Vintela Authentication Services

SSO for SAP

Enabling secure single sign-on and secure data transmission for Windows SAPgui desktop client
# CONTENTS

## OVERVIEW

<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVERVIEW</td>
<td>4</td>
</tr>
<tr>
<td>VAS AND THE VAS SAP SNC SOLUTION</td>
<td>4</td>
</tr>
<tr>
<td>SAP Secure Network Communications (SNC)</td>
<td>5</td>
</tr>
<tr>
<td>VAS and SAP SNC Solution Client Requirements</td>
<td>6</td>
</tr>
<tr>
<td>About qgsskrb5.dll</td>
<td>6</td>
</tr>
<tr>
<td>SOLUTION DESIGN: VAS AND SAP SNC IN OPERATION</td>
<td>6</td>
</tr>
<tr>
<td>SUMMARY</td>
<td>8</td>
</tr>
<tr>
<td>SAP R/3 SERVER CONFIGURATION</td>
<td>8</td>
</tr>
<tr>
<td>PREREQUISITES</td>
<td>8</td>
</tr>
<tr>
<td>Enabling SNC on the SAP R/3 Server</td>
<td>8</td>
</tr>
<tr>
<td>Creating and Using a Service Account for the SAP Service</td>
<td>10</td>
</tr>
<tr>
<td>Configuring a SAP User to Enable SNC Authentication</td>
<td>11</td>
</tr>
<tr>
<td>Installing Quest VAS SSO for SAP</td>
<td>13</td>
</tr>
<tr>
<td>Deploying SAP Using Group Policy</td>
<td>17</td>
</tr>
<tr>
<td>Configuring the SAP GUI Client on Windows XP</td>
<td>18</td>
</tr>
<tr>
<td>Configuring SAPLPD on the Front End System</td>
<td>19</td>
</tr>
<tr>
<td>Configuring SAPLPD on the SAP R/3 Server</td>
<td>21</td>
</tr>
<tr>
<td>Testing the Printer Connection</td>
<td>24</td>
</tr>
</tbody>
</table>
OVERVIEW

SAP based 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.

By using the identity and security infrastructure available with Active Directory, and extended to the UNIX environment with Vintela Authentication Services (VAS), organizations can implement tight identity integration between SAP and Active Directory user accounts.

[This allows the user] to securely authenticate SAP applications from the SAPgui client using the Kerberos credentials they acquire when initially logging in to their desktops using Active Directory, without the need to re-enter (or remember) a separate SAP username and password.

This same Kerberos credential can also be used to implement secure data transmission among SAP modules and the SAPgui client. Sensitive enterprise information that is exchanged between the user's desktop and the remote R/3 server is automatically encrypted, securing it from any network eavesdropping.

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

SNC makes use of the GSS-API services provided by VAS on the R/3 server side. The SAPgui client on the Windows desktop also uses GSS-API, invoked by means of a Quest-developed GSS-API interface library that accesses the native Windows SSPI, which in turn provides the actual GSS-API protocol network session.

VAS AND THE VAS SAP SNC SOLUTION

The VAS SAP SNC Solution is an extension of the identity integration capabilities of the Vintela Authentication Services product, which allows UNIX and Linux systems to join the Active Directory domain. By joining the UNIX hosts to the Active Directory domain in essentially the same way a Windows system does, this allows the UNIX hosts to use the same user accounts and passwords as the Windows account, eliminating the need for password synchronization or metadirectory infrastructure. UNIX users log in to their UNIX accounts using the same username and password as they use to access their Windows system. The same password complexity and expiration policies are applied.

Authentication is performed directly against Active Directory, and each UNIX user acquires the same Kerberos security token (ticket) that a Windows user receives when authenticating to the desktop.

1 The VAS SNC Solution has been the subject of an Integration Assessment by the SAP Integration and Certification Center. A copy of the executive summary of the Integration Assessment is available from your Quest representative accounts must be associated with the corresponding accounts in Active Directory whose credentials will be used to authenticate.
VAS thus integrates completely with Active Directory, fully supporting the same Kerberos authentication mechanisms as Windows provides. Because of this, in the case of SAP R/3, it can provide the same kind of secure, integrated single sign-on using a single credential. This direct integration with Active Directory using Kerberos has previously only been available for SAP R/3 servers hosted on Windows 2000 and Windows 2003 servers. Now organizations hosting their SAP solutions on UNIX can experience these same user and security advantages.

Once VAS has been installed and configured, the SAP SNC interface must be configured to register the availability of the GSS-API services that VAS provides. On the desktop, a dynamically linking library (dll) is installed that maps GSS-API calls to local SSPI calls on the Windows platform, and the desktop SAPgui client is similarly configured to use SNC. Finally, SAP user accounts must be associated with the corresponding accounts in Active Directory whose credentials will be used to authenticate.

The integration of VAS with SAP is only one of the many examples of integration and single sign-on possible once UNIX and Linux systems have been integrated with Active Directory. Other solutions supported by Vintela Authentication Services include the ability to use GSS-API to do secure single sign-on between Unix hosts or the Windows desktop and a Unix host using the ssh (secure shell) terminal session protocol, using ssh-aware clients, or the ability to authenticate Unix-hosted Apache web applications using Windows Integrated Authentication (single sign-on) and Internet Explorer.

**SAP Secure Network Communications (SNC)**

SNC is a SAP interface designed to allow external security mechanisms (such as are provided by VAS) to integrate with the SAP environment to provide additional security features. By integrating the SAP System through standard protocols such as GSS-API, SNC allows SAP applications to be isolated 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. It is this feature that allows Kerberos tickets to be used to provide 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". In typical environments, most organizations opt for the highest level of security, although there is modest performance and network overhead in providing encrypted message transmission.
VAS and SAP SNC Solution Client
Requirements

The VAS SAP SNC solution is used with SAPgui clients running on Windows Vista, 2003, XP or 2000 Professional systems that are joined to an Active Directory domain. The configuration of the SAPgui client is virtually identical to that described by Microsoft for use in connection with SAP R/3 hosted on Windows servers. Both solutions require the installation of the qgsskrb5.dll module. Other than the qgsskrb5.dll module, which is developed by Quest and available on the install cd, and the SAPgui client itself, no additional client software needs to be installed. The solution design description below explains the relationship of the SAPgui client to the complete environment.

About qgsskrb5.dll

SSPI is Microsoft's proprietary implementation of the same network protocols the GSS-API provides. On the network, SSPI and GSS-API connections are fully interoperable. From the application side, SSPI is implemented with different calling conventions than GSS-API. The qgsskrb5.dll maps the GSS-API interfaces, which the SAPgui client uses, to the corresponding SSPI system calls.

SOLUTION DESIGN: VAS AND SAP SNC IN OPERATION

Once a UNIX host has been joined to the Active Directory domain, an SAP R/3 server can be configured to use the VAS GSS-API libraries to support SNC operation. SAPgui clients running on Windows Vista, 2003, XP or 2000 Professional desktops that are also joined to the same Active Directory domain (or forest) can then be configured to also use the Kerberos credentials provided by the Active Directory KDC at network login to seamlessly authenticate to the VAS-enabled SAP R/3 server.

The VAS and SAP SNC solution is intended solely for use within the context of Active Directory as the KDC and for use with Windows clients only.

The operation of the solution is described below and illustrated in the accompanying figure (Figure 1).

The SAPgui client accesses the Windows SSPI interface using the qgsskrb5.dll interface provide by Quest. When the user wants to access an SAP application, the client requests a Kerberos service ticket either from the Active Directory KDC, or, from the ticket cache, if already available (Step 1). The configuration stored in the SAPgui profile identifies the specific SAP R/3 service, in this case, an SAP R/3 service running on a VAS-enabled UNIX host.

The SAPgui client then opens a connection to the SAP R/3 Application Server and provides the Kerberos service ticket when requested by the remote server (Step 3).
The SAP R/3 Application Server processes the service ticket, validating it using the VAS GSS-API libraries installed on the UNIX host as part of the VAS configuration (Step 4). If the ticket is successfully authenticated, the SAP R/3 Application Server can then identify the KRB5 Principal Name (KPN) of the user, and then maps this user name to the corresponding account maintained by the SAP R/3 Application Server (Step 5). The user is then logged on to the SAP Application Server with all of the attributes of the account as maintained by the SAP user database. Provided that the SAP R/3 has been configured to support this, all of the data transferred between the client and the server, for that user session, will now be encrypted as well (Step 6).

At no point was the user required to enter their username and password, because authentication took place using the existing Kerberos credential acquired when the user logged in to their desktop.

Figure 1: Authentication using Kerberos
Summary

The VAS and SAP SNC Solution provides a greatly increased level of security, identity integration, centralized auditing, data integrity and security, and user experience. The integration of Unix and Linux hosts with Active Directory through VAS allows SAP client and servers to use the capabilities of the SAP SNC interface to use a common security and authentication infrastructure and to fully leverage the ability of Windows XP and Windows Professional desktops to provide a secure authentication token in the form of a Kerberos ticket, while retaining the benefits of continued deployment of SAP R/3 server solutions on Unix hosts.

SAP R/3 Server Configuration

Prerequisites

This guidance assumes that you have already installed Vintela Authentication Services (VAS) and joined it to the Active Directory domain as described in the VAS product documentation.

SNC has been supported by SAP as of Version 3.1 G.

Enabling SNC on the SAP R/3 Server

Step 1: Enable SNC on the R/3 server by adding and configuring the SNC-specific parameters to the instance profile of the R/3 server. The SNC parameters for configuring R/3 are fully described in the SNC User’s Guide published by SAP. (https://www.sdn.sap.com/irj/sdn?rid=/webcontent/uuid/e112cb72-0501-0010-63a3-f45326c176ae)

The profile parameters may be set using transaction RZ10, and require that the user have the corresponding administrator rights to make these changes.

Add the following SNC-parameters to the instance profile of the application server. The values below are to enable test and configuration of the SNC features without impacting existing operations. You may want to change some of the SNC parameter settings subsequently, for example, to require secure rfc or to require users to only authenticate using GSS-API.

```
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:SAMACCOUNTNAME@ADDOMAIN.TLD  
snc/gssapi_lib = /opt/quest/lib/libvas-gssapi.so
```
Note: The snc/gssapi_lib path differs on HPUX as well as for 64 bit platforms. For 32 bit HPUX, the filetype is ".sl":

snc/gssapi_lib = /opt/quest/lib/libvas-gssapi.sl

For 64-bit platforms see Table 1 for the correct settings.

snc/gssapi_lib = (See Table 1 below)

<table>
<thead>
<tr>
<th>Platform</th>
<th>Path</th>
<th>Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>/opt/quest/lib</td>
<td>libvas-gssapi64.so</td>
</tr>
<tr>
<td>Linux-x86_64</td>
<td>/opt/quest/lib64</td>
<td>libvas-gssapi.so</td>
</tr>
<tr>
<td>Solaris-sparc 64</td>
<td>/opt/quest/lib/sparcv9</td>
<td>libvas-gssapi.so</td>
</tr>
<tr>
<td>Solaris-x86_64</td>
<td>/opt/quest/lib/64</td>
<td>libvas-gssapi.so</td>
</tr>
<tr>
<td>HP-UX pa-risc 64</td>
<td>/opt/quest/lib/pa20_64</td>
<td>libvas-gssapi.sl</td>
</tr>
<tr>
<td>HP-UX ia64</td>
<td>/opt/quest/lib/hpux64</td>
<td>libvas-gssapi.so</td>
</tr>
</tbody>
</table>

The snc/identity/as parameter SAMACCOUNTNAME@ADDOMAIN.TLD corresponds to the actual hosts Windows pre-2000 name (or service account, if a dedicated service account is used as discussed below) of the SAP R/3 system. 2

Step 2: Change the group ownership of /etc/opt/quest/vas/host.keytab to sapsys. This can be done by running:

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

And then by making it readable by that group with the command:

```
# chmod 640 /etc/opt/quest/vas/host.keytab or # chmod g=r /etc/opt/quest/vas/host.keytab
```

Step 3: Restart the R/3 application server. If problems occur with the startup of the SNC, they will be logged in to the work directory of the R/3 application server in the file /usr/sap/<SID>/<instance>/work/dev_w0.

**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 GSS-API v2 library.
N The internal Adapter for the loaded GSS-API mechanism identifies as:
N Internal SNC-Adapter (Rev 1.0) to Kerberos 5/GSS-API v2
```

2 The precise KRB5 principal name can be determined by examining the Kerberos ticket cache using klist or the vastool utility.
Creating and Using a Service Account for the SAP Service

The steps in this section are considered best practice and should be used to define a distinct service account for SAP authentication.

Active Directory service accounts provide a means for authenticating and managing services and services rights to access host resources. When a service account is created, a random password is generated for the account and a Kerberos keytab is created for the service.

Each service has a KRB5 Principal Name (KPN), and an optional set of Service Principal Names (SPN’s). The KPN is the sAMAccountName of the Windows AD service account (case sensitive) including the domain in the form "sAMAccountName@ADdomain.tld" where sAMAccountName is the Windows pre-2000 name and ADdomain.tld is the Kerberos realm (Active Directory domain). The keytab file will be created in the VAS configuration directory at /etc/opt/quest/vas. The default permissions on the keytab file will be 0600 and the file will be owned by root. You will need to update the ownership of the file so that the corresponding service has the rights to read from the keytab file.

**Step 1:** Create the service account using vastool on the SAP R/3 Server host:

Example: 

```
# /opt/quest/bin/vastool –u <username> service create SAP/
```

This command creates the file /etc/opt/quest/vas/SAP.keytab. The –u parameter, <username>, is the name of the active directory user with administrative privileges to create a new service account. The user will be prompted for their Active Directory (AD) password which is required to authenticate them to AD.

**Step 2:** Set the password to “never expires” and “can not be changed”.

```
# /opt/quest/bin/vastool -u administrator setattrs SAP/ userAccountControl 66048
```

**Step 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.

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

3 The HOST keytab (The Kerberos keytab used by the computer host itself) can, and should ONLY be used during the initial installation to simplify configuration and troubleshooting. When Vintela Authentication Services is properly configured, the klist command can be used to display the Kerberos ticket cache, which will contain tickets showing the hosts KRB5 principal name.
This command changes the group ownership of the keytab to the sapsys group.

    # chmod 640 /etc/opt/quest/vas/SAP.keytab
or
    # chmod g=r /etc/opt/quest/vas/SAP.keytab

These commands change the file access permissions so that group has read rights.

**Step 4:** Set the `snc/identity/as` value to `p:SAMACCOUNTNAME@ADDOMAIN.TLD`, where ADDomain.TLD is the Kerberos realm name (Active Directory domain name) to which the R/3 host is joined. See [Enabling SNC on the SAP R/3 Server](#).

You can obtain the sAMAccountName by running the following:

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

**Step 5:** Set the **SNC Name** in the Advanced Options of the SAPlogin to `p:SAMACCOUNTNAME@ADDOMAIN.TLD`. See [Configuring the SAP GUI Client on Windows XP](#).

**Step 6:** On the SAP R/3 server, set the environment variable `KR5_KTNAME` to the location of the previously created SAP.keytab file. For example, in `~<instance>/adm/.cshrc` add

    setenv KR5_KTNAME /etc/opt/quest/vas/SAP.keytab

**Step 7:** Restart the SAP services.

## Configuring a SAP User to Enable SNC Authentication

Each user must have a unique Kerberos principal name (KPN) associated with their SAP account to take advantage of the single sign-on and security features of the VAS SNC solution.

**Step 1:** Run transaction SU01 or access the user management functions under **SAP Menu -> Tools -> Administration -> User Maintenance -> Users**.

**Step 2:** Open the **SNC** tab of the user management screen.

**Step 3:** Enter the KPN or “SNC name” of the user. This is the Windows pre-2000 name of the Windows user (case sensitive) including the domain in the form “p:sAMAccountName@ADdomain.tld” where sAMAccountName is the Windows pre-2000 name and ADdomain.tld is the Kerberos realm (Active Directory domain) that corresponds to the SAP user account. This is the user whose credentials will be used to authenticate to the associated SAP user account.
Step 4: Click **Save** on the menu bar to save these changes.

Step 5: Confirm that the canonical name (SNC name) is valid. Click the User Names menu, click **Display**, and then click the SNC tab. On the SNC data property sheet, a check mark should be displayed next to the message “Canonical name determined,” as show above (The canonical names are stored in the USRACL table).
Installing Quest VAS SSO for SAP

NOTE: Run the installer as a user with Administrator rights. If the installer is run as a Domain User with no administrative rights, the SNC_LIB system environment variable will not be set. To resolve this issue an administrator can set the environment variable path for SNC_LIB.

To install the VAS_SSO_for_SAP-1.0.x.x.msi

Step 1. From the product CD, select add-ons -> VAS_SSO_for_SAP -> windows.
Step 2. Click VAS_SSO_for_SAP-1.0.x.x.msi to launch the installer.

The Welcome screen is displayed.

Step 3. Click Next.
The **License** screen is displayed. A valid license is required to install this product.

**Step 4.** Click the **Browse** button to locate the license file (.txt).

**Step 5.** Locate and select the license file and click **Open**.

**Step 6.** A window will display “License file is valid” or “License file could not be validated.” If license file is valid, as shown in the following graphic, click **Next**.
The License Agreement window is displayed.

Step 7. Click I accept the terms in the license agreement and click Next.

The Destination Folder screen is displayed.

Step 8. Click Next to install to this folder, or click Change to install to an alternate location.
Step 9. The Setup Type screen is displayed. Click **Complete** and click **Next**.

![Setup Type Screen](image)

The **Ready to Install** screen is displayed. The Wizard is now ready to begin the installation.

![Ready to Install Screen](image)

Step 10. Click **Install** to begin the installation.

If you want to review or change any installation settings, click **Back**. Click **Cancel** to exit the wizard.

Step 11. When the installation is complete, the Wizard completion screen is displayed.
Step 12. Click **Finish** to exit the wizard.

**Deploying SAP Using Group Policy**

When deploying SAP with VAS Group Policy, the installer is different in that we write to a registry key: HKLM\Software\Quest Software\VAS SSO for SAP. The path to the license is stored in the entry License.

If this registry key is set before the installer is run, and the license is valid, the selected license page will display the license information.

*To deploy using group policy (through the msi and mst file):*

**Step 1.** Download Microsoft Cabinet SDK from the following link


**Step 2.** Open a cmd prompt and navigate to the location where you extracted the Microsoft Cabinet SDK (You probably don't want to extract this to the temp folder).

**Step 3.** Rename your license to license.txt

**Step 4.** Run the following command:

```
Makecab "<path to license>" license.cab
```

**Step 5.** Copy license.cab to the same directory as the msi and mst file.

**Step 6.** Run the following command to install:

```
msiexec /i "<msi>" TRANSFORMS="VAS_SSO_for_SAP.mst" /qb
```
Configuring the SAP GUI Client on Windows XP

Step 1: Verify that the environment variable SNC_LIB contains the path to the security product library. The library can be found at C:\Program Files\Quest Software\Vintela Authentication Services\gskrsrb5.dll. (Set the SNC_LIB variable for each windows user or set it as a system environment variable.)

Step 2: Run the SAPlogin application.

Step 3: Select a server connection and click Change Item to bring up the Properties page. (The SAPgui client should already be installed and configured for normal password-based authentication.)

Step 4: Click the Advanced button to open the Advanced Options.

Step 5: Enable SNC by selecting the Enable Secure Network Communication check box.
Step 6: Enter the KPN of the SAP R/3 server (e.g., p:SAMACCOUNTNAME@ADDOMAIN.TLD). This should be the same KPN that was used for the SAP instance profile key snc/identity/as described in "Enabling SNC on the SAP R/3 Server" above.

Step 7: Select the Max. Available option on radio buttons to enable single sign-on as well as data integrity and encryption for all of the traffic between the SAPgui client and the R3 server.

Step 8: Click OK to save these settings.

You should now be able to log on to the server by clicking the server name in SAPlogon, without being prompted for a username or password.

Once the server connection has been configured 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 GSS-API 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 passwords.

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.

Step 1: Create a SAPlpd.INI file in the windows directory if one doesn’t already exist.

Step 2: Add the following section to the SAPlpd.INI file: (These settings can also be added to the WIN.INI file if you do not want to create the SAPlpd.INI file)

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

Note: The gssapi_lib= entry can be omitted when the environment variable SNC_LIB is 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. This should be in the following format: u:sAMAccountName@ADdomain.tld where sAMAccountName is the Windows pre-2000 name of the Windows user logged in and ADdomain.tld is the Kerberos realm (Active Directory domain). Assuming drive C: is your boot volume, the path to the gss-api library by default is C:\Program Files\Quest Software\Quest GSS-API for SAP\qgsskrb5.dll
Step 3: Run SAPIpd. A window appears listing the output from the SAPIpd startup.

Step 4: From the SAPLOPD.LOG – SAPIPD window, select the Options->Secured Connections menu item. The following dialog box opens:

Step 5: Click the Use if possible and Privacy protection of data radio buttons.

Step 6: Click the Add new connection button to go to the Access Control List (ACL) maintenance for SAPIpd.
Step 7: Enter the SNC-name of the application server(s) (This is the value of the `snc/identity/as` key from the instance profile on the VAS enabled SAP R/3 server).

See Enabling SNC on the SAP R/3 Server) that will be transferring print jobs to this SAPIpd, using SNC, into the field Last authenticated connection initiator.

Step 8: Click Authorize to add this name to the list of authorized connection initiators.

Step 9: Close all open SAPIpd dialog boxes by clicking their OK buttons.

Your front end desktop is now configured to securely connect to the VAS SNC solution.

**Configuring SAPIpd on the SAP R/3 Server**

Step 1: Create a new output device (Printer) by choosing Configuration -> Output devices from the Spool Administration (transaction SPAD) screen. (These same settings can be applied to an existing device)

Step 2: Click the DeviceAttributes tab.

Step 3: Fill in the fields: Output device, Short name, Device Type and Spool Server. When filling in the Spool Server, pressing the F4 key or pressing the folder icon next to the Spool Server field will list all the application servers with a color-coded background. The application servers running a spool process will be highlighted in green.
Step 4: Click the Access Method tab.

Step 5: Set the Host Spool Access Method to “S: Print Using SAP Protocol”.

Step 6: Enter the name of the Host printer.

Step 7: Enter the host name of the front end PC as the Destination host.

Step 8: Check the Do not query host spooler for output status option.
Step 9: Click the Security tab and select the level of security needed. Security options are: “Only Authentication,” “Integrity Protection,” and “Privacy Protection.”

Step 10: Specify whether SNC is required (Only Use Secure Transfer) or not, by changing the Security Mode.

Step 11: Enter the SNC name of the Active Directory user who will be logged in when using this instance of SAPlpd in the Identity of the remote SAPlpd for the security system field. This is entered in the format "u:sAMAccountName@ADdomain.tld.com" where sAMAccountName is the Windows pre-2000 name of the user and ADdomain.tld is the Kerberos realm (Active Directory domain). See Configuring SAPlpd on the Front End System.

Step 12: Save the changes and exit the Spool Administration screens.
Testing the printer connection

**Step 1:** Verify that SAPlpd is still running. From the list of output devices you can print using the ‘printer’ icon or the menu path **System → List → Print..**
Step 2: Select the SNC enabled output device that you just created and change the Time of Print to “Print out immediately”.

Step 3: Submit the print request by clicking **Continue** or the green check mark. You can track the status and progress.