Safeguard Authentication Services 5.0

# Single Sign-on for SAP Integration Guide

**Copyright 2020 One Identity LLC.**

**ALL RIGHTS RESERVED.**

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

**Patents**

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

**Trademarks**

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

**Legend**

**WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.**

**CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

Safeguard Authentication Services Single Sign-on for SAP Integration Guide
Updated - August 2020
Version - 5.0

# Contents


**Privileged Access Suite for Unix** ..... **5**
About this guide ..... 6

**Introducing Safeguard Authentication Services Single Sign-on for SAP** ..... **8**
SAP Secure Network Communications ..... 8
Client requirements ..... 9
Functional description ..... 9
Summary ..... 11

**Quick start** ..... **12**
Unix installation and join ..... 12
Unix configuration ..... 13
Windows installation ..... 14
Windows SAP GUI configuration ..... 15
Configure an SAP account for SSO/SNC ..... 18

**SAP server configuration** ..... **20**
Supported platforms ..... 20
Creating and using a service account for the SAP service ..... 20
Enabling SNC on the SAP server ..... 22
Configuring a SAP user to enable SNC authentication ..... 23
Installing Safeguard Authentication Services Single Sign-on for SAP ..... 25
Deploying Single Sign-on for SAP through Group Policy ..... 26
Creating the license CAB file ..... 26
Silent install ..... 27
Configuring the SAP GUI client on Windows XP ..... 27
Configuring the SAP GUI client on Windows Vista and above ..... 29
Prompting for user name and password ..... 32
Enabling authentication prompts ..... 32
Configuring SAPlpd on the front-end system ..... 32
Configuring SAPlpd on the SAP server ..... 35
Testing the printer connection ..... 37

**About us** ..... **39**

Contacting us ..... 39
Technical support resources ..... 39
**Index** ..... **40**

# 1

# Privileged Access Suite for Unix

## Unix security simplified

Privileged Access Suite for Unix solves the intrinsic security and administration issues of Unix-based systems (including Linux and macOS) while making satisfying compliance requirements easier. It unifies and consolidates identities, assigns individual accountability, and enables centralized reporting for user and administrator access to Unix. The Privileged Access Suite for Unix combines an Active Directory bridge and root delegation solutions under a unified console that grants organizations centralized visibility and streamlined administration of identities and access rights across their entire Unix environment.

## Active Directory bridge

Achieve unified access control, authentication, authorization, and identity administration for Unix, Linux, and macOS systems by extending them into Active Directory (AD) and taking advantage of AD's inherent benefits. Patented technology allows non-Windows resources to become part of the AD trusted realm, and extends AD's security, compliance, and Kerberos-based authentication capabilities to Unix, Linux, and macOS. See www.oneidentity.com/products/safeguard-authentication-services/ for more information about the Active Directory Bridge product.

## Root delegation

The Privileged Access Suite for Unix offers two different approaches to delegating the Unix root account. The suite either *enhances* or *replaces* sudo, depending on your needs.

- By choosing to enhance sudo, you will keep everything you know and love about sudo while enhancing it with features like a central sudo policy server, centralized keystroke logs, a sudo event log, and compliance reports for who can do what with sudo.

  See www.oneidentity.com/products/privilege-manager-for-sudo/ for more information about enhancing sudo.
- By choosing to replace sudo, you will still be able to delegate the Unix root privilege based on centralized policy reporting on access rights, but with a more granular permission and the ability to log keystrokes on all activities from the time a user logs

in, not just the commands that are prefixed with "sudo." In addition, this option implements several additional security features like restricted shells, remote host command execution, and hardened binaries that remove the ability to escape out of commands and gain undetected elevated access.

See www.oneidentity.com/products/privilege-manager-for-unix/ for more information about replacing sudo.

### Privileged Access Suite for Unix

Privileged Access Suite for Unix offers two editions: *Standard* edition and *Advanced* edition. Both editions include the Management Console for Unix, a common mangement console that provides a consolidated view and centralized point of management for local Unix users and groups; and Safeguard Authentication Services, patented technology that allows organizations to extend the security and compliance of Active Directory to Unix, Linux, and macOS platforms and enterprise applications. In addition:

- The *Standard* edition licenses you for Safeguard for Sudo.
- The *Advanced* edition licenses you for Privilege Manager for Unix.

One Identity recommends that you follow these steps:

1. Install Safeguard Authentication Services on one machine, so you can set up your Active Directory Forest.
2. Install Management Console for Unix, so you can perform all the other installation steps from the mangement console.
3. Add and profile hosts using the mangement console.
4. Configure the console to use Active Directory.
5. Deploy client software to remote hosts.

   Depending on which Privileged Access Suite for Unix edition you have purchased, deploy one of the following:

   - **Privilege Manager for Unix** software (that is, Privilege Manager Agent packages)

     -OR-

   - **Safeguard for Sudo** software (that is, Sudo Plugin packages)

# About this guide

The *Single Sign-on for SAP Integration Guide* is intended for system administrators, network administrators, consultants, analysts, and any other IT professionals who will be using Single Sign-on for SAP to provide seamless authentication to SAP using the Active Directory credentials of the logged-on user. This guide walks you through the installation and configuration process.

NOTE: The term "Unix" is used informally throughout the Safeguard Authentication

Services documentation to denote any operating system that closely resembles the trademarked system, UNIX.

# 2

# Introducing Safeguard Authentication Services Single Sign-on for SAP

SAP systems host critical enterprise applications. In today's regulatory environment, the ability to secure access to these applications, and to secure the transmission of their data, is an increasingly important compliance and security requirement.

The Safeguard Authentication Services Single Sign-on for SAP solution integrates SAP solutions with Active Directory. Using the identity and security infrastructure available with Active Directory, organizations can implement tight identity integration between SAP and Active Directory user accounts allowing users to securely authenticate with SAP applications using their desktop login credentials. This eliminates the need to re-enter (or remember) a separate SAP username and password.

You can use these same credentials to implement secure data transmission among SAP modules and the SAP GUI client. Sensitive enterprise information that is exchanged between the user's desktop and the remote SAP Application Server is automatically encrypted, securing it from any network eavesdropping.

Safeguard Authentication Services provides a solution that complies with the functional requirements of the SAP SNC interface. The ability of Safeguard Authentication Services to directly join Unix systems with the Active Directory domain is what makes the tight integration and single sign-on experience possible.

SAP SNC makes use of the GSSAPI provided by Safeguard Authentication Services on the SAP Application Server side. The SAP GUI client on the Windows desktop also uses GSSAPI through the Single Sign-on for SAP extensions.

## SAP Secure Network Communications

Secure Network Communications (SNC) is designed to allow external security mechanisms (such as Safeguard Authentication Services) to integrate with the SAP environment to provide additional security features. By integrating the SAP system through standard protocols such as GSSAPI, SNC allows you to isolate SAP applications from the specifics of

the authentication and security implementation. SNC provides three aspects of security: authentication; data integrity; and data security.

The authentication feature provides for secure authentication using an external security token such as a Kerberos ticket which allows single sign-on.

With the data integrity feature enabled, the system detects any changes or manipulation of the data which may have occurred between the two end points of a communication.

The data security or privacy protection feature encrypts message transmission making them resistant to network eavesdropping. This feature also includes data integrity support.

The level of security to be applied to the environment is determined by the SNC configuration as described in the SAP document, *Secure Network Communications: SNC User's Guide*.

# Client requirements

The Single Sign-on for SAP solution is used with SAP GUI clients running on Windows systems that are joined to an Active Directory domain. The Single Sign-on for SAP installs and configures the **qgsskrb5.dll** module which provides a SAP Secure Network Communications (SNC) compliant Generic Security Services Application Program Interface (GSSAPI) to Microsoft Security Support Provider Interface (SSPI) translation layer. You do not need to install any additional client software.

NOTE: The `qgsskrb5.dll` maps the GSSAPI interfaces used by `SAP GUI`, to the corresponding SSPI system calls.

# Functional description

Once you have joined a Unix server to the Active Directory domain using Safeguard Authentication Services, you can configure an SAP Server to use the GSSAPI libraries provided by Safeguard Authentication Services. You can then configure SAP GUI clients running on a supported operating system and joined to the same Active Directory domain (or forest) to use the credentials provided by Active Directory log-on to seamlessly authenticate to the SAP Server.

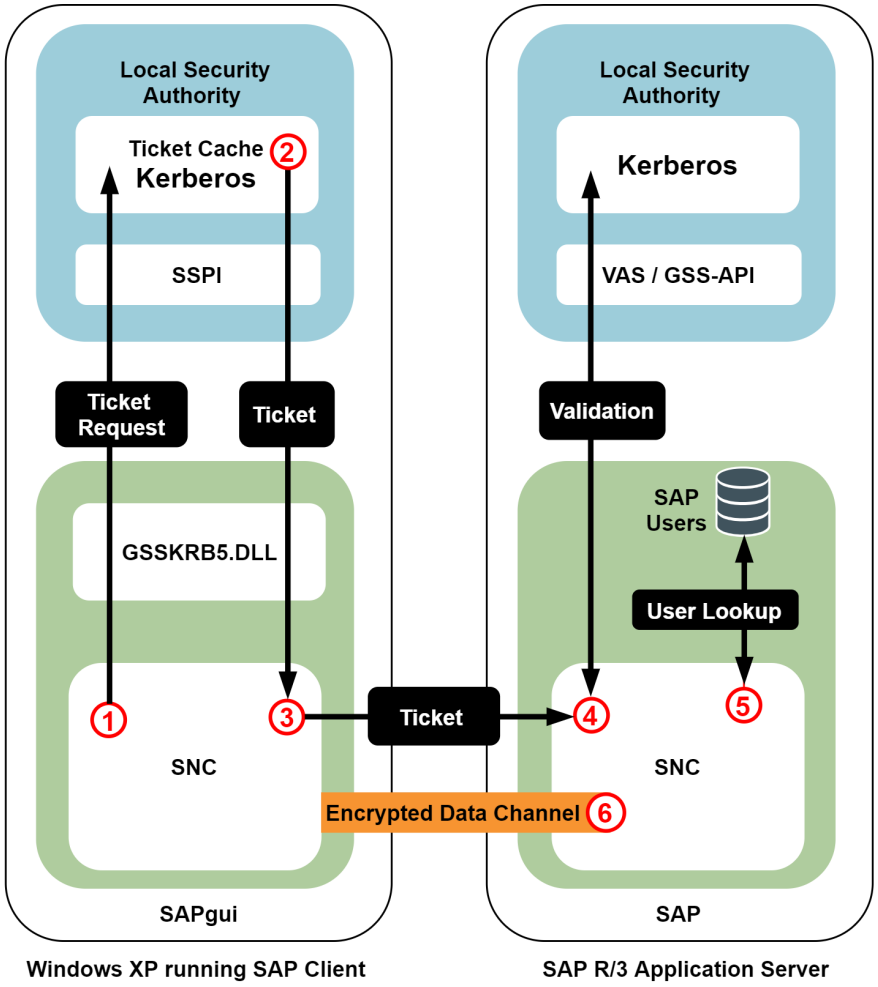
This describes and illustrates the solution's operation:

1. When the user wants to access an SAP application, the SAP GUI requests a Kerberos service ticket with the current user's log-on credentials using the Single Sign-on for SAP SNC module (GSSKRB5.DLL). The configuration stored in the SAP system profile identifies the specific SAP instance, in this case, a SAP system running on a Unix host with Safeguard Authentication Services installed.
2. The system responds with a Kerberos service ticket from the local cache or the Active Directory Key Distribution Center (KDC).

3. The SAP GUI client then opens a connection to the SAP Application Server and provides the Kerberos service ticket.
4. The SAP Application Server processes the service ticket, validating it using the SNC GSSAPI libraries provided by Safeguard Authentication Services.
5. If the ticket is successfully authenticated and the SAP Application Server can map the Active Directory user name it to the corresponding account in the SAP user database, the user is logged on to the SAP Application Server.
6. Depending on the SAP configuration, all of the network communications can then be encrypted.

The user is never required to enter a user name and password, because authentication uses the existing Active Directory credentials acquired when the user logged onto their desktop.

**Figure 1: SAP Server Configuration**



# Summary

The Single Sign-on for SAP solution provides increased security, identity integration, centralized auditing, data integrity, data privacy, and user experience. The integration of Unix and Linux hosts with Active Directory through Safeguard Authentication Services allows SAP clients and servers to use the capabilities of the SAP Secure Network Communications (SNC) interface as a common security and authentication infrastructure and to fully leverage the ability of Active Directory to provide a secure authentication token in the form of a Kerberos ticket, while retaining the benefits of continued deployment of SAP server solutions on Unix hosts.

# 3

# Quick start

The topics in this section lead you through the most common configuration of Safeguard Authentication Services Single Sign-on for SAP.

## Unix installation and join

NOTE: For more details on installing and joining the Safeguard Authentication Services client, please see the *Safeguard Authentication Services Administration Guide*. Commands prefixed with $ must be run by the SAP instance owner account. Commands prefixed with # must be run by *root*.

***To install the Safeguard Authentication Services client and join the Unix system to Active Directory***

1. Mount the product media or extract the product archive, and change directory to the base directory. For example:

   ```
   # mount /mnt/cdrom; cd /mnt/cdrom
   ```

2. Run the preflight program to check for proper connectivity and patch requirements. If failures are reported, see the *Safeguard Authentication Services Administration Guide* for requirements and troubleshooting instructions.

   ```
   # ./preflight example.com
   ```

   Replace *example.com* with your Active Directory domain name.

3. Install the Safeguard Authentication Services client.

   ```
   # ./install.sh vasclnt
   ```

4. Join the system to Active Directory.

   ```
   # /opt/quest/bin/vastool -u Administrator join --skip-config example.com
   ```

Where *Administrator* is an Active Directory user with rights to join and *example.com* is your Active Directory domain name.

NOTE: Ignore any license warnings reported from the join process. These are not relevant to SSO for SAP.

# Unix configuration

To configure the SAP server on Unix to use Single Sign-on for SAP

1. Change the group ownership and permissions of the `host.keytab` file.

```
# chgrp sapsys /etc/opt/quest/vas/host.keytab; chmod 550
/etc/opt/quest/vas/host.keytab
```

2. List the keytab and note the Principal name containing a $.

```
$ /opt/quest/bin/vastool ktutil list
/etc/opt/quest/vas/host.keytab:

Vno  Type                    Principal
  2  aes128-cts-hmac-sha1-96  host/alvlabu22.example.com@EXAMPLE.COM
  2  aes128-cts-hmac-sha1-96  ALVLABU22$@EXAMPLE.COM
  2  aes128-cts-hmac-sha1-96  cifs/alvlabu22.example.com@EXAMPLE.COM
  2  aes128-cts-hmac-sha1-96  host/ALVLABU22@EXAMPLE.COM
  2  aes256-cts-hmac-sha1-96  host/alvlabu22.example.com@EXAMPLE.COM
  2  aes256-cts-hmac-sha1-96  ALVLABU22$@EXAMPLE.COM
  2  aes256-cts-hmac-sha1-96  cifs/alvlabu22.example.com@EXAMPLE.COM
  2  aes256-cts-hmac-sha1-96  host/ALVLABU22@EXAMPLE.COM
  2  arcfour-hmac-md5         host/alvlabu22.example.com@EXAMPLE.COM
  2  arcfour-hmac-md5         ALVLABU22$@EXAMPLE.COM            <-- Take note
of this $ name to use in the next step.
  2  arcfour-hmac-md5         cifs/alvlabu22.example.com@EXAMPLE.COM
  2  arcfour-hmac-md5         host/ALVLABU22@EXAMPLE.COM
```

3. Edit the SAP instance profile by adding the following SNC parameters:

```
snc/enable = 1
snc/data_protection/min = 1
snc/data_protection/max = 3
snc/data_protection/use = 3
snc/accept_insecure_gui = 1
snc/accept_insecure_cpic = 1
snc/accept_insecure_rfc = 1
snc/accept_insecure_r3int_rfc = 1
```

```
snc/r3int_rfc_insecure = 0
snc/r3int_rfc_qop = 3
snc/permit_insecure_start = 1
snc/identity/as = p:ALVLABU22$@EXAMPLE.COM
snc/gssapi_lib = /opt/quest/lib/libvas-gssapi64.so
```

NOTE: Set `snc/identity/as` to the value collected above, prefixed with **p:**.

Use the following table to determine the proper value for the `snc/gssapi_lib` setting.

**Table 1: SNC library paths**

| Platform | Path | Filename |
|---|---|---|
| Any 32-bit (except HP-UX) | /opt/quest/lib | libvas-gssapi.so |
| HPUX 32-bit | /opt/quest/lib | libvas-gssap.sl |
| AIX 64 | /opt/quest/lib | libvas-gssapi64.so |
| Linux-x86_64 | /opt/quest/lib64 | libvas-gssapi.so |
| Oracle Solaris-SPARC 64 | /opt/quest/lib/sparcv9 | libvas-gssapi.so |
| Oracle Solaris-x86_64 | /opt/quest/lib/64 | libvas-gssapi.so |
| HP-UX pa-risc 64 | /opt/quest/lib/pa20_64 | libvas-gssapi.sl |
| HP-UX ia64 | /opt/quest/lib/hpux64 | libvas-gssapi.so |

4. Restart SAP.

```
$ stopsap
$ startsap
```

NOTE: If the SAP services fail to start, check the `/usr/sap/<SID>/DVEBMGS00/work/dev_w0` file for errors.

# Windows installation

Perform the following tasks as a user with Administrative rights.

1. In WindowsExplorer, browse to `\add-ons\qas-sso-for-sap` on the installation media and run the `qas-sso-for-sap-*.msi` installer.
2. On the Welcome screen, click **Next**
3. On the License File screen, click **Browse** to locate the Single Sign-on for SAP license file.

   Select the file and click **Open**.

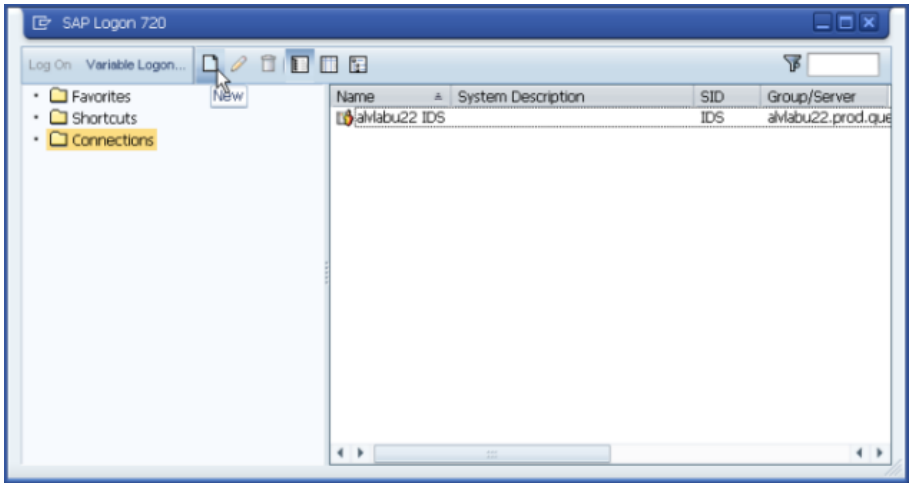
Back on the License File screen, click **Next**.

4. Read the license agreement, select **I accept the terms in the license agreement** and click **Next**.
5. On the Destination Folder screen, click **Next** to use the default installation location.
6. On the Setup Type screen, click **Next** to use the default (Complete) setup type.
7. On the Ready to Install the Program screen, click **Install**.
8. When the installer is complete, click **Finish**.

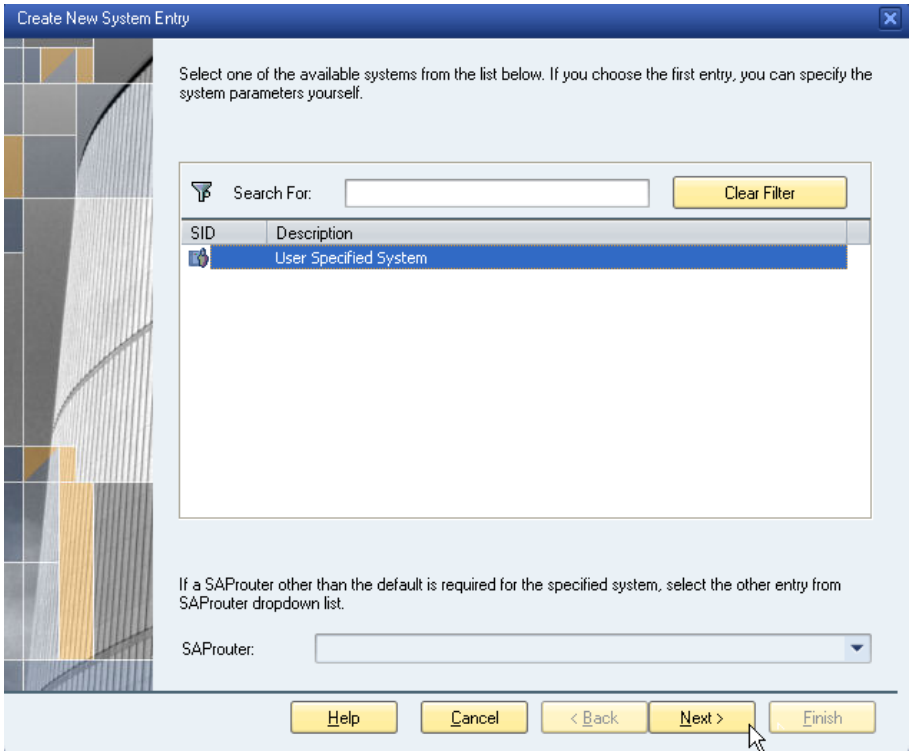
# Windows SAP GUI configuration

Configure SAP GUI for use with Single Sign-on for SAP.

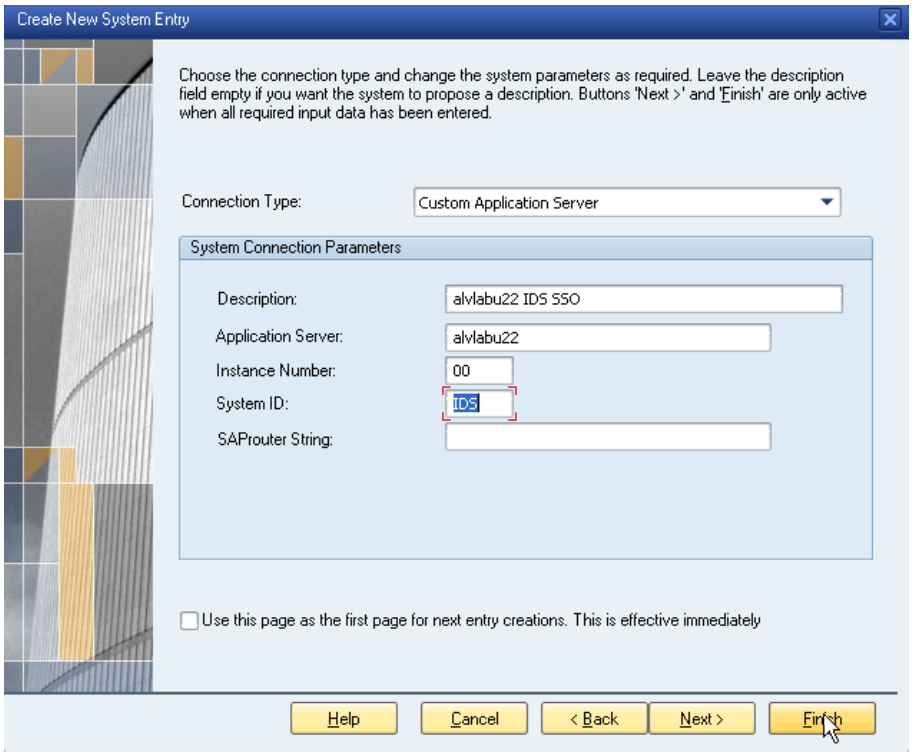
1. Open **SAP Logon** and click **New** in **Connections**.



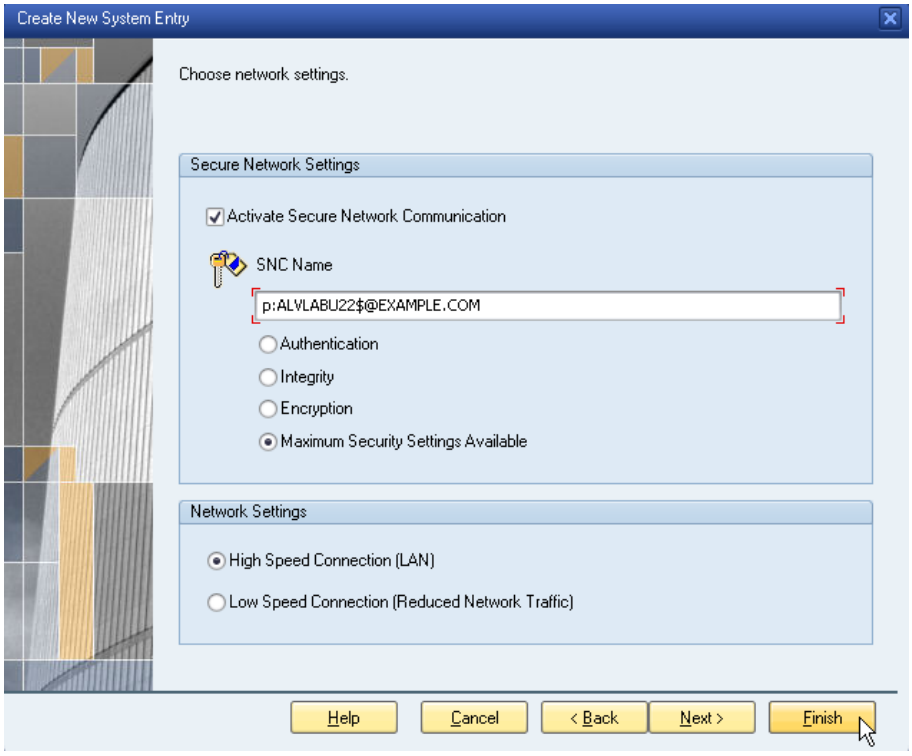
2. Click **Next**.




3. Enter a Description, Application Server address, Instance Number, and System ID, then click **Finish**.




4. Select **Activate Secure Network Communication** and enter the SNC Name derived from the Unix SAP Configuration, then click **Finish**.

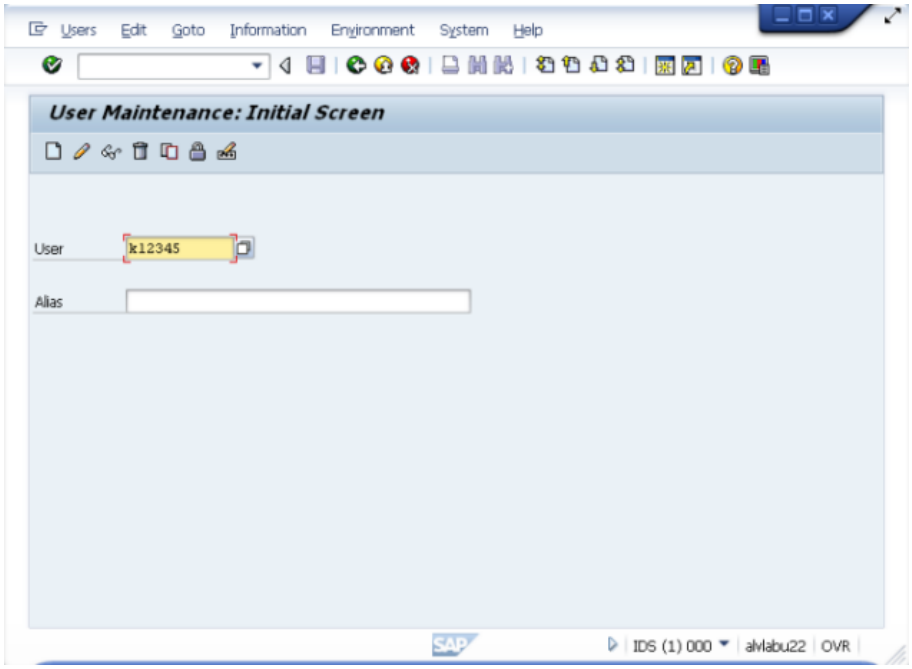


# Configure an SAP account for SSO/SNC

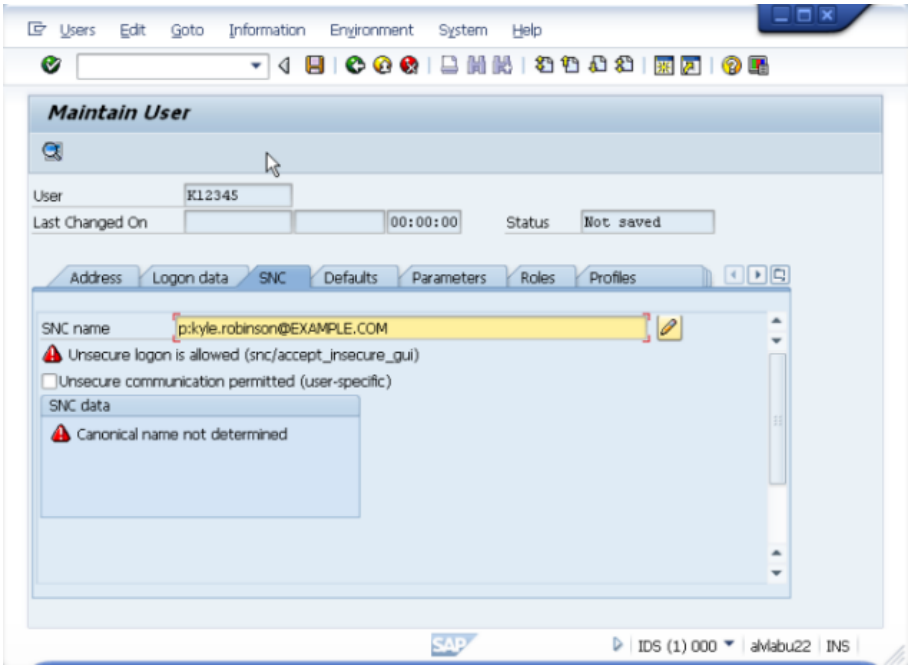
Use the following procedure to map a SAP account to an Active Directory account.

1. In SAP GUI, run transaction SU01 - User Maintenance:

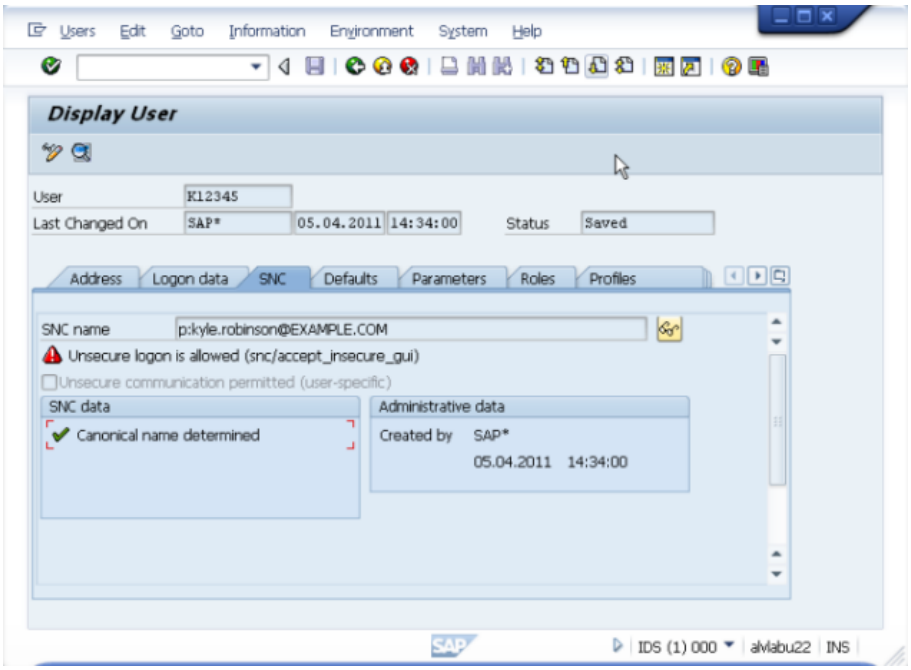
2. Create a new user or edit and existing user.




3. On the **SNC** tab, enter **p:** followed by the user's Implicit User Principal Name (sAMAccountName@DOMAIN) being careful to match case. Save the changes.




4. Return to the **SNC** tab to check for **Canonical name determined**.




5. Open the SSO configured SAP GUI connection as the Active Directory user, and connect to test SSO/SNC functionality.

# SAP server configuration

Before you can configure your SAP Server, you must have Safeguard Authentication Services installed on your Unix server and joined to the Active Directory domain. Refer to the Safeguard Authentication Services product documentation for instructions on how to install and join the domain.

## Supported platforms

Single Sign-on for SAP supports the SAP GUI on Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

For a complete list of supported Unix and Linux platforms, see the *Safeguard Authentication Services Installation Guide* or *Release Notes*.

## Creating and using a service account for the SAP service

One Identity recommends the steps described in this section as a best practice for defining a distinct service account for SAP authentication.

Active Directory service accounts provide a means for authenticating and managing services and rights to access host resources. When you create a service account, it generates a random password for the account and a Kerberos keytab for the service. The previous section described a configuration where SAP uses the host keytab, while this section describes the recommended configuration where SAP uses a service account.

Each service account has a KRB5 Principal Name (KPN) and an optional set of Service Principal Names (SPN's). The KPN is the `sAMAccountName` of the service account (case sensitive) including the domain in the form "**sAMAccountName@realm**". The keytab file is created in the Safeguard Authentication Services configuration directory at `/etc/opt/quest/vas`. The default permissions on the keytab file are 0600 and the file is owned by root. You must update the ownership of the file so that the service has rights to read from the keytab file.

### *To create and use a Service Account for the SAP Service*

1. Create the service account using `vastool` on the SAP Server host:

   ```
   vastool –u Administrator service create SAP/
   ```

   This command creates the `/etc/opt/quest/qas/SAP.keytab` file. *Administrator*, is the name of the Active Directory user with administrative privileges to create a new service account. The user is prompted for their Active Directory password.

2. Set the password to "never expires" and "can not be changed" by setting the `userAccountControl` attribute, by entering:

   ```
   vastool -u administrator setattrs SAP/ userAccountControl 66048
   ```

3. Change the file permissions on the newly created `service.keytab` file so that the corresponding service has the rights to read from the keytab file, by entering:

   ```
   chmod 640 /etc/opt/quest/vas/SAP.keytab
   ```

   Change the group ownership of the keytab to the sapsys group, by entering:

   ```
   chgrp sapsys /etc/opt/quest/vas/SAP.keytab
   ```

4. Set the `snc/identity/as` value and the SNC Name (in Advanced Options of SAPlogin) to **p:sAMAccountName@realm**

   where *example.com* is the name of the domain to which the R3 server is joined.

   You can obtain the `sAMAccountName` of the service account by running the following command:

   ```
   vastool -u host/ attrs -q SAP/ sAMAccountName
   ```

5. On the SAP Server, set the environment variable `KRB5_KTNAME` to the location of the previously created `SAP.keytab` file.

   For example, in `~<instance>adm/.cshrc` add the following:

   ```
   setenv KRB5_KTNAME /etc/opt/quest/vas/SAP.keytab
   ```

6. Restart the SAP services.

# Enabling SNC on the SAP server

***To enable Secure Network Communications (SNC) on the R3 server***

1. Add and configure the SNC-specific parameters to the instance profile of the SAP Server.

   You can set the profile parameters using transaction RZ10 if you have the corresponding administrator rights to make these changes.

2. Add the following SNC parameters to the instance profile of the application server. These settings enable the SNC features without impacting existing operations.

```
snc/enable = 1
snc/data_protection/min = 1
snc/data_protection/max = 3
snc/data_protection/use = 3
snc/accept_insecure_gui = 1
snc/accept_insecure_cpic = 1
snc/accept_insecure_rfc = 1
snc/accept_insecure_r3int_rfc = 1
snc/r3int_rfc_secure = 0
snc/r3int_rfc_qop = 3
snc/permit_insecure_start = 1
snc/identity/as = p:sAMAccountName@REALM
snc/gssapi_lib = /opt/quest/lib/libvas-gssapi.so
```

   The actual path of the GSSAPI library varies by platform. The following table lists the path and file name of `snc/gssapi_lib` in the last line of the SNC parameters listed above.

**Table 2: Object: User-Display**

| Platform | Path | Filename |
|---|---|---|
| Any 32-bit (except HP-UX) | /opt/quest/lib | libvas-gssapi.so |
| HPUX 32-bit | /opt/quest/lib | libvas-gssap.sl |
| AIX 64 | /opt/quest/lib | libvas-gssapi64.so |
| Linux-x86_64 | /opt/quest/lib64 | libvas-gssapi.so |
| Oracle Solaris-SPARC 64 | /opt/quest/lib/sparcv9 | libvas-gssapi.so |
| Oracle Solaris-x86_64 | /opt/quest/lib/64 | libvas-gssapi.so |
| HP-UX pa-risc 64 | /opt/quest/lib/pa20_64 | libvas-gssapi.sl |
| HP-UX ia64 | /opt/quest/lib/hpux64 | libvas-gssapi.so |

The `snc/identity/as` parameter, `sAMAccountName@REALM`, corresponds to the KRB5 principal name of the SAP Server. You can determine the `sAMAccountName@REALM` (or KRB5 principal name) by examining the Kerberos ticket cache using the `vastool klist` command.

3. Change the group ownership of `/etc/opt/quest/vas/host.keytab` to `sapsys` by running:

   ```
   chgrp sapsys /etc/opt/quest/vas/host.keytab
   ```

   Modify the permissions so that the `sapsys` group has read access:

   ```
   chmod 640 /etc/opt/quest/vas/host.keytab
   ```

4. Restart the SAP Application Server.

   If problems occur with the startup of the SNC, they are logged into the work directory of the SAP Application Server in the `/usr/sap/SID/instance/work/dev_w0` file.

   Here is a sample work process log containing SNC activation messages:

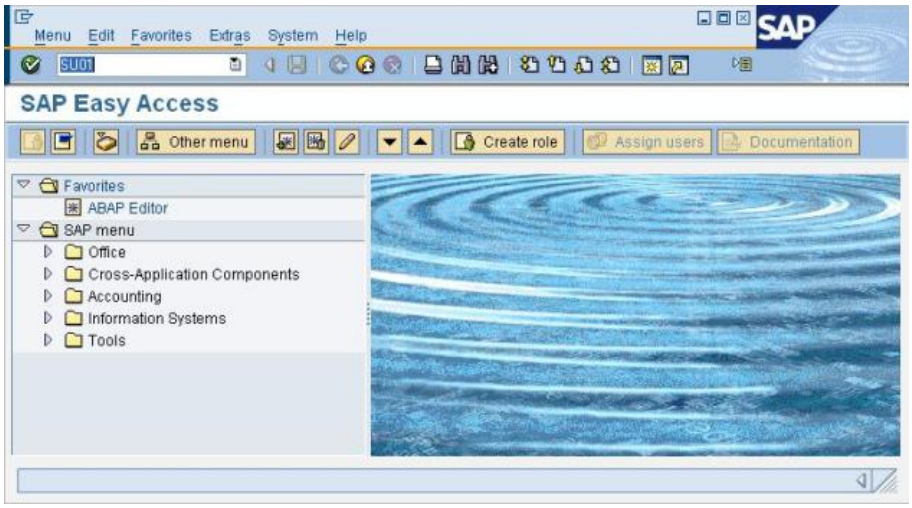
   ```
   N SncInit(): Initializing Secure Network Communication (SNC)
   N    Intel x86 with Linux (st,ascii,SAP_UC/size_t/void* = 8/32/32)
   N SncInit():  found snc/data_protection/max=3, using 3 (Privacy Level)
   N SncInit():  found snc/data_protection/min=1, using 1 (Authentication Level)
   N SncInit():  found snc/data_protection/use=9, using 3 (Privacy Level)
   N SncInit(): found snc/gssapi_lib=/opt/quest/lib/libvas-gssapi.so
   N
   N Tue Sep 30 17:11:14 2008
   N  File "/opt/quest/lib/libvas-gssapi.so" dynamically loaded as GSSAPI v2
   library.
   N  The internal Adapter for the loaded GSSAPI mechanism identifies as:
   N  Internal SNC-Adapter (Rev 1.0) to Kerberos 5/GSSAPI v2
   N SncInit():  found snc/identity/as=p:sAMAccountName@REALM
   N SncInit(): Accepting Credentials available, lifetime=Indefinite
   N
   N Tue Sep 30 17:11:15 2008
   N SncInit(): Initiating Credentials available, lifetime=09h 57m 07s
   M ***LOG R1Q=> 1& [thxxsnc.c  252]
   M SNC (Secure Network Communication) enabled
   ```

# Configuring a SAP user to enable SNC authentication

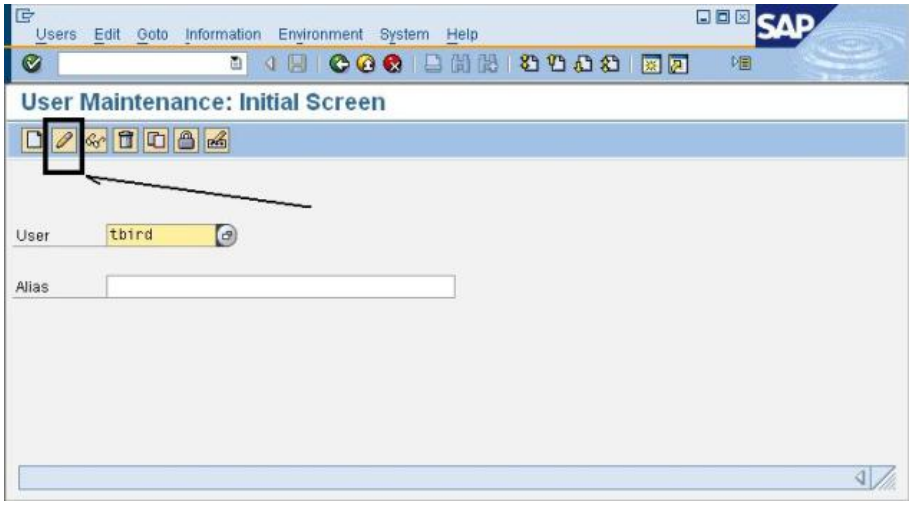
Each user must have a unique Kerberos Principal Name (KPN) associated with their SAP account to use Single Sign-on for SAP.

### *To configure a SAP user to enable SNC authentication*

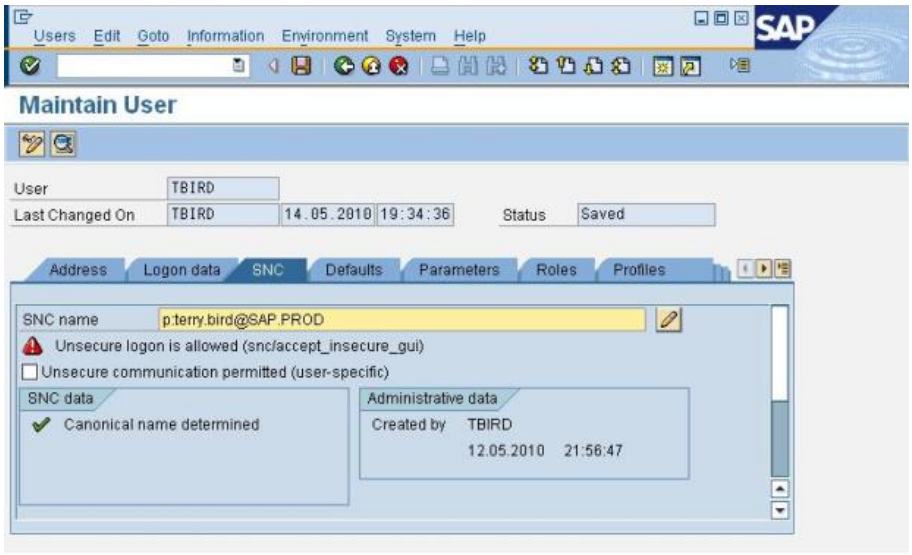
1. Log on to the SAP Server as a user with administrative permissions.
2. Enter **SU01** and click **Enter** or access the user management functions under **SAP Menu | Tools | Administration | User Maintenance | Users**.




3. In the **User** field, enter a user name and click the pencil icon.




4. Select the **SNC** tab of the User Management screen.




5. In the **SNC name** field, enter the user's Kerberos Principal Name (KPN) (`sAMAccountName@realm`).

   NOTE: You must put a "p:" in front of the user's KPN, as follows: **p:sAMAccountName@realm**

6. Click **Save** on the menu bar.

   The SNC data properties displays a check mark next to the **Canonical name determined** message.

# Installing Safeguard Authentication Services Single Sign-on for SAP

You can install Safeguard Authentication Services Single Sign-on for SAP from the installation setup wizard. From the Autorun Setup page, select **Single Sign-on for SAP** from the Related Products tab to install this add-on or follow the steps below.

NOTE: If you do not have local administrator rights, the SNC_LIB system environment variable will not be set during the installation. To resolve this issue, you can set the environment variable path for SNC_LIB to `<install folder>/qgsskrb5.dll`.

***To install Safeguard Authentication Services Single Sign-on for SAP***

1. In Windows Explorer open the Safeguard Authentication Services CD, navigate to **add-ons | qas-sso-for-sap**.
2. Double-click **qas-sso-for-sap-x.x.x.x.msi** to launch the installer.

   where "x.x.x.x" is the latest version number.

3. Click **Next**.

4. Click **Browse** to locate the license file.

   NOTE: You must have a license file to install.

5. Select **I accept the terms in the license agreement** and click **Next**.
6. Click **Next** to install to the default folder, or click **Change** to install to an alternate location.

   NOTE: If you are running the installer as a non-administrator, One Identity recommends that you specify an alternate location where you have rights to copy files.

7. Select **Complete** and click **Next**.
8. The **Ready to Install the Program** dialog displays. Click **Install**.

   NOTE: You may be prompted for permission to install. In that case, click **Allow**.

9. Click **Finish** to exit the wizard.

# Deploying Single Sign-on for SAP through Group Policy

The Single Sign-on for SAP package includes a transform file called `qas-sso-for-sap.mst` along with the main MSI installer file. This transform file together with a special `.cab` file allows you to perform a silent installation of the Single Sign-on for SAP package using your license file.

When deploying Single Sign-on for SAP using Group Policy you must first create a CAB from your license file.

# Creating the license CAB file

***To create the license CAB file***

1. Locate your license file and rename it to:

   `Quest-QAS-GSSAPI-for-SAP.asc`

2. Run the following command:

   ```
   makecab.exe Quest-QAS-GSSAPI-for-SAP.asc license.cab
   ```

   NOTE: You may need to download `makecab.exe` if it is not available on your system.

   This creates a file called `license.cab`.

3. Copy `license.cab` to the directory containing the `qas-sso-for-sap-<version>.msi` and `qas-sso-for-sap.mst` files.

# Silent install

***To deploy Single Sign-on for SAP through Group Policy silently***

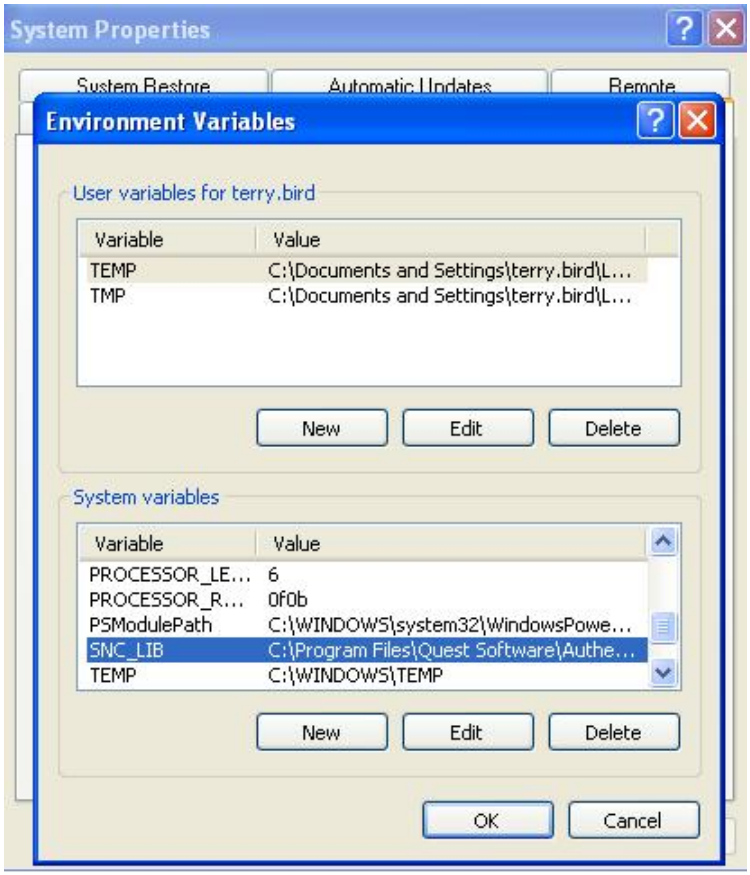
1. Open a command prompt window, navigate to the directory containing the `qas-sso-for-sap-<version>.msi`, `qas-sso-for-sap.mst` and `license.cab` files.
2. Execute the following command:

```
msiexec /i "qas-sso-for-sap-<version>.msi" TRANSFORMS="qas-sso-for-sap.mst" /qb
```

# Configuring the SAP GUI client on Windows XP

***To configure the SAP GUI client on Windows XP***

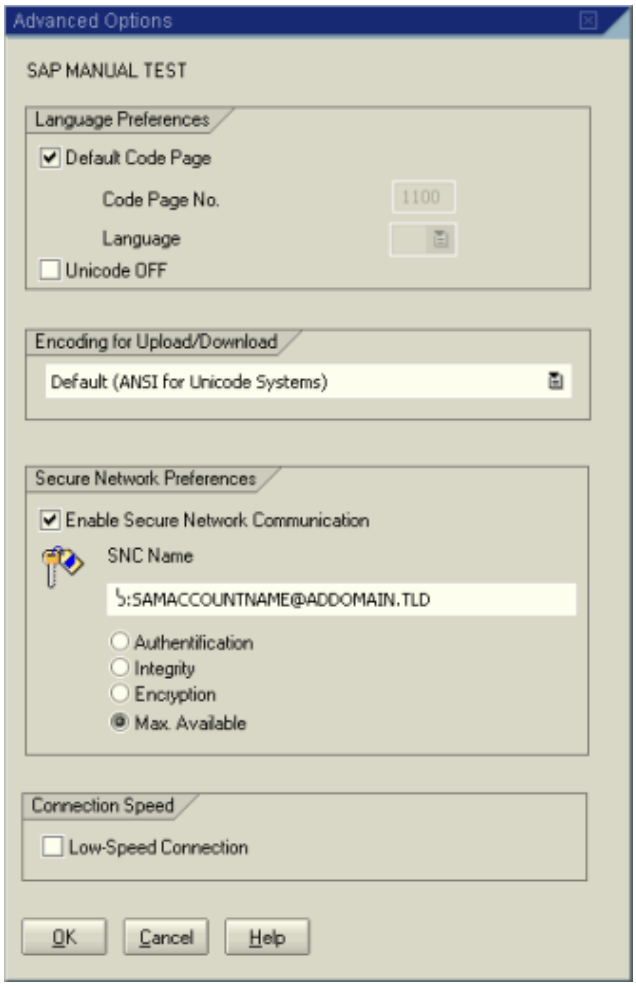
1. Verify that the environment variable SNC_LIB contains the path to `qgsskrb5.dll`.



The library is located in the folder where you installed Single Sign-on for SAP.

2. Run the SAPlogin application.
3. Select a server connection and click **Change Item** to open the properties.

   The SAP GUI client should already be installed and configured for normal password-based authentication.
4. Click the **Advanced** button to open the Advanced Options.




5. Select **Enable Secure Network Communication** to enable SNC.
6. In the **SNC Name** field, enter the KPN of the SAP Server. For example, enter:

   ```
   p:sAMAccountName@realm
   ```

   This is the same KPN that was used for the SAP instance profile key `snc/identity/as` described in Enabling SNC on the SAP server on page 22.
7. Select the **Max. Available** option to enable single sign-on as well as data integrity and encryption for all of the traffic between the SAP GUI client and the R3 server.

8. Click **OK** to save these settings.

   You can now click the server name in SAPlogon to log onto the server without being prompted for a user name or password.

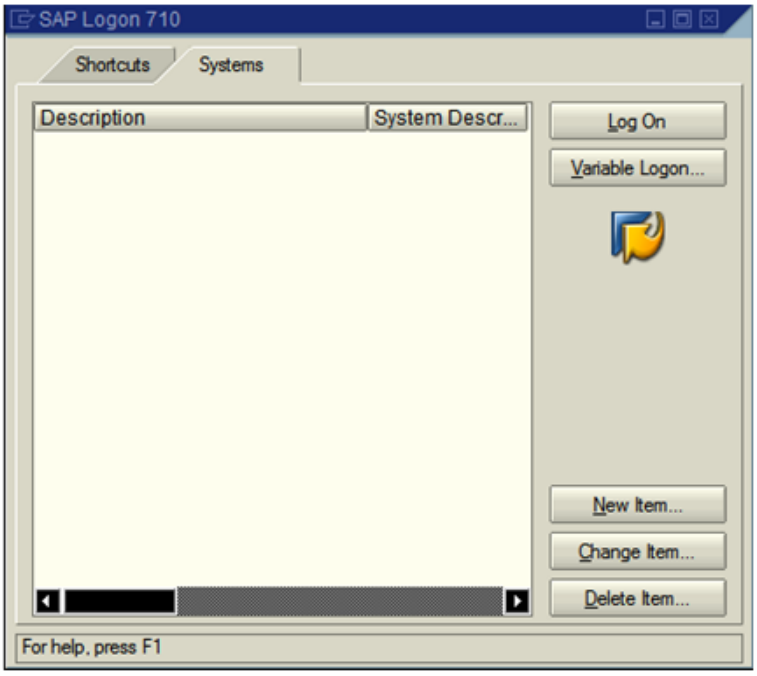
   Once you have configured the server connection to use SNC, it is now possible to create desktop shortcuts using SAPlogon. Shortcuts normally require a password to either be included with the shortcut (not recommended) or else the user is prompted for a password when the shortcut is activated. With SNC activated, however, it is only necessary to enter an arbitrary shortcut (a single letter will do) in the password field of the shortcut. This shortcut is not actually used for authentication, as the SAP system attempts authentication using GSSAPI first.

   The use of SNC and shortcuts allows SAP administrators to create desktop icons for users that will launch them directly into specific SAP applications, securely authenticating without the use of passwords.

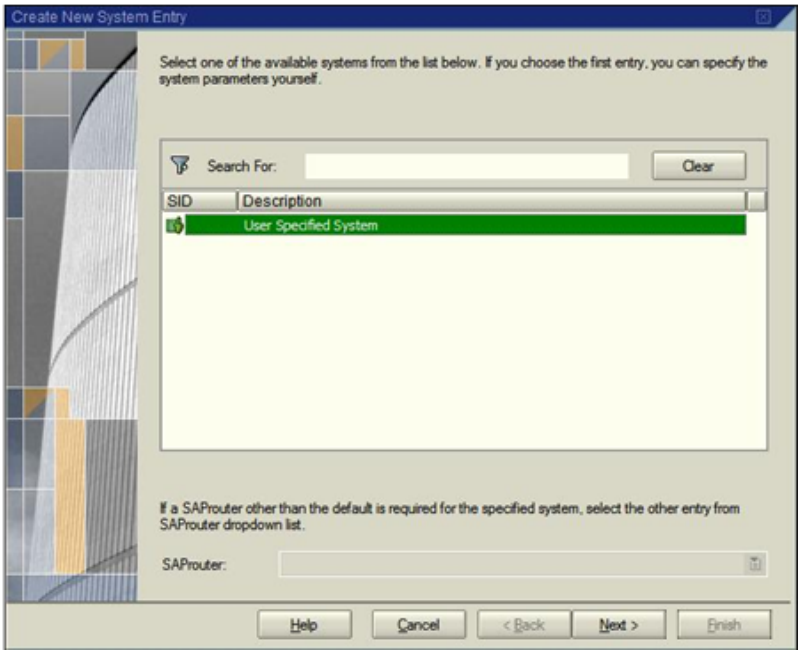
# Configuring the SAP GUI client on Windows Vista and above

***To configure the SAP GUI client on Windows Vista***

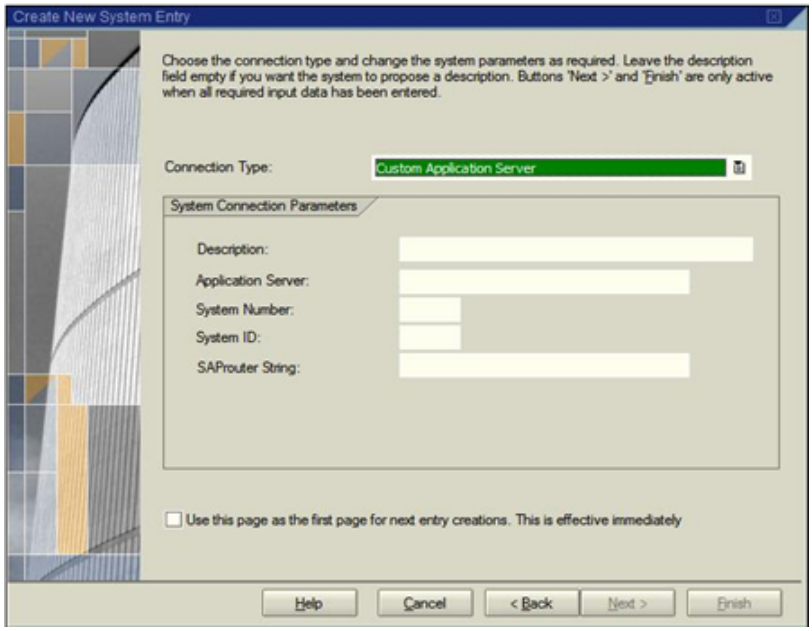
1. Open SAP GUI Logon 7.10 and click **New Item**.




2. On the **Create New System Entry** screen, select **User Specified System** and click **Next**.




3. Ensure **Connection Type** is **Custom Application Server**.



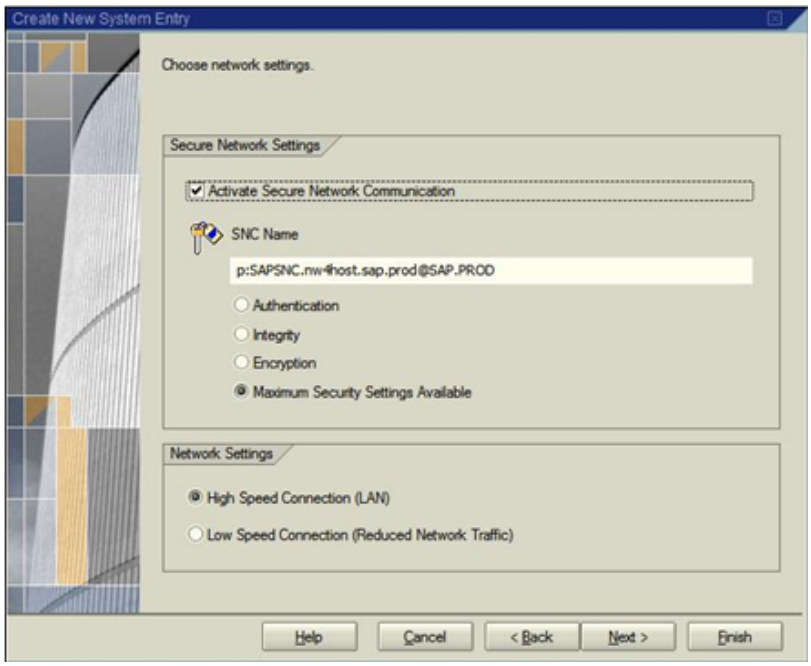

Enter the appropriate information in **Application Server**, **System Number**, and **System ID** and click **Next**.

4. Select the **Activate Secure Network Communication** option and enter the Kerberos Principal Name (KPN) of the SAP Server and click **Next**.

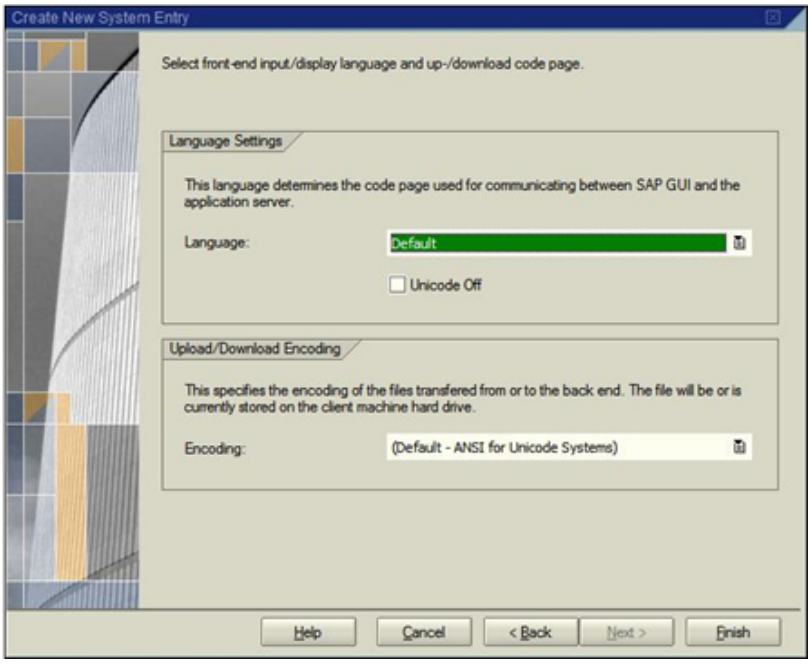
   For example, enter:

```
p:sAMAccountName@realm
```

Use the same KPN that you used for the SAP instance profile key `snc/identity/` as described in Enabling SNC on the SAP server on page 22.




5. Leave the defaults on this screen and click **Finish**.




The new item you created will now appear on the SAP GUI log on.

6. Click **Logon** and log in as a user who is set up to use SNC.

# Prompting for user name and password

By default, Single Sign-on for SAP performs automatic authentication using the credentials of the currently logged-in Windows user. In some situations, you might want users to provide an Active Directory user name and password when logging in to SAP. You can configure Single Sign-on for SAP to display a login prompt whenever a new authentication request is generated.

When you enable authentication prompting, users see an authentication dialog where they must enter an Active Directory user name and password in order to gain access to SAP. The user name can be in any one of these formats:

- SAM account name (if the computer is joined to the user's domain)
- <DOMAIN>\<SAM account name>
- <SAM account name>@<DOMAIN>

# Enabling authentication prompts

***To enable Active Directory authentication prompting from the Single Sign-on for SAP module***

1. Change the following registry value from 0 to 1.

   On 32-bit machines:

   ```
   HKEY_LOCAL_MACHINE\Software\Quest Software\SSO for SAP\Always Prompt
   ```

   On 64-bit machines:

   ```
   HKEY_LOCAL_MACHINE\Software\Wow6432Node\Quest Software\SSO for SAP\Always Prompt
   ```

# Configuring SAPlpd on the front-end system

To use SAPlpd with SNC, you must provide the SAPlpd system on the front-end desktop with the local library path and identity information.

### *To configure SAPlpd on the front-end system*

1. In the Windows directory, create a `SAPLPD.INI` file, if one does not already exist.
2. Add the following section to the `SAPLPD.INI` file:

```
[snc]
enable=1
identity/lpd=<SNC-Name_of_saplpd>
gssapi_lib=<drive>:\path\to\your\snclib.dll
```

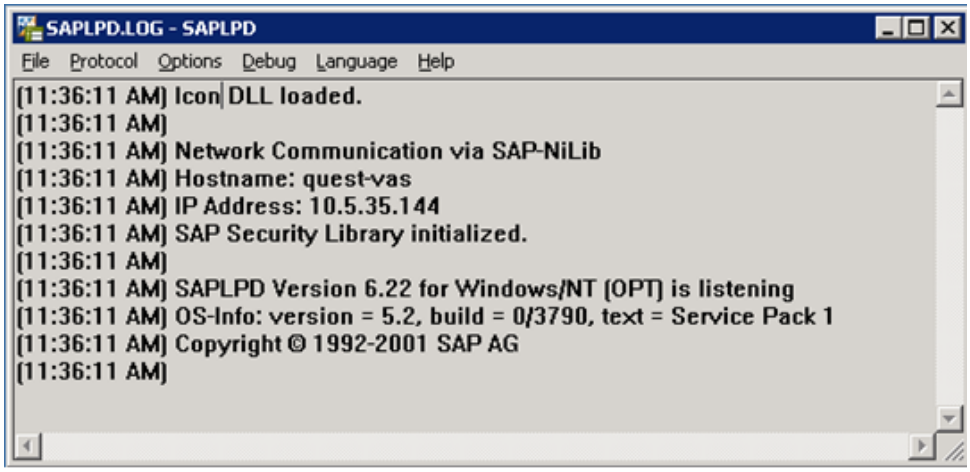
   NOTE: You can omit the `gssapi_lib=` entry when you have the environment variable, SNC_LIB, configured to be a system environment variable.

   The `identity/lpd` variable, `<SNC-Name_of_saplpd>`, is in the SNC form of the user logged in and running SAPlpd. You must use this format: `u:samaccountname@realm` where `sAMAccountName` is the SAM-Account-Name of the currently logged in user and `example.com` is the Active Directory domain name.

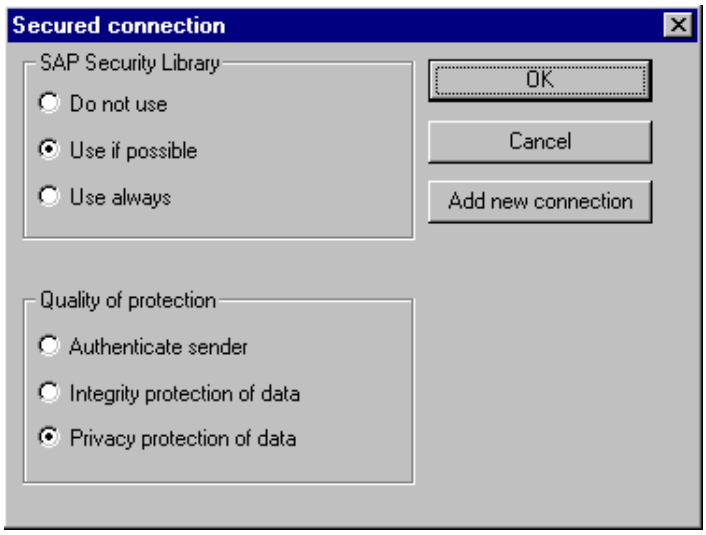
   NOTE: You can also add these settings to the `WIN.INI` file if you do not want to create the `SAPLPD.INI` file.

3. Run `SAPlpd`.

   A window appears listing the output from the SAPlpd startup:

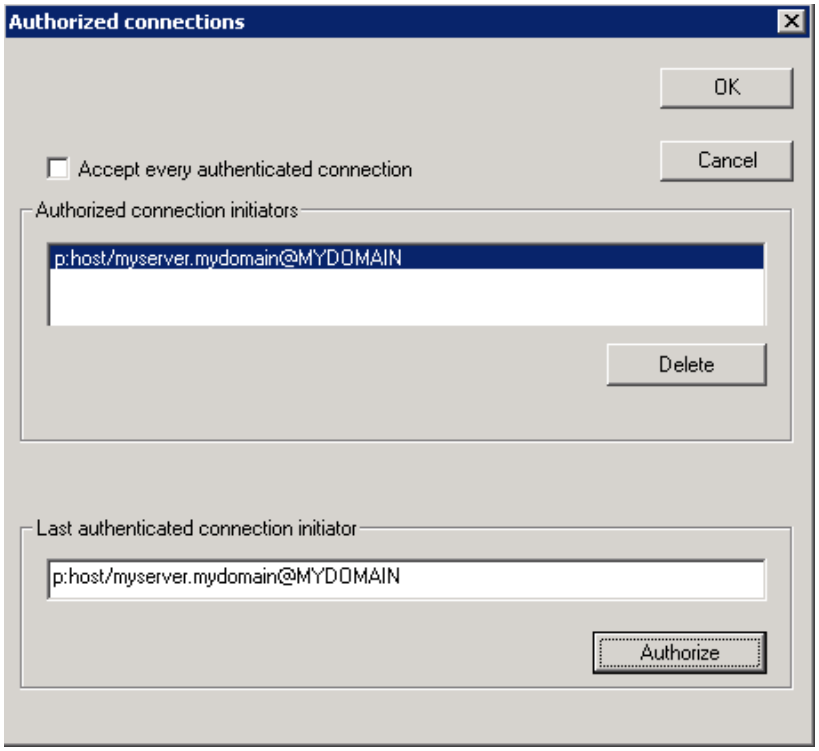



4. From the **SAPLOPD.LOG – SAPLPD** window, select the **Options | Secured Connections** menu item.
5. On the **Secured connection** dialog, select the **Use if possible** and **Privacy protection of data** options and click the **Add new connection** button to go to the Access Control List maintenance for SAPlpd.




6. On the **Authorized connections** dialog, in the **Last authenticated connection initiator** field, enter the SNC-name of the application servers that will be transferring print jobs to this SAPlpd using SNC.

   This is the value of the `snc/identity/as` key from the instance profile on the Safeguard Authentication Services-enabled SAP Server. See Enabling SNC on the SAP server on page 22.




7. Click **Authorize** to add this name to the list of authorized connection initiators.
8. Close all open SAPlpd dialogs by clicking their **OK** buttons.

Your front-end desktop is now configured to securely connect.

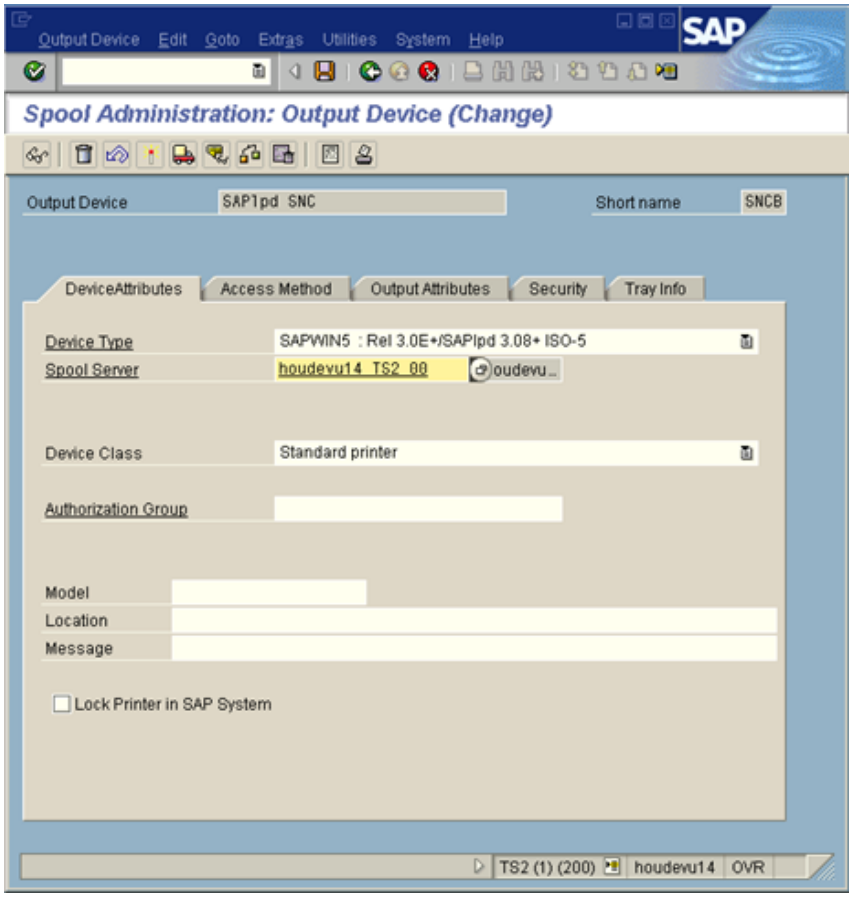
# Configuring SAPlpd on the SAP server

***To configure SAPlpd on the SAP server***

1. Create a new output device (Printer) by navigating to **Configuration | Output** devices from the Spool Administration screen.

   You can apply these same settings to an existing device.

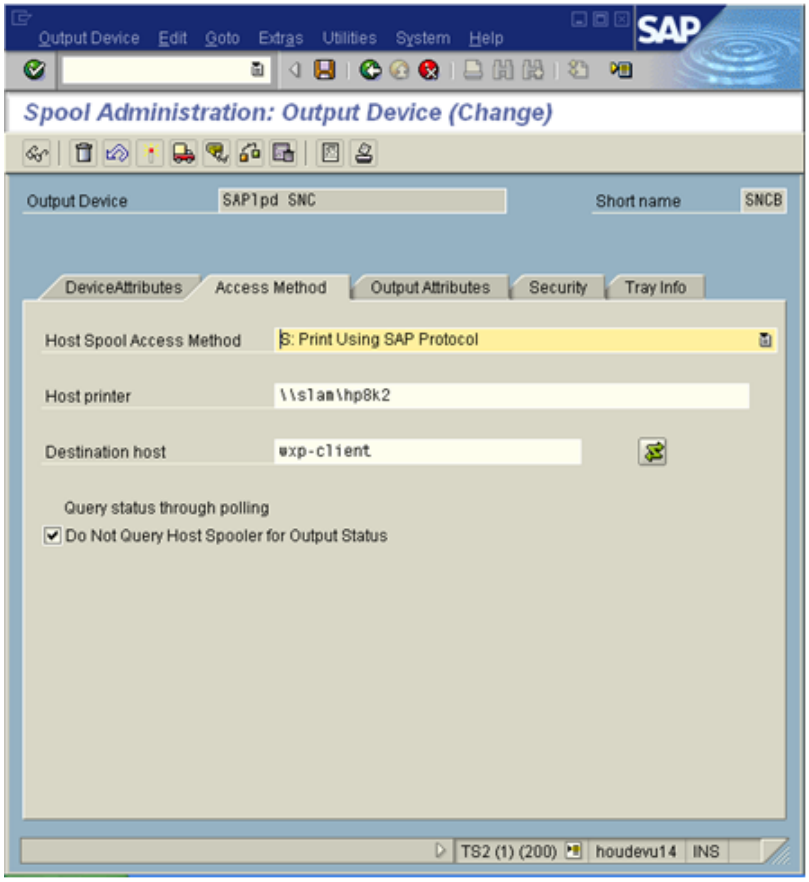
2. Click the **Device Attributes** tab.



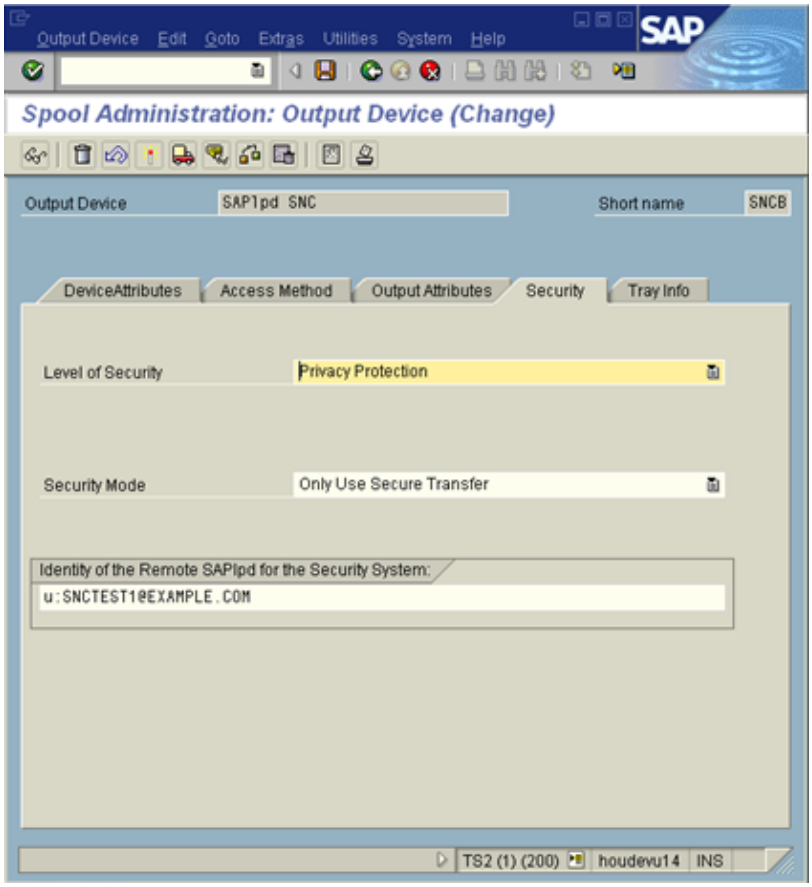

3. Enter the appropriate information:
   - **Output Device**
   - **Short name**
   - **Device Type**
   - **Spool Server**

To populate the **Spool Server** field, click **F4** or , the folder icon next to the **Spool Server** field, to list all the application servers with a color-coded background. The application servers running a spool process are highlighted in green.

4. Click the **Access Method** tab.




5. Set the **Host Spool Access Method** to **S: Print Using SAP Protocol**.
6. Enter the host name of the printer.
7. Enter the host name of the front-end system as the **Destination host**.
8. Select the **Do Not Query Host Spooler for Output Status** option.
9. Select the **Security** tab and select a level of security: **Only Authentication**, **Integrity Protection**, or **Privacy Protection**.




10. Change the **Security Mode** to **Only Use Secure Transfer** to specify that you want SNC to be required.
11. In the **Identity of the Remote SAPlpd for the Security System** field, enter the **SNC name** in the format.

    ```
    u:samaccountname@realm
    ```

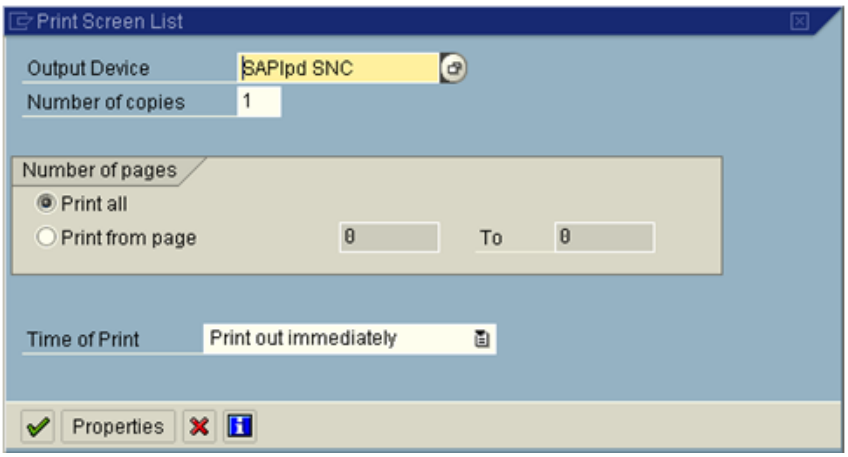
    This is the Active Directory user who will be logged in when using this instance of SAPlpd.
12. Save the changes and exit the Spool Administration screens.

# Testing the printer connection

***To test the printer connection and verify that SAPlpd is still running***

1. From the list of output devices, click the **Printer** icon or navigate to **System | List | Print.**
2. On the **Print Screen List** dialog, select the SNC-enabled output device that you just

created and change the **Time of Print** to **Print out immediately**.




3. Click **Continue** or ✓ (green check mark), to submit the print request.
   You can track the status and progress.

# About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

## Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

## Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

# Index


## B

Best Practice:
- for defining a distinct service account for SAP authentication 20

## C

CAB file
- how to create 26

## D

Deploying Single Sign-on for SAP 26

## E

environment variable
- setting 25

## F

front-end desktop
- configuring 32

## G

GSSAPI to SSPI translation 9

## I

installing
- Single Sign-on for SAP 25

## K

Kerberos Principal Name (KPN) 23

Kerberos ticket 8

KRB5 Principal Name (KPN) 20

## P

printer connection
- testing 37

## S

SAP GUI client
- configuring on Windows Vista 29
- configuring on Windows XP 27
- sub-term 9

SAP Server
- configure 9

SAP user
- configuring 23

SAPlpd
- configuring 32
- configuring on the SAP Server 35

Secure Network Communications (SNC)
- defined 8
- enabling on SAP Server 22

service account
- creating 20

silent install 27

Single Sign-on for SAP
- functional description 9
- installing 25
- prerequisites 20

SNC-parameters 22

SNC authentication
enabling 23
supported platforms 20