HP OpenView Select Access

For the HP-UX, Linux, Solaris, and Windows® Operating Systems

Software Version: 6.0

Integration Paper for mySAP resources in SAP Internet Transaction Server 2.0 deployments

September 2005

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

Trademark Notices

HP OpenView Select Access includes software developed by third parties. The software HP OpenView Select Access uses includes:

- The OpenSSL Project for use in the OpenSSL Toolkit.
- Cryptographic software written by Eric Young.
- Cryptographic software developed by The Cryptix Foundation Limited.
- JavaService software from Alexandria Software Consulting.
- Software developed by Claymore Systems, Inc.
- Software developed by the Apache Software Foundation.
- JavaBeans Activation Framework version 1.0.1 © Sun Microsystems, Inc.
- JavaMail, version 1.2 © Sun Microsystems, Inc.
- SoapRMI, Copyright © 2001 Extreme! Lab, Indiana University.
- cURL, Copyright © 2000 Daniel Stenberg.
- Protomatter Syslog, Copyright © 1998-2000 Nate Sammons.
- JClass LiveTable, Copyright © 2002 Sitraka Inc.

For expanded copyright notices, see HP OpenView Select Access `<install_path>/3rd_party_license` directory.

Support

Please visit the HP OpenView web site at:

http://www.managementsoftware.hp.com/

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

You can also go directly to the support web site at:

http://support.openview.hp.com/

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Many also require a support contract.

To find more information about access levels, go to:

http://support.openview.hp.com/access_level.jsp

To register for an HP Passport ID, go to:

https://passport2.hp.com/hpp/newuser.do

Contents

1 About this Integration Paper

This Integration Paper describes how to integrate SAP Internet Transaction Server 2.0 with Select Access.

Select Access 6.0 is the last version HP performed interoperability testing against. If you have any questions regarding the interoperability of your version of Select Access with this third-party product, contact HP's Support Services.

An overview of this document's contents is listed in Table 1.

Table 1 Integration Paper overview

This chapter...	Covers these topics...
Chapter 2, *Technologies overview*	• Introduces Select Access: what it is, what it does, and how it works. • Introduces SAP Internet Transaction Server: what it is and what integration issues exist.
Chapter 3, *Integrating Select Access with SAP Internet Transaction Server*	Describes what you need to do with SAP Internet Transaction Server and Select Access to integrate these technologies.

Who is it for?

This Integration Paper is intended to instruct individuals or teams responsible for:

- Integrating Select Access with their SAP Internet Transaction Server.
- Using Select Access to manage access to SAP Internet Transaction Server's resources.

What does it assume you already know?

This Integration Paper assumes a working knowledge of:

- **Select Access**—Ensures that you understand how integration with SAP Internet Transaction Server affects the Select Access components.
- **SAP Internet Transaction Server**—Ensures that you understand how integration with Select Access affect the SAP Internet Transaction Server.
- **LDAP directory servers—**Helps ensure that information in the Policy Builder is set up correctly.
- **Web server and plugin technology—**Combinations that are used to add a specific feature or service to a larger system. This helps you understand how different components of Select Access communicate with each other and with your existing network.

Related references

Before you begin to integrate Select Access with SAP Internet Transaction Server, you may want to begin by familiarizing yourself with the contents of the following documents:

- *HP OpenView Select Access 6.0 Installation Guide*, © Copyright 2001-2004 Hewlett-Packard Development Company, L.P. (`installation_guide.pdf`)
- *HP OpenView Select Access 6.0 Network Integration Guide*, © Copyright 2001-2004 Hewlett-Packard Development Company, L.P. (`network_integration_guide.pdf`)
- *HP OpenView Select Access 6.0 Policy Builder Guide*, © Copyright 2001-2004 Hewlett-Packard Development Company, L.P. (`policy_builder_guide.pdf`)
- *HP OpenView Select Access 6.0 Developer's Tutorial Guide*, © Copyright 2004 Hewlett-Packard Development Company, L.P. (`dev_tut_guide.pdf`)
- *HP OpenView Select Access 6.0 Developer's Reference Guide*, © Copyright 2004 Hewlett-Packard Development Company, L.P. (`dev_ref_guide.pdf`)
- Hewlett-Packard, Application/portal servers *Integration Papers*, © Copyright 2001-2004 Hewlett-Packard Development Company, L.P.

2 Technologies overview

This chapter introduces you to Select Access and SAP Internet Transaction Server. It gives you an overview of the products, what they do, what components are installed with these products, and what SAP Internet Transaction Server integration issues exist.

What is Select Access?

Select Access is a centralized access management system that provides you with a unified approach to defining authorization policies and securely managing role-based access to on-line resources. It uses a collection of components that integrate with your network, to give you and your partners the ability to capitalize on the potential of extranets, intranets and portals. These components, along with the access policies you set, offer your Web and wireless users a seamless user experience by connecting them to dispersed resources and applications.

What does Select Access do?

Several features of Select Access extend its functionality beyond that of a simple authorization administration tool. It is a complete access management system, offering you a set of features to support your online relationships with your users and your content partners:

- *Supports Single Sign-on*
- *Enables User Profiling*
- *Provides User Password and Profile Management*
- *Delegates Administration*
- *Provides an End-to-end Auditing System*
- *Automates the Discovery and Maintenance of Corporate Resources*

Together, this extended functionality provides a simplified experience for both the end user and those responsible for managing what the user sees and interacts with.

Supports Single Sign-on

To improve user satisfaction, Select Access incorporates a Web Single Sign-On (SSO) capability. This means users can sign on once to access all permitted resources and have their information stored for future access. Select Access supports transparent navigation between:

- Multiple proprietary domains: For organizations with ownership of multiple Web sites.

- Multiple partnering domains: For on-line business partners, so they can securely share authentication and authorization information across corporate boundaries that have separate:
  - user databases
  - authorization policies
  - access management products

Using SSO means that users do not have to remember multiple passwords or PINs, thereby reducing the amount of help desk support.

Enables User Profiling

A user is represented as a user entry that is stored in a directory server. When you create a user entry, you can also define a set of attributes that describe that user, which become part of the user's profile. The values contained in the attribute can be used in two ways:

- *To determine level-of-access with roles*: Role-based access allows you to configure and apply policies automatically, according to the attribute values stored in the user's profile.
- *To determine delivery-of-content*: Select Access exports user attributes and their values as environment variables, so that applications can use the profile information to personalize Web pages and to conduct transactions.

A user's profile dynamically changes as a user conducts transactions with your organization. As attributes in the profile change, so too can the role the user belongs to. For example, a customer's profile may contain his current bank balance, date of last transaction, and current credit limit—any of which can change from moment to moment.

This capability of Select Access makes development of Web applications much easier, because programmers do not have to develop (or maintain) complex directory or database access codes to extract entitlement information about each user.

Provides User Password and Profile Management

Select Access's password and profile management feature makes it easy for users to conduct business and minimize the demand on technical resources that can best be employed elsewhere. This feature includes the following principles:

- *Password administration*: Allows you to set the policies and expiration times for user passwords. Select Access automates reminders and messages. Other administration features include:
  - Profile lockout and re-activation
  - Password history lists
- *Self-servicing*: Allows users to initiate:
  - The definition of new or existing passwords, which are controlled by the password policy you create.
  - The modification of profile data, which is predefined by the attributes you select. Typically, these attributes are the same attributes the user provides when they register with your organization. If the user is already known to you (like an employee or a supplier), you can pre-populate the values for them.

By allowing users to self-manage passwords and profile data, you reduce the amount of help desk support.

Delegates Administration

Delegated Administration allows for delegation of both user and policy management, providing more control for decentralized administrators. Select Access's delegation is highly efficient: it supports sub-delegation to multiple tiers of administrators, which mimics real-world organization charts. This decentralized approach to administration:

- Reduces administrative bottlenecks and costs.
- Puts the power to manage users in the hands of those who best understand those users.

Provides an End-to-end Auditing System

Select Access can record all access and authorization actions, as well as all policy administrative changes to any number of outputs, such as:

- The HP Secure Audit server
- JDBC-compliant databases
- Local files
- Platform-specific log files
- Email

Of all output choices, the Secure Audit server is the most useful: not only does it collect messages from different components on a distributed network, but it also allows you to digitally-sign all audit entries and ultimately create a report from the outputs collected.

Automates the Discovery and Maintenance of Corporate Resources

In order to define and enforce authorization, Select Access must be aware of all the resources on your network, as well as the users who want to access them. Select Access uses the directory server as the central repository for policy data, which includes the resource listing. You can deploy special HTTP/HTTPS-specific plugins to automatically scan any given network, thereby enumerating available services and resources. As services and resources are enumerated by the plugin, it adds them hierarchically in the Policy Builder's Policy Matrix. Unlike other products that require manual data input (where a simple typing error can put the security of resources at risk) Select Access saves administrators' time and improves accuracy.

How does Select Access work?

Select Access delivers the core of its authorization and authentication functionality with the following technical components:

- Policy Builder: Allows full or delegated administrators to define the authentication methods and authorization policies with an easy-to-use administration grid.

- Policy Validator: Serves the access decision to the Enforcer plugin after it accepts and evaluates the user's access request with the policy information retrieved from the directory server that holds your Policy Store.
- Enforcer plugin: Acts as the agent for Select Access on the Web/application server. The Enforcer plugin enforces the outcome of the access request that has been evaluated by the Policy Validator.
- SAML server: Handles the logistics of transferring users between your web sites and those of your partners.

These core components form a sophisticated and consistent architecture that easily adapts to any existing network infrastructure. Primarily XML and Java-based, you can readily extend Select Access to meet the needs of future security requirements.

The Authentication Process

Select Access's authentication and authorization of Web-based or wireless users takes place within a small number of basic steps. Select Access components communicate via XML documents known as queries and responses. XML offers Select Access complete flexibility for data transmission and integration into existing and future applications, whether Web or non-Web based. Select Access's authentication and authorization process follows these steps:

1. A user makes a request to access a resource.
2. The Enforcer plugin passes details of the request to the Policy Validator, including any authentication information provided.
3. The Policy Validator collects user and policy data from the directory and then caches it for future retrieval.
4. Based on this combination of information, the Policy Validator returns a policy decision to the Enforcer plugin, including relevant information to dynamically personalize the user experience.

Other Select Access Components

Other Select Access components provide the support system for Select Access's core components:

- Administration server & Setup Tool: As a mini Web server, the Administration server is responsible for the configuration of core components and deployment of the Policy Builder applet in a user's browser. The Setup Tool is a client of the Administration server: it is the interface that allows you to quickly set up and deploy Select Access.
- Secure Audit server: Collects and manages incoming log messages from Select Access components on a network.

Third-party Components Select Access Integrates With

Other third-party components that are integral to an effective Select Access solution:

- Directory server—LDAP v3.0 compliant: is the foundation of a Select Access-protected system. It acts as the repository of information. Depending on how you have set up your directory system, Select Access can use one or more directory servers to store:
  - A single policy data location
  - One or more user data locations

- Web/Application/Portal/Provisioning servers: are third-party technologies that use Select Access as their authorization and access management system. Depending on your server technology, you can use Select Access's native SSO and/or personalization solution rather than use the server's built-in alternative for a more robust solution.

Figure 1 illustrates how Select Access and third-party components interact with each other.

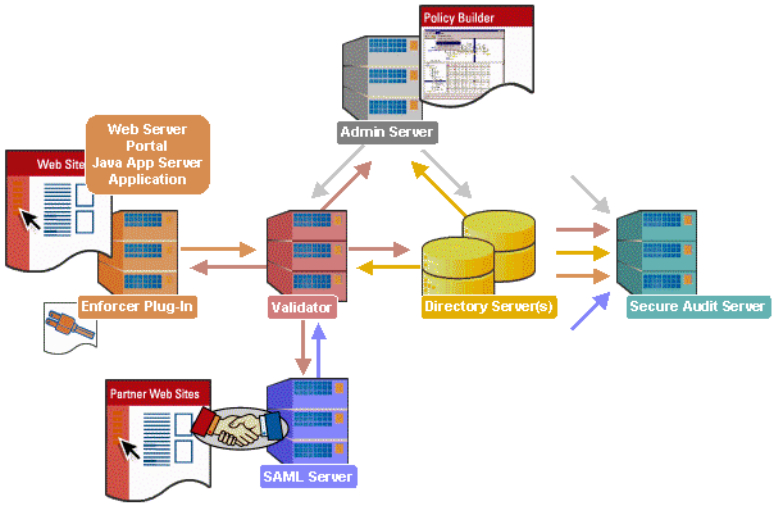


Figure 1 Select Access system architecture

Custom Plugins to Customize Functionality With

To more efficiently capture your organization's business logic, you can use Select Access's APIs to build custom plugins. Plugins that you can customize functionality with include:

- Authentication plugins: A custom Policy Builder authentication plugin allows you to tailor which kinds of authentication methods are available to better meet the needs of your organization. A Policy Builder authentication method plugin allows administrators to use and configure the authentication server for this method via a dialog box. As with the decision point plugin, this dialog box is a property editor that allows security administrators to configure the authentication server.
- Decision point plugins: A custom Rule Builder decision point plugin allows you to tailor how rules are built to better meet the needs of your organization. A Rule Builder decision point plugin allows administrators to use and configure the criteria for the decision point via:
  - The icons that represent that decision point on both the toolbar and the rule tree.
  - The dialog box, known as a property editor, that allows security administrators to configure it.
- Policy Validator decider plugins: The Validator-specific counterpart of a decision point plugin, the decider plugin allows you to capture the evaluation logic for your custom decision point (described above), so that the Policy Validator can evaluate users based on the information it collects.
- Resource discovery plugins: These plugins allow you to customize how resources are scanned on your network.

- Enforcer plugins: A new Enforcer plugin allows you to customize the backend application logic by enforcing the decision that the Policy Validator returns to the Enforcer plugin's query.
- Additional Web/Application/Portal/Provisioning server specific plugins: These plugins can be included to handle specific integration details between the third-party technology and Select Access. For example, the Domino server requires a `site_data` plugin if you need to transfer site data between Select Access and Domino.

What is SAP Internet Transaction Server?

As part of the mySAP solution set, the SAP Internet Transaction Server (SAP ITS) primarily enables SAP R/3 users the ability to access R/3 applications from a Web browser. SAP ITS acts as a gateway between the Web server and the backend SAP R/3 application server, by providing a set of HTML-based user interfaces that can:

- Mimic the SAPGUI client to SAP applications.
- Develop new HTML interfaces and flows among multiple interfaces and templates to creat an external e-commerce system.

There are two SAP ITS components, which can reside either on the same or different servers:

- `WGate` sits on the Web server (typically as an ISAPI filter if IIS is used) and intercepts all HTTP requests from the Web server. It only sends requests through specified URLs to the `AGate`.
- `AGate` acts as the HTML interface server for the SAP application server. It performs the following functions:
  - Sends application requests to the SAP R/3 application server.
  - Processes response from the SAP R/3 server.
  - Transforms the responses into HTML output, which is displayed to the user.

Integration overview

A unique HTTP header variable, `SSOSAPUSER`, is the integration cornerstone for SAP and Select Access. This variable is used by both technologies to achieve:

- Single sign-on (SSO) to SAP R/3 applications.
- Distribute personalization attributes to SAP ITS so that those applications can be customized for the user.

Two components take advantage of the data contained in this unique variable:

- *The IIS Enforcer plugin* —This plugin handles the authentication process by creating and passing this HTTP header variable to SAP ITS. Eventhough you configure the IIS Enforcer plugin's ISAPI filter to run before `WGate`'s ISAPI filter, the IIS Enforcer plugin's ISAPI filter does not change the ISAPI extension's original URL. `WGate`'s filter still assumes the duty of modifying the URL to point to the appropriate scripts directory to execute their calls.

The integration between SAP ITS and Select Access was only tested against the IIS Web server. Consequently, this document assumes the use of the IIS Enforcer plugin for most deployments.

- *The Pluggable Authentication Services (PAS) module*—This module allows Select Access to act as the external authentication mechanism. HTTP header variables allow third-party technologies like Select Access to log onto SAP ITS as the user.

For details on how to enable SSO in both technologies and thereby make use of the `SSOSAPUSER` variable, see Chapter 3, *Integrating Select Access with SAP Internet Transaction Server*.

The benefits of Select Access integration

Integrating Select Access with SAP ITS offers the following benefits:

- *Consolidated policy management*—With Select Access, you can set all the policies and resources for your corporate site—not just SAP R/3 applications. Using only one policy management tool for corporation-wide resources makes policy administration easier.
- *Multiple authentication methods*—Select Access's multiple authentication methods (digital certificates, RADIUS, SecurID, and password authentication) extend SAP ITS's security architecture. This allows administrators to do the following:
  - Tier security based on the sensitivity of the resource.
  - Use more than one authentication method to create a more secure multi-authentication mechanism.

The integrated authentication process

SAP ITS with Select Access authentication follows a similar authentication process to that of a standalone deployment of just Select Access. Figure 2 illustrates this integrated authentication process.

1. Users trigger the process with a request to the SAP ITS URL. This request typically takes the form of:

   `http://<sap_server_name>/scripts/wgate/<pas_name>/!`

   Where:

   - *<sap_server_name>* is the name of the SAP ITS server
   - *<pas_name>*`/!` is a unique URL extension that triggers the PAS module's authentication script, which signs users on to SAP ITS.

2. `WGate` recognizes this URL syntax as an SAP ITS request, and sends it to `AGate` for processing.
3. The Enforcer plugin evaluates the user credentials configured for that user. If the user enters correct credentials, the Policy Validator then proceeds to check the user's authorization policy.
4. The Policy Validator returns a policy decision to the Enforcer plugin, which allows the HTTP request to proceed to SAP ITS.
5. The PAS module receives the HTTP header and trusts Select Access as the third-party authentication system.
6. The PAS module redirects the user to other services if the user is authenticated by Select Access. Additional login prompts are not required.

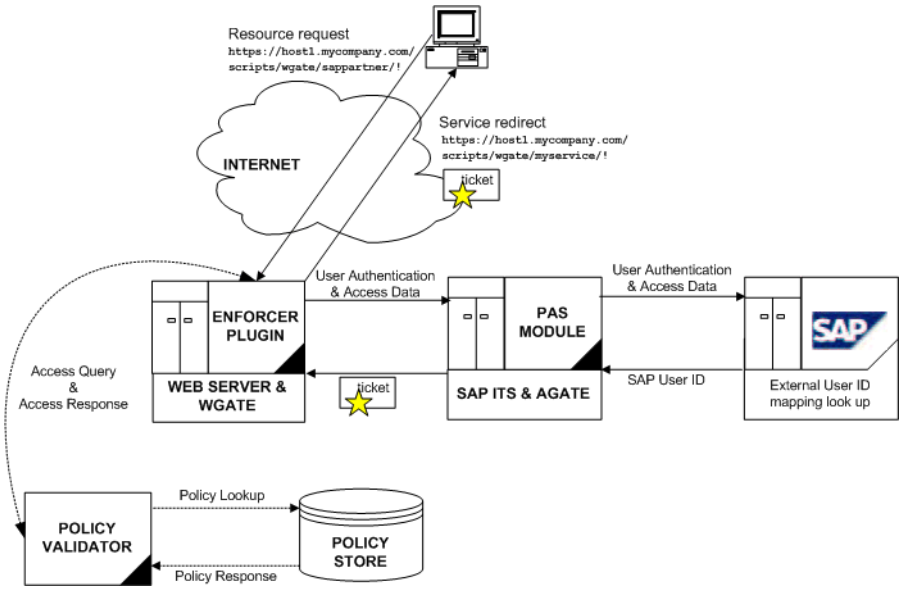


Figure 2 Authentication process in a Select Access with SAP ITS deployment

3 Integrating Select Access with SAP Internet Transaction Server

To integrate SAP ITS with Select Access, your system must meet the minimum hardware and software requirements outlined below.

- *Hardware*—Refer to the SAP ITS and Select Accesss documentation for details on client and server hardware requirements.
- *Software*—HP recommends the following software combinations to make SAP ITS and Select Access integration possible:
  - — One of the following Web servers: Microsoft IIS 5.0 on Windows 2000.
  - — Any directory servers that are supported by Select Access.

Configuring SAP Internet Transaction Server

Table 1 outlines the steps you must perform when setting up SAP ITS to work with Select Access.

Table 1 Setting up SAP Internet Transaction Server

This step...	For details, see...
Step 1: Install the following SAP Internet Transaction Server components: • `WGate` and `AGate`, either on the same or different servers. • Secured Network Communications (SNC), which is required for the PAS module. • A ticket-enabling server. • The PAS module, which you can download from SAP's Service Marketplace at http://www.sap.com/partners/marketplace/.	A combination of the following guides: *ITS Installation Guide Release 6.20* *ITS Administration Guide Release 6.20* *Pluggable Authentication Services (PAS) for Using External Authentication Mechanisms Release 6.20* *SNC User Guide Release 6.20*
Step 2: Enable PAS by activating SNC for the following communication channels: • `WGate`'s channel with `AGate` • `AGate`'s channel with the SAP application server • SAP R/3 application server	*SNC User Guide Release 6.20*

Table 1 Setting up SAP Internet Transaction Server

This step...	For details, see...
Step 3: Optionally, if you want to use Select Access user IDs to reference SAP user ids, update the `USREXTID` table in SAP ITS with the appropriate IDs for Select Access.	*Pluggable Authentication Services (PAS) for Using External Authentication Mechanisms Release 6.20*
Step 4: Configure SAP SSO and personalization for mySAP applications. This allows user credentials and attributes to be synchronized between both systems and overrides SAP security policies with Select Access's.	*ITS Administration Guide Release 6.20*
Step 5: Configure the PAS module to use HTTP header variables as an authentication method. The unique HTTP header variable, `SSOSAUSER`, is used to achieve SSO among SAP and Select Access.	*Configuring HTTP headers for SSO* on page xiv

Configuring HTTP headers for SSO

Using HTTP headers on SAP ITS allows Select Access to log into the system as the user. This prevents users from logging into SAP ITS applications multiple times to access data or access another SAP system.

The Select Access Enforcer plugin passes the HTTP header variable `SSOSAPUSER` to the PAS module. PAS uses the values in this parameter to log the user onto the backend SAP R/3 system for accessing data from RFC/BAPI or SAPGUI calls.

If you have other corporate resource protected by Select Access, the same user is not required to reauthenticate with this mechanism. The user is seamlessly passed among all resources—SAP or otherwise— until he clicks the logout button. The logout button prompts the Select Access conditional logout rule that deletes the Select Access cookie and fully logs out the user. For details on this rule, see *Configuring Select Access* on page xv.

To configure SSO for the PAS module

1. Create a service file named `<pas_name>.srvc`.
   a. Populate the newly-created service file with the following parameters:

```
~theme                  99
~xgateway               sapextauth
~extauthtype            HTTP
~extid_type             <SAP EXTID TYPE>
~remote_user_alias      SSOSAPUSER
~client                 <SAPGUI CLIENT NUMBER>
~language               <SAPGUI CLIENT LANGUAGE>
```

```
~mysapcomgetsso2cookie   1

~login_to_upcase         1

~redirectHost            <SAP ITS SERVER NAME>

~redirectPath            /scripts/wgate/webgui/!

~exitURL                 http://<sap_server>/
                         <a_logoff_page>

~login_template          redirect

~don't_recreate_ticket   1
```

2 Save this file to the services directory. For details on this file, see the *PAS Installation Guide Release 6.20*.

Configuring Select Access

Table 2 outlines the steps you must perform when setting up Select Access to work with SAP ITS.

Table 2 Setting up Select Access

This step...	Details on how to do it...
Step 1: Install and configure an: • (Required) IIS Enforcer plugin on the Web server that SAP ITS is using. Accept all IIS Enforcer plugin default configuration parameters. **Note:**The IIS Enforcer plugin is automatically given a higher priority than that of the `WGate`. Do not reprioritize these filters. • (Optional) appropriate Enforcer plugin on all other SAP servers if you configured your SAP R/3 application server as a ticket-issuing server. This ensures that Select Access authenticates and authorizes access to all SAP resources—not just to the current SAP ITS resources. **Note:** This step assumes that a Select Access Administration server and Policy Validator are already installed and configured, and running on your network.	1 Run the Select Access installer. 2 Click **Next** until you reach the **Choose Select Access components** installation screen. 3 Install and configure the Enforcer plugin on the Web server that SAP ITS is using. Choose a **Custom** configuration. 4 Enable SSO by configuring the setup screens accordingly, depending on whether you are deploying SAP ITS across a single domain, multiple domains or virtual domains. For details, see Chapter 8, *Configuring the Enforcer Plugins*, in the *HP OpenView Select Access 6.0 Installation Guide*. 5 Accept the defaults for all the other Select Access custom installation screens. 6 Check the following two boxes: — Update Web server configuration to load the Enforcer plugin — Restart Web server 7 Click **Finish**. For details, see Chapter 8, *Configuring the Enforcer Plugins*, in the *HP OpenView Select Access 6.0 Installation Guide*.

Table 2 Setting up Select Access

This step...	Details on how to do it...
Step 2: Manually add SAP ITS to the Resources Tree as a service branch.	1 Right-click a folder or the root of the Resources Tree. 2 Click **New>Service.** The **New Service** dialog box appears. 3 Name the resources and configure the service depending on whether or not the service is specific to a single server. For details see either: — *Entering Information for a Non-Server-Specific Resource Service* on page 43 in the *HP OpenView Select Access 6.0 Policy Builder Guide*. — *Entering Information for a Server-Specific Network Resource Service* on page 43 in the *HP OpenView Select Access 6.0 Policy Builder Guide*. 4 Click **OK**. **Note:** Due to restrictions with SAP servers, Select Access is prevented from running a network discovery.
Step 3: Add the SAP ITS resources you would like secured below the service entry you created in step 2: • (Required) Because it is SAP ITS's access point, you must protect the SAPGUI resource by adding it as a resource entry. • (Recommended) Because they can deliver sensitive information, you should protect any custom resources/ templates for SAP ITS.	1 Right-click the SAP ITS service you just created 2 Click **New>Resource**. The **New Resource** dialog box appears. 3 Name the resouce. For example, using the SAPGUI resource, you might enter the SAPGUI in the **Name** field: `http://mycompany_ITS.com/scripts/wgate/webgui/!` 4 Click **OK.** For details, see *To create a new network resource or edit an existing one* on page 49 in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

Table 2 Setting up Select Access

This step...	Details on how to do it...
Step 4: Enable SelectID for all resources you added in step 3. Enabling and configuring SelectID for SAP ITS resources requires the following: • Configuring an appropriate authentication server. • Enabling and configuring personalization so the authenticated user can access SAP ITS resources.	1 On the SelectID column, enable SelectID for SAP ITS's resources. The **Authentication Properties** dialog box appears. For details on SelectID, see *Setting a Select Auth Policy* on page 82 in the *HP OpenView Select Access 6.0 Policy Builder Guide*. 2 Click the **Authentication** tab and do the following: a If you have already configured some authentication servers listed, click **Add**. The **Available Authentication Servers** dialog box appears. b To configure a combination of authentication servers required by the SAP ITS resources, select one or more server names from the list of **Available Servers** and click **Add.** The server names appear in the **Selected Servers** window. To reorder the servers, select a server in the **Selected Servers** list and click the up arrow or down arrow buttons. c Click **OK**. 3 Click the **Personalization** tab and do the following: a On the **User Data** tab, check the **Store user attributes in** box to export the user's activated attributes to environment variables and then click **Add**. b In the **Directory Attribute Name** column, activate the UID attribute. c For each activated attribute, enter the corresponding **Environment Variable Name** that it is to be exported to. In this case, `SSOSAUSER`. d Click **OK** to finish. Once authenticated, the IIS Enforcer plugin forwards the `SSOSAUSER` HTTP header variable with the user's UID to the SAP ITS server. For details on enabling personalization, see Chapter 5, *Authentication Basics: Select Auth & Personalization*, in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

Table 2 Setting up Select Access

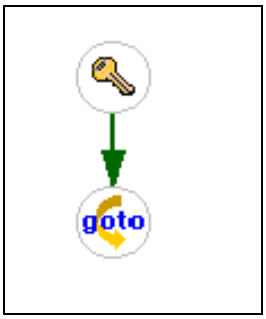
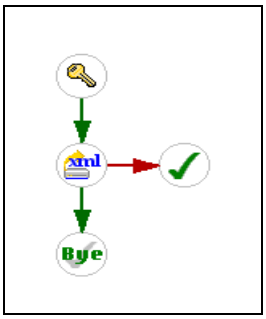
This step...	Details on how to do it...
Step 5: Create a conditional rule that contains a redirect decision point only. Apply the rule to all resources you added in step 3. This redirects users to the PAS module, which initiates it using this URL.	1 From the Rule Builder, create a conditional rule that contains the following decision as shown below:  **Figure 1 Example redirect rule** 2 In the **Redirect Properties** dialog box, configure the decision point with the following redirect destination: `http://<sap_server_name>/scripts/wgate/<pas_name>/!` For details on this URL, see *The integrated authentication process* on page xii. For details on creating conditional rules, see Chapter 8, *Creating Conditional Access Rules with the Rule Builder*, in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

Table 2 Setting up Select Access

This step...	Details on how to do it...
Step 6: Create a conditional rule that contains a query logic decision point and a logout terminal point. Apply the rule to all authenticated SAP ITS users and all SAP ITS resources.	1 From the Rule Builder, create a conditional rule that contains the following decision and terminal points, as shown below: — Query attributes — Logout  **Figure 2 Example logout rule** 2 Add a query attributes decision point that contains the following search expression: — **Query Type**: `http_query_list/~command` — **Comparison operator**: = — **Query Value**: `Logoff` For more details on this decision point, see *The Query Attributes Decision Point* on page 158 in Chapter 8, *Creating Conditional Access Rules with the Rule Builder*, of the *HP OpenView Select Access 6.0 Policy Builder Guide*. 3 Insert an Allow terminal point on the False branch. If the **Query Type** and **Query Value** do not match, the user remains logged in. 4 Add a Logout terminal point beneath the query attributes decision point. This logs out the user and deletes the Select Access cookie. For details on creating conditional rules, see Chapter 8, *Creating Conditional Access Rules with the Rule Builder* in the *HP OpenView Select Access 6.0 Policy Builder Guide*. 5 Apply the rule to all authenticated SAP ITS users and all SAP ITS resource combinations. **Note:** The rules you apply are inherited across multiple resources. For details, see Chapter 7, *Controlling Network Access* in the *HP OpenView Select Access 6.0 Policy Builder Guide*.