` directory, for example, to `SLL_OLD`. All the files from version 2.0 SP01 remain in the renamed directory.
a. If you changed the configuration in the past, keep the configuration files, which are usually files, in a separate place.

3. Create a new folder named SLL.

\$(DIR_INSTANCE)\SLL

**Example**

D:\usr\sap\ABC\DVEBMGSO\SLL

4. Extract the file SECURELOGINLIB.SAR to the new folder with the SAPCAR command line tool.

\n
sapcar -xvf <SourcePath>\SECURELOGINLIB.SAR -R \$(DIR_INSTANCE)\SLL

**Example**

sapcar -xvf D:\SECURELOGINLIB.SAR -R D:\usr\sap\ABC\DVEBMGSO\SLL

**Note**

Take care that your administrator has write permission for the extracted files.

The SLL folder contains several subfolders and the following files:

- crl.exe
- crl.pdb
- gss.xml
- sapcrypto.dll
- sapcrypto.lst
- sapcrypto.pdb
- sapgenpse.exe
- sapgenpse.pdb
- SECURE_LOGIN_LIBRARY_<Windows_platform_version>
- slcryptokernel.dll
- slcryptokernel.dll.sha256

a. (If required) Change the configuration by editing the relevant XML configuration files. For more information, see the related links.

5. Start the SAP NetWeaver Application Server.

**Related Information**

[SNC Communication Protocol Parameters](page 119)
[Configuring the CRL Tool](page 132)
4.3.3 Updating Secure Login Library to the Current Support Package on a UNIX/Linux Operating System

You can update Secure Login Library from version 2.0 SP01 to the current support package of release 2.0 on a UNIX/Linux Operating System.

Context

Before you start the update process, the current support package of the Secure Login Library software SECURELOGINLIB.SAR for Secure Login of SAP Single Sign-On 2.0 must be available. You copy the file to the target SAP NetWeaver Application Server. Secure Login Library must be installed in a folder to which the Application Server has access at runtime. We recommend that this folder is located below the SAP NetWeaver Application Server.

Procedure

1. Stop the SAP NetWeaver Application Server.
2. Rename the SLL folder, for example, to SLL_OLD. All the files from version 2.0 SP01 remain in the renamed folder.
   a. If you changed the configuration in the past, keep the configuration files, which are usually files, in a separate place.
3. Create a new folder named SLL.

   ```shell
   $(DIR_INSTANCE)/SLL
   ```

   **Example**

   ```shell
   /usr/sap/ABC/DVEBMGS00/SLL
   ```

4. Extract the file SECURELOGINLIB.SAR to the new folder with the SAPCAR command line tool.

   ```shell
   sapcar -xvf <SourcePath>/SECURELOGINLIB.SAR -R $(DIR_INSTANCE)/SLL/
   ```

   **Example**

   ```shell
   sapcar -xvf /tmp/SECURELOGINLIB.SAR -R /usr/sap/ABC/DVEBMGS00/SLL/
   ```

   **Note**

   Take care that your administrator has write permission for the extracted files. For more information, see related link.

The SLL folder contains several subfolders and the following files:

- crl.exe
4.3.4 Configuring Secure Login Library During an Update to the Current Support Package

When updating Secure Login Library 2.0 to the current support package, you can use your already existing Secure Login Library configuration or you can define a new configuration.

Context

You can change, for example, the SNC communication parameters or the use of certificate revocation lists. For more information, see related link.

Secure Login Library uses only the configuration files that are located in your installation folder. The installation folder is usually the /SLL folder.

Note

After having extracted the SAR file, you find the configuration files in the /defaults subfolder.

Procedure

- If you want to use your previous configuration files (for example, from version 2.0 SP01), proceed as follows:
a. Copy the configuration files to the installation folder, for example /SLL.
b. If you want to use Secure Login Library trace, copy sectrace.ini with your preferred trace configuration (from version 2.0 SP01) to the installation folder. For more information, see related link.
c. Save your changes.

- If you want to enter a new configuration, take the following steps:
  a. Copy the relevant configuration files from the /defaults subfolder to the installation folder.
  b. Open it in the installation folder and modify the parameters.
  c. Save your changes.

If you want to enter a new configuration, you also have the following option:

  a. Create a new configuration file in the installation folder.
  b. Add the required parameters.
  c. Save your changes.

Start the SAP NetWeaver Application Server.

Related Information

Configuration of the Cryptographic Library [page 96]
Configuring Tracing for the Cryptographic Library [page 135]

4.4 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.

Note

The SAP Cryptographic Library (which comes with SAP NetWeaver Application Server for ABAP) supports FIPS 140-2, security level 1 certification. 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 Secure Login Library 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.

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)
- libslcryptokernel.sl.sha256 (for HP-UX)

For more information on how to activate the FIPS-certified crypto kernel in an SAP NetWeaver Application Server for ABAP, see SAP Note 2180024.

4.4.1 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. Install the Secure Login Library as described in the related link.

   After the installation, you find the standard crypto kernel files in the standard SLL directory. The installation procedure creates a special subdirectory for the FIPS-certified files called fips. The fips subdirectory is the place where you find the certified crypto kernel files mentioned above.
2. (If you are using Secure Login Library) To use the certified crypto kernel files, copy them from the fips subdirectory to the SLL directory. This overwrites and replaces the standard crypto kernel files.

3. (If you are using SAP Cryptographic Library) To use the certified crypto kernel files, copy them from the fips subdirectory to the $(DIR_EXECUTABLE) or $(DIR_CT_RUN) directory, which is the default directory of the SAP Cryptographic Library. This overwrites and replaces the standard crypto kernel files.

4. To display details of the crypto kernel files that used by the Secure Login Library or 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\2.0>.sapgenpse cryptinfo

```
# License Disclaimer
SAP Single Sign-On
You are about to configure trust for single sign-on or SNC Client Encryption.
Please note that for single sign-on you require a license for SAP Single Sign-On.
As exception, the usage of SNC Client Encryption only without SSO is free
as described in SAP Note 1643878.

Properties of Secure Login Crypto Kernel:
FIPS 140-2                = YES
API-VERSION               = 1
VERSION                   = 2.0.0.1.29
FILE-VERSION              = 8.4.1.29
CPU-FEATURES-SUPPORTED    = AES-NI
CPU-FEATURES-ACTIVE       = AES-NI
HASH-ALGORITHMS           = MD2,MD4,MD5,SHA1,SHA224,SHA256,SHA512,RIPEMD128,RIPEMD160,CRC32
ENCRYPTION-ALGORITHMS     = RSA,ELGAMAL,AES128,AES192,AES256,DES,TDES2KEY,TDES2KEY,IDEA,RC2,RC4,RC5_32
ENCRYPTION-MODES          = ECB,CBC,CFB*8,OFB*8,CTR,CTSECB,CTSCBC,GCM
PADDING-MODES             = PKCS1BT01,PKCS1BT02,PKCS1PSS,PKCS1OAEP,X.923,PEM,B1,XML,SSL
KEYEDHASH-ALGORITHMS      = HMAC
SIG-ALGORITHMS            = RSA,DSA
KEYEXCHANGE-ALGORITHMS    = DH
RANDOM-ALGORITHMS         = CTR_DRBG
```
4.5 Configuration of the Cryptographic Library

You perform the secure network communication (SNC) configuration for the SAP NetWeaver server system using the instance 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 and 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).

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

i 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 SAP NetWeaver AS for ABAP. For more information, see SAP Note 1848999. If you are not running an SAP NetWeaver AS for 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 SAP NetWeaver AS for ABAP 7.0, you need to set the environment variable `<SECUDIR>` to `$(DIR_INSTANCE)/sec`. Otherwise SAP NetWeaver AS for ABAP 7.0 does not start.

Related Information

SNC X.509 Configuration [page 98]
SNC Kerberos Configuration [page 101]

4.5.1 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 SAP NetWeaver Application Server for 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.

**4.5.2 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

<table>
<thead>
<tr>
<th>Certificate Fields</th>
<th>Values</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>[No key usage field]</td>
<td>[No values]</td>
<td>[No mode]</td>
</tr>
<tr>
<td><strong>Key Usage</strong></td>
<td><strong>Digital Signature</strong></td>
<td>sigsession, ParallelSessions mode</td>
</tr>
<tr>
<td><strong>Key Usage</strong></td>
<td><strong>Data Encipherment</strong></td>
<td>Encryption</td>
</tr>
<tr>
<td><strong>Key Usage</strong></td>
<td><strong>Key Encipherment</strong></td>
<td>Encryption</td>
</tr>
</tbody>
</table>
Key Usage for X.509 Server Certificates for Client-Server and Server-Server Communication

<table>
<thead>
<tr>
<th>Certificate Fields</th>
<th>Values</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>[No key usage field]</td>
<td>[No values]</td>
<td>[No values]</td>
</tr>
<tr>
<td><strong>Key Usage</strong></td>
<td><strong>Digital Signature</strong></td>
<td>sigsession, ParallelSessions mode (client-server only) Encryption</td>
</tr>
</tbody>
</table>

### 4.5.2.1 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.

**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 303]
- Using the Single Sign-On Wizard to Configure SNC and SPNego [page 97]
4.5.2.2 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.

4.5.3 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 SAP NetWeaver Application Server for 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.

   **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 305]
Using the Single Sign-On Wizard to Configure SNC and SPNego [page 97]

### 4.5.3.1 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.

#### 4.5.3.1.1 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.

   **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*.

   **Note**
   
   The mandatory format is SAP/SAPService<SID>.

Related Information

*Configuring a Service Account* [page 115]
4.5.3.1.2 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:

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

4.5.3.1.3 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 following procedure as a fallback or legacy solution.

**Procedure**

1. Go to the SLL directory.
2. Set the variable `<SECUDIR>`.
   
   Microsoft Windows:
   ```
   set SECUDIR=$(DIR_INSTANCE)\sec
   ```
   UNIX/Linux (depends on shell):
   ```
   setenv SECUDIR $(DIR_INSTANCE)/sec
   export SECUDIR=$(DIR_INSTANCE)/sec
   ```
3. Use the following command:
   
   Microsoft Windows:
   ```
   \usr\sap\ABC\DVEBMGS00\SLL\sapgenpse keytab -p SAPSNCSKERB.pse -x <PSE_password> -y <service_user_password> -a <sAMAccountName>@<WINDOWS-2000-DOMAIN-UPPERCASE>
   ```
Note

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

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

Example

AD_KerbAdminABC@IT.CUSTOMER.COM

UNIX/Linux:

/usr/sap/ABCadm/DVEBMGS00/SLL/sapgenpse keytab -p SAPSNCSKERB.pse -x ****** -y ****** -a SAPServiceNW1@EXAMPLE.COM

You have created the keytab file SAPSNCSKERB.pse for Kerberos authentication.

Caution

The Secure Login Library always uses a PSE file called SAPSNCSKERB.pse file for the keytab. The server does not start if the file has a different name.

4. Set the credentials using the following command:

sapgenpse seclogin -p <path>/SAPSNCSKERB.pse -x <PSE_password> -O <system_user>

Example

sapgenpse seclogin -p /usr/sap/abc/dvebmgS00/sec/SAPSNCSKERB.pse -x <PSE_password> -O abcadm

Caution

In a Microsoft Windows environment, it can happen that the sapgenpse command changes the spelling of the system user specified in -O. Due to the different spelling of the system user, the required credential is not found. This can lead to an error at the start of an Application Server ABAP. You exclude this risk by using the argument -N.

sapgenpse seclogin -p <path>/SAPSNCSKERB.pse -x <PSE_password> -O <system_user> -N

For more information, see the related link.

5. (If applicable) Add a new keytab file for each child or trusted domain. Use the following command:

sapgenpse keytab -p <path>/SAPSNCSKERB.pse -x <PSE_password> -nopsegen -X <keytab_password> -a SAPServiceNW1@EU.EXAMPLE.COM

Note

For more information, use the following command:

sapgenpse -h
Related Information

Creating a keytab [page 117]
No Credentials Found at Start of Application Server ABAP [page 316]

4.5.3.1.4  Verifying keytabs for SNC Authentication

The SAP Cryptographic Library or Secure Login Library provide 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 **SAPSNC Kerb.pse** file using the **sapgenpse** command

With SAP Cryptographic Library 8.4.20 and SAP NetWeaver AS for 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 **SAPSNC Kerb.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 SAP NetWeaver AS for ABAP 7.4 SP07 or lower, the library verifies the keytab differently. For more information, see SAP Note 2029258. If you activate Secure Login Library trace, it contains some of the following messages:

<table>
<thead>
<tr>
<th>Trace Message</th>
<th>keytab Verification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos ticket verified successfully with global keyTab configured in SPNEGO (have global keyTab configured in SPNEGO and keyTab from PSE)</td>
<td>Successful</td>
<td>The cryptographic library has found the global keytab provided by the SPNEGO or SNCWIZARD transaction and the keytab located in the SAPSNC Kerb.pse file. Verification was successful using the global keytab.</td>
</tr>
<tr>
<td>Kerberos ticket verified successfully with global keyTab configured in SPNEGO (have only this one)</td>
<td>Successful</td>
<td>The library has found and verified the global keytab provided by the SPNEGO or SNCWIZARD transaction, and no keytab located in the SAPSNC Kerb.pse file is available.</td>
</tr>
<tr>
<td>Kerberos ticket verified successfully with keyTab from PSE (have global keyTab configured in SPNEGO and keyTab from PSE)</td>
<td>Successful</td>
<td>The library has found and verified the keytab located in the SAPSNC Kerb.pse file and has found the global keytab (provided by the SPNEGO or SNCWIZARD transaction).</td>
</tr>
</tbody>
</table>
### Trace Messages

<table>
<thead>
<tr>
<th>Trace Message</th>
<th>keytab Verification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos ticket verified successfully with keyTab from PSE (have only this one)</td>
<td>Successful</td>
<td>The library has found and verified the keytab located in the SAPSNCSKERB.pse file. No global keytab provided by either the SPNEGO or SNCWIZARD transaction is available.</td>
</tr>
<tr>
<td>Kerberos ticket verification failed with global keyTab configured in SPNEGO</td>
<td>Failed</td>
<td>The library failed to verify the global keytab provided by either the SPNEGO or SNCWIZARD transaction.</td>
</tr>
<tr>
<td>Kerberos ticket verification failed with keyTab from PSE</td>
<td>Failed</td>
<td>The library failed to verify the keytab located in the SAPSNCSKERB.pse file.</td>
</tr>
<tr>
<td>Kerberos ticket verification not successfully because no global keyTab</td>
<td>Failed</td>
<td>The library failed to verify a global keytab and a file-based keytab (in SAPSNCSKERB.pse) because none of these keytabs is available.</td>
</tr>
</tbody>
</table>

### 4.5.3.1.5 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.

**Note**

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

### 4.5.3.2 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*.

Note
Make sure the password is as complex as possible.

4.5.4 X.509 and Kerberos Authentication

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

4.5.4.1 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
4.5.4.2 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 or Secure Login Library is installed on SAP NetWeaver AS for ABAP systems ONE and TWO. This makes an SNC communication with X.509 certificates possible.

**Note**

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

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

<table>
<thead>
<tr>
<th>Systems</th>
<th>Software Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows client</td>
<td>Secure Login Client</td>
</tr>
<tr>
<td>SAP NetWeaver AS for ABAP system ONE</td>
<td>Secure Login Library or SAP Cryptographic Library (SNC library)</td>
</tr>
<tr>
<td>SAP NetWeaver AS for ABAP system TWO</td>
<td>Secure Login Library, SAP Cryptographic Library or SAPCRYPTOLIB (SNC library)</td>
</tr>
</tbody>
</table>

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 SAP NetWeaver AS for 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 SAP NetWeaver AS for ABAP. Specify a Service Principal Name for this user. (See options 1 and 2).

2. Use Edit Profiles (transaction RZ10 on SAP NetWeaver AS for ABAP systems (ONE and TWO) to configure the SNC parameters in the instance profile.

3. On SAP NetWeaver AS for ABAP system ONE, use the service account of the Microsoft Active Directory, create a Kerberos keytab file in the Secure Login Library as described in SNC Kerberos Configuration [page 101].

4. On SAP NetWeaver AS for ABAP system ONE, generate X.509 certificates in the Trust Manager (transaction STRUST).
   - Option 1
     a. Create an X.509 certificate for SAP NetWeaver AS for ABAP.

     Example

     \[\text{CN=SAPServiceABC, OU=SAP Security, C=DE}\]

     b. Start Edit Profiles (transaction RZ10).
c. Choose an instance 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 SAP NetWeaver AS for 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 SAP NetWeaver AS for ABAP system TWO, generate X.509 certificate in Trust Manager (transaction **STRUST**).

   If you use self-signed certificates, import them from SAP NetWeaver AS for ABAP system ONE.

6. Restart SAP NetWeaver AS for ABAP systems ONE and TWO.

7. Configure SNC user mapping in User Maintenance (transaction **SU01**) on SAP NetWeaver AS for ABAP system ONE.

8. Depending on the communication direction, configure secure network communication (SNC) in Configuration of RFC Connections (transaction **SM59**) on SAP NetWeaver AS for ABAP systems ONE and TWO.

**Related Information**

Secure Login Library Installation [page 84]


http://help.sap.com/saphelp_nw73ehp1/helpdata/en/4c/5db17f85640f1e1000000a42189c1/frameset.htm

http://help.sap.com/saphelp_nw73ehp1/helpdata/en/7e/6ca46b1ee4468a98280ff00db4d97d1/frameset.htm

**4.5.5 Kerberos Authentication for HTML-Based User Interfaces Using SAP NetWeaver AS for 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 SAP NetWeaver AS for 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 17]

4.5.5.1 System Landscape for Kerberos Authentication on SAP NetWeaver AS for 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 SAP NetWeaver AS for ABAP.

Component Required for SPNego on SAP NetWeaver AS for ABAP

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web client</td>
<td>The web client requests a service or a resource from SAP NetWeaver AS for 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 SAP NetWeaver AS for ABAP. The web client of the user must support SPNego.</td>
</tr>
<tr>
<td>Kerberos Key Distribution Center (KDC)</td>
<td>SAP NetWeaver AS for 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 SAP NetWeaver AS for ABAP.</td>
</tr>
</tbody>
</table>
### 4.5.5.2 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 or instance 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>spnego/enable</td>
<td>Set to 1.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Setting</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>spnego/krbsnego_lib</code></td>
<td>Set to the path to the Kerberos library (SAP Cryptographic Library or Secure Login Library of SAP Single Sign-On 2.0 or higher).</td>
</tr>
<tr>
<td>Note</td>
<td>For Secure Login Library, use the path to the respective file of SAP Single Sign-On:</td>
</tr>
</tbody>
</table>

### Kerberos Library File Names

<table>
<thead>
<tr>
<th>File Name</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>spnego/construct_SNC_name</code></td>
<td>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 111. For more information, see SAP Note 1819808 - SPNego: Collective Corrections.</td>
</tr>
<tr>
<td>Note</td>
<td>Changing this dynamic profile parameter does not require a restart.</td>
</tr>
</tbody>
</table>

7. Save and activate your entries.
8. Restart SAP NetWeaver AS for 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.
4.5.5.3 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 SAP NetWeaver AS for 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 116]
- Define Service Principal Name [page 102]

### 4.5.5.3.1 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 SAP NetWeaver Application Server for 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**

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.

4.5.5.3.2 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 SAP NetWeaver AS for 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.

4.5.5.4 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.

  **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 117]
SNC Parameters for the SAP Cryptographic Library [page 303]
Profile Parameters for SPNego [page 306]

### 4.5.5.5 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

### 4.5.6 SNC Communication Protocol Parameters

In the file `gss.xml`, you can configure the SNC communication protocol for server-to-server and client-to-server communication.

You can, for example, configure formats for the Distinguished Name. You can shorten long and complicated names, integrate elements such as e-mail addresses, define the communication protocols to use, configure algorithms for the protection of application data, keys, and algorithms for encryption and digital signatures.

**Example (section of `gss.xml`)**

Include one value in the parameters. List several values in a list separated by blanks. Use the following syntax:

```xml
<namecharset>latin1</namecharset>
```
4.5.6.1 Configuring Certificate Lifetime in sigsession and ParallelSessions Mode

Every time you use a token (smart card or soft token) to authenticate, you enter a PIN. If you do not want to be forced to enter this PIN every time you open a session, you have the following options:

- In sigsession mode, the client creates a temporary key, which has a period of validity specified in age and ttl. (age is the server system time offset relative to the client system time.) During this period, the session remains valid. ttl is the validity of the certificate in seconds. It is the time the key cache remains valid. The default is 180 s starting 60 s earlier.
- In ParallelSessions mode, the parameter ParallelSessionsTTL specifies the validity period of the temporary key. This period of time is identical with the maximum session length.

Whenever you reauthenticate, the temporary key and the associated session length are reused for a new session.

4.5.6.1.1 Configuring sigsession Mode

Context

If you use the 1993 protocol on the client and server, you must choose from the following authentication modes:

- enc: encryption certificate
- sig: signature certificates and sign a temporary RSA key with it
- sigsession: signature certificate and sign a temporary RSA key with it. This temporary key is cached for further sessions until you close the last session.

Example
If you use a token (smart card or soft token) to authenticate, you enter a PIN. In sigsession mode, the client creates a temporary key, which gets a period of validity specified in `age` and `ttl`. `age` is the server system time offset relative to the client system time. During this period, the session remains valid. `ttl` is the validity of the certificate in seconds. The default is 180 s starting 60 s earlier.

**Note**

If the value in `ttl` in the client exceeds the server value of `acceptedttl`, the SNC connection produces an error message.

Use the following syntax for the configuration:

**Configuration example**

**Client configuration of gss.xml:**

```xml
<protocol_1993>
  <authop>sigsession</authop>
  <age>300</age>
  <ttl>1899</ttl>
</protocol_1993>
```

**Server configuration of gss.xml:**

```xml
<protocol_1993>
  <acceptsigmode>true</acceptsigmode>
  <acceptedttl>2000</acceptedttl>
</protocol_1993>
```

To specify the lifetime of a certificate in sigsession, proceed as follows:

**Procedure**

1. Set a value for the system time tolerance in the parameter `age` in the gss.xml file of the client, for example, 300.
2. Set a value in parameter `ttl` in the same file, for example, 3900.
3. Save the file.
4. Set the same value for `acceptedttl` as in `ttl` (3900) in the gss.xml file of the server.
5. Save the file.
6. Restart the server.

To calculate the desired lifetime of the certificate, subtract the period specified in `age` from the period specified in `ttl`. This results in a desired lifetime of 3600 s.

Example

\[3900 \text{ s} - 300 \text{ s} = 3600 \text{ s}\]

To illustrate the behavior of the client and server parameters in the gss.xml files, see the following figure.
Ensure that the configuration of acceptedttl (server gss.xml) and ttl (client gss.xml) are identical.

The vertical dotted lines indicate the time when the certificate is issued or when it is verified. If you verify the validity of the certificate within the period specified by ttl, the verification is successful. Outside the period specified in the ttl parameter, the verification fails.

4.5.6.1.2 Configuring ParallelSessions Mode

Context

Use parallel session mode for the 2010 protocol.

Example

If you use a token (smart card or soft token) to authenticate, you must enter a PIN. In parallel session mode, the client creates a temporary RSA key, which is cached for re-authentication in further sessions until you close the last session.
Procedure

1. Enter `true` in `ParallelSessions`.
2. Enter a period of time (in seconds) in `ParallelSessionsTTL` to specify the period of time during which reauthentication can occur.
3. Restart the server.

If the value in `ParallelSessionsTTL` in the client exceeds the server value of `acceptedttl`, the SNC connection produces an error message.

Configuration example

Client configuration of gss.xml:

```
<protocol_2010>
  <ParallelSessions>true</ParallelSessions>
  <ParallelSessionsTTL>1800</ParallelSessionsTTL>
</protocol_2010>
```

Server configuration of gss.xml:

```
<protocol_2010>
  <acceptedttl>2000</acceptedttl>
</protocol_2010>
```

4.5.7 Use Case for Defining a Symmetric Algorithm

This section explains how to define the symmetric algorithm, which is used to secure communication.

By default, the SAP Cryptographic Library and the Secure Login Library provides the following symmetric algorithm (priority in this order).

- AES256
- AES192 ("old" protocol 1993 only)
- AES128
- 3DES ("old" protocol 1993 only)
- RC4 ("new" protocol 2010 only)

The SAP Cryptographic Library and the Secure Login Library have implemented two protocols named `protocol_1993` ("old") and `protocol_2010` ("new"). The "old" protocol is compatible with the SAP Cryptographic Library (CommonCryptoLib). The "new" protocol supports X.509 certificates and Kerberos tokens in parallel.

If SAP GUI establishes a secure communication to the SAP NetWeaver Application Server, the symmetric algorithm is agreed between both partners. It is possible to force the use of, for example, the AES256 symmetric algorithm. You can define this configuration file `gss.xml`. 
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;algs_encr&gt;XXX&lt;/algs_encr&gt;</code></td>
<td>Use this parameter to define the symmetric algorithm for the “old” protocol, which is defined in section <code>&lt;protocol_1993&gt;</code>. This protocol is compatible with the SAP Cryptographic Library (CommonCryptoLib). By default, the strongest symmetric algorithm that is available on both sides is agreed. It is possible to allow the acceptance of only aes256, for example. You can define the following algorithms: <strong>aes256</strong>  <strong>aes192</strong>  <strong>aes128</strong>  <strong>des3</strong>  Default is <code>&lt;empty&gt;</code>. The symmetric algorithm is arranged during the authentication process.</td>
</tr>
</tbody>
</table>

| `<ciphers>XXX</ciphers>` | Use this parameter to define the symmetric algorithm for the “new” protocol, which is defined in section `<protocol_2010>`. This protocol supports the Kerberos solution. By default, the strongest symmetric algorithm that is available on both sides is agreed. It is possible to allow only the acceptance of only AES256, for example. You can define the following algorithms: **AES256**  **AES128**  **RC4**  Default is `<empty>`. The symmetric algorithm is arranged during the authentication process. |

**Section of gss.xml**

```xml
<gss>
  <server>
    <protocol_1993>
      <algs_encr>xxx</algs_encr>
    </protocol_1993>
    <protocol_2010>
      <ciphers>xxx</ciphers>
    </protocol_2010>
  </server>
</gss>
```
4.5.8 User SNC Name Mapping

The following section describes how you configure the user SNC name in the SAP Cryptographic Library or in the Secure Login Library.

4.5.8.1 Uppercase Distinguished Name

To support case insensitivity for user certificate names used by SNC, the GSS Distinguished Names presented to SAP SNC may be converted to uppercase.

This can be defined in the configuration file gss.xml for the SAP Cryptographic Library or for the Secure Login Library.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;UpperCaseClientName&gt;XXX &lt;/UpperCaseClientName&gt;</td>
<td>Define the configuration in parameter &lt;UpperCaseClientName&gt;.</td>
</tr>
<tr>
<td>true</td>
<td>The distinguished name is provided in uppercase.</td>
</tr>
<tr>
<td>false</td>
<td>The distinguished name is provided in mixed case.</td>
</tr>
<tr>
<td>Default is false.</td>
<td></td>
</tr>
</tbody>
</table>

Section of gss.xml

```xml
<server>
  <UpperCaseClientName>xxx</UpperCaseClientName>
</server>
```

4.5.8.2 Alternative Name DN Feature

It is possible to use the Subject Alternative Name from the user certificate that is presented to the SAP SNC interface.

You can define this in the configuration file gss.xml for the SAP Cryptographic Library or for the Secure Login Library.
Section of gss.xml

```xml
<gss>
  <server>
    <ClientNameSource>xxx</ClientNameSource>
  </server>
</gss>
```

You can enter several values separated by commas or spaces. The system uses the first value. If this is not possible, it proceeds to the second value etc. An error occurs when no value can be used.

**Example 1**

The SAP Cryptographic Library or the Secure Login Library uses the URI. If the URI is not available, it uses the subject (Distinguished Name).

```xml
<ClientNameSource>AltNameURI Subject</ClientNameSource>
```

**Example 2**

The SAP Cryptographic Library or the Secure Login Library uses the E-mail address and, as first alternative, the Microsoft User Principal Name. If the second alternative value is not available, an error occurs.

```xml
<ClientNameSource>AltNameEMAIL AltNameUPN</ClientNameSource>
```

⚠️ **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.

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:

```plaintext
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.
4.5.8.3 Default User Schema Settings

The default user schema of the Secure Login Library is RFC2256. The configuration is located in the file gss.xml.

**Note**

Customers who run Secure Login Library 2.0 SP0 or SP1 and want to use patch 1 of Secure Login Library 2.0 SP1 or higher might be forced to edit the name schema in Secure Login Library 2.0 SP1 Patch 1 and enter their own name schema they used in the original release. For more information, see SAP Note 1864123 and related links.

By default, the configuration of the user schema in the file gss.xml is empty (meaning RFC2256). If you prefer, you can also enter **RFC2256** for clarity.

**Example**

```xml
<gss>
  <nameencoding>UTF8</nameencoding>
  <nameschema>rfc2256</nameschema>
  <!-'secude'/'sapcryptolib' of 'rfc2256' (default) specifies the schema for order and keywords of name components -->
</gss>
```

**Related Information**

- SNC Communication Protocol Parameters [page 119]
- Communication and Protocol Parameters (Server and Client) [page 298]

4.5.8.3.1 SNC Name Compatibility with a SECUDE SAPCRYPTOLIB Release

User schemas for SNC names

The SNC names for a certificate-based logon consist of user schema attributes for example, CN (common name), O (organization), OU (organizationalUnit), or C (country). These attributes comply with the RFC2256 default for user schemas. For more information, see the **Summary of the X.500(96) User Schema for Use with LDAPv3**.
Previous releases of SAPCRYPTOLIB and old SECUDE releases still use a user schema with obsolete attributes. The table below shows RFC2256-compliant attributes and the corresponding obsolete SAPCRYPTOLIB or SECUDE attributes, and the related keywords.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>RFC2256-Compliant Attribute (Default)</th>
<th>Obsolete SAPCRYPTOLIB or SECUDE Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>surname</td>
<td>SN</td>
<td>S</td>
</tr>
<tr>
<td>street</td>
<td>STREET</td>
<td>ST</td>
</tr>
<tr>
<td>title</td>
<td>TITLE</td>
<td>T</td>
</tr>
<tr>
<td>serialNumber</td>
<td>SERIALNUMBER</td>
<td>SN</td>
</tr>
<tr>
<td>businessCategory</td>
<td>BUSINESSCATEGORY</td>
<td>BC</td>
</tr>
<tr>
<td>description</td>
<td>DESCRIPTION</td>
<td>D</td>
</tr>
<tr>
<td>stateOrProvinceName</td>
<td>ST</td>
<td>SP</td>
</tr>
</tbody>
</table>

### 4.5.8.3.2 Setting for SAPCRYPTOLIB or SECUDE Release

If customers want to keep their old user schema attributes, overwrite the user schema setting. To switch the Secure Login Library to use the attributes for obsolete SAPCRYPTOLIB or SECUDE releases, open the `gss.xml` file and enter the schema `sapcryptolib` or `secude`.

**Example**

```xml
<gss>
  <nameencoding>UTF8</nameencoding>
  <nameschema>sapcryptolib</nameschema> <!--'secude'/'sapcryptolib' of 'rfc2256' (default) specifies the schema for order and keywords of name components -->
</gss>
```

**Example**

```xml
<gss>
  <nameencoding>UTF8</nameencoding>
  <nameschema>secude</nameschema> <!--'secude'/'sapcryptolib' of 'rfc2256' (default) specifies the schema for order and keywords of name components -->
</gss>
```
4.5.8.4  Shorten Long Distinguished Names

It is possible to shorten parts of the distinguished name (SNC Name) from the user certificates that are presented to the SAP SNC interface. The character limit for SAP server systems is 255 characters (in older systems 80 characters).

For example, you can remove entire parts such as a company name which are identical for all users. You can define this in the Secure Login Library configuration file gss.xml.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;searchstr&gt;XXX&lt;/searchstr&gt;</td>
<td>In the &lt;nameconversions&gt; section, use the &lt;searchstr&gt; parameter to define the part of the distinguished name to be shortened.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong></td>
</tr>
<tr>
<td></td>
<td>OU=Very Long Organization Unit Name</td>
</tr>
<tr>
<td>&lt;replstr&gt;XXX&lt;/replstr&gt;</td>
<td>In the &lt;nameconversions&gt; section, the &lt;replstr&gt; parameter is used to define the part of the distinguished name to be replaced.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong></td>
</tr>
<tr>
<td></td>
<td>OU=Short Name</td>
</tr>
</tbody>
</table>

The following source code represents a section of the code of the gss.xml file:

```xml
<gss>
  <nameconversions>
    <searchstr>VeryLongNameComponent</searchstr>
    <replstr>ShorterNameComponent</replstr>
  </nameconversions>
  <nameconversions>
    <searchstr>AnotherVeryLongNameComponent</searchstr>
    <replstr>AnotherShorterNameComponent</replstr>
  </nameconversions>
</gss>
```

4.5.9  Using Certificate Revocation Lists

The SAP Cryptographic Library or the Secure Login Library supports certificate revocation lists, which enable you to revoke certificates that have been declared invalid.

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 or the Secure Login Library provides a tool that enables you to regularly download new CRLs from CRL distribution points (LDAP.
or HTTP) 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 or the LibrarySecure Login Library must download CRLs from an external CRL distribution point.

**Note**

Include the component NWSSO for CommonCryptoLib 2.0 in the installation. It enables you to use the full scope of the CRL tool in conjunction with the SAP Cryptographic Library. For more information, see the related link.

To use the CRL functions, make the appropriate settings in the configuration files. For more information, see related link.

The local cache for the CRLs is \SECUDIR\dbcrl.

**Limitations**

The SAP Cryptographic Library or the Secure Login Library covers only basic functions on the server side, such as checking client certificates with CRLs, getting CRLs from a distribution point, and storing it in a local cache. The SAP Cryptographic Library or the Secure Login Library has the following limitations:

- Customers cannot use the extension IssuingDistributionPoint in CRLs.
- No use of delta CRLs
- At present the SAP Cryptographic Library or the Secure Login 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 (liboldap.*).
- The Secure Login Client does not check CRLs.

**Related Information**

- **Configuring the CRL Tool** [page 132]
- **Configurable Features of SAP Cryptographic Library** [page 81]

### 4.5.9.1 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.
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 `crl -H`. For more information, see the related link.

### Related Information

CRL Tool Commands [page 295]

### 4.5.9.2 Getting a CRL from a CRL Distribution Point

This topic contains a variety of 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:
  ```
crl get -u <LDAP_server> -f <CRL_file>
  
  Example
  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:
  ```
crl get -u <LDAP_server> store
  
  Example
  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).
  ```
crl get -u <LDAP_server> store -u <LDAP_server>
  
  Example
  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).
crl get –u <HTTP_server> store -u <LDAP_server>
Example
  crl get –u http://server/ store -u ldap:///sap.example.com

Related Information

CRL Tool Commands [page 295]

4.5.9.3 Configuring the CRL Tool

This topic describes the CRL configuration files.

The following configuration files are available in the \SLL folder:

- pkix.xml
- base.xml
- ldap.xml

The parameters are similar to tags surrounding the values. You may use uppercase or lowercase for entering values.

4.5.9.3.1 pkix.xml

In the configuration file pkix.xml, you can configure whether a CRL check is used at all.

CRL checking is active if the parameter revCheck is set to the value CRL. The default setting of this parameter is no (no use of CRLs).

i Note

After you have entered changes in the configuration files, restart your ABAP server so that the newly-set parameters take effect.

Example

```
<pkix>
  <profile>
    <acceptNoBCwithKeyUsage>true</acceptNoBCwithKeyUsage>
    <revCheck>CRL</revCheck>
    <certificatePolicies>noCheck</certificatePolicies>
  </profile>
</pkix>
```

The following table contains all parameters and parameter options that are available in pkix.xml.
4.5.9.3.2 base.xml

You can configure the cache and the verification of the CRL download in the file base.xml.

If you use CRLs that are located in the cache, performance will improve considerably.

By default, the parameter verificationonlineaccess is set to false to disable the function that verifies the CRLs online, for example on an LDAP server or HTTP server.

If you want to activate CRL verification with the cache, set the parameter usepkicache to true (default setting is false).

Example

If you want to define a different location for the cache directory, you may optionally use the parameter pkicachedir and enter the location there (for multiple servers accessing the cache, you could use an NFS cache).

```xml
<base>
  <verificationonlineaccess>false</verificationonlineaccess>
  <usepkicache>true</usepkicache>
  <pkicachedir>\usr\sap\T2D\DVEBMGS00\sec</pkicachedir>
</base>
```

Example

```xml
<base>
  <verificationonlineaccess>true</verificationonlineaccess>
  <usepkicache>false</usepkicache>
  <pkicachedir></pkicachedir>
</base>
```

Example

If you want to carry out a CRL check from a remote LDAP directory, set the parameter verificationonlineaccess to true and set the parameter usepkicache to false. In this case, you need not enter any value in pkicachedir.

```xml
<base>
  <verificationonlineaccess>true</verificationonlineaccess>
  <usepkicache>false</usepkicache>
  <pkicachedir></pkicachedir>
</base>
```
Example

If you want to make a CRL request from a proxy server, you must enter the host name and the port number of the proxy server.

```xml
<base>
  <proxy>
    <url>host.example.com:8003</url>
  </proxy>
</base>
```

The following table contains all parameters and parameter options that are available in `base.xml`.

Related Information

Configuration Parameters of `base.xml` [page 296]

4.5.9.3.3  ldap.xml

This configuration file is only relevant if you have an Active Directory environment.

You only need to modify this file in an Active Directory environment. If an LDAP URL that does not contain the server name is used as a CRL distribution point (in the default setting, the relevant section is commented out), define the name of the LDAP server in the configuration file `ldap.xml`.

If you are in a Microsoft Windows domain and Active Directory is used as LDAP server, you must enter the value `ADS` in the parameter name.

```xml
<ldap>
  <server>
    <name>ADS</name>
  </server>
</ldap>
```

The following table contains all parameters and parameter options that are available in `ldap.xml`.

Related Information

Configuration Parameters of `ldap.xml` [page 297]
4.5.10 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 212]

4.6 Configuration Options

This section describes useful configuration and troubleshooting issues of the SAP Cryptographic Library or of the Secure Login Library.

4.6.1 Configuring Tracing for the Cryptographic Library

In the case of an error, you can activate tracing for the SAP Cryptographic Library, the Secure Login Library, or any other cryptographic library you are using.

Context

The `sectrace.ini` configuration file defines the location of the trace directory.
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 SLL installation directory (for Secure Login Library) 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
```

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, for example, for the Secure Login Library, proceed as follows:

**Procedure**

1. Go to the directory where the Secure Login Library is located.

   `$ (DIR_INSTANCE) \SLL`

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:
   - The trace directory is % .BINDIR.% /../SLLTrace.
   - 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 Sever ABAP.

Related Information

Tracing Secure Login Client [page 62]
5 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.

5.1 Installation and Installation File Names

This chapter describes how to install Secure Login Server for different support packages of SAP Single Sign-On 2.0.

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.

<table>
<thead>
<tr>
<th>File Name for Installing Secure Login Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version and Support Package</strong></td>
</tr>
<tr>
<td>Secure Login Server 2.0 SP00</td>
</tr>
<tr>
<td>Secure Login Server 2.0 SP03</td>
</tr>
</tbody>
</table>

The installation files have the following format:

SLSERVER<support_package_number_<patch_level>-<ID>.sca

**Example**

SLSERVER03_0-10012314.sca

The ID attached to the file name is a temporary download ID.

Secure Login Server 2.0 SPx is integrated in SAP Solution Manager. You can update Secure Login Server 2.0 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

http://service.sap.com/sap/support/notes/1946068

5.1.1 Prerequisites for Installing SecureLoginServer

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 Secure Login Library installation is optional and required for SAP user authentication only. The Secure Login Library will be used to establish secure communication to SAP NetWeaver Application Server for 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 related link.

Related Information

http://support.sap.com/pam
Authentication Servers Supported by Secure Login Server [page 139]
https://service.sap.com/%7Esapidb/011000358700000178192012E

5.1.2 Authentication Servers Supported by Secure Login Server

The Secure Login Server supports the following authentication servers:

Supported Authentication Servers

<table>
<thead>
<tr>
<th>Supported by Secure Login Server</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP server system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• openLDAP</td>
</tr>
<tr>
<td></td>
<td>• Oracle Directory Server Enterprise Edition</td>
</tr>
<tr>
<td></td>
<td>For more information, see the related link.</td>
</tr>
<tr>
<td></td>
<td>Check the Product Availability Matrix for the most current releases.</td>
</tr>
</tbody>
</table>
Supported by Secure Login Server | Details
---|---
SAP server system | SAP NetWeaver Application Server for ABAP 6.20 or higher version
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 63]

5.1.3 Installing Secure Login Library (Optional)

The Secure Login Library installation is optional. The Secure Login Library can be used as an alternative cryptographic library for user authentication and RFC connections at an SAP NetWeaver Application Server for ABAP.

**Note**
The default cryptographic library for the SAP NetWeaver Application Server is the SAP Cryptographic Library. For more information, see SAP Note [1848999](#).

You can use the Secure Login Library to establish secure communication to an AS ABAP and to verify SAP credentials.

**Note**
Keep in mind that there are different Secure Login Library software packages available depending on the desired operating system. This document describes the installation for Microsoft Windows and Linux operating systems.
5.1.3.1 Installing Secure Login Library for Microsoft Windows Operating Systems

Procedure

1. Copy library files.
   
   Copy the Secure Login Library software for Microsoft Windows to the target SAP NetWeaver Application Server and extract the file SECURELOGINLIB.SAR with the SAPCAR command line tool to a separate folder, which is a subfolder of exe.
   
   `sapcar -xvf <source_path>\SECURELOGINLIB.SAR -R <DIR_INSTANCE>\exe\SLL`

   **Example**
   
   `sapcar -xvf D:\InstallSLS\SECURELOGINLIB.SAR -R D:\usr\sap\ABC\J00\exe\SLL`

2. Set the environment variable `<SECUDIR>`.
   
   Set the system environment variable `<SECUDIR>` to the following directory:
   
   `SECUDIR=<DIR_INSTANCE>\sec`

   **Example**
   
   `SECUDIR=D:\usr\sap\ABC\J00\sec`

3. Verify Secure Login Library.
   
   To verify the Secure Login Library, use the `sapgenpse` command:
   
   `<DIR_INSTANCE>\exe\SLL\sapgenpse.exe`

   **Example**
   
   `D:\usr\sap\ABC\J00\exe\SLL\sapgenpse.exe`

   As a result, you get further information about the Secure Login Library. The test is successful if the version is displayed.
5.1.3.2 Installing Secure Login Library for Linux Operating Systems

Procedure

1. Copy library files

Copy the Secure Login Library software for Linux to the target SAP NetWeaver Application Server and extract the file `SECURELOGINLIB.SAR` with the `SAPCAR` command line tool to the following folder.

```
sapcar -xvf <source_path>/SECURELOGINLIB.SAR -R <ASJava_installation>/exe/SLL
```

Example

```
sapcar -xvf /InstallSLS/SECURELOGINLIB.SAR -R /usr/sap/ABC/J00/exe/SLL
```

2. Define file attributes

To use shared libraries in a shell, it is necessary to set the file permission attributes with the following command:

```
chmod +rx <DIR_INSTANCE>/exe/SLL/sapgenpse lib*
```

Example

```
chmod +rx /usr/sap/ABC/J00/exe/SLL/sapgenpse lib*
```

3. Define the file owner.

Grant access rights to the user account that is used to start the SAP application (for example, `<SID>adm>`).

Change to the folder `<DIR_INSTANCE>/exe/SLL` and use the following command:

```
chown [OWNER]:[GROUP] *
```

Example

```
chown abcadm:sapsys *
```

4. Verify Secure Login Library.

To verify the Secure Login Library use the `sapgenpse` command (with user `<SID>adm>`):

```
<DIR_INSTANCE>/exe/SLL/sapgenpse
```

Example

```
/usr/sap/ABC/J00/exe/SLL/sapgenpse
```

As a result, further information about the Secure Login Library should be displayed. The test is successful if the version is displayed.
5.1.4 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/sitoolset
https://service.sap.com/sap/support/notes/1563579
https://service.sap.com/sap/support/notes/1707161
Installation and Installation File Names [page 138]
5.1.5 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 2.0 SP00:
   
   ```
   deploy <source>\SECURELOGINSERVER00_0.sca
   ```

   ✨ Example

   ```
   deploy D:\InstallSLS\SECURELOGINSERVER00_0.sca
   ```

   For Secure Login Server 2.0 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:
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

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy Secure Login Server</td>
<td><code>deploy SECURELOGINSERVER00&lt;sp_pl&gt;.sca</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;sp_pl&gt;</code> stands for the support package number with two digits and the patch level number with one digit.</td>
</tr>
<tr>
<td>Undeploy Secure Login Server</td>
<td><code>undeploy name=securelogin.ui vendor=sap.com</code></td>
</tr>
<tr>
<td></td>
<td><code>undeploy name=securelogin.ui.alias vendor=sap.com</code></td>
</tr>
<tr>
<td></td>
<td><code>undeploy name=securelogin.umep vendor=sap.com</code></td>
</tr>
<tr>
<td></td>
<td><code>undeploy name=SecureLoginServer vendor=sap.com</code></td>
</tr>
<tr>
<td></td>
<td>`list_app</td>
</tr>
</tbody>
</table>

**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 144]
- Secure Login Server Uninstallation [page 146]
5.1.6 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.
5.2 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).

5.2.1 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
5.2.2 Initial Configuration

This section describes the modes that are possible for the initial configuration wizard.

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 212]
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
   
   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 258]

5.2.2.2 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 258]
Importing Certificate Entries from a File [page 151]
Parameters for Certificate Configuration [page 285]

5.2.2.3 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.

Context

If you want to use the automatic initial configuration of Secure Login Server during the migration of Secure Login Server 2.0 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 147]

**5.2.2.4 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*.
5.3 Administration

This topic contains administration tasks such as starting Secure Login Administration Console, password management, and stopping and starting Secure Login Server.

5.3.1 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.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
</table>
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 of SAP Single Sign-On 2.0.

   https://<host_name>:<port>/webdynpro/resources/sap.com/securelogin.ui/Main

   Shortcut:

   https://<host>:<port>/slac

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
</table>
   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.
5.3.2 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.

5.3.3 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
   ```

   ```
   start_app sap.com/securelogin.ui
   ```

5.3.4 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:
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*

   This displays the AS Java components of Secure Login Server.
4. Choose *Action* *Stop* or *Action* *Start* for stopping and starting.

5.4 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 155]
Parameters for Secure Login Web Client Configuration [page 274]
http://support.sap.com/pam

5.4.1 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
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.

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

Example:

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

**Related Information**

- [Connection with Redirect to URL](#)
- [Direct SAP GUI Connection with Secure Login Web Client](#)
- [Load-Balanced SAP GUI Connection with Secure Login Web Client (Using the Message Server)](#)
- [Launch SAP Logon Pad](#)

### 5.4.1.1 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**

<table>
<thead>
<tr>
<th>Action</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Redirect to URL</td>
<td>Enter the URL to which the Secure Login Web Client is redirected after successful authentication, for example, to an enterprise portal.</td>
</tr>
</tbody>
</table>
5.4.1.2 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

<table>
<thead>
<tr>
<th>Actions</th>
<th>Parameters</th>
<th>Connection String</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log On to ABAP System</strong></td>
<td>• IP Address/Host Name</td>
<td>/H/&lt;host&gt;</td>
</tr>
<tr>
<td></td>
<td>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 /H/&lt;host&gt;.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Port</td>
<td>/S/&lt;port&gt;</td>
</tr>
<tr>
<td></td>
<td>Port of ABAP server: Default is 3200. SAP GUI starts with the connection string /S/&lt;port&gt;.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SNC Name</td>
<td>SNC_PARTNERNAME=&lt;SNC_name&gt;</td>
</tr>
<tr>
<td></td>
<td>SNC name of ABAP server. SAP GUI starts with SNC_PARTNERNAME</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>p:CN=ABAP System</td>
<td></td>
</tr>
<tr>
<td><strong>Redirect to URL and Log On to ABAP System</strong></td>
<td>* Redirect to URL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter the URL to which the Secure Login Web Client is redirected after successful authentication, for example, to an enterprise portal.</td>
<td></td>
</tr>
</tbody>
</table>

Optional Parameters
### 5.4.1.3 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

<table>
<thead>
<tr>
<th>Actions</th>
<th>Parameters</th>
<th>Connection String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log On to ABAP Message Server</td>
<td>* Message Server</td>
<td>/\M/&lt;host&gt;</td>
</tr>
<tr>
<td></td>
<td>IP address or fully qualified host name of the ABAP Message Server. SAP GUI starts with an \M/host connection string.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Message Server Service</td>
<td>/\S/&lt;port&gt;</td>
</tr>
<tr>
<td></td>
<td>IP address or fully qualified host name of the ABAP Message Server. SAP GUI starts with an \M/host connection string.</td>
<td></td>
</tr>
</tbody>
</table>

---

*SAP GUI Description*

Name of the server profile in SAP GUI for Microsoft Windows (*Description* 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 `<saplogon.ini>` file with the respective entry.
### Actions

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Connection String</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group</strong></td>
<td>/G/&lt;group&gt;</td>
</tr>
<tr>
<td></td>
<td>The ABAP group. SAP GUI starts with a /G/&lt;group&gt; connection string.</td>
</tr>
</tbody>
</table>

### Redirect to URL and Log On to ABAP Message Server

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Connection String</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Redirect to URL</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter the URL the Secure Login Web Client is redirected to after successful authentication, for example, to an enterprise portal.</td>
</tr>
</tbody>
</table>

### Optional Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Connection String</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SAP GUI Description</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Restriction</strong></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Name of the server profile in SAP GUI for Microsoft Windows (Description 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Gateway Host</strong></td>
<td>/H/&lt;host&gt;</td>
</tr>
<tr>
<td>Specifies the SAP router for the connection to the ABAP server. SAP GUI starts with an /H/&lt;host&gt; connection string.</td>
<td></td>
</tr>
<tr>
<td><strong>Gateway Port</strong></td>
<td>/S/&lt;port&gt;</td>
</tr>
<tr>
<td>Specifies the port of the SAP router. SAP GUI starts with an /S/&lt;port&gt; connection string.</td>
<td></td>
</tr>
</tbody>
</table>
5.4.1.4 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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch SAP Logon Pad</td>
<td></td>
</tr>
<tr>
<td>Redirect to URL and Launch SAP Logon Pad</td>
<td>* Redirect to URL</td>
</tr>
<tr>
<td></td>
<td>Enter the URL to which the Secure Login Web Client is redirected after successful authentication, for example, to an enterprise portal.</td>
</tr>
</tbody>
</table>

5.4.2 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 24]
5.4.2.1 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.

5.4.3 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\n
5.4.4 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 162]
SAP-Signed Secure Login Web Client JAR Package to Protect SNC Libraries [page 163]
PKI Check before Storing in a Client Certificate Store [page 164]
Removing Certificates of the Secure Login Web Client [page 165]

5.4.4.1 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.

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 163]
5.4.4.1.1 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 » System Security » System Security for AS Java Only » Using the AS Java Key Storage

5.4.4.2 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.

### 5.4.4.3 PKI Check before Storing in a Client Certificate Store

You must have established a trust relationship for the Secure Login Web Client.

#### Context

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>This section only refers to Microsoft Windows and Mac OS operating systems.</td>
</tr>
</tbody>
</table>

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.
5.4.4.4 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 session 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.

5.4.4.5 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

<table>
<thead>
<tr>
<th>JavaScript Function in <code>securelogin.js</code></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seclogin.isSLCLogoutAvailable()</code></td>
<td>This JavaScript function checks whether the sign-off feature is available. It is active in the default web client.</td>
</tr>
<tr>
<td><strong>JavaScript section: seclogin.doLogout()</strong></td>
<td>This JavaScript function is the implementation of sign-off. It is active in the default client with the Sign Off button.</td>
</tr>
<tr>
<td><code>seclogin.startBrowserMonitor()</code></td>
<td>(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.</td>
</tr>
</tbody>
</table>

#### 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)`.

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
<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'>
<!--[if !IE]>
<!-- 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");
</SCRIPT>
</HEAD>
</HTML>
```
`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() + '"></script>);
  $('#startSAP').hide();
  seclogin.initPages();
  seclogin.initContainer( "#AppletContainer");
});

</SCRIPT>
</HEAD>
<BODY class= "prtlBody urFontBaseFam urScrl">

<SPAN id= "UMELogon">

</DIV>
</DIV>
</TD>
</TR>

</TD colSpan= "3">
<!---- Authentication Table -->

<TABLE cellspacing= "3" cellPadding= "0" valign= "top" id= "PageAuth" style= "display: none">

</TBODY>

<TBODY>

</DIV>

</FORM id= "SNCForm1" method= "POST" name= "SNCForm1" AUTOCOMPLETE= "off"
action= "/SecureLogin/login">

<TABLE class= "urLogonTable" cellspacing= "3" cellPadding= "0" valign= "top">
5.4.5Mozilla Firefox Plug-In for Storing Secure Login User Certificates

Mozilla Firefox stores the certificate in the browser’s certificate store using the plug-in of Secure Login Web Client. 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.

5.4.5.1Install Firefox Extension

Firefox Extension for Secure Login Web Client

Prerequisites

You have installed Firefox Extension XPI. The Firefox Extension is provided by the Secure Login Server and can be downloaded using the following URL:

http://<host_name>:<port>/SecureLoginServer/webclient/firefox

Browser and operating system are recognized automatically.

Procedure

1. Install the Firefox extension.
If your Mozilla Firefox browser does not open an extension installation dialog, but only allows you to save this file, you have the following choices:

- Choose the option *Open with* and choose the Mozilla Firefox application.
- Save the file to your Desktop, then drag and drop it into any Firefox window.
- Ask your Web portal administrator to add a new MIME type `application/x-xpinstall` for XPI files.

2. Install the Firefox Extension by choosing *Install Now*.
3. Restart Mozilla Firefox.

### 5.4.5.2 Uninstall Mozilla Firefox Extension

This topic describes how you uninstall the Firefox extension for Secure Login Web Client.

**Procedure**

1. Start the Mozilla Firefox application.
2. Choose *Add-ons Manager* and *Extensions* from the menu.
3. To uninstall, select the Firefox Extension Secure Login Security Module and choose the **Remove** button.

### 5.4.6 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.

#### 5.4.6.1 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\servlet_jsp\SecureLoginServer\webclient\root
   ```
   **Example**
   ```
   D:\usr\sap\NJ4\J00\j2ee\cluster\apps\sap.com\SecureLoginServer\servlet_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.

5.4.7 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.

5.5 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

5.5.1 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 SAP NetWeaver AS for 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 283]

5.6 Certificate Lifecycle Management Using Secure Login Server

You want to automatically renew long-lived X.509 certificates, which are stored in the trust manager of SAP NetWeaver Application Server for 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 2194174.

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

SAP NetWeaver Application Server for 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

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

### 5.6.2 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.
- The user authentication in Secure Login Administration Console runs on a policy configuration using a certificate-based login module.
- You are using SAP NetWeaver 7.31 SP 17, 7.4 SP13 or 7.5 SP00 higher.

### 5.6.3 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 SAP NetWeaver Application Server for 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.

### 5.6.3.1 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.

### 5.6.3.1.1 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.
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, which appears in the metadata information.

11. Choose Finish to complete the configuration.

5.6.3.1.2 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 for the PSE types of the certificates 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.

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.

12. Choose Finish to complete the configuration.

**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 178]

### 5.6.3.1.3 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.
      
      **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.

### 5.6.4 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**.

   **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 2194174.

### 5.6.4.1 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*).

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>New Cert</em></td>
<td>The report renews the certificates.</td>
</tr>
<tr>
<td><em>New Key</em></td>
<td>The report renews the certificates and generates a new private key.</td>
</tr>
</tbody>
</table>

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 174]

**5.6.4.2 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 SAP NetWeaver AS for 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).
5.7  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.

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

5.7.1 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 285]
5.8 Configuration

In the following, you find information about how you can configure Secure Login Server.

5.8.1 Overview of Login Modules Supported by SAP Single Sign-On 2.0

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 2.0. 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 2.0

<table>
<thead>
<tr>
<th>Login Module</th>
<th>Login Module Name</th>
<th>Destination Configured in</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPNego login module</td>
<td>SPNegoLoginModule</td>
<td>(No destination required)</td>
</tr>
<tr>
<td>LDAP login module</td>
<td>SecureLoginModule20LDAP</td>
<td>Secure Login Administration Console</td>
</tr>
<tr>
<td>RADIUS login module</td>
<td>SecureLoginModule20RADIUS</td>
<td>Secure Login Administration Console</td>
</tr>
<tr>
<td>ABAP login module</td>
<td>SecureLoginModule20ABAP</td>
<td>SAP NetWeaver Administrator</td>
</tr>
<tr>
<td>SAP NetWeaver AS for Java User Management Engine (UME). For more information on basic authentica...</td>
<td>BasicPasswordLoginModule</td>
<td>(No destination required)</td>
</tr>
</tbody>
</table>
Login Module | Login Module Name | Destination Configured in
--- | --- | ---
One-Time Password Authentication login module. It can be configured to support single-factor authentication or two-factor-authentication. For more information on One-Time Password Authentication, see the related link. | TOTPLoginModule | (No destination required)

Related Information

Creating Destinations [page 189]
Managing Destinations [page 206]
One-Time Password Authentication

5.8.2 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.
4. To add a policy configuration for a login module stack (for example, for LDAP) for SAP Single Sign-On 2.0, 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.

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 2.0. 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 2.0 [page 184]
Parameters for the Policy Configuration [page 269]
5.8.3 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.
   
   \( https://<\text{host\_name}>:<\text{port}>/\text{webdynpro}/\text{resources}/\text{sap.com/securelogin.ui/Main} \)
   
   You can also use the following short command:
   
   \( https://<\text{host\_name}>:<\text{port}>/\text{slac} \)

   ![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

   ![Note](https://example.com:50001/webdynpro/resources/sap.com/securelogin.ui/Main)

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.
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.

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 185]
Initial Configuration [page 148]
Parameters for Client Configuration [page 269]
Configuring Secure Login Web Client Connections to SAP GUI [page 155]
Parameters for Secure Login Web Client Configuration [page 274]
Configuring Secure Communication [page 214]
5.8.4 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.
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, you must use the correct communication protocol. The enrollment URL for SAP Single Sign-On 2.0 has the following syntax:

```plaintext
<Server host:port>/SecureLoginServer/sl2/doLogin?profile=<profile uuid>
<Server host:port>/SecureLoginServer/sl1/doLogin?profile=<profile uuid>
```

sl2 stands for the protocol for SAP Single Sign-On 2.0 and sl1 for 1.0.

To configure the protocol in the enrollment URL, proceed as follows:

Procedure

1. Start the Secure Login Administration Console.

   ```plaintext
   https://<host_name>:<port>/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.
5.8.6 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.

   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 280]
5.8.7 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 (SAP NetWeaver AS for 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

**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 285]
- Parameters for Certificate Attribute Configuration [page 286]
- Parameters of User Mapping Destinations and Attributes [page 287]
- Parameters for User Logon ID Padding [page 288]

5.8.7.1 Certificate User Mapping in the Secure Login Server

This topic describes certificate user mapping.

**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 289]
(Optional) Configuring User Logon ID Padding in Secure Login Server [page 198]

5.8.7.2 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.
5.8.7.3 (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 201]

5.8.7.3.1 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 SAP NetWeaver AS for 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:
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 199]**

### 5.8.7.3.2 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.
   
   ```text
   https://<host_name>:<port>/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 289]

5.8.7.4 (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 SAP NetWeaver AS for 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.
5.8.7.5 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:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(AUTH:USERID)</td>
<td>User name only</td>
</tr>
<tr>
<td>(AUTH:UPN)</td>
<td>User principal name</td>
</tr>
<tr>
<td>(AUTH:DCS)</td>
<td>All domain components are displayed.</td>
</tr>
</tbody>
</table>

Prerequisites

- You use the SPNego login module in the Secure Login Server.
- You have a Microsoft Active Directory environment.

Procedure
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

<table>
<thead>
<tr>
<th>Values for Appendix Subject Name</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>If a user <a href="mailto:smith@example.com">smith@example.com</a> logs on, the following Distinguished Name is used:</td>
<td></td>
</tr>
<tr>
<td>(AUTH:USERID)</td>
<td>CN=smith</td>
</tr>
<tr>
<td>(AUTH:UPN)</td>
<td>CN=<a href="mailto:smith@example.com">smith@example.com</a></td>
</tr>
<tr>
<td>(AUTH:DCS)</td>
<td>CN=smith,DC=example,DC=com</td>
</tr>
</tbody>
</table>

### Example

<table>
<thead>
<tr>
<th>Variables with Output of Domain Components</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>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:</td>
<td></td>
</tr>
</tbody>
</table>
| Common Name with (AUTH:UPN) | CN=smith@sub1.example.com  
CN=smith@sub2.example.com |
| Common Name with (AUTH:USERID) | CN=smith,DC=sub1,DC=example,DC=com  
CN=smith,DC=sub2,DC=example,DC=com |
| Appendix Subject Name with (AUTH:DCS) | CN=smith,DC=sub1,DC=example,DC=com  
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.
<table>
<thead>
<tr>
<th>Values for Appendix Subject Name</th>
<th>Result</th>
</tr>
</thead>
</table>
| With different users called Smith in two subdomains (sub1.example.com and sub2.example.com) | 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.

**Note**

Use *Appendix Subject Name* to configure a Relative Distinguished Name.

### 5.8.7.6 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 286]

### 5.8.7.7 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.

**Note**

5.8.7.8 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 \textit{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, \texttt{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 \texttt{PADDEDNAME} in the \textit{Common Name} field of the certificate attribute configuration. However, you can fix the length of the Distinguished Name in the \textit{Padding Length} and \textit{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

<table>
<thead>
<tr>
<th>Action</th>
<th>Configuration</th>
<th>Result Variable(s)</th>
<th>Result Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>PolicyConfigurations-Name=&quot;&lt;client_authorization_profile&gt;&quot;</td>
<td>(AUTH:USERID)</td>
<td>denisesmith</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(AUTH:UPN)</td>
<td><a href="mailto:denisesmith@domain.org">denisesmith@domain.org</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(AUTH:DCS)</td>
<td>DC=domain, DC=org</td>
</tr>
<tr>
<td>LDAP User Name Mapping</td>
<td>userNameMappingLDAP-SearchAttributeName=&quot;sAMAccountName&quot;</td>
<td>(LDAP:userPrincipal)</td>
<td><a href="mailto:denisesmith@domain.org">denisesmith@domain.org</a></td>
</tr>
<tr>
<td>(optional)</td>
<td>userNameMappingLDAP-SearchAttribute-Value=&quot;(AUTH:USERID)&quot;</td>
<td>(LDAP:name)</td>
<td>Denise Smith</td>
</tr>
<tr>
<td></td>
<td>userNameMappingLDAPAttributes=&quot;userPrincipal,name.email&quot;</td>
<td>(LDAP:email)</td>
<td><a href="mailto:denisesmith@mail.domain.org">denisesmith@mail.domain.org</a></td>
</tr>
<tr>
<td>Action</td>
<td>Configuration</td>
<td>Result Variable(s)</td>
<td>Result Values</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>User Name Padding (optional)</td>
<td>Padding</td>
<td>(PADDEDNAME)</td>
<td>0denisesmith</td>
</tr>
<tr>
<td></td>
<td>For=&quot;(AUTH:USERID)&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Padding Character=&quot;0&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Padding Length=12</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maximum Length=14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate creation</td>
<td>Common Name=&quot;(PADDEDNAME)&quot;</td>
<td>&quot;0denisesmith&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Organizational Unit Name =&quot;BI ADM&quot;</td>
<td>&quot;BI ADM&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Organizational Name=&quot;&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Locality=&quot;&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Country Name=&quot;&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Appendix Subject Name=&quot;(AUTH:DCS)&quot;</td>
<td>&quot;DC=domain, DC=org&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Certificate Distinguished Name</td>
<td>&quot;CN=0denisesmith, OU=BI ADM, DC=domain, DC=org&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject Alternative Name (RFC822 Name)=&quot;(LDAP:email)&quot;</td>
<td>&quot;<a href="mailto:denisesmith@mail.domain.org">denisesmith@mail.domain.org</a>&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject Alternative Name (Principal Name)=&quot;(LDAP:userPrincipal)&quot;</td>
<td>&quot;<a href="mailto:denisesmith@domain.org">denisesmith@domain.org</a>&quot;</td>
<td></td>
</tr>
</tbody>
</table>

**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"
5.8.7.9 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.

<table>
<thead>
<tr>
<th>Parameter for Certificate Attribute Configuration</th>
<th>Value for Certificate Attribute Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name</td>
<td>(AUTH:UPN)</td>
</tr>
<tr>
<td>Country Name</td>
<td>DE</td>
</tr>
<tr>
<td>Organizational Name</td>
<td>ARAdev</td>
</tr>
<tr>
<td>Organizational Unit Name</td>
<td>BI ADM</td>
</tr>
</tbody>
</table>

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=ARAdev,C=DE

The test output displays the common name as it appears in the certificate.

5.8.8 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 289]
Creating Destinations [page 189]
LDAP User Mapping with Multiple Search Base DNs [page 207]

5.8.8.1 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 DNs 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

### 5.8.9 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).
5.8.9.1 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.
5.8.9.2 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

\[
\text{[timestamp]} \text{[profile_ID]} \text{[user_name]} \text{[client_ID\_<port>]} \text{[SAP\_NetWeaver\_instance\_number]}.\text{ext}
\]

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:

<table>
<thead>
<tr>
<th>File Name Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| timestamp         | Timestamp with year, month, day, hours, minutes, seconds, and milliseconds.  
|                   | Format: yyyymmdddhhmssmm |
| profile_ID        | Authentication profile ID |
| user_name         | User name of the user who authenticated or tried to authenticate. |
| 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:  
|                   |  
|                   | ● p10 Extension for PKCS#10 files for archived certificate requests.  
|                   | ● p7c Extension for PKCS#7 files for archived certificates. |
**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.

### 5.8.10 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` 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**

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.
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 258]

5.8.11 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

- 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), you have installed the Secure Login Library. 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 or to the Secure Login 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)

**Example**

For Secure Login Library
/usr/sap/<SID>/<instance_number>/SLL/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**

Secure Login Library Installation [page 84]
Parameters for Initial Configuration (PKI Certificates) [page 258]
5.8.12 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 187]
5.8.13 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.

- Security Check
  This section provides information whether SSL is configured correctly. If you choose this link, you access the SSL configuration in SAP NetWeaver Administrator.

- 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.
5.9 Configuration Examples

This section describes some configuration examples for Secure Login Server.

5.9.1 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.

5.9.2 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.

<table>
<thead>
<tr>
<th>Certificate Attribute</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>V3</td>
</tr>
<tr>
<td>Asymmetric Algorithm</td>
<td>RSA Algorithm</td>
</tr>
<tr>
<td>Key Usage</td>
<td>Digital Signature</td>
</tr>
<tr>
<td></td>
<td>Non-Repudiation</td>
</tr>
<tr>
<td></td>
<td>Key Encipherment</td>
</tr>
<tr>
<td></td>
<td>Data Encipherment</td>
</tr>
<tr>
<td></td>
<td>Certificate Signing</td>
</tr>
<tr>
<td></td>
<td>Off-line CRL Signing</td>
</tr>
<tr>
<td></td>
<td>CRL Signing</td>
</tr>
<tr>
<td>Basic Constraints</td>
<td>Subject Type=CA</td>
</tr>
<tr>
<td></td>
<td>Path Length Constraint=None</td>
</tr>
</tbody>
</table>

**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.
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.
5.9.3 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 or AS Java ➤ AS Java Cluster Architecture.

You can also ensure failover for the Secure Login Client by using Secure Login Server(s) with multiple enrollment URLs. For more information, see related link.

Related Information

Configuring Secure Login Servers as Failover Servers for High Availability [page 218]

5.9.3.1 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 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. If the first Secure Login Server is down, it goes to the next Secure Login Server that is specified in the list.
You can also use one Secure Login Server and add multiple enrollment URLs. The Secure Login Client or Secure Login Web Client goes through the enrollment URLs and checks which one it can use to authenticate.

Configuration

Procedure

1. Log on to the Secure Login Administration Console.
2. Choose the relevant client authentication management in Profile Management > Authentication Profile > Secure Login Client Settings.
3. Go to the Enrollment URL section.
4. Choose the Add button to add other enrollment URLs to a failover Secure Login Server.
5. Configure the enrollment URL for Secure Login Client. For more information, see related link.
6. Save your entries.

We recommend that you maintain this failover configuration in all Secure Login Servers you use. For more information about the parameter Enrollment URL, see related link.

Related Information

Setting the Enrollment URL for Secure Login Client [page 190]

5.9.3.2 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 2.0 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

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).

5.9.4 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 37].
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 37].
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 264]
Parameters for Client Configuration [page 269]
Downloading Policies from the Secure Login Server [page 36]

5.9.4.1 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 37].
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 264]
Parameters for Client Configuration [page 269]
Downloading Policies from the Secure Login Server [page 36]

5.9.4.2 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 220]

5.9.4.3 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.
5.9.5 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 37].
5. Go to User Profile Groups.
6. Choose the profile group that contains the relevant authentication profile.
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. 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.
5.9.5.1 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.
5.9.6 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.
- An SNC library is installed. For more information, see related link.

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.
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 37].
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.

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 Library [page 79]
Secure Login Client Installation [page 24]
Creating a Destination with an RFC Destination Type [page 227]

5.9.6.1 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.
5.9.7 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 277].
- 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 37].
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 24]) 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 37].
   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 269]
Parameters for Secure Login Web Client Configuration [page 274]

5.9.7.1 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.
5.9.8 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.

5.9.8.1 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.
5.9.8.2 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**

<table>
<thead>
<tr>
<th>Server</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Login Server 2.0 SP04 or higher on an SAP NetWeaver Application Server for Java</td>
<td></td>
</tr>
<tr>
<td>SPNego or X.509 client certificate authentication is enabled on the AS Java</td>
<td></td>
</tr>
<tr>
<td>A directory server that can map a UID to a user name</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Client</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Login Client 2.0 SP04 or higher (running on a Microsoft Windows platform) with a dedicated RFID-enabled authentication profile</td>
<td></td>
</tr>
</tbody>
</table>

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.

**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](#)

5.9.8.3 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.

**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.
5.9.8.4 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

<table>
<thead>
<tr>
<th>Prerequisites</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Login Client 2.0 SP04</td>
<td>You have installed Secure Login Client 2.0 SP04 or higher on your kiosk PCs.</td>
</tr>
<tr>
<td>PC/SC (reader type)</td>
<td>You have installed the respective device drivers for PC/SC readers.</td>
</tr>
<tr>
<td></td>
<td>A Microsoft Windows smart card service is active.</td>
</tr>
<tr>
<td>Wave ID (reader type)</td>
<td>You have installed the respective device drivers for Wave ID readers.</td>
</tr>
<tr>
<td></td>
<td>You have placed the runtime DLL of RFIDeas (file name pcProxAPI.dll) in the folder C:\Windows\System32 (32-bit Microsoft Windows) or C:\Windows \SysWOW64 (64-bit Microsoft Windows) of the kiosk PCs, and you have registered the DLL.</td>
</tr>
</tbody>
</table>

5.9.8.5 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 264]
- Adding a Policy Configuration [page 185]
- Managing Destinations [page 206]

## 5.9.8.5.1 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.
5.9.8.5.2 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.

5.9.8.5.2.1 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.
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

   **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.

8. **Example**

    | Value   | Description                                                                 |
    |---------|-----------------------------------------------------------------------------|
    | (.*)    | Allow access to all realms or all Microsoft Windows (domain) users           |
    | ABC(.*) | Allow access to all Microsoft Windows (domain) users or realms starting with ABC |
    | ABC     | 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                                                                 |
    |---------------|-----------|-----------------------------------------------------------------------------|
    | Rule1.principal | KIOSK(.*) | This configuration allows the user principal name KIOSK02@DOMAIN.LOCAL, but not K.IOS@DOMAIN.LOCAL. |
    | Rule1.realm    | DOMAIN.LOCAL |                                                                         |

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.

### 5.9.8.5.2.2 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.


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**

<table>
<thead>
<tr>
<th>Values for Login Module Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(.*)</td>
<td>Allow access to all issuer or subject names</td>
</tr>
<tr>
<td>CN=ABC (.*)</td>
<td>Allow access to all issuer or subject names starting with CN=ABC</td>
</tr>
<tr>
<td>CN=ABC</td>
<td>Allow access only to issuer or subject name called CN=ABC</td>
</tr>
</tbody>
</table>

   If no rule value matches, the authentication fails.

   **Login Module Option Configuration Examples**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Rule1.subjectName</code></td>
<td>CN=KIOSK(.*).</td>
<td>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.</td>
</tr>
<tr>
<td><code>Rule1.issuerName</code></td>
<td>CN=KIOSK ISSUING CA, O=LOCAL, C=DE</td>
<td>This configuration allows the distinguished name CN=KIOSK02, O=SHOP, C=US issued by CN=KIOSK ISSUING CA, O=TEST, C=UK.</td>
</tr>
</tbody>
</table>

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.

### 5.9.8.5.3 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:
      - RFID (WaveID based)
      - 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 189]
Parameters for Destination Management Configuration [page 289]
(Optional) Configuring the User Logon ID Mapping with Added Attributes [page 194]
Creating a Profile Group of Authentication Profiles [page 37]
LDAP User Mapping with Multiple Search Base DNs [page 207]

5.9.8.5.4 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 34]
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.

6.1 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.

6.1.1 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

For more information, see the related links.

Related Information

- Common Settings [page 242]
- PCSC Settings [page 244]
- CAPI Settings [page 247]
- Single Sign-On Setting for Kerberos-Based SNC Profile [page 251]
- Single Sign-On Setting for SPNego Profile [page 254]
## 6.1.1.1 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]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DisableSNCUserSelectionCache</td>
<td>DWORD</td>
<td>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. Default value is 0. If you want to prompt users to select from multiple certificates, enter the value 1. For more information, see SAP Note 2067284.</td>
</tr>
</tbody>
</table>
| Locale | STRING | Language setting for Secure Login Client. The language is usually recognized automatically. Use this parameter for customizing. Possible values are:  
ar_SA Arabic (Saudi-Arabia)  
de_DE German (Germany)  
en_US English (USA)  
es_ES Spanish (Spain)  
fr_FR French (France)  
hi_IN Hindi (India)  
it_IT Italian (Italy)  
ja_JP Japanese (Japan)  
kk_KZ Kazakh (Kazakhstan)  
nl_NL Dutch (Netherlands)  
pt_BR Portuguese (Brazil)  
ru_RU Russian (Russia)  
tr_TR Turkish (Turkey)  
zh_CN Simplified Chinese (China) |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HideTrayIcon</td>
<td>DWORD</td>
<td>Use this option to remove the Secure Login Client tray icon. To display the tray icon, set the value 0. To hide the tray icon, set the value 1. The default setting is that the tray icon is displayed.</td>
</tr>
<tr>
<td>TrustDB</td>
<td>STRING</td>
<td>Use this option to define where Secure Login Client searches for trusted root certificates. The following values are possible: capi (default) Get trust from Microsoft Certificate Store token Use root certificates on tokens Get trust from files (.crt, .p7c, ...) in a single directory</td>
</tr>
<tr>
<td>ResourcePath</td>
<td>STRING</td>
<td>Use this option to specify an alternate location for the language files (.res). The default value is &lt;install_path&gt;/etc.</td>
</tr>
<tr>
<td>ShowUserPoliciesPage</td>
<td>DWORD</td>
<td>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. To enable profile selection in a client, set the value 1. For more information, see the related link.</td>
</tr>
<tr>
<td>TurnOnSSHAgent</td>
<td>DWORD</td>
<td>You can enable and disable the Secure Login Client to run as an SSH agent using a checkbox in the SSH Agent tab under File Options. This function is a default function. You do not need to set any registry parameter for this. Use this registry parameter to force the user to enable the SSH agent in the Secure Login Client. If you set the value to 1, you enable the Secure Login SSH Agent. The user of the client PC cannot disable it. If you set the value to 0, you completely hide the SSH Agent tab from the Options menu of the Secure Login Client and thus disable the use of the Secure Login Client as an SSH agent. For more information, see the related link.</td>
</tr>
</tbody>
</table>
6.1.1.2 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.

[\texttt{HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\common\pcsc\}] [\texttt{HKEY_CURRENT_USER\SOFTWARE\SAP\SecureLogin\common\pcsc\}]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IgnoredReadersPattern</td>
<td>STRING</td>
<td>Use this option to disable some PCSC smart card readers. \nThe default value is \texttt{&lt;empty&gt;} (do not disable any PCSC smart card reader).</td>
</tr>
<tr>
<td>AllowedReadersPattern</td>
<td>STRING</td>
<td>Use this option to use only some specified PCSC smart card readers. This option is evaluated after IgnoredReadersPattern. \nThe default value is * (use every PCSC smart card reader) \nImportant: If you use an empty string \“, all readers are used (same as *).</td>
</tr>
</tbody>
</table>

6.1.1.3 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.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| GSSTTargetName    | STRING | 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\<SNC_application_policy_name>` 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. You can use the wildcards `*` and `?`. 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 `OU=SAP`, the application policy is valid for all servers where the character string ‘SAP’ occurs in the SNC name. **Note** This parameter is mandatory. **Example:**
  - `CN=SAP, OU=SAP Security, C=DE`
  - `CN=Server*, O=Company xyz`
  - Using the value `*` means that the client profile is used for all SAP servers. **Note** If `GSSTargetName` is not available in the registry, the Secure Login Client uses the application policies top down (as they appear in the registry tree). |
| TokenType         | STRING | You define the authentication type of the Secure Login Client here. **Values:**
  - `kerberos` for Kerberos authentication
  - `tokcapi` for Microsoft Cryptography API authentication |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any CAPI filter setting</td>
<td>STRING</td>
<td>You enter any available CAPI filter here. For more information, see the related link. The values of the common CAPI settings override these settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example for CAPIFilterissuerDN:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN=SSO_CA, O=SAP-AG, C=DE</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This parameter is only relevant for X.509 authentication.</td>
</tr>
<tr>
<td>allowFavorite</td>
<td>DWORD</td>
<td>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 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example 1:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example 2:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A user cannot select the authentication profile manually in the Secure Login Client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>reAuthentication</td>
<td>DWORD</td>
<td>This parameter determines whether or not you want to use Single Sign-On. The default value is 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example 1:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The selected Secure Login Client profile supports Single Sign-On.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example 2:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The selected Secure Login Client profile does not support Single Sign-On.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 (or higher)</td>
</tr>
</tbody>
</table>

**Related Information**

CAPI Settings [page 247]
### 6.1.1.4 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 third party Cryptographic Service Providers may be used.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\common\capi] [HKEY_CURRENT_USER\SOFTWARE\SAP \SecureLogin\common\capi]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPIProviderFilter</td>
<td>STRING</td>
<td>Use this option to use only certificates provided by specific cryptographic service providers (the cryptographic service provider’s name must begin with this string). You find the cryptographic service provider names in HKLM/Software/Microsoft/Cryptography/Defaults/Provider. Example: <strong>Microsoft</strong> Use only certificates provided by CSPs from Microsoft</td>
</tr>
<tr>
<td>CAPIFilterValidOnly</td>
<td>DWORD</td>
<td>Use this option to use only certificates that are valid (issued in the past and not expired). The default is 0.</td>
</tr>
<tr>
<td>CAPIFilterIssuerDN</td>
<td>STRING</td>
<td>Use this option to use only certificates that have an issuer’s Distinguished Name that contains <strong>CAPIFilterIssuerDN</strong>. To specify the certificates of a certain server, enter the whole Distinguished Name or only a part of it. You cannot use wildcards. Example: <strong>CN=My Companies CA</strong></td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CAPIFilterSubjectDN</td>
<td>STRING</td>
<td>Use this option to use only certificates that have a subject Distinguished Name that contains CAPIFilterSubjectDN. To specify the certificates of a certain server, enter the whole Distinguished Name or only a part of it. You cannot use wildcards. Example: \textit{O=My Org Unit}</td>
</tr>
<tr>
<td>CAPIFilterExcludeIssuerDN</td>
<td>STRING</td>
<td>Use this option to disable certificates that have an issuer’s Distinguished Name that contains CAPIFilterExcludeSubjectDN. To specify the certificates of a certain server, enter the whole Distinguished Name or only a part of it. You cannot use wildcards. Example: \textit{CN=Test CA}</td>
</tr>
<tr>
<td>CAPIFilterExcludeSubjectDN</td>
<td>STRING</td>
<td>Use this option to disable certificates that have a subject Distinguished Name that contains CAPIFilterExcludeSubjectDN. To specify the certificates of a certain server, enter the whole Distinguished Name or only a part of it. You cannot use wildcards. Example: \textit{O=Testing only}</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CAPIFilterKeyUsage  | STRING | Use this option to use only certificates that have a specific key usage. The `CAPIFilterKeyUsage` may contain the following strings (you can specify multiple strings):  
+KEYUSAGE  
Use only certificates that have the specified key usage.  
-KEYUSAGE  
Do not use certificates that have the specified key usage.  
Where KEYUSAGE can be one of the following:  
dataEncipherment  
Data encipherment key usage  
digitalSignature  
Digital-Signature Key-Usage  
keyAgreement  
Key agreement key usage  
keyEncipherment  
Key encipherment key usage  
nonRepudiation  
Non-repudiation key usage  
cRLSign  
CRL signature key usage |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| CAPIFilterExtendedKeyUsage    | STRING | Use this option to use only certificates that have a specific key usage. The syntax of this option is similar to CAPIFilterKeyUsage. The CAPIFilterExtendedKeyUsage may contain the following strings:  

+EXTKEYUSAGE

Use only certificates that have the specified extended key usage

-EXTKEYUSAGE

Do not use certificates that have the specified extended key usage

Where EXTKEYUSAGE can be one of the following:  

ServerAuthentication (1.3.6.1.5.5.7.3.1)  
ClientAuthentication (1.3.6.1.5.5.7.3.2)  
CodeSigning (1.3.6.1.5.5.7.3.3)  
EmailProtection (1.3.6.1.5.5.7.3.4)  
IpsecEndSystem (1.3.6.1.5.5.7.3.5)  
IpsecTunnel (1.3.6.1.5.5.7.3.6)  
IpsecUser (1.3.6.1.5.5.7.3.7)  
TimestampSigning (1.3.6.1.5.5.7.3.8)  
OcspSigning (1.3.6.1.5.5.7.3.9)  
MicrosoftEfs (1.3.6.14.1.311.10.3.4)  
MicrosoftEfsRecovery (1.3.6.14.1.311.10.3.4.1)  
MicrosoftKeyRecovery (1.3.6.14.1.311.10.3.11)  
MicrosoftDocumentSigning (1.3.6.14.1.311.10.3.12)  
MicrosoftSmartcardLogon (1.3.6.14.1.311.20.2.2)
### 6.1.1.5 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| inactivityTimeout | DWORD | Value in seconds until an automatic logout is performed (due to mouse and keyboard inactivity). 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). It depends on the third-party cryptographic service provider you use whether the inactive timeout is available. Some cryptographic service providers do not allow logout; some always prompt the user for a password. The following values are possible: 

- `ffffffff` (equivalent to -1)
  - No single sign-on. Each SNC connection forces a new login.
- `0` (default)
  - Single sign-on and no timeout
- Enter a value > 0.
  - Seconds until an automatic logout is executed. |
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.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSOMode</td>
<td>DWORD</td>
<td>Use this option to configure the setting of the Kerberos-based SNC profile of the Secure Login Client for SNC connection. Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 The SNC connection uses the existing Microsoft Windows credentials. There is an automatic logon to the Secure Login Client Kerberos profile.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 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 User field, and the cursor is in the Password field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 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 User field, and the cursor is in the Password field.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>If single sign-on has failed, users are prompted for user name and password to log on to an SNC session.</td>
</tr>
</tbody>
</table>

### 6.1.1.6 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.

**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.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSOMode</td>
<td>DWORD</td>
<td>Use this option to configure the setting of the SPNego profile of the Secure Login Client for SNC connection. Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 The SNC connection uses the existing Microsoft Windows credentials. There is an automatic logon to the Secure Login Client SPNego profile.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 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 logon to Microsoft Windows, the SPNego profile is grayed out. The SNC connection remains until users logs off from their profiles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 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 logon to Microsoft Windows, the Kerberos profile is grayed out. The session remains valid until you log off from this profile. Your user name appears in the User field, and the cursor is in the Password field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 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 certifi-</td>
</tr>
</tbody>
</table>
cate expires. There is no auto-enrollment with the certificate. Your user name appears in the User field, and the cursor is in the Password field.

### 6.1.2 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 256]

### 6.1.2.1 SSF User Configuration

The following table contains parameter for the SSF user configuration in SAP GUI.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSF-ID</td>
<td>Define the Distinguished Name of the user certificate. Example: CN=Username, OU=SAP Security</td>
</tr>
<tr>
<td>SSF-ID Part 2</td>
<td>Define an additional Distinguished Name of the user certificate.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **SSF Profile** | Define the Secure Login Client profile. There are three options available.  
- Use Secure Login Client Profile  
  The desired certificate is used for SSF, based on the Secure Login Client profile name.  
  Example: `toksw:mem://securelogin/<profile_name>`  
- Use Secure Login Client Profile and Re-authentication  
  Adding the `[reauth]` option means that the user needs to authenticate again to the Secure Login Client profile, before a certificate is provided.  
  Example: `[reauth]toksw:mem://securelogin/<profile_name>`  
You can also use a profile for smart cards. Enter the SSF profile with the following syntax:  
`tokcapi:<token_ID>`  
Example: `tokcapi:2B15-3774-844B #1 nFast PCI device, bus 6, slot 0`  
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:  
`tokcapi:*(*)` |
| Destination  | The RFC destination (logical destination) where the SSF RFC server program has been defined.  
Enter the value `SAP_SSFATGUI` (SSF for digital signatures on the front ends). |

For more information, see the SAP NetWeaver Library under `Function-Oriented View > Security > Digital Signatures and Encryption`.

### 6.2 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.
6.2.1 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry Name (mandatory)</td>
<td>Enter the name of the Certification Authority</td>
<td>Root CA</td>
</tr>
<tr>
<td>Key Length (mandatory)</td>
<td>Select the encryption key length for the server (1024, 1536, 2048, 3072, or 4096 bits).</td>
<td>2048</td>
</tr>
<tr>
<td>Valid From (mandatory)</td>
<td>Enter the start date for the validity of this certificate.</td>
<td>11/29/2013</td>
</tr>
<tr>
<td>Valid To (mandatory)</td>
<td>Enter the end date for the validity of this certificate.</td>
<td>04/25/2014</td>
</tr>
<tr>
<td>Country Name</td>
<td>Enter the country abbreviation in this field (C)</td>
<td>DE</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Enter the company name in this field (O)</td>
<td>Company xyz</td>
</tr>
<tr>
<td>Locality Name</td>
<td>Enter the regional information in this field (L).</td>
<td>Walldorf</td>
</tr>
<tr>
<td>Organization Unit Name</td>
<td>Enter the company name in this field (OU)</td>
<td>SAP Security Department</td>
</tr>
<tr>
<td>Common Name (mandatory)</td>
<td>Enter the common name of the certificate (CN).</td>
<td>Root CA SAP Security</td>
</tr>
<tr>
<td>Subject Alternative Name (DNS)</td>
<td>Enter the subject alternative names in this field.</td>
<td><a href="mailto:ServerName@FQDN.local">ServerName@FQDN.local</a></td>
</tr>
<tr>
<td></td>
<td>Enter the alternative name in this field. Typically this is the Fully Qualified Domain Name (FQDN).</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry Name (mandatory)</td>
<td>Enter the name of the Certification Authority</td>
<td>User CA</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description, for example, of the hardware security token.</td>
<td>HSM token number 12</td>
</tr>
<tr>
<td>Key ID (mandatory)</td>
<td>HSM token key identifier</td>
<td>Example</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA8E7B48B22531680AB4920C7D820999D739166</td>
</tr>
<tr>
<td>PIN</td>
<td>Password or PIN for the PSE file you specify in Token URI</td>
<td>mypassword or myPIN</td>
</tr>
<tr>
<td>Token URI (mandatory)</td>
<td>The token URI contains the token type, the location of the middleware, and the name of the slot.</td>
<td>Example</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tokp11:/usr/local/pkcs11driver/driverpkcs11.so#HSM Reader</td>
</tr>
</tbody>
</table>

Related Information

Initial Configuration (Automatic) [page 148]
Adding Certification Authorities [page 211]
Setting the AS ABAP Profile Parameters [page 113]
6.2.2 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 SAP NetWeaver Application Server for 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 SAP NetWeaver Application Server for 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.

Note

Entries marked with * are mandatory.
### Parameters for Signing Certificate Requests

<table>
<thead>
<tr>
<th>Option</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base64 Encoded Certificate Request (PKCS #10) *</td>
<td>The content of the certificate request in base64 encoding format. Use the option Select a File to Insert to import a certificate request file. Use the button Read Content to import. Another option is to copy and paste the content of the certificate request to the Base64-Encoded Certificate Request (PKCS#10) field. The Show Certificate Request button displays the content of the certificate request. The Reset button enables you to clear the fields Base64-Encoded Certificate Request (PKCS#10), Certificate Request, and Base64-Encoded Certificate Response (PKCS #7). Thus, you can also use it to undo the signing of certificates that have been signed already.</td>
</tr>
<tr>
<td>Validity Period of Certificate (Months)*</td>
<td>Define the period of time for which the certificate is valid.</td>
</tr>
<tr>
<td>Certificate Template</td>
<td>If needed, select the desired certificate template. The default certificate template is used for the SAP environment.</td>
</tr>
<tr>
<td>Issuer*</td>
<td>Choose the desired CA certificate. The certificate request should be signed.</td>
</tr>
<tr>
<td>Signature Algorithm*</td>
<td>Choose the signature algorithm you want to use. The default value is sha265WithRSAEncryption. If you choose the Sign Certificate button, you sign a certificate at the selected CA using the certificate request and the parameters.</td>
</tr>
<tr>
<td>Base64-Encoded Certificate Response (PKCS#7)</td>
<td>This field displays the signed certificate response.</td>
</tr>
<tr>
<td>Certificate Encoding Type</td>
<td>Select PEM or DER encoding type. A certificate response should be generated. Using the Download function, you can save or open the certificate for further use.</td>
</tr>
</tbody>
</table>

### 6.2.3 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.
### 6.2.3.1 Client Policy

Information about client policy parameters for the Secure Login Client. These parameters are defined in the file `ProfileDownloadPolicy<profile_group_name>.reg`.

```plaintext
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SAP\SecureLogin\System]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PolicyURL</td>
<td>STRING</td>
<td>Network resource from which the latest Secure Login Client profiles can be downloaded. 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.</td>
</tr>
<tr>
<td>PolicyTTL</td>
<td>DWORD</td>
<td>The lifetime in minutes for verifying (updating) a new client policy on the Secure Login Server. The default is 0 minutes (hexadecimal value: 0). By default, the Secure Login Client verifies during system startup of the client PC.</td>
</tr>
<tr>
<td>NetworkTimeout</td>
<td>DWORD</td>
<td>Network timeout in seconds before the connection is closed if the Secure Login Server does not respond. The default is 45 seconds (hexadecimal value: 2d).</td>
</tr>
<tr>
<td>DisableUpdatePolicyOnStartup</td>
<td>DWORD</td>
<td>By default, the Secure Login Client verifies a new client policy during system startup of the client PC. You can use this parameter to disable this feature. 1 Disable automatic policy download. 0 Enable automatically policy download. Default value is 0.</td>
</tr>
<tr>
<td>proxyIsPACURL</td>
<td>DWORD</td>
<td>You can configure the use of a proxy server using a proxy auto-config (PAC) URL for Secure Login Client policy download. If you want to use a proxy auto-config (PAC) file, set this parameter to 1. In this case, <code>HttpProxyURL</code> must have a valid URL. Default value is 0.</td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Type</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>httpProxyURL</code></td>
<td>STRING</td>
<td>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. You can only use this proxy auto-config (PAC) URL if you set <code>proxyIsPACURL</code> to 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://example.address.com:8888/wpad.dat">http://example.address.com:8888/wpad.dat</a></td>
</tr>
<tr>
<td><code>useWindowsHttpProxy</code></td>
<td>DWORD</td>
<td>You can only use this parameter if <code>httpProxyURL</code> is set to AUTO. If you use the value 1, 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. For more information, see Automatically Using the Proxy Configuration of Microsoft Internet Explorer for Secure Login Client [page 47].</td>
</tr>
<tr>
<td><code>showErrorMsg</code></td>
<td>DWORD</td>
<td>Users get an error message whenever their authentication failed. Default value is 1.</td>
</tr>
<tr>
<td><code>showSuccessMsg</code></td>
<td>DWORD</td>
<td>Users get a success message whenever their authentication was successful. Default value is 0.</td>
</tr>
</tbody>
</table>
6.2.3.2 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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GssTargetName</td>
<td>STRING</td>
<td>Application-specific PSE URI (SAP server SNC name) that is matched when a suitable profile is searched. You can use the wildcards * and ?. Example: CN=SAP, OU=SAP Security, C=DE CN=Server*, O=Company xyz Using the value * means that the client profile is used for all SAP servers.</td>
</tr>
<tr>
<td>profile</td>
<td>STRING</td>
<td>The name of the client profile to be used for the desired application.</td>
</tr>
<tr>
<td>allowFavorite</td>
<td>DWORD</td>
<td>Allow the user to select the authentication profile manually in Secure Login Client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 User cannot select the authentication profile manually in Secure Login Client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 User can select authentication profile manually in Secure Login Client.</td>
</tr>
<tr>
<td>reAuthentication</td>
<td>DWORD</td>
<td>Use single sign-on to log on to the SAP NetWeaver Application Server for ABAP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 Single sign-on is not available to log on to the SAP NetWeaver Application Server for ABAP. Users must enter their user names and passwords to log on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 The default value is 0.</td>
</tr>
</tbody>
</table>

In addition, it is possible to download the configuration using the ProfileGroup<profile_group_name>.reg file.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>profileName</code></td>
<td>STRING</td>
<td>The name of the client profile to be used for the desired application.</td>
</tr>
<tr>
<td><code>pseType</code></td>
<td>STRING</td>
<td>Authentication type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>promptedlogin</strong> Using this profile, the user will be requested to enter the user credentials.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>windowslogin</strong> Using this profile, the user credentials will be provided automatically (only available for Microsoft Windows authentication).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default value is <code>windowslogin</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In a client authentication profile for RFID tokens, this parameter defines the RFID reader type of the kiosk PCs.</td>
</tr>
<tr>
<td><code>rfidpcsc</code></td>
<td></td>
<td>This profile enables kiosk PCs to use RFID readers with the reader type PC/SC.</td>
</tr>
<tr>
<td><code>rfidwaveid</code></td>
<td></td>
<td>This profile enables kiosk PCs to use RFID readers with the reader type Wave ID.</td>
</tr>
<tr>
<td><code>enrollURL0</code></td>
<td>STRING</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>https://&lt;server&gt;:port/SecureLoginServer/slc(x)/doLogin?profile=&lt;profile_ID&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can configure a path for a Secure Login Client 1.0 or for a Secure Login Client 2.0. Use <code>slc1</code> for Secure Login Client 1.0 and <code>slc2</code> for Secure Login Client 2.0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example for Secure Login Client 2.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>https://example.address.com:50201/SecureLoginServer/slct/doLogin?profile=6506265a-3c5f-4fd1-88fd-5e962f92fe6c</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the Add 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.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>httpProxyURL</td>
<td>STRING</td>
<td>HTTP proxy to be used with enrollment URLs. Only HTTP proxies without authentication and without SSL to proxy are supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: \textit{<a href="http://example.address.com:8888%7D">http://example.address.com:8888}</a></td>
</tr>
<tr>
<td>reAuthentication</td>
<td>DWORD</td>
<td>This parameter defines how many login attempts are permitted with the Secure Login Client login form before it is closed again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example with value 4: The Secure Login Client offers the login form 4 times (for example, wrong credential information), before the login form will be closed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default value is 0. The login form will never be closed. User needs to use the button Cancel to close the login form.</td>
</tr>
<tr>
<td>gracePeriod</td>
<td>DWORD</td>
<td>Value in seconds when an enrollment is to be carried out before the certificate expires. Default value is 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value: -1 An expiration of a certificate does not trigger an automatic re-enrollment.</td>
</tr>
<tr>
<td>inactivityTimeout</td>
<td>DWORD</td>
<td>Value in seconds until an automatic logout is performed (due to mouse and keyboard inactivity).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value: 0 No timeout. SSO without constraints.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 0. Enter a value &gt; 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Seconds until an automatic logout is executed.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>autoReenrollTries</td>
<td>DWORD</td>
<td>The number of failed authentications in a row after which automatic re-enrollment is stopped. User name and password caching can be turned on to provide the automatic re-enrollment of certificates that are going to expire. Possible values: 0: Turn off. Do not re-enroll automatically; do not cache user name and password. A re-enrollment must always be performed manually by the user. Value &gt;0 (n): Turn on with n tries to succeed: 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. The default value is 0.</td>
</tr>
<tr>
<td>autoEnroll</td>
<td>DWORD</td>
<td>A user automatically gets an X.509 certificate when the Secure Login Client starts. 0: Turn off 1: Automatic provisioning of user certificates If pseType is set to windowslogin, user credentials are provided automatically (only applies for Microsoft Windows authentication). If pseType is set to promptedlogin, the system prompts the users to enter their credentials.</td>
</tr>
<tr>
<td>keySize</td>
<td>DWORD</td>
<td>RSA Key Length. The default value is 1024 (hexadecimal value: 400).</td>
</tr>
<tr>
<td>UniqueClientID</td>
<td>STRING</td>
<td>Custom-defined string; will be displayed in the instance log or can be used for network filtering issues.</td>
</tr>
<tr>
<td>networkTimeout</td>
<td>DWORD</td>
<td>Network timeout (in seconds) before the connection is closed if the server does not respond. The default value is 45 (hexadecimal value: 2d).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sslHostCommonNameCheck</td>
<td>DWORD</td>
<td>This applies to the SSL server certificate – this checks if the peer host name is given in the Common Name (CN) field of the SSL Server certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify the SSL server host name with the Common Name (CN) field of the SSL server certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Do not verify SSL server host name with the Common Name (CN) field of the SSL Server certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 0.</td>
</tr>
<tr>
<td>sslHostAlternativeNameCheck</td>
<td>DWORD</td>
<td>This applies to the SSL server certificate – this checks whether the peer host name is given in its Subject Alternative Name attribute of the certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify the SSL server host name with the Subject Alternative Name attribute of the SSL Server certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Do not verify the SSL server host name with the Subject Alternative Name attribute of the SSL server certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>sslHostExtensionCheck</td>
<td>DWORD</td>
<td>This applies to the SSL server certificate – this checks if the extended key usage ServerAuthentication is defined.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify whether the extended key usage ServerAuthentication is defined in the SSL Server certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Do not verify whether the extended key usage ServerAuthentication is defined in the SSL Server certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 0.</td>
</tr>
<tr>
<td>newPinType</td>
<td>STRING</td>
<td>Message text value is used for messages (change PIN/password) to the Secure Login Client and Secure Login Web Client. Available values are pin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and password.</td>
</tr>
</tbody>
</table>
6.2.4 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 275]
Parameters for RADIUS Login Modules [page 277]
Parameters for ABAP Login Modules [page 279]

6.2.4.1 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.

Note

The fields with the asterisk (*) are mandatory fields.
### Auto-enroll

A user automatically gets an X.509 certificate when the Secure Login Client starts.

- **False:** Turn off
- **True:** Automatic provisioning of user certificates

If `pseType` is set to `windowslogin`, user credentials are provided automatically (only applies for Microsoft Windows authentication with SPNegoLoginModule AA).

If `pseType` is set to `promptedlogin`, 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 `promptedlogin`.

### Automatic Re-enroll Attempts

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:

- **0**: Turn off:
  - Does not re-enroll automatically, does not cache user name and password. A re-enrollment must always be performed manually by the user.
- **>0 (n)**: Turn on with n tries to succeed:
  - 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.

The default value is **0**.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auto-enroll</strong></td>
<td>A user automatically gets an X.509 certificate when the Secure Login Client starts.</td>
</tr>
<tr>
<td></td>
<td><strong>False:</strong> Turn off</td>
</tr>
<tr>
<td></td>
<td><strong>True:</strong> Automatic provisioning of user certificates</td>
</tr>
<tr>
<td></td>
<td>If <code>pseType</code> is set to <code>windowslogin</code>, user credentials are provided automatically (only applies for Microsoft Windows authentication with SPNegoLoginModule AA).</td>
</tr>
<tr>
<td></td>
<td>If <code>pseType</code> is set to <code>promptedlogin</code>, 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 <code>promptedlogin</code>.</td>
</tr>
<tr>
<td><strong>Automatic Re-enroll Attempts</strong></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td><strong>0</strong>: Turn off: \n  - Does not re-enroll automatically, does not cache user name and password. A re-enrollment must always be performed manually by the user.</td>
</tr>
<tr>
<td></td>
<td><strong>&gt;0 (n)</strong>: Turn on with n tries to succeed: \n  - 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.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Details</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Enrollment URL**  | Secure Login Server URL that is used for user authentication and certificate request. Enroll URL depends on the configuration of the authentication profile.  
  https://<host_name>:<port>/SecureLoginServer/<protocol_version>/doLogin?profile=<profile_ID>  
  Enrollment URL defined in a authentication profile <profile_ID> of the Secure Login Server.  
  To configure further enrollment URLs, use the Add 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. |
| **Grace Period (Seconds)** | Integer value in seconds for the time in which an enrollment is to be carried out before the certificate expires. -1 means that you disable automatic re-enrollment.  
  The default value is 0 |
| **HTTP Proxy URL**  | HTTP proxy to be used with enrollment URLs. Only HTTP proxies without authentication and without SSL to proxy are supported.  
  Example: http://example.address.com:8888  
  If you want to use the proxy server settings configured in Microsoft Internet Explorer, set the parameter AUTO. 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 Automatically Using the Proxy Configuration of Microsoft Internet Explorer for Secure Login Client [page 47]. |
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inactivity Timeout (Seconds)</strong></td>
<td>Value in seconds until an automatic logout is performed (due to mouse and keyboard inactivity). Possible values:</td>
</tr>
<tr>
<td></td>
<td><strong>Value</strong> -1</td>
</tr>
<tr>
<td></td>
<td><strong>Value</strong> 0</td>
</tr>
<tr>
<td></td>
<td>No timeout. SSO without constraints.</td>
</tr>
<tr>
<td></td>
<td>The default value is <strong>0</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Value</strong> n</td>
</tr>
<tr>
<td></td>
<td>Seconds until an automatic logout takes place.</td>
</tr>
<tr>
<td><strong>Network Timeout (Seconds)</strong></td>
<td>Network timeout (in seconds) before the connection is closed if the server does not respond</td>
</tr>
<tr>
<td></td>
<td>The default value is <strong>45</strong></td>
</tr>
<tr>
<td><strong>New PIN/Password Response Text</strong></td>
<td>Message text value used for messages (change PIN/password) to the Secure Login Client and Secure Login Web Client.</td>
</tr>
<tr>
<td></td>
<td>Available values are <strong>pin</strong> and <strong>password</strong>.</td>
</tr>
<tr>
<td><strong>Policy Configuration Name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Profile Type</strong></td>
<td>If you are using kiosk PCs as clients with RFID identification, this parameter defines the RFID reader type.</td>
</tr>
<tr>
<td></td>
<td>Available values are <strong>RFID (PCSC based)</strong> or <strong>RFID (WaveID based)</strong>.</td>
</tr>
<tr>
<td><strong>Re-authentication</strong></td>
<td>This parameter defines how many logon attempts are permitted with the Secure Login Client logon form before it is closed again.</td>
</tr>
<tr>
<td></td>
<td>Example with the value <strong>4</strong>:</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>The default value is <strong>0</strong>.</td>
</tr>
<tr>
<td></td>
<td>With this value, the logon form is never closed. The user needs to use the <strong>Cancel</strong> button to close the logon form.</td>
</tr>
<tr>
<td><strong>Show Error Message</strong></td>
<td>The default value is <strong>true</strong>. Error messages are displayed in the client.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Details</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Show Success Message</td>
<td>The default value is <code>true</code>. Success messages are displayed.</td>
</tr>
<tr>
<td>SSL Host Alternative Name Check</td>
<td>This applies to the SSL server certificate – this checks if the peer host name is given in the <code>Subject Alternative Name</code> attribute of the certificate.</td>
</tr>
<tr>
<td></td>
<td><strong>True</strong></td>
</tr>
<tr>
<td></td>
<td>Verifies the SSL server host name with the <code>Subject Alternative Name</code> attribute of the SSL Server certificate.</td>
</tr>
<tr>
<td></td>
<td><strong>False</strong></td>
</tr>
<tr>
<td></td>
<td>Does not verify the SSL server host name with the <code>Subject Alternative Name</code> attribute of the SSL Server certificate.</td>
</tr>
<tr>
<td></td>
<td>The default value is <code>False</code></td>
</tr>
<tr>
<td>SSL Host Common Name Check</td>
<td>This applies to the SSL Server certificate – this checks if the peer host name is given in the <code>Common Name</code> (CN) field of the SSL Server certificate.</td>
</tr>
<tr>
<td></td>
<td><strong>True</strong></td>
</tr>
<tr>
<td></td>
<td>Verifies the SSL server host name with the <code>Common Name</code> (CN) field of the SSL Server certificate.</td>
</tr>
<tr>
<td></td>
<td><strong>False</strong></td>
</tr>
<tr>
<td></td>
<td>Does not verify the SSL server host name with the <code>Common Name</code> (CN) field of the SSL Server certificate.</td>
</tr>
<tr>
<td></td>
<td>The default value is <code>False</code></td>
</tr>
<tr>
<td>SSL Host Extension Name Check</td>
<td>This applies to the SSL server certificate – this specifies whether the system checks if the extended key usage <code>ServerAuthentication</code> is defined.</td>
</tr>
<tr>
<td></td>
<td><strong>True</strong></td>
</tr>
<tr>
<td></td>
<td>Verify if the extended key usage <code>ServerAuthentication</code> is defined in the SSL server certificate.</td>
</tr>
<tr>
<td></td>
<td><strong>False</strong></td>
</tr>
<tr>
<td></td>
<td>Does not verify if the extended key usage <code>ServerAuthentication</code> is defined in the SSL server certificate.</td>
</tr>
<tr>
<td></td>
<td>The default value is <code>False</code></td>
</tr>
</tbody>
</table>
### 6.2.4.2 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.

<table>
<thead>
<tr>
<th>Secure Login Web Client Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Post Authentication Actions</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Actions</strong></td>
<td></td>
</tr>
<tr>
<td>No Action</td>
<td>The action to be performed by the Secure Login Web Client after successful user authentication. The following options are available:</td>
</tr>
<tr>
<td>Redirect to URL</td>
<td></td>
</tr>
<tr>
<td>No Action</td>
<td>After successful user authentication, no action is performed.</td>
</tr>
<tr>
<td>Redirect to URL</td>
<td>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.</td>
</tr>
<tr>
<td>Log On to ABAP System</td>
<td>After successful authentication, the user logs on to an ABAP system.</td>
</tr>
<tr>
<td>Log On to ABAP Message Server</td>
<td></td>
</tr>
<tr>
<td>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 SAP GUI Description field empty.</td>
<td></td>
</tr>
<tr>
<td>Redirect to URL and Log On to ABAP Message Server</td>
<td></td>
</tr>
<tr>
<td>Redirect to URL and Log On to ABAP Message Server</td>
<td></td>
</tr>
<tr>
<td>Launch SAP Logon Pad</td>
<td>After successful authentication, the SAP Logon pad is started automatically.</td>
</tr>
<tr>
<td>Redirect to URL and Launch SAP Logon Pad</td>
<td></td>
</tr>
<tr>
<td>For more information on connection types for starting SAP GUI, see Configuring Secure Login Web Client Connections to SAP GUI [page 155].</td>
<td></td>
</tr>
<tr>
<td><strong>Web Client URL</strong></td>
<td></td>
</tr>
<tr>
<td><strong>IP Address/Host Name</strong></td>
<td>IP address or host name of Secure Login Server which is used to generate to Web Client URL.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Port of Secure Login Server for the Web Client URL.</td>
</tr>
</tbody>
</table>
## 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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>This URL is made up of the IP address/host name and of the port</td>
</tr>
</tbody>
</table>

### Client Behavior

**Web Adapter Mode (requires Secure Login Client installation)**

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 `slwc.exe`.

### Note

You have installed a Secure Login Client and activated Secure Login Server Support during the installation procedure. This feature is only available on Microsoft Windows.

### Platform Binaries Download Path

**Microsoft Windows**

Enter the download location for the security libraries. By default, the location of the Secure Login Web Client files depends on the operating system.

Default:
- For Microsoft Windows XP: `%APPDATA%`
- For Microsoft Windows Vista/7 or higher: `%LOCALAPPDATA%`

Example for Microsoft Windows XP:

```
%USERPROFILE%\%APPDATA%\sapsnc
```

Example for Microsoft Windows Vista/7:

```
%USERPROFILE%\%LOCALAPPDATA%\sapsnc
```

**OS X**

Default:

```
$HOME/sapsnc
```

Example:

```
$HOME/.sap_webclient/sapsnc
```
## Parameters for LDAP Login Modules

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>In Options of login module of the SAP NetWeaver Administrator</strong></td>
<td></td>
</tr>
<tr>
<td>LdapDestination</td>
<td>Enter the exact name of the LDAP destination.</td>
</tr>
<tr>
<td>LdapServerType</td>
<td>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. Values for LDAP servers:</td>
</tr>
<tr>
<td></td>
<td><strong>AD</strong> (default) for Active Directory</td>
</tr>
<tr>
<td></td>
<td><strong>ODSEE</strong> for Oracle Directory Server</td>
</tr>
<tr>
<td></td>
<td>For more information, see the related link.</td>
</tr>
<tr>
<td>MappingMode</td>
<td>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="https://support.sap.com/">2058282</a>. The default is no value.</td>
</tr>
<tr>
<td></td>
<td><strong>&lt;none&gt;</strong> or <strong>DEFAULT</strong></td>
</tr>
<tr>
<td></td>
<td>Mapping with the user principal name</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong></td>
</tr>
<tr>
<td></td>
<td>The user name <strong>jdoe</strong> is mapped to UPN <strong><a href="mailto:jdoe@DOMAIN.COM">jdoe@DOMAIN.COM</a></strong></td>
</tr>
<tr>
<td>LogonID</td>
<td>Mapping with the user logon ID</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong></td>
</tr>
<tr>
<td></td>
<td>The user name <strong>jdoe</strong> is mapped to the user logon ID <strong>jdoe</strong></td>
</tr>
</tbody>
</table>
## Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PasswordExpirationAttribute</strong></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>Generalized time formats:</td>
</tr>
<tr>
<td></td>
<td>20120630181530Z = 30. June 2012 18:15:30 (UTC)</td>
</tr>
<tr>
<td></td>
<td>20120630191530+0100Z = 30. June 2012 20:15:30 (CET)</td>
</tr>
<tr>
<td></td>
<td>20120630181530.0Z = 30. June 2012 18:15:30 (UTC)</td>
</tr>
<tr>
<td></td>
<td>20120630191530.0+0100Z = 30. June 2012 20:15:30 (CET)</td>
</tr>
<tr>
<td></td>
<td>MS Gregorian calendar time format (100-nanosecond intervals since 1. January 1601 (UTC))</td>
</tr>
<tr>
<td></td>
<td>129855537300000000 = 30. June 2012 18:15:30 (UTC)</td>
</tr>
<tr>
<td></td>
<td>Netscape Password Expiring time format (seconds until password expires)</td>
</tr>
<tr>
<td></td>
<td>864000 = 10 days from current date until password expires</td>
</tr>
<tr>
<td></td>
<td>If a password expiration warning message is configured, the LdapBaseDN property must be given in complete DN form (UPN on Microsoft Active Directory) in the configuration of the LDAP destination.</td>
</tr>
<tr>
<td></td>
<td>The PasswordExpirationAttribute value is used for the password expiration warning message only. By default no value is defined.</td>
</tr>
<tr>
<td><strong>PasswordExpirationGracePeriod</strong></td>
<td>The interval (in days) for a password expiration warning message to be sent to the Secure Login Client prior to a password expiring.</td>
</tr>
</tbody>
</table>

### Related Information

- Creating Destinations [page 189]
- Enabling the Display of LDAP Messages in Secure Login Client [page 63]

### 6.2.4.4 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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>RadiusDestination</td>
<td>Enter the exact name of your RADIUS destination.</td>
</tr>
</tbody>
</table>

Parameters in the Secure Login Administration Console

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Method*</td>
<td>Authentication method for the RADIUS server. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>PAP</td>
</tr>
<tr>
<td></td>
<td>CHAP</td>
</tr>
<tr>
<td></td>
<td>MSCHAP</td>
</tr>
<tr>
<td></td>
<td>The default value is PAP.</td>
</tr>
<tr>
<td>IP Address/Host Name*</td>
<td>Host address of the RADIUS server (used for user authentication).</td>
</tr>
<tr>
<td>Port*</td>
<td>The port number used by the RADIUS server for authentication requests. Typical values are 1645 or 1812. The default value is 1645.</td>
</tr>
<tr>
<td>Timeout (Milliseconds)*</td>
<td>Period of time the Secure Login Server waits for a response before trying the next RADIUS Server (in milliseconds). The default value is 5000 milliseconds.</td>
</tr>
<tr>
<td>Shared Secret*</td>
<td>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.</td>
</tr>
<tr>
<td>Confirm Shared Secret*</td>
<td>Paste your Shared Secret again for confirmation.</td>
</tr>
</tbody>
</table>

Advanced Configuration for RSA Authentication

Import Server Message File:

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you import a RADIUS Server message file, the following parameters are filled automatically.</td>
</tr>
</tbody>
</table>

ExtInputMustChoose_C:
Enter a new PIN having n alphanumeric characters:

ExtInputMustChoose_C_C:
Enter a new PIN having from n to n alphanumeric characters:

ExtInputMustChoose_D:
Enter a new PIN having n digits:

ExtInputMustChoose_D_D:
Enter a new PIN having from n to n digits:

ExtInputNextCode: Wait for token to change, then enter the new tokencode:
### 6.2.4.5 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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
<td>The destination is already available in the SAP NetWeaver Administrator.</td>
</tr>
<tr>
<td><strong>maxNbrConnections</strong></td>
<td>Maximum number of connections.</td>
</tr>
</tbody>
</table>
| **PasswordAlphanummeric**   | This parameter is part of the password policy for the client-side policy consistency check. Possible values:  
                                *true*  
                                The password can contain only alphanumeric characters (A-Z, a-z, 0-9).  
                                *false*  
                                The password can contain alphanumeric and special characters (such as !$%&).  
                                This parameter must be consistent with the SAP password policy.  
                                The default value is *true*. |
| **PasswordMax**             | 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.  
                                This parameter must be consistent with the SAP password policy.  
                                The default value is *30*. |
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Details</th>
</tr>
</thead>
</table>
| **PasswordMin** | 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.  
This parameter must be consistent with the SAP password policy.  
The default value is 1. |
| **SAPTimeout** | Timeout for login  
Maximum number of connections until authentication is blocked |

### 6.2.4.6 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`.

#### Note

The fields with the asterisk (*) are mandatory fields.

<table>
<thead>
<tr>
<th>Parameters for Downloading Policies Using Profile Groups</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Name:</strong> *</td>
<td>The profile group name appears here.</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Protocol:</strong> *</td>
<td>Default is https. For security reasons, we recommend to use https.</td>
</tr>
</tbody>
</table>
| **IP Adress./Host Name:** * | Default is `<host_name>`. The current host name appears.  
You can also use the IP address or the computer name.  
Example:  
vmx6032 |
### Parameters

<table>
<thead>
<tr>
<th>Port:*</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default is 50,001. The port that is currently configured in the SAP NetWeaver Administrator appears automatically. If you use http, choose 50,000.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy Update Interval (Minutes):*</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifetime in minutes for verifying (update) a new client policy. Default is 0 minutes. By default, the Secure Login Client verifies a new client policy during the system startup of the client PC.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Timeout (Seconds):*</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network timeout in seconds before the connection is closed if the server does not respond. The default value is 45 seconds.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Update Policy on Startup (Default:Yes):</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>By default the Secure Login Client verifies a new client policy during the system startup of the client PC. You can use this parameter, to disable this feature. <strong>Yes</strong> Secure Login Client updates the client policy at startup. <strong>No</strong> Secure Login Client does not update the client policy at startup. Default value is <strong>Yes</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

### Actions at Policy Download

- Secure Login for SAP Single Sign-On Implementation Guide
- Parameter Reference
- PUBLIC 281
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Actions on SAP AS ABAP Application Settings:</strong></td>
<td>Existing profiles are handled as configured by action.</td>
</tr>
<tr>
<td></td>
<td><strong>Clean</strong></td>
</tr>
<tr>
<td></td>
<td>Deletes all existing profiles in the selected policy key before the given ones are written.</td>
</tr>
<tr>
<td></td>
<td><strong>Replace</strong></td>
</tr>
<tr>
<td></td>
<td>Replaces any existing profiles of the same name in the selected policy key with a given one.</td>
</tr>
<tr>
<td></td>
<td><strong>Keep</strong></td>
</tr>
<tr>
<td></td>
<td>Keeps any existing profiles of the same name in the selected policy. Does not overwrite the given one (default).</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>In a migration setup from SAP NetWeaver Single Sign-On 1.0 to 2.0, it makes sense to use <strong>Keep</strong>. The Secure Login Server keeps the profile group configuration of the Secure Login Server 1.0 for fallback purposes.</td>
</tr>
<tr>
<td></td>
<td>The default value is <strong>Clean</strong>.</td>
</tr>
<tr>
<td><strong>Action on Client Settings:</strong></td>
<td>Existing profiles are handled as configured by action.</td>
</tr>
<tr>
<td></td>
<td><strong>Clean</strong></td>
</tr>
<tr>
<td></td>
<td>Deletes all existing profiles in the selected policy key before the given ones are written.</td>
</tr>
<tr>
<td></td>
<td><strong>Replace</strong></td>
</tr>
<tr>
<td></td>
<td>Replaces any existing profiles of the same name in the selected policy key with a given one.</td>
</tr>
<tr>
<td></td>
<td><strong>Keep</strong></td>
</tr>
<tr>
<td></td>
<td>Keeps any existing profiles of the same name in the selected policy. Does not overwrite the given one (default).</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>In a migration setup from SAP NetWeaver Single Sign-On 1.0 to 2.0, it makes sense to use <strong>Keep</strong>. The Secure Login Server keeps the profile group configuration of the Secure Login Server 1.0 for fallback purposes.</td>
</tr>
</tbody>
</table>
6.2.5 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.

6.2.5.1 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy Configuration Name</strong></td>
<td>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.</td>
<td>Policy configuration with <code>SecureLoginModule20LDAP</code> in the authentication stack</td>
</tr>
</tbody>
</table>

| **Link to: Authentication and Single Sign-On** | 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)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reuse User Authentication Session</strong></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use Policy Configuration with Policy Name</td>
<td>If you choose this parameter, you can open a dropdown list and choose the policy configuration you want to use.</td>
<td>In the case of SAML 2.0 authentication, choose a policy configuration where SAML2LoginModule has been configured earlier.</td>
</tr>
<tr>
<td>Note</td>
<td>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 Standard Authentication Form in Select Authentication Form. For more information, see the related link.</td>
<td></td>
</tr>
<tr>
<td>Select Authentication Form with Policy Name</td>
<td>This parameter determines which authentication form the browser uses. The following authentication forms are possible:</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>If you are using SAML 2.0 authentication with Secure Login Web Client, choose Standard Authentication Form to enable the Secure Login Server to communicate with the identity provider that provides the users' identities. Whenever users start the Secure Login Web Client, they can choose the identity provider that manages the users' identity information and authentication.</td>
<td></td>
</tr>
<tr>
<td>Link to: Authentication and Single Sign-On</td>
<td>Using this link to the SAP NetWeaver Administrator, you can set the policy configuration in the SAP NetWeaver AS for Java.</td>
<td></td>
</tr>
</tbody>
</table>
6.2.6 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.

6.2.6.1 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.

The fields with the asterisk (*) are mandatory fields.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Name</td>
<td>Enter the country abbreviation in this field (C)</td>
<td>DE</td>
</tr>
<tr>
<td>Organizational Name</td>
<td>Enter the company name in this field (O)</td>
<td>Company xyz</td>
</tr>
<tr>
<td>Locality Name</td>
<td>Enter the regional information in this field (L)</td>
<td>Walldorf</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td><strong>Organization Unit Name</strong></td>
<td>Enter the company name in this field (OU)</td>
<td><strong>SAP Security Department</strong></td>
</tr>
<tr>
<td><strong>Validity Period (Minutes)</strong></td>
<td>Enter the period of validity of the certificate (CN). Default value is 600.</td>
<td>600</td>
</tr>
<tr>
<td><strong>Validity Offset</strong></td>
<td>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 -5.</td>
<td>-5</td>
</tr>
<tr>
<td><strong>Key Length</strong></td>
<td>Select the encryption key length for the server (1024, 1536, 2048, 3072, or 4096 bits).</td>
<td>2048</td>
</tr>
<tr>
<td><strong>Signature Algorithm</strong></td>
<td>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 sha256WithRSAEncryption</td>
<td>sha256WithRSAEncryption</td>
</tr>
</tbody>
</table>

### Related Information

X.509 Certificates [page 347]

### 6.2.6.2 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name *</td>
<td>Here you enter the common name. You can also use the following values from the destination:</td>
</tr>
<tr>
<td></td>
<td><strong>AUTH:USERID</strong></td>
</tr>
<tr>
<td></td>
<td><strong>AUTH:UPN</strong>                                                                      <strong>AUTH:DCS</strong></td>
</tr>
<tr>
<td></td>
<td><strong>PADDEDNAME</strong> Use this value to enable padding of the common name or any additionally defined certificate attributes.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>                                                                            You define the attributes for the certificate in the destination.</td>
</tr>
<tr>
<td>Country Name</td>
<td>Enter the two-character country code or use the above-mentioned values.</td>
</tr>
<tr>
<td>Organizational Name</td>
<td>Enter the organizational name or use the above-mentioned values.</td>
</tr>
<tr>
<td>Organizational Unit Name</td>
<td>Enter the organizational unit name or use the above-mentioned values.</td>
</tr>
<tr>
<td>Locality</td>
<td>Enter the locality or use the above-mentioned values.</td>
</tr>
<tr>
<td>Appendix Subject Name</td>
<td>Values: <strong>AUTH:DCS</strong> variable or a complete Relative Distinguished Name (RDN) Example: <strong>OU=SAP, CN=Demo</strong></td>
</tr>
<tr>
<td>Subject Alternative Name (RFC822 Name)</td>
<td>In this certificate attribute, the RFC822 name appears in a sequence.</td>
</tr>
<tr>
<td>Subject Alternative Name (Principal Name)</td>
<td>The principal name appears in a sequence.</td>
</tr>
</tbody>
</table>

### 6.2.6.3 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mapping Destinations</strong></td>
<td>Here you select the LDAP or Active Directory destination.</td>
</tr>
<tr>
<td><strong>Enable User Logon ID Mapping</strong></td>
<td>Activate this checkbox to enable user logon ID mapping. The default is not active.</td>
</tr>
<tr>
<td><strong>LDAP Search Attribute</strong></td>
<td>Here you enter the LDAP search attribute with search values. Default is <code>userPrincipalName</code>.</td>
</tr>
<tr>
<td><strong>Search Value</strong></td>
<td>The default LDAP search value is <code>AUTH:UPN</code>.</td>
</tr>
<tr>
<td><strong>Mapping Attributes</strong></td>
<td>Select one or several of the following mapping attributes values:</td>
</tr>
<tr>
<td></td>
<td><code>displayName</code></td>
</tr>
<tr>
<td></td>
<td><code>givenName</code></td>
</tr>
<tr>
<td></td>
<td><code>mail</code></td>
</tr>
<tr>
<td></td>
<td><code>name</code></td>
</tr>
<tr>
<td></td>
<td><code>sAMAccountName</code></td>
</tr>
<tr>
<td></td>
<td><code>sn</code> (first name)</td>
</tr>
<tr>
<td></td>
<td><code>userPrincipalName</code></td>
</tr>
<tr>
<td>Example:</td>
<td>If you add the attribute name <code>userPrincipal, name, mail</code>, the following resulting values are displayed in dropdown list for the Certificate Attribute Configuration section:</td>
</tr>
<tr>
<td></td>
<td>(LDAP:userPrincipal), (LDAP:name), (LDAP:mail).</td>
</tr>
</tbody>
</table>

### 6.2.6.4 Parameters for User Logon ID Padding

If you want to use user logon ID padding, use the following parameters.

**Note**

The fields with the asterisk (*) are mandatory fields.
Parameters for User Logon ID Padding

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>**Padding for *</td>
<td>Here you enter for which user name the padding is applied. Default: <strong>AUTH:USERID</strong></td>
</tr>
<tr>
<td>**Maximum Length *</td>
<td>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. Default value: <strong>12</strong></td>
</tr>
<tr>
<td></td>
<td>Example: &quot;LongUsernameSAP&quot; is cut off to &quot;LongUsername&quot; with the default settings.</td>
</tr>
<tr>
<td>**Padding Length *</td>
<td>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. Default value: None</td>
</tr>
<tr>
<td>**Padding Character *</td>
<td>The padding character is used to fill user names on the left side if their size is smaller than the configured padding length (Padding Length). Default value: None</td>
</tr>
<tr>
<td></td>
<td>Example: Padding Length = 11 and Padding Character = 0. The result is &quot;ShortName&quot; is extended to 00ShortName.</td>
</tr>
<tr>
<td></td>
<td>Typically this configuration is used if personnel numbers are used.</td>
</tr>
</tbody>
</table>

6.2.7 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
6.2.7.1 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.

**Note**

Parameters with * (asterisk) are mandatory.

### Parameters for Destination Management

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address/Host Name</strong> *</td>
<td>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. Example: <strong>ldapserver.demo.local</strong></td>
</tr>
</tbody>
</table>

**Note**

We recommend that you configure secure communication.

<table>
<thead>
<tr>
<th><strong>Port</strong> *</th>
<th>Enter a port for the LDAP or Microsoft Active Directory server. Example: <strong>389</strong></th>
</tr>
</thead>
</table>

**Use SSL for LDAP Access**

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.

**Note**

Before activating, import the server certificates into the keystore view *Trusted CAs* in SAP NetWeaver Key Storage.

<table>
<thead>
<tr>
<th>Connection Timeout (Milliseconds) *</th>
<th>The connection timeout in milliseconds: <strong>500</strong> 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 <strong>500</strong> milliseconds.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Provider Language *</th>
<th>Language of the LDAP or Microsoft Active Directory Server. Default is <strong>en-US</strong></th>
</tr>
</thead>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Details</th>
</tr>
</thead>
</table>
| **Login Base DN**| For Microsoft Active Directory:  
For LDAP servers other than Microsoft Active Directory:  
Enter the base DN of the LDAP Server (Start Search Path). There are several configuration options. Secure Login Server replaces the variable $USERID with the user name for user verification with the authentication server. |
| **Search Base DN**| 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 Login Base DN and user logon ID mapping with Microsoft Active Directory. When searching, the user mapping goes through all subtrees of the search base DN. |
| **Service User Name**| 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. |
| **Password**     | This parameter is only relevant for user mapping with an LDAP or Microsoft Active Directory Server. |
6.2.8 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 SAP NetWeaver Application Server for ABAP.

6.2.8.1 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 SAP NetWeaver Application Server for ABAP.

A wizard in Secure Login Administration Console enables you to easily create application server profile groups.

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Tab</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Group Name</strong></td>
<td>Name of the application server profile group</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Profiles Tab</strong></td>
<td></td>
</tr>
</tbody>
</table>
Application Server Authentication Profiles

You can add application server authentication profiles with the following types:

- **Registration Agent**
  Enables an administrator’s enrollment with credentials
- **Application**
  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.

**i Note**

Always add an application server profile of the profile type Registration Agent.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Server Authentication Profiles</strong></td>
<td>You can add application server authentication profiles with the following types:</td>
</tr>
<tr>
<td></td>
<td><strong>Registration Agent</strong></td>
</tr>
<tr>
<td></td>
<td>Enables an administrator’s enrollment with credentials</td>
</tr>
<tr>
<td></td>
<td><strong>Application</strong></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>System Identifiers</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

### 6.2.8.2 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 SAP NetWeaver Application Server for ABAP.

A wizard in Secure Login Administration Console enables you to easily create application server profiles.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Tab</strong></td>
<td>Name of the application server authentication profile</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Name of the application server authentication profile</td>
</tr>
<tr>
<td><strong>Profile ID</strong></td>
<td>This is a unique profile ID that is generated automatically.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>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.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Here you determine which kind of authentication profile your client has. In the context of certificate renewal, choose Secure Login Application Server Profile.</td>
</tr>
<tr>
<td></td>
<td>● Registration Agent</td>
</tr>
<tr>
<td></td>
<td>Enables an administrator’s enrollment with credentials</td>
</tr>
<tr>
<td></td>
<td>● Application</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Always add an application server authentication profile of the type Registration Agent.</td>
</tr>
</tbody>
</table>

**Authentication Configuration Tab**

**Use Policy Configuration**  
**Policy Configuration Name**  
In an application server authentication profile of the type Application, the user of Secure Login Administration Console authenticates runs on a policy configuration using a certificate-based login module.

**Certificate Configuration Tab**

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).

**CA for Issuing Certificates**

Already contains a value for the user CA.

**Certificate Template**

The certificate templates cover PSEs that belong to a special PSE type, for example SSL Server PSEs.

**Client Configuration Tab**

You find all the parameters in the parameters for certificate configuration (see the related link).
6.3 Parameter Overview for Secure Login Library

This parameter section gives you an overview of the parameters for Secure Login Library, for example, for certificate revocation, SNC, or the communication protocols used.

6.3.1 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.

6.3.1.1 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crl get</td>
<td>Downloads a CRL from a given CRL distribution point using a given URL (Web server or LDAP server). For an Active Directory server, the user must be a domain user, and ADS has to be configured in ldap.xml.</td>
</tr>
<tr>
<td>crl status</td>
<td>Shows the current status of the configuration and of the module</td>
</tr>
<tr>
<td>crl list</td>
<td>Shows the CRLs currently located in the local cache</td>
</tr>
<tr>
<td>crl remove</td>
<td>Removes the CRL from the local cache</td>
</tr>
<tr>
<td>crl show</td>
<td>Shows the content of a CRL file</td>
</tr>
<tr>
<td>crl store</td>
<td>Stores a CRL in the local cache. If the certificates contain a CRL distribution point, specify its location with -u so that the CRL can be found during certificate verification.</td>
</tr>
</tbody>
</table>

If you want to know how you can use the CRL command, for example to download CRLs, see the related link.
### 6.3.1.2 Configuration Parameters of pkix.xml

The following table contains all parameters and parameter options that are available in pkix.xml.

If you want to know how to configure the CRL tool with pkix.xml, see the related link.

#### Configuration parameters of pkix.xml

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile (with parameter options)</td>
<td></td>
<td>CRL checking profile</td>
</tr>
<tr>
<td>acceptNoBCwithKeyUsage</td>
<td>true/false</td>
<td>pkix.xml defines that CA certificates must have the BasicConstraint extension. Default: true</td>
</tr>
<tr>
<td>revCheck</td>
<td>NO/CRL</td>
<td>Enables/disables revocation checking. Default: NO</td>
</tr>
<tr>
<td>certificatePolicies</td>
<td>noCheck/&lt;trusted_certificate_policy_object_identifiers&gt;</td>
<td>List of trusted certificate policy object identifiers separated by a semicolon (;). Default: noCheck</td>
</tr>
</tbody>
</table>

**Note**

If the parameter `acceptNoBCwithKeyUsage` has the value `true`, the system checks whether certificates without the BasicContraints extension have the keyCertSign key usage. In this case, they are accepted as CA certificates. If the parameter `acceptNoBCwithKeyUsage` has the value `false`, the certificates are not accepted.

### 6.3.1.3 Configuration Parameters of base.xml

The following table contains all parameters and parameter options that are available in base.xml.

If you want to know how to configure the CRL tool with base.xml, see the related link.

---

**Related Information**

- Downloading CRLs with the CRL Tool [page 130]
- pkix.xml [page 132]
Configuration parameters of base.xml

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>verification onlineaccess</td>
<td>true/false</td>
<td>If set to true, missing CRLs and certificates are being searched online. Default: false</td>
</tr>
<tr>
<td>usepkicache</td>
<td>true/false</td>
<td>Specifies whether a CRL check uses a cache directory or a remote LDAP directory. Default: false</td>
</tr>
<tr>
<td>pkicachedir</td>
<td>&lt;directory_path&gt;</td>
<td>Location of dbcert and dbcris directories. Default: &lt;PSE_directory&gt;</td>
</tr>
<tr>
<td>proxy(with parameter options)</td>
<td></td>
<td>Defines the proxy if you use a proxy server for the CRL request.</td>
</tr>
<tr>
<td>url</td>
<td>&lt;host_name:port&gt;</td>
<td>Host name and port number of the proxy</td>
</tr>
</tbody>
</table>

**Note**

This parameter does not support proxy URLs.

| name(with parameter options) |  | Distinguished Name |
|-------------------------------|  | Delimiters of the values. Default: double-quote |

**Related Information**

base.xml [page 133]

### 6.3.1.4 Configuration Parameters of ldap.xml

The following table contains all parameters and parameter options that are available in ldap.xml.

If you want to know how to configure the CRL tool with ldap.xml, see the related link.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout</td>
<td>&lt;milliseconds&gt;</td>
<td>Timeout of the LDAP server in milliseconds. Default: 40000</td>
</tr>
</tbody>
</table>
Related Information

ldap.xml [page 134]

6.3.2 Communication and Protocol Parameters (Server and Client)

In the file gss.xml, you can configure the SNC communication protocol for server-to-server and client-to-server communication.

The configuration file gss.xml enables you to configure the SNC communication protocol for server-to-server and client-to-server communication.

6.3.2.1 Reference of the Communication Protocol Parameters (Server)

The following table contains the parameters that are valid for SNC on the server:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KerberosClientNameUserPart</td>
<td>noconversion/lowercase/upper</td>
<td>Converts the user part of the SNC Kerberos name to uppercase, lowercase, or no conversion takes place. Default: uppercase</td>
</tr>
<tr>
<td>Parameter</td>
<td>Values</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>KerberosClientNameDomainPart</td>
<td>noconversion/lowercase/uppercase/remove</td>
<td>Converts the domain part of the SNC Kerberos name to uppercase, lowercase, or no conversion takes place. If you use the value remove, you can remove @ and the domain part. Default: uppercase</td>
</tr>
<tr>
<td>namecharset</td>
<td>utf8/latin1</td>
<td>Character set used to exchange names with the application. Default: latin1</td>
</tr>
<tr>
<td>nameconversions(with parameter options)</td>
<td></td>
<td>Replaces excessively long name components with shorter ones. Useful when a server application stores the client name in a database field with an insufficient maximum size.</td>
</tr>
<tr>
<td>nameencoding</td>
<td>UTF8/T.61</td>
<td>Character set used for encoding Distinguished Names in ASN.1. Default: UTF8</td>
</tr>
<tr>
<td>nameschema</td>
<td>sapcryptolib/rfc2256</td>
<td>Schema for the sequence and keywords of the name elements. Default: rfc2256</td>
</tr>
<tr>
<td>searchstr</td>
<td>&lt;long_client_name&gt;</td>
<td>Enter the complete client name for name conversion.</td>
</tr>
<tr>
<td>replstr</td>
<td>&lt;short_client_name&gt;</td>
<td>Enter the abbreviated client name to save storage space in the database.</td>
</tr>
</tbody>
</table>
|UpperCaseClientName                    | true/false                           | During SNC communication, the client sends the Distinguished Name (DN) of the client certificate in mixed case by default. Set to true to send the DN in uppercase.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClientNameSource</td>
<td>AltNameEMail</td>
<td>Subject alternative name from the user certificate to be sent as the SAP SNC name. Enter the options separated by a space. The server tries the subject alternative names in this order. It takes the first option it can use.</td>
</tr>
<tr>
<td></td>
<td>RFC 822 name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AltNameEMAILWithoutDomain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AltNameDNS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AltNameDName</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AltNameURI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>URI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Directory name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AltNameIP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AltNameUPN</td>
<td>otherName with object identifier. Here the Microsoft User Principal Name is used (otherName type with OID 1.3.6.1.4.1.311.20.2.3).</td>
</tr>
<tr>
<td></td>
<td>AltNameEMAILWithoutDomain</td>
<td>RFC 822 name without domain. Here you can use the local part of an E-mail address without the domain part (j.smith instead of <a href="mailto:j.smith@company.com">j.smith@company.com</a>).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AltNameUPNWithoutDomain</td>
<td>otherName with object identifier and without domain. Here the Microsoft User Principal Name is used (otherName type with OID 1.3.6.1.4.1.311.20.2.3) without the domain part of the e-mail address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td>Distinguished Name</td>
<td>Default is <code>&lt;empty&gt;</code>. In this case, the Subject (Distinguished Name) is used.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Values</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>protocol_1993 (with parameter options)</td>
<td>&lt;SNC_CRYPTOLIB_protocol&gt;</td>
<td>Specifies whether to use the 1993 communication protocol, which is compatible to SAPCRYPTOLIB 5.5.</td>
</tr>
<tr>
<td>use</td>
<td>true/false</td>
<td>Specifies whether or not the 1993 communication protocol is used. Default: true</td>
</tr>
<tr>
<td>algs_encr</td>
<td>aes256 aes192 aes128 des3</td>
<td>List of encryption algorithms available. The system uses the first one that is possible. Default: all</td>
</tr>
<tr>
<td>algs_hash</td>
<td>sha512 sha384 sha256 shal ripemd160</td>
<td>List of available hash algorithms: The system uses the first algorithm that is possible. Default: all</td>
</tr>
<tr>
<td>acceptsigmode</td>
<td>true/false</td>
<td>Specifies whether the client key used for digital signatures is accepted as an authentication method. Default: true</td>
</tr>
<tr>
<td>acceptencrmode</td>
<td>true/false</td>
<td>Specifies whether the client key used for encryption is accepted as an authentication method. Default: true</td>
</tr>
<tr>
<td>acceptedttl</td>
<td>&lt;temporary_key_lifetime&gt;</td>
<td>Accepted lifetime of temporary keys (digital signature to keep the session alive) in seconds. Default: 86400 (24 hours)</td>
</tr>
<tr>
<td>protocol_2010 (with parameter options)</td>
<td>&lt;SNC_CRYPTOLIB_protocol&gt;</td>
<td>Defines whether the server accepts the 2010 communication protocol</td>
</tr>
<tr>
<td>use</td>
<td>true/false</td>
<td>Enables/disables the use of the 2010 protocol. This protocol supports authentication with X.509 and Kerberos certificates.</td>
</tr>
<tr>
<td>acceptedttl</td>
<td>&lt;temporary_key_lifetime&gt;</td>
<td>Accepted lifetime of temporary keys (digital signature to keep the session alive) in seconds. Default: 86400 (24 hours)</td>
</tr>
<tr>
<td>ciphers</td>
<td>aes256 aes128 rc4</td>
<td>Algorithms used for handshake and application data protection. Default: all</td>
</tr>
<tr>
<td>data_macs</td>
<td>HMAC-SHA256 HMAC-SHA1 HMAC-SHA512 HMAC-RIPEMD160</td>
<td>Algorithms used for handshake and application data protection. Default: HMAC-SHA256 HMAC-SHA1</td>
</tr>
</tbody>
</table>
### 6.3.2.2 Reference of the Communication Protocol Parameters (Client)

The following table contains the parameters that are valid for SNC on the client:

A gss.xml file also exists in the client. You must specify the same communication protocol on both sides (client and server). Depending on your SNC CRYPTOLIB, use either protocol_1993 or protocol_2010.

**Configuration Parameters of gss.xml (Client Functions Only)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nameencoding</td>
<td><strong>UTF8/T.61</strong></td>
<td>Character set used for encoding Distinguished Names in ASN.1. Default: UTF8</td>
</tr>
<tr>
<td>nameschema</td>
<td><strong>sapcryptolib/rfc2256</strong></td>
<td>Schema for the sequence and keywords of the name elements. Default: rfc2256</td>
</tr>
<tr>
<td>protocol_1993</td>
<td><strong>&lt;SNC_CRYPTOLIB_protocol&gt;</strong></td>
<td>Specifies whether to use the 1993 communication protocol, which is compatible to SAPCRYPTOLIB 5.5.</td>
</tr>
<tr>
<td>use</td>
<td><strong>true/false</strong></td>
<td>Specifies whether or not to use the 1993 communication protocol. Default: true</td>
</tr>
<tr>
<td>algs_encr</td>
<td><strong>aes256 aes192 aes128 des3</strong></td>
<td>List of encryption algorithms available. The system uses the first one that is possible. Default: all</td>
</tr>
<tr>
<td>algs_hash</td>
<td><strong>sha512 sha384 sha256 sha1 ripemd160</strong></td>
<td>List of available hash algorithms: The system uses the first algorithm that is possible. Default: all</td>
</tr>
<tr>
<td>authop</td>
<td><strong>enc (encryption certificate) sig (signature certificate) sigsession (signature certificates for key cached for further sessions) auto (automatic)</strong></td>
<td>Specifies the authentication mode in the client. Default: auto</td>
</tr>
<tr>
<td>age</td>
<td><strong>&lt;period_in_seconds&gt;</strong></td>
<td>Specifies a period of the key validity before the signing (in seconds). This period acts as a tolerance period if system times vary by a couple of minutes. Default: 600</td>
</tr>
<tr>
<td>ttl</td>
<td><strong>&lt;period_in_seconds&gt;</strong></td>
<td>Validity of temporary key in seconds. Default: None</td>
</tr>
<tr>
<td>protocol_2010</td>
<td><strong>&lt;SNC_CRYPTOLIB_protocol&gt;</strong></td>
<td>Defines whether the server accepts the 2010 communication protocol</td>
</tr>
<tr>
<td>Parameter</td>
<td>Values</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>use</td>
<td>true/false</td>
<td>Enables/disables the use of the 2010 protocol. This protocol supports authentication with X.509 and Kerberos certificates.</td>
</tr>
<tr>
<td>ciphers</td>
<td>aes256 aes128 rc4</td>
<td>Algorithms used for handshake and application data protection. Default: all</td>
</tr>
<tr>
<td>data_macs</td>
<td>HMAC-SHA256 HMAC-SHA1 HMAC-SHA512 HMAC-RIPEDM160</td>
<td>Algorithms used for handshake and application data protection. Default: HMAC-SHA256 HMAC-SHA1</td>
</tr>
<tr>
<td>ParallelSessions</td>
<td>true/false</td>
<td>Enable use of signature certificate with a temporary key. Default: false</td>
</tr>
<tr>
<td>ParallelSessionsTTL</td>
<td>&lt;period_in_seconds&gt;</td>
<td>Validity of temporary key in seconds. Default: 86400 (one day)</td>
</tr>
</tbody>
</table>

### 6.4 Parameter Overview for the SAP Cryptographic Library

This section contains the parameters for the SAP Cryptographic Library, for example, parameters for SNC.

### 6.4.1 SNC Parameters for the SAP Cryptographic Library

SNC profile parameters for X.509 and Kerberos certificates and SPNego profile parameters in SAP NetWeaver Application Server for 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 SAP NetWeaver Application Server for ABAP (transaction RZ10).

### 6.4.1.1 SNC Parameters for X.509 Configuration

Use these parameters to configure SNC in the SAP NetWeaver Application Server for ABAP.

In the following, you find an overview of the profile parameters you can use to configure the SNC parameters in SAP NetWeaver Application Server for ABAP. (transaction RZ10).
### SNC Parameters for the SAP Cryptographic Library

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snc/enable</code></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Activate SNC</td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Deactivate SNC</td>
</tr>
<tr>
<td><code>snc/gssapi_lib</code></td>
<td>Define the SNC library.</td>
</tr>
<tr>
<td></td>
<td><code>${DIR_EXECUTABLE}${DIR_SEP}${FT_DLL_PREFIX}sapcrypto${FT_DLL}</code></td>
</tr>
<tr>
<td><code>snc/identity/as</code></td>
<td>Define the SNC name of the SAP server's security token. X.509 Certificate Token</td>
</tr>
<tr>
<td></td>
<td><code>p:&lt;X.509_Distinguished_Name&gt;</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>p:CN=ABC, OU=SAP Security</code></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><code>snc/data_protection/max</code></td>
<td>3</td>
</tr>
<tr>
<td><code>snc/data_protection/min</code></td>
<td>2</td>
</tr>
<tr>
<td><code>snc/data_protection/use</code></td>
<td>3</td>
</tr>
<tr>
<td><code>snc/r3int_rfc_secure</code></td>
<td>0</td>
</tr>
<tr>
<td><code>snc/r3int_rfc_qop</code></td>
<td>8</td>
</tr>
<tr>
<td><code>snc/accept_insecure_cpic</code></td>
<td>1</td>
</tr>
<tr>
<td><code>snc/accept_insecure_gui</code></td>
<td>1 Accept insecure communication</td>
</tr>
<tr>
<td></td>
<td>Use this value if both insecure and secure communication is to be allowed for SAP GUI.</td>
</tr>
<tr>
<td></td>
<td>0 Disallow insecure communication</td>
</tr>
<tr>
<td></td>
<td>Use this value only if secure communication is to be allowed only (no insecure communication) for SAP GUI.</td>
</tr>
<tr>
<td></td>
<td>U User-defined (User Management SU01)</td>
</tr>
<tr>
<td></td>
<td>Use this value if insecure or secure communication for SAP GUI application is to be configured in the user management tool (SU01).</td>
</tr>
<tr>
<td></td>
<td>We recommend that you set this value to 1. If you want to enforce higher security, change this value to 0 (for all) or U (user dependent).</td>
</tr>
</tbody>
</table>
### 6.4.1.2 SNC Parameters for Kerberos Configuration

**SNC parameters for AS ABAP**

**SNC Parameters for the SAP Cryptographic Library**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>snc/accept_insecure_rfc</td>
<td>1</td>
</tr>
<tr>
<td>snc/permit_insecure_start</td>
<td>1</td>
</tr>
<tr>
<td>snc/force_login_screen</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>
| snc/enable         | 1 Activate SNC
0 Deactivate SNC |
| snc/gssapi_lib     | Define the SNC library.
$(DIR_EXECUTABLE)$(DIR_SEP)$(FT_DLL_PREFIX)sapcrypto$(FT_DLL) |
| snc/identity/as    | Define the SNC name of the SAP server’s security token. Kerberos Token
p:CN=<service_User_Principal_Name> |
|                   | Example:
p:CN=KerberosABC8DEMO.LOCAL |
|                   | 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. |
| snc/data_protection/max | 3                                                                  |
| snc/data_protection/min  | 2                                                                  |
| snc/data_protection/use   | 3                                                                  |
| snc/r3int_rfc_secure    | 0                                                                  |
| snc/r3int_rfc_qop       | 8                                                                  |
| snc/accept_insecure_cpic | 1                                                                  |
### 6.4.1.3  Profile Parameters for SPNego

SPNego profile parameters for SAP NetWeaver Application Server for ABAP

(If applicable) SPNego Profile Parameters for SAP Cryptographic Library

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>spnego/enable</td>
<td>Set to 1.</td>
</tr>
</tbody>
</table>

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>
| snc/accept_insecure_gui | 1 Accept insecure communication  
Use this value if both insecure and secure communication is to be allowed for SAP GUI.  
0 Disallow insecure communication  
Use this value only if secure communication is to be allowed only (no insecure communication) for SAP GUI.  
U User-defined (User Management SU01)  
Use this value if insecure or secure communication for SAP GUI application is to be configured in the user management tool (SU01).  
We recommend that you set this value to 1. If you want to enforce higher security, change this value to 0 (for all) or U (user dependent). |
<p>| snc/accept_insecure_rfc | 1                      |
| snc/permit_insecure_start | 1                    |
| snc/force_login_screen  | 0                      |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>spnego/krbsnego_lib</code></td>
<td>Set to the path to the Kerberos library (SAP Cryptographic Library or Secure Login Library of SAP Single Sign-On 2.0 or higher).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>For Secure Login Library, use the path to the respective file of SAP Single Sign-On.</td>
</tr>
<tr>
<td></td>
<td><strong>Kerberos Library File Names</strong></td>
</tr>
<tr>
<td></td>
<td><strong>File Name</strong></td>
</tr>
<tr>
<td></td>
<td>sapcrypto.dll</td>
</tr>
<tr>
<td></td>
<td>libsapcrypto.so</td>
</tr>
<tr>
<td></td>
<td>libsapcrypto.sl</td>
</tr>
<tr>
<td><code>spnego/construct_SNC_name</code></td>
<td>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 111.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Changing this dynamic profile parameter does not require a restart.</td>
</tr>
</tbody>
</table>
7 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**

Troubleshooting Guide for SAP Single Sign-On

7.1 Troubleshooting Secure Login Client

This section describes some troubleshooting issues of Secure Login Client and how to solve them.

**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 62]
### 7.1.1 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.

![SAP GUI for Windows 720](image)

#### 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.
     3. Try with the option Use Profile for SAP Applications if the desired profile is used.
2. Verify if SNC is enabled in SAP GUI for the desired SAP server.
3. 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

7.1.2 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

7.1.3 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 or the Secure Login 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 135]

7.1.4 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”.

![SAP GUI for Windows 720](image)

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
7.1.5 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 206]
Parameters for Destination Management Configuration [page 289]

7.1.6 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 Secure Login Library’s GSS module. You find the complete list of the SNC error codes in the related link.
Related Information

SNC Error Codes [page 317]

7.2 Troubleshooting Secure Login Library

This section provides further information about how to perform troubleshooting for Secure Login Library.

7.2.1 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 or the Secure Login Library is installed correctly.
   Verify the installation described in section Secure Login Library Installation [page 84].
3. Verify the SNC configuration.
   a. Log on to SAP ABAP server using SAP GUI and start transaction RZ10.
   b. Choose the instance 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 or the Secure Login 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 or a Secure Login Library with 32-bit or 64 bit. To determine the architecture, use the following command:
   ```
   file sapgenpse
   ```
Related Information

Configuration of the Cryptographic Library [page 96]
Configuring Tracing for the Cryptographic Library [page 135]

7.2.2 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 or the Secure Login Library is installed correctly. Verify the installation described in section Secure Login Library Installation [page 84].
3. Verify the SNC configuration.
   a. Log on to the AS ABAP server using SAP GUI and start transaction RZ10.
   b. Choose the instance 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 Secure Login Library PSE environment.
   a. (For SAP Cryptographic Library) 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. (For Secure Login Library) Start a command line shell and change to the Secure Login Library folder $(DIR_INSTANCE)/SLL.
   c. Set the environment SECUDIR=$(DIR_INSTANCE)/sec.
   d. Use the command: sapgenpse seclogin -O -l <SAP_service_user>.

Example

Microsoft Windows: sapgenpse seclogin -O -l SAPServiceABC
Linux: sapgenpse seclogin -O -l abcadm

6. Enable the trace of the SAP Cryptographic Library or of the Secure Login Library and analyze the problem.
7.2.3 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 or of the Secure Login 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> -N

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>\SAPNSCSPERB.pse -O <system_user> -N

See also SAP Note 1942749.
Related Information

Creating Keytab for Kerberos [page 104]

7.2.4 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 or a Secure Login Library configuration cannot find the SNC name in the database. For further information, see the related SAP Note.

Related Information


7.2.5 Monitoring the Secure Login Library or 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 SAP NetWeaver AS for 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 ➔.

7.2.6 Error Occurred with sapgenpse

If errors occur with sapgenpse, see the following SAP Note.


7.2.7 SNC Error Codes

In case of an error from a calling application with the SAP Cryptographic Library or with the Secure Login 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 or of the Secure Login Library and analyze traces. For more information, see the related link.

Related Information
Configuring Tracing for the Cryptographic Library [page 135]

7.3 Troubleshooting Secure Login Server

This section gives additional information about troubleshooting for Secure Login Server.

7.3.1 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.
7.3.2 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).

7.3.3 Error Codes of SAP Stacktrace Errors

This chapter describes the error codes and return codes, their meaning and possible corrections.

7.3.3.1 SAP Stacktrace Error Codes

This table contains the SAP stacktrack error codes.

<table>
<thead>
<tr>
<th>Runtime Error Codes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALL_BACK_ENTRY_NOT_FOUND</td>
<td>The called function module is not released for RFC.</td>
</tr>
<tr>
<td>CALL_FUNCTION_DEST_TYPE</td>
<td>The type of the destination is not allowed.</td>
</tr>
<tr>
<td>CALL_FUNCTION_NO_SENDER</td>
<td>Current function is not called remotely.</td>
</tr>
<tr>
<td>CALL_FUNCTION_DESTINATION_NO_T</td>
<td>Missing communication type (I for internal connection, 3 for ABAP) when executing an asynchronous RFC.</td>
</tr>
<tr>
<td>CALL_FUNCTION_NO_DEST</td>
<td>The specified destination does not exist.</td>
</tr>
<tr>
<td>CALL_FUNCTION_OPTION_OVERFLOW</td>
<td>Maximum length of options for the destination exceeded.</td>
</tr>
<tr>
<td>CALL_FUNCTION_NO_LB_DEST</td>
<td>The specified destination (in load distribution mode) does not exist.</td>
</tr>
<tr>
<td>Runtime Error Codes</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CALL_FUNCTION_NO_RECEIVER</td>
<td>Data received for unknown CPI-C connection.</td>
</tr>
<tr>
<td>CALL_FUNCTION_NOT_REMOTE</td>
<td>The function module being called is not flagged as being &quot;remotely&quot; callable.</td>
</tr>
<tr>
<td>CALL_FUNCTION_REMOTE_ERROR</td>
<td>While executing an RFC, an error occurred that has been logged in the calling system.</td>
</tr>
<tr>
<td>CALL_FUNCTION_SIGNON_INCOMPL</td>
<td>Logon data for the user is incomplete.</td>
</tr>
<tr>
<td>CALL_FUNCTION_SIGNON_INTRUDER</td>
<td>Logon attempt in the form of an internal call in a target system not allowed.</td>
</tr>
<tr>
<td>CALL_FUNCTION_SIGNON_INVALID</td>
<td>RFC from external program without valid user ID.</td>
</tr>
</tbody>
</table>
| CALL_FUNCTION_SIGNON_REJECTED | Logon attempt in target system without valid user ID. This error code may have any of the following meanings:  
  - Incorrect password or invalid user ID.  
  - User locked.  
  - Too many logon attempts.  
  - Error in authorization buffer (internal error).  
  - No external user check.  
  - Invalid user type.  
  - Validity period of the user exceeded. |
| CALL_FUNCTION_SINGLE_LOGIN_REJ | No authorization to log on as a trusted system. The error code may have any of the following meanings:  
  - Incorrect logon data for valid security ID.  
  - Calling system is not a trusted system or security ID is invalid.  
  - 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*.  
  - Time stamp of the logon data is invalid. |
<p>| 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. |
| CALL_FUNCTION_TASK_YET_OPEN | For asynchronous RFC only: the specified task is already open. |</p>
<table>
<thead>
<tr>
<th>Runtime Error Codes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALL_FUNCTION_NO_AUTH</td>
<td>No RFC authorization.</td>
</tr>
<tr>
<td>CALL_RPERF_SLOGIN_AUTH_ERROR</td>
<td>No trusted authorization for RFC caller and trusted system.</td>
</tr>
<tr>
<td>CALL_RPERF_SLOGIN_READ_ERROR</td>
<td>No valid trusted entry for the calling system.</td>
</tr>
<tr>
<td>RFC_NO_AUTHORITY</td>
<td>No RFC authorization for user.</td>
</tr>
<tr>
<td>CALL_FUNCTION_BACK_REJECTED</td>
<td>Destination “BACK” is not permitted in current program.</td>
</tr>
<tr>
<td>CALL_XMLRFC_BACK_REJECTED</td>
<td>Destination “BACK” is not permitted in current program.</td>
</tr>
<tr>
<td>CALL_FUNCTION_DEST_SCAN</td>
<td>Error while evaluating RFC destination.</td>
</tr>
<tr>
<td>CALL_FUNCTION_CONFLICT_TAB_TYP</td>
<td>Type conflict while transferring table.</td>
</tr>
<tr>
<td>CALL_FUNCTION_CREATE_TABLE</td>
<td>No memory available for creating a local internal table.</td>
</tr>
<tr>
<td>CALL_FUNCTION_UC_STRUCT</td>
<td>Type conflict while transferring structure.</td>
</tr>
<tr>
<td>CALL_FUNCTION_DEEP_MISMATCH</td>
<td>Type conflict while transferring structure.</td>
</tr>
<tr>
<td>CALL_FUNCTION_WRONG_VALUE_LENG</td>
<td>Invalid data type while transferring parameters.</td>
</tr>
<tr>
<td>CALL_FUNCTION_PARAMETER_TYPE</td>
<td>Invalid data type while transferring parameters.</td>
</tr>
<tr>
<td>CALL_FUNCTION_ILLEGAL_DATA_TYP</td>
<td>Invalid data type while transferring parameters.</td>
</tr>
<tr>
<td>CALL_FUNCTION_ILLEGAL_INT_LEN</td>
<td>Type conflict while transferring an integer.</td>
</tr>
<tr>
<td>CALL_FUNCTION_Ill_INT2_Leng</td>
<td>Type conflict while transferring an integer.</td>
</tr>
<tr>
<td>CALL_FUNCTION_Ill_FLOAT_FORMAT</td>
<td>Type conflict while transferring a floating point number.</td>
</tr>
<tr>
<td>CALL_FUNCTION_Ill_FLOAT_Leng</td>
<td>Type conflict while transferring a floating point number.</td>
</tr>
<tr>
<td>CALL_FUNCTION_ILLEGAL_LEAVE</td>
<td>Invalid LEAVE statement on RFC Server.</td>
</tr>
<tr>
<td>CALL_FUNCTION_OBJECT_SIZE</td>
<td>Type conflict while transferring a reference.</td>
</tr>
<tr>
<td>CALL_FUNCTION_ROT_REGISTER</td>
<td>Type conflict while transferring a reference.</td>
</tr>
</tbody>
</table>
7.3.4 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.

7.3.5 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.
7.3.5.1 Enable Fully Qualified Distinguished Name for SAP NetWeaver 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.

**7.3.5.2 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
   ```
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.

### 7.3.6 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.

### 7.3.7 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 or for the Secure Login Library.
5. (If Ping Destination failed) Verify whether the SAP Cryptographic Library or the Secure Login Library is installed correctly. Verify the installation described in section Secure Login Library Installation [page 84].
6. Verify whether an SNC certificate was provided to the SAP Cryptographic Library or to the Secure Login 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/SLL.
   - 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.
Enable trace for the SAP Cryptographic Library or for the Secure Login 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 or of the Secure Login Library in the section of the cryptographic library.

**Related Information**

Configuring Tracing for the Cryptographic Library [page 135]

**7.3.8 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.

**7.3.9 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 289]

**7.3.10 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.
## 7.3.10.1 Secure Login Web Client Error Codes

The following table provides you with an overview of the Secure Login Server error codes.

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Error Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Error 0x01</td>
<td>Problem during download or saving the native components.</td>
<td>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. To remedy the error, it is generally sufficient to restart SAP GUI and your browser. Thus the configuration is newly read in.</td>
</tr>
<tr>
<td>Client Error 0x02</td>
<td>Insecure HTTP connection to Secure Login Server is rejected.</td>
<td>Attempted buildup of an HTTP connection instead of a (secured) HTTPS connection. For more information, see Forced Use of HTTPS [page 162].</td>
</tr>
<tr>
<td>Client Error 0x03</td>
<td>Checksum error in local or remote Secure Login Web Client libraries.</td>
<td>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. To remedy the error, restart your browser, log off from SAP GUI, and log on again. This removes the locking mechanism. 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.</td>
</tr>
</tbody>
</table>

⚠️ **Caution**

If this error persists, the native libraries on your server system might be manipulated. In the log file on...
<table>
<thead>
<tr>
<th>Error Code</th>
<th>Error Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Error 0x04</td>
<td>Unknown or untrustworthy Secure Login Server user certificate issuer is rejected.</td>
<td>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.</td>
</tr>
<tr>
<td>Client Error 0x05</td>
<td>This Platform is not supported by the web client, abort.</td>
<td>The Secure Login Web Client can only run in Mac OS X or Microsoft Windows, otherwise you get this error.</td>
</tr>
<tr>
<td>Client Error 0x06</td>
<td>Communication Error with the native SLWC agent, abort.</td>
<td>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 Secure Login Web Client while the Secure Login Web Client was running. Try again or contact your IT support if the issue persists.</td>
</tr>
<tr>
<td>Client Error 0x07</td>
<td>Please install SAP GUI</td>
<td>This happens when the SAP GUI is not installed on the users' client. Users must install the SAP GUI on their systems.</td>
</tr>
<tr>
<td>Client Error 0x08</td>
<td>Web Client is running in Web Adapter Mode, but no Web Adapter installation is found, abort.</td>
<td>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.</td>
</tr>
<tr>
<td>Client Error 0x09</td>
<td>Cannot load configuration for web client.</td>
<td>The Secure Login Web Client could not load the configuration. Contact the</td>
</tr>
</tbody>
</table>

Note: This error only occurs in Microsoft Windows and Mac OS operating systems.

If this error occurs, proceed as described in *PKI Check before Storing in a Certificate Store* [page 164].
### Error Code Table

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Error Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

### 7.3.11 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 |

### 7.3.12 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.

#### 7.3.12.1 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. |
7.3.12.2 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:

<table>
<thead>
<tr>
<th>Category</th>
<th>Default Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications/Common/Security/SecureLoginServer/Authentication</td>
<td>INFO</td>
</tr>
<tr>
<td>Applications/Common/Security/SecureLoginServer/Certificates</td>
<td>INFO</td>
</tr>
<tr>
<td>Applications/SecureLoginServer/Server</td>
<td>INFO</td>
</tr>
<tr>
<td>Applications/Common/Security/NetweaverSSO/Certificates</td>
<td>INFO</td>
</tr>
<tr>
<td>Applications/Common/Security/NetweaverSSO/KeyStore</td>
<td>INFO</td>
</tr>
<tr>
<td>Applications/NetweaverSSO/Server</td>
<td>INFO</td>
</tr>
<tr>
<td>Applications/SecureLoginServer/SLAC</td>
<td>INFO</td>
</tr>
<tr>
<td>System/Security/SecureLoginServer/SLAC</td>
<td>INFO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.sap.securelogin.* (and subnodes)</td>
<td>INFO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap.com/SecureLoginServer</td>
</tr>
</tbody>
</table>
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

### 7.3.12.3 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.
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADS</td>
<td>Active Directory Service</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CAPI</td>
<td>Microsoft Crypto API</td>
</tr>
<tr>
<td>CSP</td>
<td>Cryptographic Service Provider</td>
</tr>
<tr>
<td>DN</td>
<td>Distinguished Name</td>
</tr>
<tr>
<td>EAR</td>
<td>Enterprise Application Archive</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper Text Transport Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hyper Text Transport Protocol with Secure Socket Layer (SSL)</td>
</tr>
<tr>
<td>IAS</td>
<td>Internet Authentication Service (Microsoft Windows Server 2003)</td>
</tr>
<tr>
<td>JAAS</td>
<td>Java Authentication and Authorization Service</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>NPA</td>
<td>Network Policy and Access Services (Microsoft Windows Server 2008)</td>
</tr>
<tr>
<td>PEM</td>
<td>Privacy Enhanced Mail</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PKCS</td>
<td>Public Key Cryptography Standards</td>
</tr>
<tr>
<td>PKCS#10</td>
<td>Certification Request Standard</td>
</tr>
<tr>
<td>PKCS#11</td>
<td>Cryptographic Token Interface Standard</td>
</tr>
<tr>
<td>PKCS#12</td>
<td>Personal Information Exchange Syntax Standard</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PSE</td>
<td>Personal Security Environment</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>RFC</td>
<td>Remote function call (SAP NetWeaver term)</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir and Adleman</td>
</tr>
<tr>
<td>SAR</td>
<td>SAP Archive</td>
</tr>
<tr>
<td>SCA</td>
<td>Software Component Archive</td>
</tr>
<tr>
<td>SLAC</td>
<td>Secure Login Administration Console</td>
</tr>
<tr>
<td>SLC</td>
<td>Secure Login Client</td>
</tr>
<tr>
<td>SLL</td>
<td>Secure Login Library</td>
</tr>
<tr>
<td>SLS</td>
<td>Secure Login Server</td>
</tr>
<tr>
<td>SLWC</td>
<td>Secure Login Web Client</td>
</tr>
<tr>
<td>SNC</td>
<td>Secure Network Communication (SAP term)</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>UPN</td>
<td>User Principal Name</td>
</tr>
<tr>
<td>WAR</td>
<td>Web Archive</td>
</tr>
<tr>
<td>WAS</td>
<td>Web Application Server</td>
</tr>
</tbody>
</table>
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.

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 211] and Using External User Certification Authorities [page 212].

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.
10 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.

10.1 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 SAP NetWeaver AS for 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.

<table>
<thead>
<tr>
<th>Title</th>
<th>SAP Note</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Note SAP Single Sign-On 2.0</td>
<td>2039196</td>
<td>The release note for SAP Single Sign-On 2.0 describes the components and features of this release.</td>
</tr>
<tr>
<td>Central note for SAP Single Sign-On 2.0</td>
<td>1912175</td>
<td>The central note provides product-specific information.</td>
</tr>
</tbody>
</table>

**Related Information**

- [https://service.sap.com/securitynotes](https://service.sap.com/securitynotes)
- [http://scn.sap.com/community/security](http://scn.sap.com/community/security)
- [http://support.sap.com/solutionmanager](http://support.sap.com/solutionmanager)

**10.2 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**

<table>
<thead>
<tr>
<th>Entity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Login Library</td>
<td>Optional cryptographic library and security protocol provider for SAP NetWeaver Application Server for ABAP (SNC), SAP RFC (SNC), and SAP NetWeaver Application Server for Java (SSL). Supports X.509 and Kerberos security tokens. The SAP Cryptographic Library is the default cryptographic library of the SAP NetWeaver Application Server for ABAP.</td>
</tr>
<tr>
<td>Entity</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Secure Login Client</td>
<td>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.</td>
</tr>
<tr>
<td>Secure Login Server</td>
<td>X.509 certificate provider running on SAP NetWeaver Application Server for Java. Supports end user authentication to several SAP and third-party services.</td>
</tr>
<tr>
<td>Secure Login Web Client</td>
<td>Browser-embedded and zero-footprint end-user client, which comes as an integrated component of Secure Login Server.</td>
</tr>
<tr>
<td>Microsoft Windows server (domain controller)</td>
<td>For Kerberos and SPNego based authentication in Secure Login Library, Secure Login Client, and Secure Login Server, service users from the respective Windows domains are required.</td>
</tr>
<tr>
<td>NWSSO for CommonCryptoLib 2.0</td>
<td>NWSSO for CommonCryptoLib 2.0 enables you to use the full scope of functions of the SAP Cryptographic Library, which is the default cryptographic library of the SAP NetWeaver Application Server for ABAP. For more information on the SAP Cryptographic Library, see SAP Note 1848999.</td>
</tr>
<tr>
<td>Microsoft Windows server (Active Directory)</td>
<td>For LDAP-based end-user authentication. Windows domain users and their passwords are managed here.</td>
</tr>
<tr>
<td>LDAP directory server</td>
<td>For LDAP-based end-user authentication, classical LDAP directories can also be used.</td>
</tr>
<tr>
<td>RSA authentication server</td>
<td>For RADIUS-based end-user authentication, RSA SecurID tokens can be used.</td>
</tr>
</tbody>
</table>

### 10.3 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.
10.4 Secure Login Library

10.4.1 Installation Procedures and Settings for Secure Login Library

Secure Login Library is shipped 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. No XML files are required. Only add those files you need to change.

To avoid conflicts with an existing installation of the SAP Cryptographic Library (see SAP Note 1848999) or SAPCRYPTOLIB version 5.5, a different installation folder is required, as both security libraries use the same library and utility file names (libsapcrypto, sapgenpse).

Example Alternate Installation Folders

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Alternate Installation Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>D:\usr\sap\SE1\SCS02\exe\SLL\</td>
</tr>
<tr>
<td>Unix/Linux</td>
<td>/usr/sap/NW1/DVEBMGS00/exe/SLL/</td>
</tr>
</tbody>
</table>

10.4.1.1 INTEL AES-NI Support

Secure Login 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.

10.4.2 Initialization Procedures for Secure Login Library

Secure Login 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.
10.4.2.1 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 Secure Login Library set such minimum file permissions if possible. We recommended that you check these automatically generated permissions after write operations.

10.4.2.2 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

<table>
<thead>
<tr>
<th>PKI Role</th>
<th>Key Lifetime</th>
<th>RSA Key Size</th>
<th>Recommended Signature Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root certification authority</td>
<td>10 years</td>
<td>4096 bits</td>
<td>sha256WithRSAEncryption</td>
</tr>
<tr>
<td>Intermediate server CA</td>
<td>10 years</td>
<td>4096 bits</td>
<td>sha256WithRSAEncryption</td>
</tr>
<tr>
<td>Intermediate user CA</td>
<td>5 years</td>
<td>2048 bits</td>
<td>sha256WithRSAEncryption</td>
</tr>
<tr>
<td>SSL or SNC server</td>
<td>10 years</td>
<td>2048 bits</td>
<td>sha256WithRSAEncryption</td>
</tr>
<tr>
<td>End user</td>
<td>&lt; 1 year</td>
<td>2048 bits</td>
<td>sha256WithRSAEncryption</td>
</tr>
<tr>
<td>End user short-lived</td>
<td>&lt; 1 day</td>
<td>2048 bits</td>
<td>sha256WithRSAEncryption</td>
</tr>
</tbody>
</table>

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.

10.4.2.3 STRUST Managed PSEs and X.509 Certificates

A PSE file with X.509 certificate identity can also come from SAP NetWeaver AS for 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.

10.4.2.4 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
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 recommended 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 Secure Login Library works in a so-called offline Kerberos verification mode, there is no technical communication between SAP NetWeaver AS for 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 recommended 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.

### 10.4.2.5 Single Sign-On Credentials

To allow unattended server restart (for example, no need for entering PSE passwords at restart), Secure Login 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.
10.4.2.6 SAP NetWeaver AS for ABAP Instance Profile (SNC)

Secure Login Library can be used by SAP NetWeaver AS for ABAP to act as a protocol provider for SNC. The respective configuration is done in the ABAP instance profile, which is a text property file that is either edited manually or by ABAP transaction RZ10.

Note

The SAP Cryptographic Library is the default cryptographic library, which is included in the SAP NetWeaver Application Server for ABAP.

It is important to understand how to configure SNC for SAP NetWeaver AS for 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 instance profile and command line allow you to repair and restart the server again.

For more information, see the documentation for SNC.

Related Information


10.4.3 Configuration Procedures and Settings for Secure Login Library

Secure Login 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 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.
10.4.4 Runtime Security Considerations for Secure Login 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 135]

10.5 Secure Login Client

10.5.1 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 or Secure Login 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.

<table>
<thead>
<tr>
<th>Security Token</th>
<th>Security Level</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows authentication (Kerberos)</td>
<td>Medium</td>
<td>+ Very high usability, very easy to rollout, infrastructure given existing Microsoft Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>· SNC authentication only, no SSL or SSF</td>
</tr>
<tr>
<td>Windows authentication (SPNego to X.509)</td>
<td>Medium</td>
<td>+ Very high usability, easy to rollout, infrastructure given existing Microsoft Domain, supports SNC/SSL/SSF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ Secure Login Server allows to generate X.509 on the fly</td>
</tr>
<tr>
<td>Security Token</td>
<td>Security Level</td>
<td>Assessment</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Software Certificate (X.509)         | Medium         | + High usability, supports SNC/SSL/SSF  
- Enterprise PKI or public trust center services required to roll-out X.509                                                             |
| 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                                                  |

**10.5.2 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**


Configuration [page 184]

### 10.5.3 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.

### 10.5.4 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 62]

### 10.6 Secure Login Server
10.6.1 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 143]

10.6.2 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.

10.6.2.1 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.

<table>
<thead>
<tr>
<th>PKI Role</th>
<th>Key Lifetime</th>
<th>RSA Key Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root certification authority</td>
<td>10 years</td>
<td>4096 bits</td>
</tr>
<tr>
<td>Intermediate server CA</td>
<td>10 years</td>
<td>4096 bits</td>
</tr>
</tbody>
</table>
## 10.6.2.2 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.

### PKI Role

<table>
<thead>
<tr>
<th>PKI Role</th>
<th>Key Lifetime</th>
<th>RSA Key Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intermediate user CA</td>
<td>5 years</td>
<td>2048 bits</td>
</tr>
<tr>
<td>SSL or SNC server</td>
<td>10 years</td>
<td>2048 bits</td>
</tr>
<tr>
<td>End user</td>
<td>&lt; 1 year</td>
<td>2048 bits</td>
</tr>
<tr>
<td>End user short-lived</td>
<td>&lt; 1 day</td>
<td>2048 bits</td>
</tr>
</tbody>
</table>

### Actions

<table>
<thead>
<tr>
<th>Actions</th>
<th>Pages</th>
<th>Authentication Profile</th>
<th>Profile Groups</th>
<th>Destinations</th>
<th>PKI Structure</th>
<th>Certificate Management</th>
<th>System Management</th>
<th>System Check</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Write</td>
<td>Read</td>
<td>Write</td>
<td>Read</td>
<td>Write</td>
<td>Read</td>
<td>Write</td>
</tr>
<tr>
<td>SLAC_</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ClientM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ngt_All</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SLAC_</td>
<td></td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ClientM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ngt_Rea</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dOnly</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SLAC_</td>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CertMn</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gt_All</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SLAC_</td>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CertMn</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gt_Rea</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dOnly</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actions</td>
<td>Pages</td>
<td>Profile Authentication</td>
<td>Page Groups</td>
<td>Destination Management</td>
<td>Certificate Management</td>
<td>System Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>-------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>-------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Write</td>
<td>Read</td>
<td>Write</td>
<td>Read</td>
<td>Write</td>
<td>Read</td>
<td>Write</td>
</tr>
<tr>
<td>SLAC_SignCert Req_All</td>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SLAC_SignCert Req_ReadOnly</td>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SLAC_SystemCheck_All</td>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SLAC_SystemCheck_ReadOnly</td>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
<th>Roles</th>
<th>SLAC_CERT_ADMIN</th>
<th>SLAC_CERT_READONLY</th>
<th>SLAC_OPERATOR</th>
<th>SLAC_OPERATOR_READONLY</th>
<th>SLAC_SUPERADMIN</th>
<th>SLAC_SUSP_PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SLAC_ClientMgmt_All</td>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SLAC_ClientMgmt_ReadOnly</td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SLAC_CertMgmt_All</td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SLAC_CertMgmt_ReadOnly</td>
<td></td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SLAC_SignCert Req_All</td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
### 10.6.3 Configuration Procedures and Settings for Secure Login Server

Use the Secure Login Administration Console to change the security configuration of the Secure Login Server.

#### 10.6.3.1 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 SAP NetWeaver AS for ABAP servers with SNC, LDAP with SSL, and RADIUS with Challenge-Handshake Authentication Protocol (CHAP) and a shared secret for session key agreement.

#### 10.6.3.2 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.

<table>
<thead>
<tr>
<th>PKI Role</th>
<th>Key Lifetime</th>
<th>RSA Key Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root certification authority</td>
<td>10 years</td>
<td>4096 bits</td>
</tr>
<tr>
<td>Intermediate server CA</td>
<td>10 years</td>
<td>4096 bits</td>
</tr>
<tr>
<td>Intermediate user CA</td>
<td>5 years</td>
<td>2048 bits</td>
</tr>
<tr>
<td>SSL or SNC server</td>
<td>10 years</td>
<td>2048 bits</td>
</tr>
<tr>
<td>End user</td>
<td>&lt; 1 year</td>
<td>2048 bits</td>
</tr>
<tr>
<td>End user short-lived</td>
<td>&lt; 1 day</td>
<td>2048 bits</td>
</tr>
</tbody>
</table>

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
10.6.3.3 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.

10.6.3.4 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.
10.6.4 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 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.

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.

10.6.5 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.

10.7 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 Secure Login 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 SAP NetWeaver AS for ABAP or SAP NetWeaver AS for Java SPNego configuration to make sure there is no interruption in your Kerberos authentication.

10.8 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.

10.9 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.

10.10 RSA Authentication Server

In addition to the security guidelines provided by the RSA, we have a few additional recommendations 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

Coding Samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP’s gross negligence or willful misconduct. All links are categorized for transparency (see: https://help.sap.com/viewer/disclaimer).