Pluggable Authentication Services for External Authentication Mechanisms

MYSAP.WP_SEC

Release 6.20

Document Version 2.2

12/27/2002

Copyright

Icons

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Typographic Conventions

Type Style	Description
Example text	Words or characters that appear on the screen. These include field names, screen titles, pushbuttons as well as menu names, paths and options. Cross-references to other documentation.
`Example text`	Emphasized words or phrases in body text, titles of graphics and tables.
EXAMPLE TEXT	Names of elements in the system. These include report names, program names, transaction codes, table names, and individual key words of a programming language, when surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Screen output. This includes file and directory names and their paths, messages, source code, names of variables and parameters as well as names of installation, upgrade and database tools.
`EXAMPLE TEXT`	Keys on the keyboard, for example, function keys (such as `F2`) or the `ENTER` key.
`Example text`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Pointed brackets indicate that you replace these words and characters with appropriate entries.

Contents

Pluggable Authentication Services for External Authentication

Use

Using pluggable authentication services (PAS) allows you to authenticate your SAP users using external mechanisms instead of those provided by SAP. Based on the external authentication, the PAS issues the user a logon ticket, which is then used for further authentication when accessing the SAP services. In this way, you can integrate your SAP services into an existing Single Sign-On (SSO) environment that uses non-SAP authentication.

There are a number of external authentication mechanisms that you can use, for example:

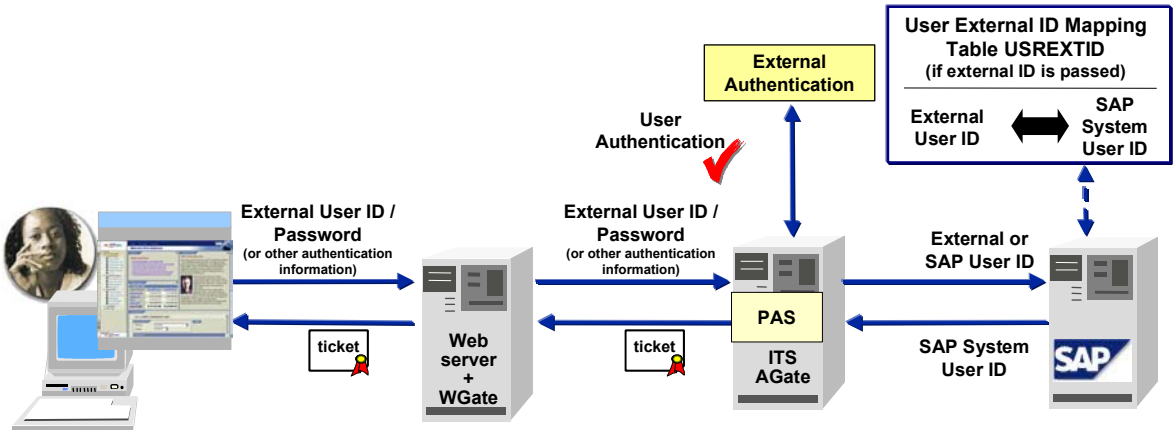
- Windows NT LAN Manager (NTLM) authentication
- User ID and password verification using the Windows NT domain controller
- Authentication using an LDAP bind to a directory server
- Authentication using the Secure Sockets Layer (SSL) protocol and X.509 client certificates
- An arbitrary authentication mechanism on the Web server that sets the user's ID in an HTTP header variable
- An arbitrary mechanism on the AGate that is provided by a certified partner

Integration

When using PAS, the actual user authentication takes place outside of the SAP system. When the user accesses the SAP system via the ITS, the external mechanism authenticates the user and informs the PAS of the result. If the external authentication was successful, the PAS passes this information on to the SAP system so that it can issue the user his or her logon ticket. Depending on the mechanism you use, the user's ID for the logon ticket is either sent with his or her authentication information from the external mechanism or it is obtained from the user external ID mapping table in the SAP system.

The external authentication can take place on either of the ITS components, the AGate or the WGate. See the graphics below.

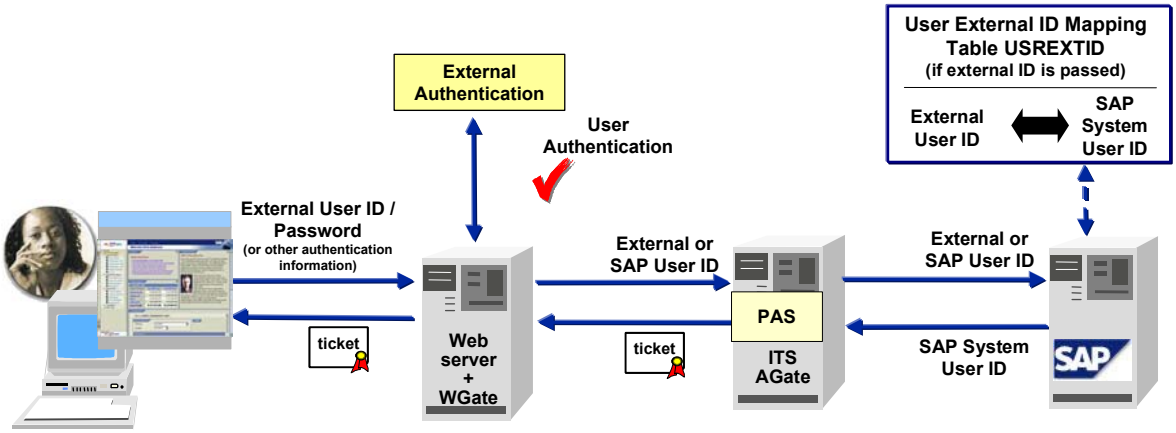
Pluggable Authentication Services on the AGate



Examples of external authentication mechanisms that take place on the AGate include:

- Verifying the user's Windows NT domain and password on the domain controller
- LDAP bind to a directory server
- An authentication mechanism provided by a certified partner that occurs on the AGate

Pluggable Authentication Services on the Web Server (WGate)



Examples of external authentication mechanisms that take place on the Web server (WGate) include:

- Windows NTLM authentication
- SSL and X.509 client certificates
- An arbitrary authentication mechanism on the Web server that sets the user's ID in an HTTP header variable

Platform Availability

The supported PAS mechanisms are available for the ITS platforms as shown in the table below.

Availability of PAS

PAS Type	Authenticating Component (AGate / WGate)	Available Platforms
Windows NTLM	WGate	Microsoft Internet Information Server (IIS)
Verifying Windows NT User ID / Password	AGate	Windows NT/2000/XP
X.509 Client Certificates	WGate	All supported Web server platforms
LDAP bind	AGate	All supported AGate platforms
HTTP header variables	WGate	All supported Web server platforms
Partner mechanisms	AGate	Determined by availability of the partner product

The other ITS component can run on a different platform. For example, when using Windows NTLM authentication, the AGate can run on a Linux host.

For more information about ITS availability and supported platforms, see the SAP Service Marketplace at http://service.sap.com/sap-its.

Prerequisites

For your SAP system to be able to use PAS, it must meet the following prerequisites:

- One system must be set up as a ticket-issuing system, for example, an SAP system application server, and the corresponding ITS.
- The other SAP systems in your SSO environment must be set up to accept the logon tickets. The prerequisites for using logon tickets must therefore also be met:
  - The user must have the same user ID in all systems that are to accept logon tickets.
  - Accepting systems must meet the system requirements as described in SAP note 177895.
  - Users must configure their Web browsers to accept cookies. (The logon ticket is a session cookie with the name MYSAPSSO2.)
  - The Web servers used to access the various systems must all reside in the same DNS domain.

- Because the authentication occurs externally and not within the SAP system itself, you must use Secure Network Communications (SNC) between the ITS AGate and the SAP system to guarantee the integrity and security of the user's authentication.

  For cases where the ITS is installed as a dual host installation and where the pluggable authentication takes place on the Web server, we also recommend using SNC between the ITS WGate and the AGate components.

- The ticket-issuing SAP system must be able to recognize the user's ID.

  The system searches for an entry in the user external ID mapping table (USREXTID) that maps the user's external ID to his or her user ID for the SAP system. Alternatively, when using LDAP bind, HTTP header variables, or a mechanism provided by a partner, then the external authentication mechanism can provide the user's ID for the SAP system directly. In this case, no mapping entry in the table USREXTID is necessary.

  For example, you can store the user's ID for the SAP system in the directory server used for the LDAP bind authentication. In this case, the user's ID is obtained from the directory server instead of from the mapping table in the SAP system.

In addition, you must also meet any requirements for the specific scenario you use. For more information, see the sections provided for each of these scenarios.

Authentication Mechanisms Supported by the PAS

The authentication mechanisms supported by the PAS are described individually in the topics that follow. See:

- Authentication Using Windows NTLM [Page 8]
- Verifying User ID/Password on the Windows NT Domain Controller [Page 10]
- Authentication Using X.509 Client Certificates [Page 11]
- Authentication Using an LDAP Bind to a Directory Server [Page 13]
- Authentication Using an Arbitrary Mechanism on the Web Server [Page 14]
- Authentication Using a Mechanism Provided by a Partner [Page 16]

Authentication Using Windows NTLM

Purpose

With this PAS option, the user is authenticated using the Windows NTLM protocol, which takes place between the user's Web browser and the Web server. The user's Windows ID is then passed to the SAP system using the PAS service. The user's SAP system ID is obtained from the mapping table USREXTID in the SAP system and a logon ticket is created for the user. Single Sign-On is then available to additional SAP services using the logon ticket.

Prerequisites

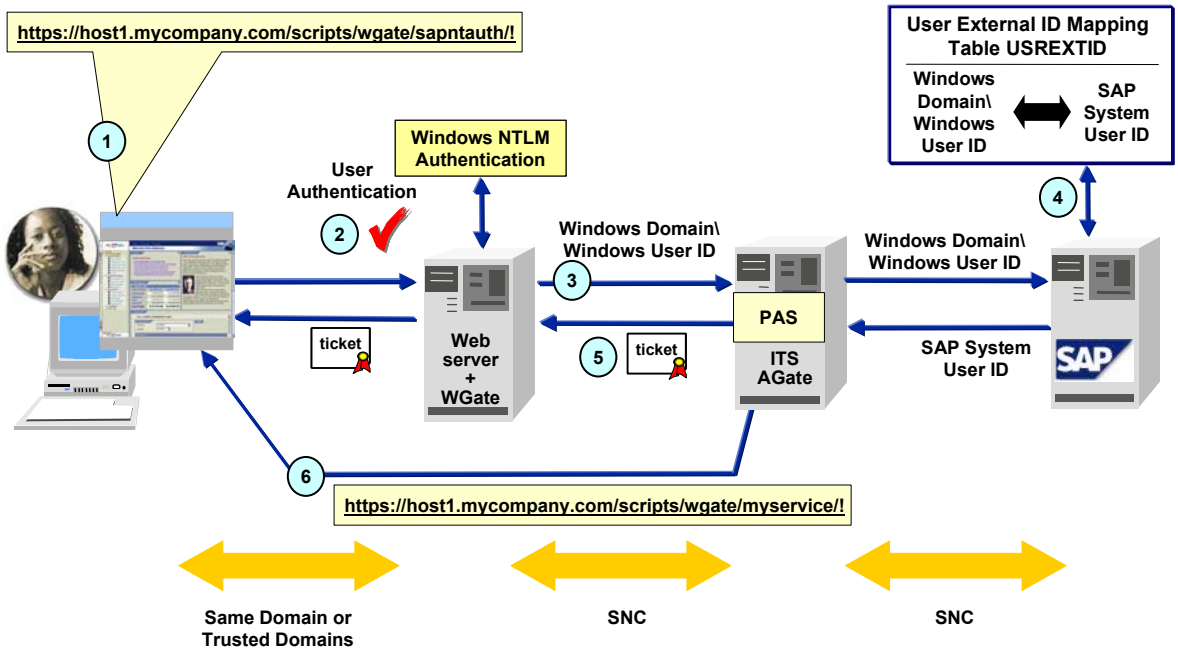
For the prerequisites for using Windows NTLM authentication for PAS, see the following topics:

- Logon Tickets [Page 18]
- Prerequisites for Using Windows NTLM Authentication [Page 18]
- Secure Network Communications [Page 22]

Process Flow

See the graphic below:

Using Windows NTLM Authentication



The user must be logged onto the Windows domain. The process is then as follows:

1. The user accesses the PAS service for using Windows NTLM authentication (for example, `sapntauth`).
2. The Web server authenticates the user using the Windows NTLM protocol between the Web browser and the Web server. If successful, the Web server provides the user's information (`<Windows_domain>\<Windows_user_ID>`) to the WGate.
3. The WGate passes this information to the PAS service on the AGate, which passes it on to the SAP system application server.

4. The SAP system searches for a matching user ID in the user external ID mapping table.
5. If successful, the PAS creates a logon ticket for the user, which it sets in the user's Web browser.
6. The PAS redirects the user to the designated service (for example, `myservice`).

Result

No user ID and passwords entries are necessary for accessing the SAP system.

When the user accesses further SAP services, the logon ticket is used for Single Sign-On access.

Verifying User ID/Password on the Windows NT Domain Controller

Purpose

With this PAS option, the user's Windows ID and password are verified on the Windows NT domain controller. The user must therefore provide his or her Windows domain user ID and password when he or she accesses the PAS service. The PAS then verifies this information with the Windows domain controller. If successful, then the user's ID in the SAP system is obtained from the user external ID mapping table and a logon ticket is created for the user. Single Sign-On is then available to SAP services using the logon ticket.

Prerequisites

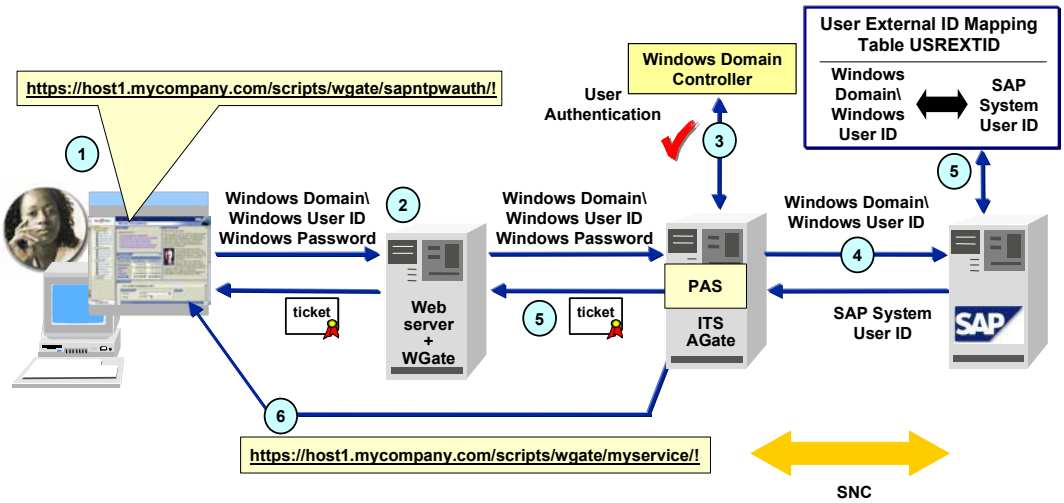
For the prerequisites for using Windows NT domain authentication for PAS, see the following topics:

- Logon Tickets [Page 18]
- Prerequisites for Verifying Users on the Domain Controller [Page 19]
- Secure Network Communications [Page 22]

Process Flow

See the graphic below:

Using User ID and Password Verification on the Windows NT domain controller



The process is as follows:

1. The user accesses the PAS service for using the Windows NT domain controller password verification (for example, `sapntpwauth`).
2. The user provides his or her Windows NT user ID (with domain) and password.
3. The PAS sends the user's ID and password to the Windows NT domain controller to be verified.
4. If the user's ID and password could be verified, then the PAS passes this ID to the SAP system application server.
5. The SAP system searches for a matching user ID in the user external ID mapping table.
6. If successful, the PAS creates a logon ticket for the user, which it sets in the user's Web browser.
7. The PAS redirects the user to the designated service (for example, `myservice`).

Result

The user accesses the SAP service after authenticating him or herself using his or her Windows NT domain user ID and password.

When the user accesses further SAP services, the logon ticket is used for Single Sign-On access.

Authentication Using X.509 Client Certificates

Purpose

With this PAS option, the user is authenticated using the SSL protocol and X.509 client certificates, which takes place between the user's Web browser and the Web server. If successful, the user's Distinguished Name that is contained in his or her certificate is passed to the SAP system. The user's SAP system ID is obtained from the mapping table USREXTID in the SAP system and a logon ticket is created for the user. Single Sign-On is then available to additional SAP services using the logon ticket.

Prerequisites

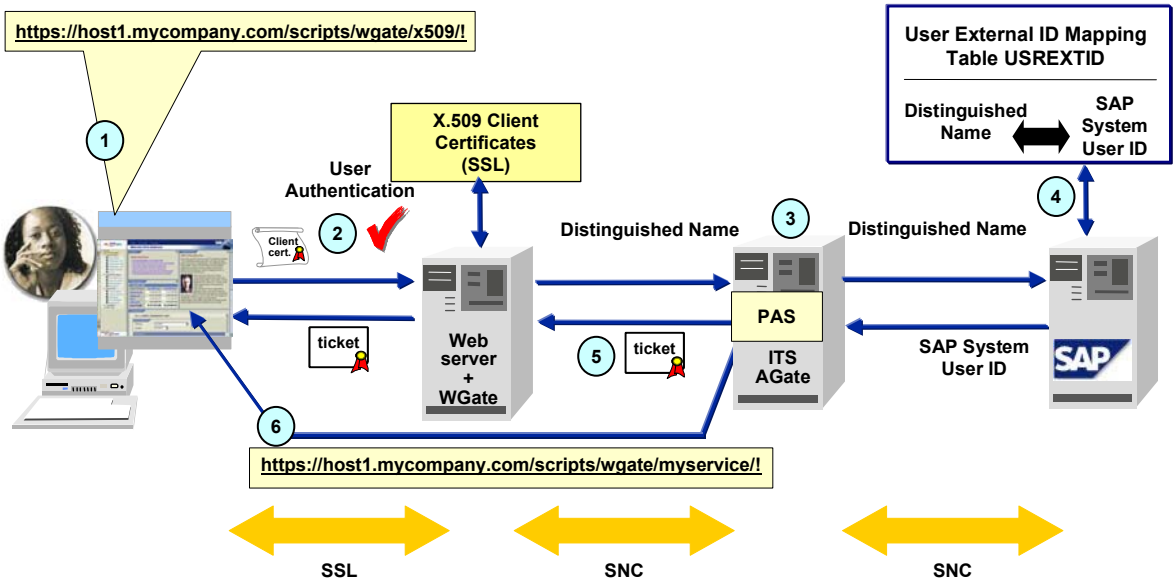
For the prerequisites for using X.509 client certificates for PAS, see the following topics:

- Logon Tickets [Page 18]
- Prerequisites for Using X.509 Client Certificates [Page 19]
- Secure Network Communications [Page 22]

Process Flow

See the graphic below:

Using SSL and X.509 Client Certificates for Authentication



The process is as follows:

1. The user accesses the PAS service for using X.509 client certificates (for example, `x509`).
2. Based on the information contained in the user's client certificate, the Web server authenticates the user using the SSL protocol. This takes place in the protocol layer between the Web browser and the Web server. If successful, the Web server provides the user's Distinguished Name to the WGate.
3. The WGate passes this information to the PAS service on the AGate, which passes it on to the SAP system application server.
4. The SAP system searches for a matching user ID in the user external ID mapping table.
5. If successful, the PAS creates a logon ticket for the user, which it sets in the user's Web browser.
6. The PAS redirects the user to the designated service (for example, `myservice`).

Result

No user ID and passwords entries are necessary for accessing the SAP system.

When the user accesses further SAP services, the logon ticket is used for Single Sign-On access.

Authentication Using an LDAP Bind to a Directory Server

Purpose

With this PAS option, the user is authenticated using an LDAP bind to a directory server. The PAS verifies the LDAP bind and then issues the user a logon ticket for access to further SAP services. Note that in this case, you can alternatively store the user's ID to use for the logon ticket in the directory server instead of using the user external ID mapping table in the SAP system.

Prerequisites

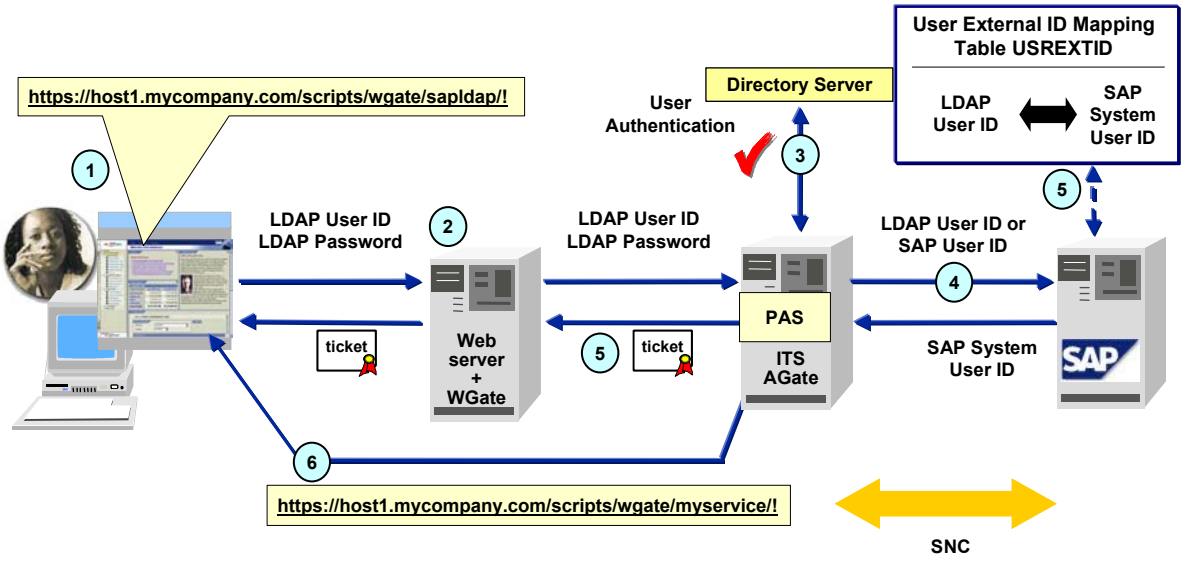
For the prerequisites for using an LDAP bind for PAS, see the following topics:

- Logon Tickets [Page 18]
- Prerequisites for Using an LDAP Bind to a Directory Server [Page 20]
- Secure Network Communications [Page 22]

Process Flow

See the graphic below:

Using an LDAP Bind to a Directory Server for Authentication



The process is as follows:

1. The user accesses the PAS service for using the LDAP bind (for example, `sapldap`).
2. The user provides his or her user ID and password for the directory server.
3. The PAS attempts an LDAP bind on the directory server using the user's ID and password.

4. If the LDAP bind was successful, then:
    a. If the user's ID for the SAP system is stored in the directory, then the PAS passes this ID to the SAP system application server.
    b. Otherwise, it passes the user's ID for the directory server to the SAP system application server. The SAP system then searches for a matching user ID in the user external ID mapping table.
5. The PAS then creates a logon ticket for the user, which it sets in the user's Web browser.
6. The PAS redirects the user to the designated service (for example, `myservice`).

Result

The user accesses the SAP service after authenticating him or herself using an LDAP bind on the directory server.

When the user accesses further SAP services, the logon ticket is used for Single Sign-On access.

Authentication Using an Arbitrary Mechanism on the Web Server

Purpose

With this PAS option, the user is authenticated using an arbitrary authentication mechanism that occurs on the Web server. This mechanism sets the user's ID in an HTTP header variable so that it can be retrieved by the WGate and passed on to the AGate. As with the LDAP bind option, the arbitrary mechanism can provide the user's ID for the SAP system directly. Otherwise, the system obtains the SAP user ID from the user external ID mapping table USREXTID. The system then issues the user his or her logon ticket.

Prerequisites

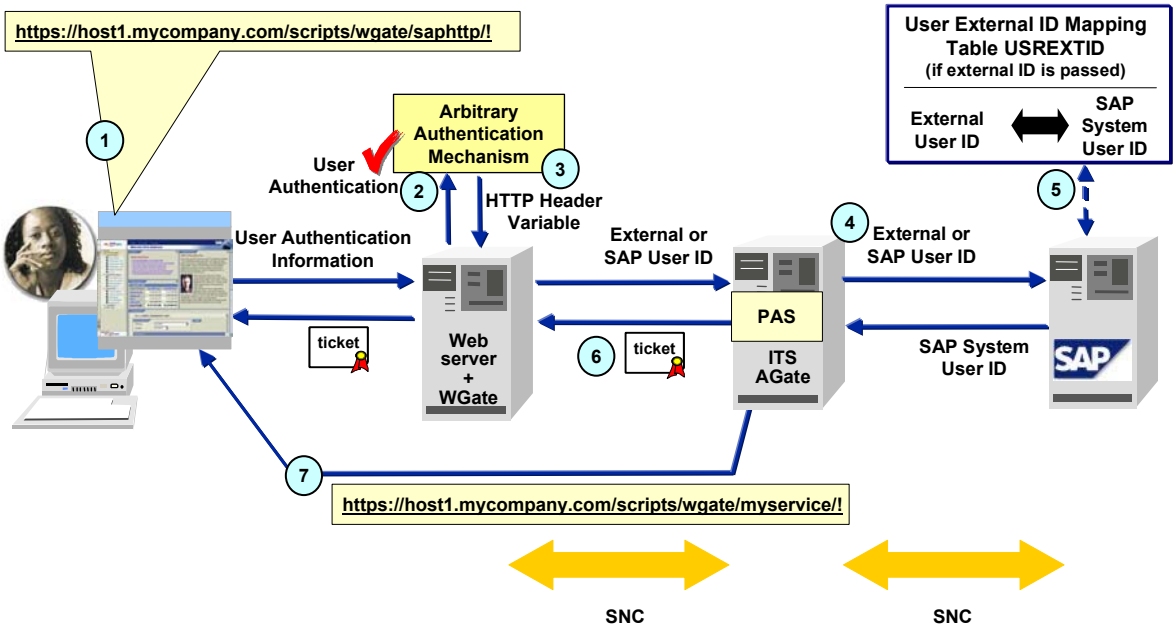
For the prerequisites for using an arbitrary authentication mechanism on the Web server for PAS, see the following topics:

- Logon Tickets [Page 18]
- Prerequisites for Using an Arbitrary Mechanism on the Web Server [Page 21]
- Secure Network Communications [Page 22]

Process Flow

See the graphic below:

Using an Arbitrary Authentication Mechanism on the Web Server



The process is as follows:

1. The user accesses the PAS service for using the arbitrary authentication mechanism (for example, `saphttp`).
2. The user is authenticated by the external authentication mechanism. (Depending on the authentication mechanism used, the user may have to provide authentication information, for example, user ID and password.)
3. If the authentication was successful, the authentication mechanism sets the user's ID in the HTTP header variable.
4. The WGate retrieves the user ID from the HTTP header variable and passes it to the AGate, which passes it to the SAP system application server.
5. If the user ID that is passed is not the SAP user ID, then the SAP system searches for a matching user ID in the user external ID mapping table.
6. If successful, the PAS issues the user a logon ticket, which it sets in the user's Web browser.
7. The PAS redirects the user to the desired service (for example, `myservice`).

Result

The user accesses the SAP service after authenticating him or herself using the arbitrary authentication mechanism.

When the user accesses further SAP services, the logon ticket is used for Single Sign-On access.

Authentication Using a Mechanism Provided by a Partner

Purpose

With this PAS option, the user is authenticated using an authentication mechanism that is provided by an SAP-certified partner. The PAS verifies the user's authentication with the partner product. Also in this case, the authenticating mechanism can provide the user's ID for the SAP system directly. Otherwise, the system obtains the SAP user ID from the user external ID mapping table USREXTID. The system then issues the user his or her logon ticket.

Prerequisites

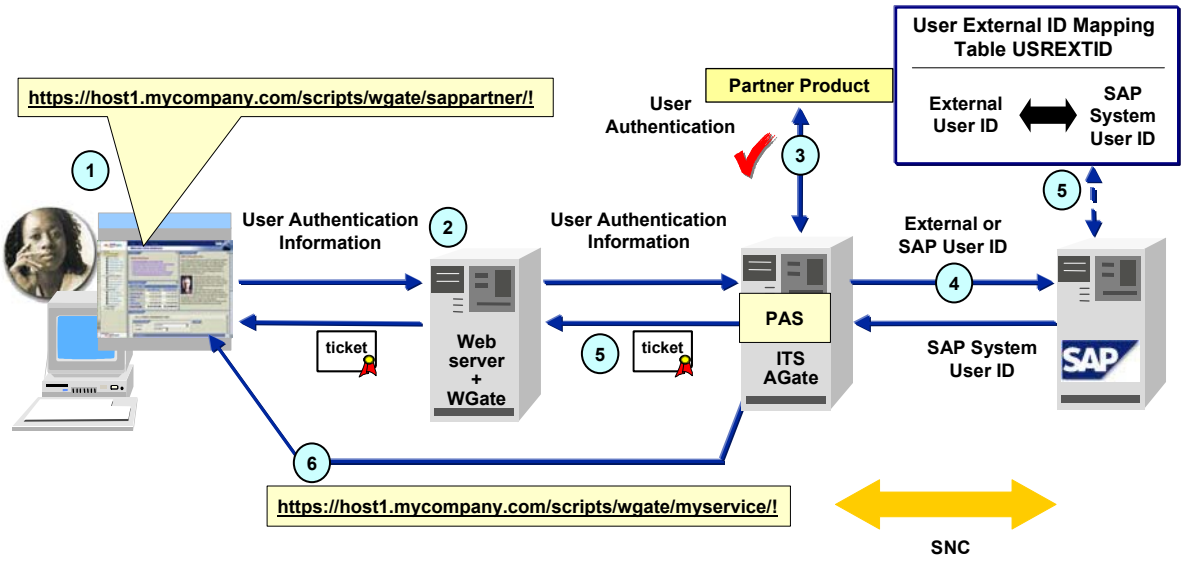
For the prerequisites for using a partner mechanism for PAS, see the following topics:

- Logon Tickets [Page 18]
- Prerequisites for Using a Partner Mechanism [Page 21]
- Secure Network Communications [Page 22]

Process Flow

See the graphic below:

Using an Authentication Mechanism Provided by a Partner



The process is as follows:

1. The user accesses the PAS service for using the partner's authentication (for example, `sappartner`).
2. The user provides his or her user ID and password (or other authentication information) for the partner product.
3. The PAS verifies the user's authentication information with the partner product.

4. If successful, then:
    a. If the partner product provides the user's ID for the SAP system directly, then the PAS passes this ID to the SAP system application server.
    b. Otherwise, it passes the user's ID for the partner product to the SAP system application server. The SAP system then searches for a matching user ID in the user external ID mapping table.
5. The PAS then creates a logon ticket for the user, which it sets in the user's Web browser.
6. The PAS redirects the user to the designated service (for example, `myservice`).

Result

The user accesses the SAP service after authenticating him or herself using the partner product.

When the user accesses further SAP services, the logon ticket is used for Single Sign-On access.

Prerequisites for Using PAS

There are a number of prerequisites that your system must fulfill before you can use the PAS. Some of these are dependent on the PAS option that you use. See:

- Logon Tickets [Page 18]
- Scenario-specific prerequisites:
    - Prerequisites for Using Windows NTLM Authentication [Page 18]
    - Prerequisites for Verifying Users on the Domain Controller [Page 19]
    - Prerequisites for Using X.509 Client Certificates [Page 19]
    - Prerequisites for Using an LDAP Bind to a Directory Server [Page 20]
    - Prerequisites for Using an Arbitrary Mechanism on the Web Server [Page 21]
    - Prerequisites for Using a Partner Mechanism [Page 21]
- Secure Network Communications [Page 22]

Logon Tickets

So that the system can issue a logon ticket to the user after being authenticated using the external authentication mechanism, your system must meet the following requirements:

- One system must be set up as a ticket-issuing SAP system, for example, an SAP system application server, along with its corresponding ITS. This system and any other systems that are to accept logon tickets must also be configured accordingly. For more information, see Configuring the Use of Logon Tickets [Page 23].
- Accepting systems must meet the following release requirements:
  - Release 4.0x: Release 4.0B kernel, patch level 758 or higher
  - Release 4.5x: Release 4.5B kernel, patch level 459 or higher
  - Release 4.6x: Release 4.6D kernel, patch level 74 or higher
  - All Release 4.x systems: The Workplace Plug-In must be installed.
  - Release 6.xx: no kernel or patch level requirements

    For more information, see SAP Note 177895.

    The release requirements for the servers used for the ticket-issuing system depend on the PAS option that you are using. Therefore, see the prerequisites for your specific scenario.
- The Web servers used to access the various systems must all reside in the same DNS domain.
- The user must have the same user ID in all systems that are to accept logon tickets.
- Users must configure their Web browsers to accept session cookies.

Prerequisites for Using Windows NTLM Authentication

When using the Windows NTLM authentication as the external authentication mechanism, your system must meet the following requirements:

- The ticket-issuing application server must be at least Release 4.6D, patch level 317.
- The ticket-issuing system's ITS must be at least Release 4.6D C4.
- The Web server must be a Microsoft Internet Information Server (IIS).
- The Web server must be configured for using Windows NTLM authentication mechanism. See Configuring Windows NTLM Authentication on the Web Server [Page 26].
- The user's frontend clients must either reside in the same Windows NT domain as the Web servers, or the domains must trust each other.
- The user's Web browser must be a Microsoft Internet Explorer.
- SNC is required between the AGate and the ticket-issuing application server.

  Because the user authentication takes place on the Web server, we also recommend using SNC for the connection between the WGate and the AGate if the ITS installation is a dual host installation.

  We also recommend using SNC for the connections to systems that accept logon tickets.

Prerequisites for Verifying Users on the Domain Controller

When verifying the user's ID and password on the Windows NT domain controller, your system must meet the following requirements:

- The ticket-issuing application server must be at least Release 4.6D, patch level 317.
- The ticket-issuing system's ITS must be at least Release 4.6D. For Release 4.6D we also recommend using a patch level higher than 343. For Release 6.10 C1, use patch level 11 or higher.

  Prior to these ITS Releases, the AGate's user must have the additional right to *Act as part of the operating system*.
- The AGate must run on a Windows server and must run under a valid user account that exists in the Windows domain.
- SNC is required for the connection between the AGate and the ticket-issuing application server.

  We also recommend using SNC for the connections to systems that accept logon tickets.
- The user must have an account on the Windows domain. The standard *Guest* account cannot be used.
- You must also provide a logon screen so that the user can enter the Windows domain, his or her Windows user ID, and his or her password. Specify this screen in the login template for the PAS service.

  For a sample template file, see the PAS installation package [Page 32].

Prerequisites for Using X.509 Client Certificates

When using X.509 client certificates as the PAS option, the user authentication takes place using the Secure Sockets Layer (SSL) protocol between the user's Web browser and the Web server. For this scenario, your system must meet the following prerequisites:

- The ticket-issuing application server must be at least Release 4.6D, patch level 258.
- The ticket-issuing system's ITS must meet the following release requirements:
  - Release 4.6D C4, patch level 172 or higher
  - Release 6.10 C1, patch level 2 or higher
  - As of Release 6.20, no patch level requirements

- The Web server must be configured to use SSL with mutual authentication. Therefore:
  - The Web server must possess a public and private key pair and a corresponding X.509 server certificate that it can use for SSL.
  - The user must also possess a public and private key pair and a corresponding X.509 client certificate.
  - The user's Web browser must trust the issuer of the Web server's certificate.
  - The Web server must trust the issuer of the user's client certificate.
- SNC is required for the connection between the AGate and the ticket-issuing application server.

  Because the user authentication takes places on the Web server, we also recommend using SNC for the connection between the WGate and the AGate if the ITS installation is a dual host installation.

  We also recommend using SNC for the connections to systems that accept logon tickets.
- The user type defined in the user external ID mapping table must be the type `DN`.

Prerequisites for Using an LDAP Bind to a Directory Server

When using an LDAP bind to a directory server as the external authentication mechanism with PAS, your system must meet the following requirements:

- If the user's ID for the SAP system is stored in the directory and passed directly to the PAS, then the ticket-issuing application server must be at least Release 4.6D, patch level 317. If you maintain the user's ID for the directory in the user external ID mapping table USREXTID, the ticket-issuing application server must be at least Release 6.10.
- The ticket-issuing system's ITS must be at least Release 6.10 C1, patch level 14.
- The AGate must have access to the LDAP client library to perform the LDAP bind. For Windows NT/2000/XP systems the PAS uses the LDAP library `wldap32.dll`. On LINUX systems you must have installed the **`openldap2-client`** package.
- SNC is required for the connection between the AGate and the ticket-issuing application server.

  We also recommend using SNC for the connections to systems that accept logon tickets.
- The user must have a user ID for the directory that he or she can use to connect to the directory using an LDAP bind.
- You must provide a login screen so that the user can enter his or her user information for the directory.

  For a sample template file, see the PAS installation package [Page 32].

Prerequisites for Using an Arbitrary Mechanism on the Web Server

To be able to use an arbitrary authentication mechanism that sets the user information in HTTP header variables, your system must meet the following requirements:

- The ticket-issuing application server must be at least Release 4.6D, patch level 317.
- The ticket-issuing system's ITS must meet the following release requirements:
  - Release 4.6D C4, patch level 340 or higher
  - Release 6.10, patch level 11 or higher
  - Release 6.20, no patch level requirements
- SNC is required for the connection between the AGate and the ticket-issuing application server.

  Because the user authentication takes places on the Web server, we also recommend using SNC for the connection between the WGate and the AGate if the ITS installation is a dual host installation.

  We also recommend using SNC for the connections to systems that accept logon tickets.
- The authentication mechanism must set the user's ID in an appropriate HTTP header variable.

  Each Web server has pre-defined HTTP header variables that it uses for various purposes. For example, the Microsoft Internet Information Server (IIS) and the Apache Web server use the header variable `REMOTE_USER` to store the user's ID. The arbitrary authentication mechanism that you use can either set this variable directly or it can use a self-defined one.

Prerequisites for Using a Partner Mechanism

To be able to use an authentication mechanism that is provided by a partner, the following requirements must be met:

- The ticket-issuing application server must be at least Release 4.6D, patch level 317.
- The ticket-issuing system's ITS must be at least Release 4.6D.
- SNC is required for the connection between the AGate and the ticket-issuing application server.

  We also recommend using SNC for the connections to systems that accept logon tickets.
- The partner product must be certified by the SAP Software Partner Program.

Secure Network Communications

Because the user authentication occurs externally and not within the SAP system itself, you must use Secure Network Communications (SNC) between the ITS AGate and the ticket-issuing application server. When using SNC, the data transfer is encrypted so that the logon ticket cannot be stolen or manipulated.

We also recommend the following:

- If you use an external mechanism that takes place on the Web server, and the ITS is a dual host installation, then we also recommend using SNC for the connection between the WGate and the AGate.
- We also recommend using SNC for the connections between the ITS components and application servers for systems that accept logon tickets.
- For connections that use the HTTP protocol, for example, connections to an SAP Web Application Server, we recommend using the Secure Sockets Layer (SSL) protocol instead of SNC.

SNC requires the use of an external security product to provide the protection. For server-to-server connections such as the connection between the application server and the AGate, you can use the SAP Cryptographic Library, which is available on the SAP Service Marketplace for authorized customers at http://service.sap.com/swcenter.

Otherwise, you must use an SAP-certified partner product. For a list of these products, see the SAP Software Partner Program at http://www.sap.com/softwarepartner. Search in the Software Partner Directory using the software category *Network Security*.

See also:

- *SNC User's Guide*
- Using the SAP Cryptographic Library for SNC [SAP Library]

These documents are available on the SAP Service Marketplace at http://service.sap.com/security.

Configuring the PAS

Use

Use the procedure below to configure your system for using PAS.

Procedure

1. Make sure your system meets the requirements for using PAS.
   a. Configure the use of logon tickets [Page 23].
   b. Perform any scenario-specific configuration steps. For example:
      - If you are using the Windows NTLM authentication as the PAS option, then configure your Web server to use Windows NTLM authentication [Page 26].
      - If you are using SSL and X.509 client certificates, then configure your Web server for using SSL. (See your Web server documentation.)
   c. Configure SNC [Page 26].
2. Install the PAS [Page 32].
3. Configure the PAS service file [Page 33].
4. If you are using an arbitrary mechanism on the Web server that sets the user's ID in an HTTP header variable that differs from the Web server's standard variable to use for the user's ID, then specify the HTTP header variable to use in the WGate's configuration file [Page 38].
5. Either maintain the user mapping [Page 39] or configure the PAS [Page 40] for the case that the authentication mechanism provides the user's ID for the SAP system directly.

Result

The system issues the user a logon ticket based on an external authentication.

Configuring the Use of Logon Tickets

Use

The system's ticket-issuing application server(s) and corresponding ITS server(s) must be configured to create and accept logon tickets. Systems that should be accessible using Single Sign-On based on the logon ticket must also be configured to accept tickets. See the procedure below for an overview of the configuration.

Procedure

Use the SSO administration wizard (transaction SSO2) to view and maintain the application server's logon ticket configuration as described in the tables below. Note the following:

- To view and maintain the configuration on the ticket-issuing system, enter the RFC destination **NONE** in the initial screen.
- Otherwise, to view and maintain the configuration on an accepting system, enter the RFC destination to the corresponding ticket-issuing system.

- Red traffic lights indicate configurations that are not operational for SSO. Choose *Activate* ( ) to correct any errors.
- If you make changes to the profile parameters, then restart the application server and execute the SSO administration wizard again.

Configuration on the Ticket-Issuing System's Application Server

Profile Parameter	Value	Comment
`login/create_sso2_ticket`	1 or 2	Use the value 1 if the server possesses a public-key certificate signed by the SAP CA. Use the value 2 if the certificate is self-signed. If you are not sure, then use the value 2.
`login/accept_sso2_ticket`	1	Use the value 1 so that the system will also accept logon tickets.
`login/ticket_expiration_time`	Desired value	Default = 60 hours

Configuration on the Ticket-Issuing System's ITS

Service File Parameter	Value	Comment
`~login`	(space)	User information contained in these parameters will override the use of logon tickets for the logon.
`~password`	(space)	
`~cookies`	1	Enables the storage of cookies.
`~mysapcomgetsso2cookie`	1	Use the value 1 so that the ITS will request the ticket creation from the application server.
`~mysapcomusesso2cookie`	1	Use the value 1 so that the ITS will pass an existing logon ticket to the application server.
`~mysapcomnosso1cookie`	0 or 1	Use the value 0 if you have to use SSO cookies in addition to logon tickets for Single Sign-On (for example, to SAP systems with Release 3.1). Otherwise, use the value 1.
`~mysapcomssonoits`	1	Use the value 1 if the logon ticket will be used across different SAP system clients. Otherwise, the ticket contains the SAP system client and cannot be used to access a system with a different client.

Configuration on the Accepting System's Application Server

Profile Parameter	Value	Comment
`login/accept_sso2_ticket`	1	Use the value 1 so that the server will accept logon tickets.
Access Control List	**Entry**	**Comment**
Table TWPSSO2ACL	Issuing system's ID and client	The system accepts logon tickets that have been issued by the systems entered in this table.
Certificate List	**Entry**	**Comment**
Certificate list in server's system PSE (Personal Security Environment)	Issuing system's public-key certificate	The accepting system can verify logon tickets that have been issued by the system that possesses this public-key certificate. An entry is only necessary if the parameter `login/create_sso2_ticket` = 2 on the ticket-issuing system. (If `login/create_sso2_ticket` = 1 on the ticket-issuing system, then the issuing system's public-key certificate is sent with the logon ticket.)

Configuration on the Accepting System's ITS

Service File Parameter	Value	Comment
`~login`	(space)	User information contained in these parameters will override the use of logon tickets for the logon.
`~password`	(space)	
`~mysapcomusesso2cookie`	1	When set to 1, the ITS will pass an existing logon ticket to the application server.

See also:

- For the configuration on the SAP Web Application Server, see Using Logon Tickets [SAP Library] in the documentation for *SAP Web Application Server Security*.
- For the configuration on an SAP system application server <= Release 4.6D, see the documentation for *Single Sign-On in the mySAP Workplace*.

The logon ticket configuration described in the *Single Sign-On in the mySAP Workplace* document also applies to application servers that are not integrated into the mySAP Workplace.

These documents are available on the SAP Service Marketplace at http://service.sap.com/security.

Configuring Windows NTLM Authentication on the Web Server

Use

If you use Windows NTLM authentication, then you have to configure the Workplace Server's Web server accordingly.

Procedure

Under the properties for the virtual Web server used for the ITS:

1. Choose *Directory Security*.
2. Deactivate *Anonymous Access*.
3. Activate *Windows NT Challenge Response* (Windows NT) or *Integrated Windows NT authentication* (Windows 2000).

Configuring SNC

All of the PAS options require that you use SNC between the AGate and the ticket-issuing application server. In addition, if the user authentication takes place on the Web server and you have a dual host ITS installation, then we also recommend using SNC for the connection between the WGate and the AGate. This protects the user information from being eavesdropped, stolen or manipulated by someone for the complete path between the authentication point and the backend system. We also recommend using SNC for the connections to systems that accept logon tickets.

For connections that use the HTTP protocol, for example, connections to an SAP Web Application Server, use the Secure Sockets Layer (SSL) protocol instead of SNC. In this case, see the component's documentation for the SSL configuration.

To configure SNC for each of the components see the following topics:

- Configuring SNC on the Application Server [Page 27]
- Configuring SNC on the AGate [Page 29]
- Configuring SNC on the WGate [Page 31]

Configuring SNC on the Application Server

Use

Use this procedure to configure SNC on the application server for the connection between the server and its corresponding ITS.

Prerequisites

- You have obtained the external security product to use for SNC.
- You know the SNC names used for the application server and the AGate. The SNC name is the name that identifies the server for using SNC and is determined by the security product used.

Procedure

1. Install the security product used for SNC on the application server.
2. Perform any product-specific tasks. For example, you may have to set certain environment variables or establish a security environment for the application server.
3. Set the following profile parameters on the application server:

Parameter	Value	Comment
`snc/enable`	1	Activate SNC on the application server
`snc/gssapi_lib`	Path and file name of the security library	Determined when installing the security product
`snc/identity/as`	SNC name of the application server	Determined when installing the security product
`snc/data_protection/max`	Maximum level of protection to use	Possible values: 1: authentication only 2: data integrity protection 3: data privacy protection
`snc/data_protection/min`	Minimum required data protection level	Possible values: 1: authentication only 2: data integrity protection 3: data privacy protection
`snc/data_protection/use`	Default level of data protection to use	Possible values: 1: authentication only 2: data integrity protection 3: data privacy protection 9: use the value from `snc/data_protection/max`
`snc/accept_insecure_gui`	1	Allows users to log on to the system without using an SNC logon.
`snc/accept_insecure_cpic`	1	Allows non-secured CPIC connections.
`snc/accept_insecure_rfc`	1	Allows non-secured RFC connections.

Parameter	Value	Comment
snc/accept_insecure_r3int_rfc	1	Allows non-secured internal RFC connections.
snc/extid_login_diag	1	Enable login with external identity (dialog)
snc/extid_login_rfc	1	Enable login with external identity (RFC)

4. Specify the AGate's SNC information in the system access control list for SNC (table SNCSYSACL, view VSNCSYSACL, TYPE=E).
   a. Enter the SNC name for the AGate in the *SNC name* field. The *System-ID* field is optional.
   b. Activate the options:
      - *Entry for RFC activated*
      - *Entry for diag activated*
      - *Entry for ext. ID activated*
   c. Save the data.
5. Create a generic entry for the AGate in the extended user access control list (table USRACLEXT):
   a. Enter an asterisk (*) in the *User* field.
   b. If multiple entries exist for the AGate's SNC name, then enter a value in the *Seq.number* field. If this is the only entry in the table for the AGate, then use the sequence number 000.
   c. Enter the AGate's SNC name in the *SNC name* field.
   d. Save the data.

   You receive a warning due to the wildcard entry in the *User* field.
6. If you made changes to the profile parameters, then restart the application server.

Result

The application server can use SNC to communicate with the AGate, provided that the AGate has also been configured for using SNC.

Configuring SNC on the AGate

Use

Use this procedure to configure SNC on the AGate for the connection between the AGate and the application server. The SNC configuration for the connection between the AGate and the WGate is also provided, but only necessary if the user's authentication takes place on the Web server.

Prerequisites

- You have obtained the external security product to use for SNC.
- You know each of the component's SNC names. The naming convention is determined by the security product used for SNC.

Procedure

Proceed as described below.

The changes made in the following procedure only take effect after you restart the AGate.

If you use the SAP Cryptographic Library as the security product, then you can use the ITS Administration tool to perform the configuration. See the options under *Security* → *Network Security* and *SAPCRYPTO Admin*. The tool sets the appropriate environment variables and registry keys for using the SAP Cryptographic Library. For more information, see Using the SAP Cryptographic Library for SNC [SAP Library].

1. Install the security product.
2. Set the environment variable `SNC_LIB` to the path and file name of the security product's library.

   As of Release 6.20, use the XML configuration file `ITSRegistry<SID>.xml` that is located in the `config` sub-directory for the ITS installation. Make the entry in the `- <key name="Envars">` block.

   Prior to Release 6.20, use the registry key

   ```
   HKEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<virtual
   ITS>\Programs\AGate\environment\<variable>
   ```

3. Perform any other product-specific tasks. For example, the AGate may have to log on to the security product to establish its security environment. For more information, see the product's documentation.

4. Specify the following parameters:

Parameter	Value
`Type`	2: Use NISNC based connection (SAP protocol NI plus SNC)
`SncNameAGate`	AGate's SNC name
`SncNameWGate`	WGate's SNC name (This parameter is only necessary if SNC is to be used for the connection between the AGate and the WGate.)

As of Release 6.20, make these entries in the XML configuration file in the `<key name="Instances">` block for the AGate's instance.

Prior to Release 6.20, use the registry key:

```
KEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<virtual
ITS>\Connects\<Parameter>
```

5. Set the following parameters in the global or the PAS service file (for example, `sapntauth.srvc`):

Parameter	Value	Comment
`~sncNameR3`	SNC name of the application server	This entry activates SNC for the AGate ← → application server connection and should therefore be the last step you perform in the configuration process.
`~sncQoPR3`	Quality of protection level to use for the communication	Possible values: 1: authentication only 2: data integrity protection 3: data privacy protection 9: use the value from the application server's profile parameter `snc/data_protection/max` If omitted, the default level of protection is used (as defined in the application server's profile parameter `snc/data_protection/use`)

6. If your WGate resides on the same host, and you want to use SNC for the connection between the AGate and the WGate, then continue with the WGate's configuration. Otherwise, restart the AGate.

Result

The AGate can use SNC to communicate with the application server and the WGate, provided that these servers have also been configured for using SNC.

See also:

- *SNC User's Guide*
- Using the SAP Cryptographic Library for SNC [SAP Library]

Configuring SNC on the WGate

Use

Use this procedure to configure SNC on the WGate for the connection between the WGate and the AGate.

Prerequisites

- You have obtained the external security product to use for SNC.
- You know the SNC names for the AGate and the WGate. The naming convention is determined by the security product used for SNC.

  If the WGate connects to multiple AGate instances, then note the following:

  – If you use SNC for one of the WGate ←→ AGate connections, then you must use SNC for all of the WGate ←→ AGate connections specified in the WGate's configuration file.

  – The WGate's security environment and the SNC name must be the same for all of these connections.

Procedure

Proceed as described below.

The changes made in the following procedure only take effect after you restart the Web server.

1. Install the security product.
2. Set the environment variable `SNC_LIB` to the path and file name of the security product's library.

   As of Release 6.20, use the XML configuration file `ITSRegistryWGate.xml` that is located in the `config` sub-directory for the ITS installation. Make the entry in the – `<key name="Envars">` block.

   Prior to Release 6.20, use the WGate configuration file `wgate.conf`. Make the entry in the `<global>` section using the `setenv` parameter.
3. Establish the security environment for each of the components and perform any other product-specific tasks. For example, the component may have to log on to the security product under its own security environment. For more information, see the product's documentation.

4. In the WGate configuration file, specify the following parameters:

Parameter	Value
`Type`	2: Use NISNC based connection (SAP protocol NI plus SNC)
`SncNameAGate`	SNC name of the AGate and ITS Manager
`SncNameWGate`	SNC name of the WGate

As of Release 6.20, use the XML configuration file `ITSRegistryWGate.xml` that is located in the `config` sub-directory for the ITS installation. Make the entries in the – `<key name="Instances">` block for each of the corresponding AGate instances.

Prior to Release 6.20, use the WGate configuration file `wgate.conf`. Make the entries in the `<instances xxx>` block.

5. Restart the Web server. If you have not already done so, then also restart the AGate.

Result

The WGate can use SNC to communicate with the AGate, provided that the AGate has also been configured for using SNC.

See also:

- *SNC User's Guide*
- Using the SAP Cryptographic Library for SNC [SAP Library]
- *ITS Administration Guide*
  - Release 6.20: WGate Configuration [SAP Library]
  - Prior to Release 6.20: *WGate Configuration → WGate Configuration File*

Installing the PAS

Use

Use the procedure below to install the PAS templates and service files on the AGate.

Prerequisites

You have the necessary PAS templates and service files. Sample files are contained in the ITS package `ntauth.sar`, which is attached to SAP Note 493107. For more information about unpacking `sar` packages, see SAP Note 331407.

If you use an authentication mechanism provided by a partner, then the partner must provide the appropriate service file(s) and templates.

Procedure

Install the service files and templates in the ITS sub-directories `\services` and `\templates` respectively.

The sample files provided with the ITS package are set up per default for using the Windows NTLM authentication mechanism. If you are using a different mechanism, then copy these files to different files, for example, copy `sapntauth.srvc` to `saphttp.srvc`. Use the copied files when configuring your PAS service.

Result

The PAS files are installed on the ITS. Continue with Configuring the PAS Service File [Page 33].

Configuring the PAS Service File

To configure the PAS's service file specify the parameters as indicated in the tables below.

General PAS Service File Parameters

Parameter	Allowed Values	Description
`~xgateway`	`sapextauth`	Specifies that the XGateway `sapextauth` should be used.
`~extauthtype`	`NTLM`, `NTPassword`, `LDAP`, `X509`, `HTTP`, `DLL`	Not case sensitive Specifies the type of external authentication. The following types are allowed: • Windows NTLM authentication (`NTLM`) • Verification of user ID and password on the Windows NT domain controller (`NTPassword`) • Authentication on a directory server using an LDAP bind (`LDAP`) • X.509 client certificates and SSL client authentication (`X509`) • Authentication using an arbitrary mechanism that sets the user ID in an HTTP header variable (`HTTP`) • Authentication using a partner product (`DLL`)

Parameter	Allowed Values	Description
~extid_type	NT, LD, UN, or <user-defined>	The type of external identification used for the mapping in table USREXTID. This parameter does not need to be specified if ~extauthtype = NTLM, NTPassword, or x509. If you set the type to UN, then you do not need to maintain the user mapping in USREXTID. In this case, the external authentication mechanism must provide the user's ID for the SAP system directly.
~mysapcomgetsso2cookie	1	Requests the creation of a logon ticket after the user has been authenticated.
~dont_recreate_ticket	0 (create ticket with each request), 1 (create ticket once only)	Determines whether a ticket should be created with each request or only created if no ticket is present.
~redirectHost	<Host_name>	Data that is used for the redirect URL. The defaults for each of the parameters is the value of the current request. In ~redirectQS you can define extra parameters for the redirected service.
~redirectPath	<Path>	
~redirectQS	<Query_string>	
~redirectHttps	0 (use HTTP), 1 (use HTTPS)	
~login_to_upcase	0 (do not convert), 1 (convert)	Convert the ~login string (user ID) to uppercase before submitting the ticket request to the backend. This may be necessary if the user ID entries in the mapping table (USREXTID) are maintained in capital letters. (The entries in USREXTID are case-sensitive.)

Parameters Specific for the Authentication Mechanism Type NTPassword

Parameter	Allowed Values	Description
~ntdomain	<Windows NT domain>	If your users exist in a single Windows NT domain, then you can use this parameter to define the domain in the service file. Otherwise, you need to include the domain in the login template.

Parameters Specific for the Authentication Mechanism Type LDAP

Parameter	Allowed Values	Description
`~ldaphost`	`<Directory server host>`	Host name for the directory server.
`~ldapport`	`<LDAP port>`	LDAP port used on the directory server. Default = 389
`~timeout`	`<integer value>`	Time out in seconds for a directory search.
`~maxtrials`	`<integer value>`	Maximum number of logon attempts before terminating.
`~ldapsapuid`	`<ldap_attribute>`	The name of the directory server's attribute that contains the SAP System user ID.
`~ldapuid`	`<ldap_attribute>`	The name of the attribute that contains the user's ID for the directory server.
`~ldapbasedn`	`<base_Distingiushed_Name>`	The base Distinguished Name to use when searching for the user's ID in the directory.

Specify the parameters `~ldapuid` and `~ldapbasedn` in the PAS service file as the generic parts of the user's Distinguished Name for the directory. The user then only has to provide his or her user-specific part at logon.

For example, Alice's complete Distinguished Name for the directory is `CN=ALICE, O=MyCompany, C=US`. If you specify `~ldapuid` = `CN` and `~ldapbasedn` = `O=MyCompany, C=US` in the PAS service file then Alice only has to provide her user ID **`ALICE`** when logging on.

Parameters Specific for the Authentication Mechanism Type HTTP

Parameter	Allowed Values	Description
`~remote_user_alias`	`<header_variable>`	Name of the HTTP header variable that contains the user's ID.

Parameters Specific for the Partner Mechanism Type DLL

Parameter	Allowed Values	Description
~extauthmodule	<Path>	Path and file name to your external library. The exact method to use depends on your operating system. For example, for Windows NT/2000/XP systems, you can specify this parameter to refer to a library located in a directory that the system can find using the PATH environment variable. However, to make sure the system can find the library, we recommend using the complete path and file name. For example: Windows: C:\SAP\ITS\extmodule.dll Unix/Linux: /usr/lib/extmodule.so

Examples

Example Service File for Using Windows NTLM Authentication

```
############################################################
# Copyright SAP AG 2002
# Example Service File for the Pluggable Authentication
# Service (PAS) Using Windows NTLM Authentication
#
~theme                  99
~xgateway               sapextauth
~extauthtype            NTLM
~extid_type             NT

~client                 001
~language               en

~mysapcomgetsso2cookie  1
~login_to_upcase        1

~redirectHost           host123.mycompany.com
~redirectPath           /scripts/wgate/webgui/!
~redirectQS             ~client=001&~language=en
~redirectHttps          1

~login_template         login
~dont_recreate_ticket   1
```

Example Service File for Using LDAP Bind

```
#################################################################
# Copyright SAP AG 2002
# Example Service File for the Pluggable Authentication
# Service (PAS) Using LDAP Bind where SAP User ID is stored
# in the directory server (~extid_type = UN)
~theme                  99
~xgateway               sapextauth
~extauthtype            LDAP
~extid_type             UN

~ldaphost               ldap123.mycompany.com
~ldapport               389
~timeout                30
~maxtrials              5

~ldapsapuid             sapuid
~ldapuid                CN
~ldapbasedn             O=MyCompany, C=US

~client                 001
~language               en

~mysapcomgetsso2cookie  1
~timeout                2
~login_to_upcase        1

~redirectHost           host123.mycompany.com
~redirectPath           /scripts/wgate/webgui/!
~redirectQS             ~client=001&~language=en
~redirectHttps          1

~login_template         login
~dont_recreate_ticket   1
```

Example Service File for Using HTTP Header Variables

```
#################################################################
# Copyright SAP AG 2002
# Example Service File for the Pluggable Authentication
# Service (PAS) Using HTTP Header Variables and where the
# SAP User ID is stored in the external ID user mapping table
# USREXTID (~extid_type = HV)
~theme                  99
~xgateway               sapextauth
~extauthtype            HTTP
~extid_type             HV

~remote_user_alias      REMOTE_USER

~client                 001
~language               en

~mysapcomgetsso2cookie  1
~login_to_upcase        1

~redirectHost           host123.mycompany.com
~redirectPath           /scripts/wgate/webgui/!
~redirectQS             ~client=001&~language=en
~redirectHttps          1

~login_template         login
~dont_recreate_ticket   1
```

Specifying the HTTP Header Variable to Use

Use

If you are using an arbitrary authentication mechanism on the Web server that sets the user's ID in an HTTP header variable, and the header variable used differs from the Web server's standard one, then use this procedure to specify the HTTP header variable that is used.

Both Microsoft's IIS and the Apache Web server use the HTTP header variable `REMOTE_USER` to store the user's ID. Therefore, if the authentication mechanism sets this HTTP header variable on one of these Web servers, then you can skip this procedure.

Procedure

Specify the name of the HTTP header variable used in the WGate's configuration file `ITSRegistryWGate.xml`. Make the entry in the `Headers` section using the following information:

HTTP Header Variable Parameters

Parameter	Value	Comment
`Name`	`<HTTP_Header_Variable>`	The syntax to use for your HTTP header variable depends on the Web server. For example, the Microsoft IIS Web server uses the syntax `HTTP_<header_variable>` for externally set header variables.
`Set`	0	The value 0 specifies that the value of the HTTP header variable should be passed to the AGate. Using the value 1 would specify that the HTTP header variable should be set using the value contained in the `Value` parameter.
`Value`	(empty)	

See the example below.

The following `Headers` section specifies that the WGate is to pass the contents of the HTTP header variable `HTTP_SAP_USER_ID` to the AGate.

```
<key name="Headers">
<key name="Header1">
<value name="Name" type="text">HTTP_SAP_USER_ID</value>
<value name="Set" type="text">0</value>
<value name="Value" type="text"></value>
</key>
```

See also:

ITS Administration → WGate Configuration → WGate Registry Configuration [SAP Library]

Maintaining the User Mapping in the SAP System

Use

The PAS must be able to determine the user's ID in the SAP system so that it can issue the user his or her SAP logon ticket. For this purpose, maintain the user's information in the user external ID mapping table (USREXTID).

If you use an external authentication mechanism that provides the user's ID for the SAP system directly, then you can skip this procedure. For more information, see Configuring the PAS for Providing the SAP User ID Directly [Page 40].

Prerequisites

The type of external user ID that you define in the mapping table must match the type of user ID defined in the PAS's service file.

Procedure

Maintain the table USREXTID on the ticket-issuing application server. You can either use table maintenance (transaction SM30, view VUSREXTID) or the reports RSUSREXT or RSUSREXTID to maintain the user information.

Use the following information:

Field	Description	Possible Values	Default
Type of external ID	Type of external ID. The value must match the type of authentication used.	**DN** (Distinguished Name for X.509) **NT** (Windows NTLM or password verification using the Windows domain controller) **LD** (LDAP bind) **<User-defined>** (For other external authentication mechanisms)	None
External ID	User's external ID. The syntax is determined by the authentication mechanism used.	String value (case-sensitive)	None
Seq. no.	Optional. Use if multiple entries for the same user ID exist.	000 – 999	None
User	User's ID for the SAP system	Valid user in the SAP system	None
Min. date	Optional. First valid date for the external ID mapping.	Date	None
Indicator: *Activated*	Check to activate the user mapping.	On or off	Off

The external ID entries in USREXTID are case-sensitive. Therefore, to avoid case problems, we recommend maintaining the external ID entries in capital letters and setting the ITS parameter `~login_to_upcase` = 1 in the PAS's service file.

Configuring the PAS for Providing the SAP User ID Directly

Use

As an alternative to maintaining the user mapping in the SAP system table USREXTID, the external authentication mechanism can provide the user's ID for the SAP system directly when passing the user's information to the PAS. This option is primarily useful when using either the LDAP bind for authentication or when using an arbitrary mechanism that sets the user's ID in an HTTP header variable.

If you configure the PAS accordingly and the external authentication mechanism does not provide the user's ID for the SAP system directly, then an error occurs. The user mapping table in the SAP system is **not** used as a fallback mechanism.

Prerequisites

- If you are using an LDAP bind to a directory server as the authentication mechanism, then the user's ID for the SAP system must be defined in an attribute in the directory server.
- When using HTTP header variables, the external authentication mechanism must set the user's ID for the SAP system in the header variable.

Procedure

1. Set the service file parameter `~extid_type` in the PAS service file to the value **`UN`**.
2. If you are using an LDAP bind to a directory server as the authentication mechanism, then set the service file parameter `~ldapsapuid` in the PAS service file to the name of this attribute.

Result

The PAS obtains the user's ID for the SAP system directly from the authentication mechanism instead of using the mapping table.

Testing the Configuration

Testing the Configuration Using the ITS Administration Tool

Use

You can use the ITS Administration tool to test the PAS configuration if you use the SAP Cryptographic Library as the security product for SNC. See the procedures below.

Prerequisites

- The SAP Cryptographic Library has been installed and SNC has been configured on both the ticket-issuing system's AGate and application server. If you use SNC for the connection between the WGate and the AGate, then SNC has also been configured on the system's WGate.
- The system has been configured for issuing logon tickets.
- The system has been configured for using the PAS external authentication mechanism.

Procedure

Testing the Use of SNC for the Connection Between the AGate and the Application Server

The first test is to test the use of SNC for the connection between the AGate and the application server.

Using the ITS Administration tool:

1. Choose `<server>` → *Security* → *SAPCRYPTO Admin*.

   The SNC administration page appears. If SNC is configured correctly, then the lights are green and the AGate's SNC connection information appears in the various fields. If any lights are red, then correct the SNC configuration before continuing with the test.

2. Choose *SNC Connection Maintenance*.

   The *SNC Connection Maintenance* screen appears.

3. Under *SNC Connection Maintenance*, either enter the load balancing group or the application server's host name and system number in the corresponding fields.

4. Under *SAP SNC Test*, enter your user ID and password for the SAP system and the SAP system's client in the corresponding fields.

5. Activate the option *Get ticket*.

6. Choose *Login*.

   The connection is tested. If successful, then SNC works for the connection and you received a logon ticket. Otherwise, you receive an error message. See SAP Note 320991 for a list of possible errors and the corresponding return codes.

Testing the Use of PAS for Logon

Test if the user can use his or her external ID for logon. This test is not necessary if the external authentication mechanism provides the SAP user ID directly.

This test only makes sure that the user mapping is maintained correctly in the mapping table USREXTID.

1. Under *SAP Extid Login Test (Used for PAS):*, enter your user ID for the external authentication mechanism, the type, and the SAP system client in the corresponding fields.
2. Choose *Login*.

   This test makes sure that the user mapping is maintained correctly in the mapping table USREXTID. See SAP Note 320991 for a list of possible errors and the corresponding return codes.

Result

The use of logon tickets and PAS are configured correctly on the AGate and the ticket-issuing application server. SNC is also configured correctly between the AGate and the application server.

If you use SNC between the WGate and the AGate, then see Testing the Use of SNC [Page 42].

Testing the Use of SNC

Use

Use this procedure to test the use of SNC for connections between the AGate and SAP system application server and the AGate and the WGate.

If you are using the SAP Cryptographic Library as the security product for SNC, then you can use the ITS Administration tool to test SNC for the connection between the AGate and the application server. See Testing the Configuration Using the ITS Administration Tool [Page 41].

Prerequisites

- The security product to use for SNC is installed on each of the components.
- SNC is activated on each of the components as follows:
  - Application server: `snc/enable` is set to 1.
  - AGate: `~sncnameR3` is specified in the AGate's corresponding service file.
  - WGate (if used): `SNCNameAGate` is set in the WGate's configuration file.

Procedure

Access an ITS service for which SNC is activated, for example, the `webgui` service:

```
http://<server>.<domain>:<port>/scripts/wgate/webgui/!
```

Result

If you are prompted for a user ID and password, then the connection could be established using SNC protection.

Otherwise, deactivate SNC and test the connection without using SNC.

To deactivate SNC for the connection between the AGate and the application server, proceed the service file parameter `~sncNameR3` in the AGate's service file with a number sign (#).

To deactivate SNC for the connection between the WGate and the AGate, remove the value for `SNCNameAGate` from the WGate's configuration file.

 Testing Logon Tickets and PAS

Use

If you do not use the SAP Cryptographic Library as the security product for SNC, then you cannot use the ITS Administration tool to test the logon ticket and PAS configuration. In this case, use the procedure below.

Prerequisites

The corresponding application server and ITS are configured for using SNC, PAS, and for issuing logon tickets.

Procedure

1. Configure your Web browser to prompt you for accepting session cookies.

   For example, for Microsoft Internet Explorer, choose *Prompt* for session cookies in the local intranet zone.

2. Access your PAS authentication ticket-issuing application server via the ITS using the corresponding URL.

   ```
   https://host123.mycompany.com:443/scripts/wgate/
   <PAS_Service>/!
   ```

3. If necessary, enter your user authentication information (for example, user ID and password for the authenticating mechanism).

   If the authentication was successful, you receive several session cookies for the connection and are prompted whether you want to accept these cookies.

4. View the contents of each of the cookies that you receive. (For Microsoft Internet Explorer, choose *More Info*.)

   If you receive a cookie named MYSAPSSO2, then you have received your logon ticket.

   Otherwise, check the AGate's trace file. See SAP Note 320991 for a list of the possible return codes.

   If you are able to log on to the SAP system but did not receive a cookie with the name MYSAPSSO2, then the PAS authentication has worked, but the logon ticket could not be set in the Web browser. This is most likely caused by a DNS domain conflict. Make sure that the Web server exists in the DNS domain and that you are accessing the Web server using the fully-qualified host name.

Checking the HTTP Header Variable

Use

If you are using an arbitrary authentication mechanism on the Web server that passes the user's ID to the ITS using an HTTP header variable, then use the procedure below to check the name and contents of the corresponding HTTP header variable.

Prerequisites

The key `AdminEnabled` is set to the value 1 for the AGate. This key activates remote debugging on the AGate. For more information, see AGate Parameters [SAP Library].

Procedure

1. Call the PAS service. Include the parameter **`~command=fielddump`** in the URL.

   `https://host123.mycompany.com/scripts/wgate/http/!?~command=fielddump`

   The ITS displays a page showing the contents of the various ITS parameters, including HTTP header variables. HTTP header variables are proceeded with the prefix `~http_`.

2. Check for the value of the HTTP header variable parameter `~http_<header_variable>`.

   If your Web server also automatically proceeds the specified HTTP header variable with the prefix `HTTP_`, then the parameter shown using the field dump will be displayed as:

   `~http_http_<header_variable>  <user>`

3. If the HTTP header variable is not displayed, then check the WGate's configuration for header variables and the value of `~remote_user_alias` in the PAS service file. See the examples below.

Examples

Example WGate Configuration in `ITSRegistryWGate.xml`

```
<key name="Headers">
<key name="Header1">
<value name="Name" type="text">HTTP_SAP_USER_ID</value>
<value name="Set" type="text">0</value>
<value name="Value" type="text"></value>
</key>
```

Example AGate Service File Parameter `~remote_user_alias`

```
~remote_user_alias      HTTP_SAP_USER_ID
```

Example Output Using `~command=fielddump`

```
~http_http_sap_user_id     ALICE
```

Sample Trace File: SNC Initialization

The following shows the SNC initialization information in the AGate's trace file (`initial.trc`). This information is displayed in the other component's trace files, for example, the application server or the WGate. You can find the following information:

- The value of the environment variable `SNC_LIB`
- The name and location of the specified library
- The component's SNC name (`myname`)
- The communication partner's SNC name (`target`)
- The quality of protection used (`qop`)
- Product-specific information

  For example, `Initiating Credentials available` when the SAP Cryptographic Library is used.
- Status of the SNC initialization (`SncProcessOutput()==SAP_O_K`)

SNC Initialization Information in the AGate Trace File

```
TmConnect: handle = 0
[Thr 1508] TmISncSetOptions: set tm_mode for 0 to
  TM_SNC_ON
[Thr 1508] SncInit(): Trying environment variable SNC_LIB
  as a gssapi library name: "D:\Program Files\SAP\ITS\2.0\
  programs\sapcrypto.dll".
[Thr 1508] load shared library (D:\Program Files\SAP\ITS\
  2.0\programs\sapcrypto.dll), hdl 0
[Thr 1508]   File "D:\Program Files\SAP\ITS\2.0\programs\
  sapcrypto.dll" dynamically loaded as GSS-API v2 library.
[Thr 1508]   The internal Adapter for the loaded GSS-API
  mechanism identifies as: Internal SNC-Adapter (Rev 1.0)
  to SECUDE 5/GSS-API v2
[Thr 1508] SncInit(): Initiating Credentials available,
  lifetime=16369h 28m 09s
[Thr 1508] <<- SncInit()==SAP_O_K
```

```
[Thr 1508]          sec_avail = "true"
[Thr 1508] disp service:     sapdp00
[Thr 1508] TmIGetName: no DISPLAY set
[Thr 1508] terminal name: host123
[Thr 1508] connect to dispatcher on host
  /H/10.17.73.88/S/3227
[Thr 1508] <<- SncSessionInit()==SAP_O_K
[Thr 1508]     out: &snc_hdl = 01B95518
[Thr 1508] <<- SncSetMyName()==SAP_O_K
[Thr 1508]      in: myname = "p:CN=ABC_AGate, O=MyCompany,
  C=US"
[Thr 1508] <<- SncSessionInitiator()==SAP_O_K
[Thr 1508]      in: target    = "p:CN=ABC, O=MyCompany,
  C=US"
[Thr 1508]          parses to = "p:CN=ABC, O=MyCompany,
  C=US"
[Thr 1508] <<- SncSetQOP()==SAP_O_K
[Thr 1508]      in: qop values = "min=9 (max default),
  max=9 (max default), use=9 (max default)"
[Thr 1508]           resulting = "min=3 (old:2), max=3
  (old:3), use=3 (old:3)"
[Thr 1508] handle 0 state mode 0 MOD_SNC_OK
[Thr 1508] ->> SncProcessOutput(snc_hdl=01B95518,
  ibuf=01B69680, ilen=75, &idone=06E4E18B, &obuf=06E4E180,
  &oused=06E4E184)
[Thr 1508] <<- SncProcessOutput()==SAP_O_K
```

Sample Trace File (AGate): Successful PAS Authentication Using NTLM

The following shows an excerpt from the AGate's trace file for PAS (`sapextauth.trc`) when using the Microsoft NTLM authentication mechanism. The trace level used was trace level 2. You can see the following:

- The authentication used was Windows NTLM. (`XGetHandleLogin set login for NTLM: MYDOMAIN\ALICE`)
- The user's ID is `ALICE` in the Windows NT domain `MYDOMAIN`.
- The Windows NTLM authentication was successful and that Alice received her logon ticket. (`PAS OK -> SSO2 LOGON TICKET received.`)
- The PAS redirected Alice to the URL `http://host123.mycompany.com/scripts/wgate/webgui/!?~language=EN&~client=000`.

AGate Trace Information for Successful PAS Authentication Using NTLM (Trace Level 2)

```
[sapextauth, 416]: *W* sapextauth: PAS session begins...
[sapextauth, 665]: *W* sapextauth: XGatHandleLogin sets
  login for NTLM: MYDOMAIN\ALICE
[sapextauth, 2599]: *W* sapextauth: PAS sets new ~login
  parameter to: "ALICE"
[sapextauth, 1564]: *W* sapextauth: PAS OK -> SSO2 LOGON
  TICKET received. set it to MYSAPSSO2 ...
[sapextauth, 2258]: *W* sapextauth: Setting
  ~ExtAuthRedirectURL = http://host123.mycompany.com/

  scripts/wgate/webgui/!?~language=EN&~client=000.
[sapextauth, 1812]: *W* sapextauth: PAS session ends...
```

Sample Trace File (AGate): SAP User ID not Found

A common error when using PAS is that no mapping exists between the user's external ID and his or her user ID for the SAP system. The following sample trace file for the AGate shows the error message produced when the SAP user ID could not be found in the external user ID mapping table (error code 41).

AGate Trace File Information When the User ID Mapping Does not Exist

```
[sapextauth, 2561]: *E* sapextauth: Error in Rfc Login:
  connect string was: (TRACE=0 SNC_MODE  SNC_QOP=8
  SNC_MYNAME="p:CN=AGATE, O=MYCOMPANY, C=US"
  SNC_PARTNERNAME="p:CN=ABC, O=MYCOMPANY, C=US" SNC_LIB=
  "C:\Program Files\SAP\ITS\2.0\programs\sapcrypto.dll"
  CLIENT=000 LANG="en" ASHOST="host123.mycompany.com"
  SYSNR=18 GETSSO2=1 EXTIDTYPE="NT" EXTIDDATA=
  "MYDOMAIN\ALICE")
[sapextauth, 2562]: *E* sapextauth: Error in Rfc Login:
  System returned: "You are not authorized to logon to the
  target system (error code 41)."
[sapextauth, 1567]: *E* sapextauth: Could not get ticket.
  PAS return code = 4.
```

For a complete list of the possible error codes, see SAP Note 320991.