

HP OpenView Select Access

SAML Solution Guide

Software Version: 5.2

for HP-UX, Linux, Solaris, and Windows operating systems



October 2003

© Copyright 2000-2003 Hewlett-Packard Development Company, L.P.

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

© Copyright 2000-2003 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

OpenView Select Access includes software developed by third parties. The software 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 OpenView Select Access's `<install_path>/3rd_party_license` directory.

Trademark Notices

- Intel® and Pentium® are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- Java™ is a US trademark of Sun Microsystems, Inc.
- Linux is a U.S. registered trademark of Linus Torvalds.
- Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.
- Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.
- UNIX® is a registered trademark of The Open Group.

Support

Please visit the HP OpenView OpenView Select Access web site at:

<http://www.openview.hp.com/products/select/index.html>

There you will find contact information and details about the products, services, and support that HP OpenView offers.

You can go directly to the HP OpenView support web site at:

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

The support site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

Contents

Chapter 1: About this guide	1
Who is it for?	1
What does it assume you already know?	1
Related references	1
Chapter 2: Introduction	3
What does SAML do?	3
Optimizing online relationships	3
Securing data among your partners	4
How does SAML work?	4
What is a typical deployment scenario?	6
The companies	6
The relationship	6
The problem	7
The solution	7
The things they need to agree upon	7
Chapter 3: Deploying an outbound SAML server	11
Select Access components for a SAML-enabled network	12
Cataloging attributes on Oracle	13
Adding SAML-specific folders to the Policy Matrix	13
The impact on the SAML server setup	13
Configuring the Select Access SAML server for outbound user transfers	14
Before beginning	14
Setting SAML-specific policy	22
Configuring SAML authentication and authorization policy	23
What GenoType's configured Policy Matrix looks like	27
Activating attributes for SAML personalization	28
Configuring the Secure Audit server to record SAML events	31
Available SAML-specific audit policies	31
Preparing Web servers and Web content for SAML-enablement	33
Understanding SAML's redirect syntax	34
Chapter 4: Deploying an inbound SAML server	37
Select Access components for a SAML-enabled network	38
Adding SAML-specific folders to the Policy Matrix	39
The impact on the SAML server setup	39
Configuring the Select Access SAML server as a "to partner" server	40
Before beginning	41
Setting SAML-specific policy	48
Configuring SAML authentication and authorization policy	48
Activating attributes for personalization	50
How it works	50
Taking advantage of roles with SAML	52
Creating roles and setting policy dynamically	52
What E*nsure's configured Policy Matrix looks like	54
Configuring the Secure Audit server to record SAML events	55
Available SAML-specific audit policies	56

Chapter 5: Putting SAML deployment to the test	59
Testing user transfers	59
What can typically go wrong	59
Successful SAML server communication	61
Successful user transfers	64
Changing the SAML server's configuration	66
Index	69

Chapter 1

About this guide

This guide introduces the Security Assertions Markup Language (SAML) and discusses HP OpenView Select Access's implementation of this protocol – the Select Access SAML server. This guide describes a typical deployment scenario for the SAML server and guides you through the process of deploying the server as part of your Select Access-protected network.

Who is it for?

This guide is for users or teams responsible for deploying the SAML server to accept inbound users and/or send outbound users. You can also use it if you are the administrator responsible for configuring delegated administration across organizational boundaries.

What does it assume you already know?

This guide assumes a basic knowledge of single sign-on (SSO) and of the traditional limitations that exist with cookies. It also assumes a working knowledge of Select Access in general and of the components that are available to you as part of its larger access management and authorization system.



HP recommends that you understand the basic technologies used by your partnering organization and what specific configuration details you need to make (for example, what directory it uses and what object classes the directory does not support) to ensure you implement SAML successfully.

Related references

Before you begin to implement SAML, you may want to begin by familiarizing yourself with the contents of the following documents:

- *HP OpenView Select Access v5.2 Network Integration Guide*, © Copyright 2000-2003 Hewlett-Packard Development Company, L.P. ([network_integration_guide.pdf](#))

- *HP OpenView Select Access v5.2 Installation Guide*, © Copyright 2000-2003 Hewlett-Packard Development Company, L.P.
([installation_guide.pdf](#))
- *HP OpenView Select Access v5.2 Policy Builder Guide*, © Copyright 2000-2003 Hewlett-Packard Development Company, L.P.
([policy_builder_guide.pdf](#))
- *HP OpenView Select Access v5.2 Developer's Guide*, © Copyright 2000-2003 Hewlett-Packard Development Company, L.P.
([developers_guide.pdf](#))

Integration Papers for third-party technologies that you can deploy with HP OpenView Select Access are also available on the product CD in the `docs/solutions` folder.

The SAML server is HP OpenView Select Access's implementation of the Security Assertions Markup Language (SAML) protocol. SAML support extends Select Access's Web single sign-on (SSO) capabilities beyond traditional corporate boundaries, to partners who are not necessarily using the same user and/or security management software. Select Access's SAML server allows partners to pass user credentials and other information between them – despite having very different systems.

What does SAML do?

The benefit of using SAML is that it gives you a way of:

- Exchanging authentication and authorization data with partners that have different databases and different security technologies.
- Transferring additional user characteristics with specific user attributes that a partner can use to personalize the transferred user's experience.
- Breaking down external user management boundaries between different organizations. Partners do not need to worry about delegating administration of resources back to the originating organization. Authorization and authentication are configured by the partner performing out-bound not in-bound transfers.
- Breaking down internal user and/or resource management between separate groups within the *same* organization with different back-end systems.
- Defining security mechanisms to encode SAML conversations as well as preventing:
 - Replay attacks
 - Excessive growth of SAML user data repositories
 - Certain denial-of-service attacks
 - Third-party theft attacks

Optimizing online relationships

Unlike typical Web environments where users must register multiple identities with duplicated information, SAML streamlines the registration process for users and businesses alike. This avoids the

data excesses that organizations with a strong online presence are prone to.

Using a well-defined structure, SAML allows one partner to assert the characteristics of a user, allowing the user to transfer seamlessly between the two Web sites. These characteristics come in the form of one or more SAML assertions—the XML used to encapsulate user characteristics so they can be shared among partners. Because partners are trusted, data being shared is accepted without requiring direct proof from the user herself. For example, typical assertions can include the following “statements of fact” about a user:

- The user’s name is Akira Yamamoto.
- The user is a graphic designer.
- The user is a Gold-level client.

By sharing known information, the user needs only one set of user credentials that acts as a passport to different Web sites.

Securing data among your partners

When the system is using SAML to communicate between separate networks, the SAML server that is initiating the interaction, the “from” site (for example, Site1), creates the SAML information and stores it locally. The memory store, and the SAML exchange itself, is at risk. The SAML standard specifies how to counter the potential vulnerabilities as follows:

- The handles that refer to the current connection must have a limited lifetime. That is, they must expire if not used quickly.
- You can only use handles once. This and the above requirements protect against replay attacks and prevent SAML servers from being subject to some types of denial-of-service attacks.
- A SAML server only gives information about a user trying to access resources to the site for which the handle was generated. Thus, if Site1 generates a handle for Site2 and Site3 queries Site1 for the information, Site1 does not pass the information to Site3. This prevents a third site from being able to access the SAML assertions that are meant to go to a legitimate partner site.

How does SAML work?

Any Web site that wants to share user credentials needs a SAML server to SAML-enable their system. Highlights of the system include:

- Currently, you can only implement SAML for Web servers. HP is investigating other services, such as EJB application servers, portal servers to test their viability of being implemented in the future.

- Partners' SAML servers may or may not be Select Access's SAML server. However, this guide assumes that both partners use the Select Access SAML server.
- SAML servers may share the same host computer as the Web/application/portal server or may be hosted by a separate computer on the network.

Figure 1 illustrates the basic network architecture required for a SAML-compliant site that is installed on the same host machine as the partners' Web servers.

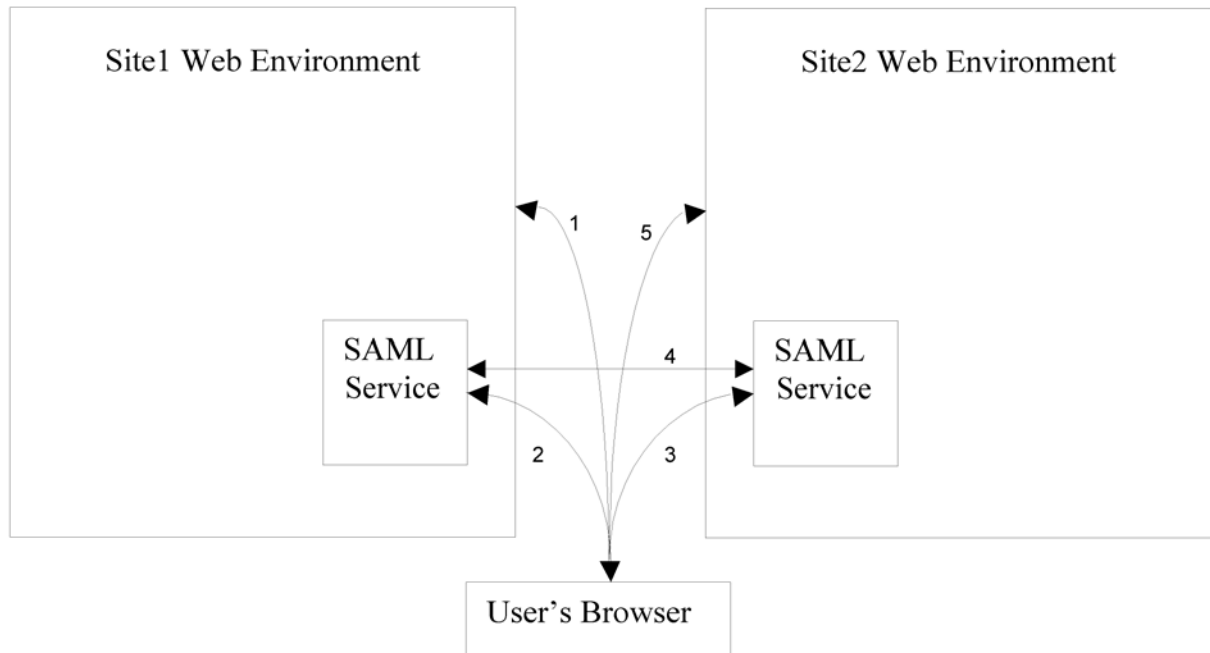


Figure 1: Basic SAML architecture

The steps shown in Figure 1 are described as follows:

1. The user authenticates to Site1's Web system and browses through the system.
2. The user clicks a link that takes her to Site2. The browser is first transparently forwarded to Site1's SAML service. This SAML service adds a partner ID and handle to the link, so that Site2 can identify the session as having originated from Site1.

i The ID and handle are binary data of a fixed size.

3. The browser is redirected to Site2's SAML service, which retrieves the initial link and the additional information. The partner ID tells Site2 how to contact Site1, and the handle tells Site2 how to ask for the information for this connection.

4. Site2's SAML service calls back to Site1's SAML service directly (using the partner ID), and using the handle created in Step 2, retrieves the identity of the user and any additional information that is available from Site1.



The data exchanged between the partners is encoded in XML using Simple Object Access Protocol. SAML-enabled sites use this protocol to structure data between disparate systems so that partners can share information despite the systems' inherent differences.

5. Site2's authorization solution decides whether or not it will let the user access the information.

What is a typical deployment scenario?

While SAML servers have the capability of being configured to accept inbound and perform outbound user transfers, today's current business and technological infrastructures indicate that most deployments will follow a single direction.



We use the scenario introduced in the following subsections as a reference point for the remaining chapters of this guide.



Any group of partner sites can have one or more SAML servers among them. They do not need to be Select Access's SAML servers.

The companies

For example, a typical deployment scenario usually includes two Web-enabled companies:

- GenoType, a biotechnology company, is using the Select Access SAML server to perform outbound transfers. GenoType with several national research and development offices, employs approximately 1,000 scientists, technology, support, and senior management staff.
- E*nsure, a Web-based group Life & Health company, is using the Select Access SAML server to receive inbound transfers.

The relationship

GenoType has recently named E*nsure as their benefits provider. The insurance products they are to provide include:

- Life insurance
- Health benefits
- Self-directed pension plan

The services they are to provide entail:

- Informing employees of plan updates

- A method of monitoring payouts and remaining balances of benefits
- A way of checking and modifying pension details
- One-to-one consulting and user support

The problem

The two companies have identified the following problems:

- Geographical dispersement of GenoType R&D offices means that each office has different legal requirements. This not only creates differences between each regional benefits package, but also in how these packages are communicated. The intranet's Human Resources site is maintained by head office's Web server.
- Each office maintains its own user database. This database is updated as employees come and go. Because some offices exist as a result of acquisitions, some offices use different database technologies.
- GenoType uses token-based authentication systems. This system is incompatible with E*nsure's recently implemented PKI system.
- E*nsure wants to delegate access management to specific resources to regional managers who best know what content each employee needs.

The solution

Both companies are deploying the Select Access SAML server as a means of:

- Integrating E*nsure's services and product information seamlessly from GenoType's Human Resources site.
- Displaying personalized content, not just for displaying personalized portfolio information, but including details on governmental requirements.
- Maintaining a consistent set of user data between the two organizations, without needing users to maintain two sets of login IDs and without requiring either party to change database technologies.
- Separating the management of policy from the deployment process, so that each partner organization worries about the access policies for its own systems only.

The things they need to agree upon

Select Access's SAML solution requires that both parties predetermine specific configuration details. Both parties have therefore come to an agreement on the following configuration parameters that are required by the SAML 1.0 specification document:

- *Namespaces* for GenoType and E*nsure. The SAML namespace is an XML namespace. Because each partner defines its own namespace, a SAML-enabled system uses the namespaces to create a universally unique set of attribute names (described

further below) – irrespective of the number of partners that may exist.

- *Attributes* used to exchange data between them via SAML assertions. The SAML protocol uses attributes to create assertions about a subject, which in this case is a specific, authenticated user identity. An attribute assertion asserts that the specified user has the defined attribute(s). The data in this attribute assertion are used to:
 - Create the temporary SAML user entry using values defined in the attribute assertion.
 - Determine which personalized content the user can access based on the attributes in the assertion.



The Select Access SAML server also supports other types of assertions: authentication and authorization. Authentication assertions declare that the issuer has authenticated the specified subject—in this case, a particular user. Authorization assertions declare that a subject can access one or more resources. In addition to attribute assertions, the inbound SAML server can request any of these assertions to validate the user and create the user directory for that person, before access to local resources is granted.

-
- *Other parameters from the SAML 1.0 specification* like security domain, Issuer, and IDs that you need to carefully enter in the SAML server setup to ensure transfers happen seamlessly:
 - Security domain is typically the same as the domain of the Web site that authenticated and transferred the user.
 - Issuer is any unique tag for the administrator of the Select Access SAML server. The SAML server uses this string to construct attribute assertions.
 - IDs are used to construct or deconstruct a SAML-specific artifact for redirecting users. The IDs use 20 bytes of a 42-byte artifact. The remaining 22 bytes consist of 2 bytes of type code, and 20 bytes of random data. When the user is redirected to E*nsure's SAML server, the artifact is added to the redirect URL. E*nsure's server extracts the artifact and deconstructs it with the ID configured on their side. Once it knows which partner it needs to contact, it creates an artifact request containing the artifact handle (which is the 20 bytes of random data). For details on this artifact exchange, see *What happens when the user clicks the redirect link?* on page 61.



If the values between one or more servers do not match, the SAML server cannot successfully transfer users.

- Other non-SAML parameters that you also need to predefine include:
 - *SSL/PKI systems* and how partners plan to coordinate CA and client certificates. PKI setup is not trivial, and partners must implement SSL correctly before the two sides can communicate securely with no threat of impersonation attacks.
 - *Object class, attribute name, and group name restrictions* among different directory servers. Because of the differences among the various vendor implementations of LDAP, partners must evaluate their directory servers to see where limitations occur in their different schemas.
 - *Roles* that both organizations will share. If one or both partners intend to delegate administration privileges across organizational boundaries, roles are a way to accomplish this. Initially, however, E*nsure wants to use roles so it can set policies quickly and easily.
 - *Policy Builder access policies* they wish to apply locally, leveraging the roles they define.

Deploying an outbound SAML server

This chapter discusses how to set up a Select Access SAML server on a network with other Select Access components. It uses the scenario introduced in *What is a typical deployment scenario?* on page 6. Please read this scenario before continuing.

i If you are configuring your own outbound SAML server, you can follow the examples discussed in this chapter. For each step where we use a GenoType value to illustrate a typical scenario, simply substitute your own value.

Table 1 summarizes what high-level steps GenoType needs to perform to ensure that its Select Access SAML server runs smoothly with E*nsure's SAML server. As the SAML server administrator, these are the steps you too need to perform for your organization.

Table 1: Setting up an outbound SAML server

Step...	For details, see...
1. Install the correct combination of Select Access components.	<i>Select Access components for a SAML-enabled network on page 12</i>
2. Index the Oracle directory server.	<i>Cataloging attributes on Oracle on page 13</i>
3. Create SAML-specific folders in the Policy Builder so you can set up the SAML server smoothly.	<i>Adding SAML-specific folders to the Policy Matrix on page 13</i>
4. Set up the Select Access SAML server.	<i>Configuring the Select Access SAML server for outbound user transfers on page 14</i>

Table 1: Setting up an outbound SAML server (Continued)

Step...	For details, see...
5. Set the corresponding policies in the Policy Builder for the SAML resources required for outbound transfers.	<i>Setting SAML-specific policy on page 22</i>
6. Set up your server's audit settings to ensure it captures the correct SAML messages.	<i>Available SAML-specific audit policies on page 31</i>
7. Modify/set up Web content so it meets the requirements of their SAML environment.	<i>Preparing Web servers and Web content for SAML-enablement on page 33</i>

Select Access components for a SAML-enabled network

As an organization that performs outbound user transfers, the first step in SAML-enabling a network is to first assess what Select Access component combinations you need for this type of deployment.

GenoType ascertains that, at minimum for a company its size, they need to install and configure the following Select Access components:

- One SAML server to send authenticated employees to E*nsure's Web site, as well as any additional personalization information required to allow users to see specific content for them. The GenoType administrator installs the SAML server on the same host computer as the Sun ONE Web server. For details, see *Configuring the Select Access SAML server for outbound user transfers* on page 14.



GenoType installs its SAML server on their De-Militarized Zone (DMZ) network so that partner sites can contact it.

- Two Policy Validators for load balancing and high availability, which ensures faster throughput of users.
- Three Enforcer plugins:
 - One to enforce access decisions on their Sun ONE Web server, which GenoType also installs on their DMZ. The GenoType administrator actively installs this Sun ONE Enforcer plugin with the InstallAnywhere wizard.
 - One to protect the SAML server specifically using Select Access. The Setup Tool automatically installs this Enforcer plugin when the GenoType administrator configures their SAML server. For details, see *To configure a SAML server so it transfers users to a partner* on page 15.

- One to control delegated administrators (internally). Select Access automatically installs and sets up this Enforcer plugin when the GenoType administrator sets up their internal delegated administration privileges.
- One Administration server to manage and coordinate Select Access components.
- One Secure Audit server to monitor Select Access components as well as record SAML transactions.

Cataloging attributes on Oracle

Because they are using an Oracle directory server as a user source, GenoType must index their attributes. Otherwise, searches based on attributes fail and so does the Policy Validator. To catalogue your SAML user attributes:

1. Watch for a “schema is read only” message while running the setup wizard.
2. Change the permissions on your schema to become writable.
3. Index all user attributes by running Oracle's catalog utility called `catalog.sh` to add all required user attributes to the index list. For example, a sample command on Unix is:

```

$<ORACLE_HOME>/ldap/bin/catalog.sh -connect
connectiondescriptor -add -attr nxAccountDeleteTime

```

Adding SAML-specific folders to the Policy Matrix

The GenoType administrator adds folders to the Policy Matrix before setting up their SAML server. This preliminary step avoids an interruption in the setup process.

The impact on the SAML server setup

GenoType adds a new folder below the Known Users branch called “SAML partners.” This folder location holds the E*nsure entry that the Administration server creates as part of their SAML server setup and startup. These instructions assume you are the GenoType administrator.




A single SAML partner location makes relationship maintenance easier. As the number of partnerships increases, the entries for them are centrally located.


To add a SAML partner folder for outbound SAML servers

1. In the Policy Builder, right-click a user data source on the Users Tree and select **New>Folder**.
2. In the **New Folder** dialog, configure the following folder properties:
 - **Folder Name**=SAML Partners

- **Description**—This folder holds all current partners to which GenoType sends authenticated users.

 The **Folder Name** value becomes the RDN of the entry. It is the name that appears on the Users Tree.

3. Click **OK** to commit these changes to the directory server.

 For additional details on how to create a new folder, see Chapter 5, *Organizing users and resources*, in the *HP OpenView Select Access v5.2 Policy Builder Guide*.

Configuring the Select Access SAML server for outbound user transfers


Having installed the SAML server, GenoType now needs to go about configuring it for their needs. Because GenoType is only going to need the SAML server to perform outbound user transfers, they use the wizard in the Setup Tool. Configuring a SAML server to perform outbound user transfers involves these basic steps:

- Providing the Administration server's contact information. This enables the SAML server to register with it and retrieve configuration details from it.
- Configuring basic setup parameters for the host computer of the SAML server and specifying what kind of SAML server it is. This is so GenoType can set up the host computer as a SAML server.
- Configuring the assertions and the partner's user location in the Policy Store. GenoType's SAML server then knows how to function in its SAML-enabled environment. That is, the server knows how to handle partners and knows what type of user information it needs to deliver to E*nsure's server.
- Configuring E*nsure's SAML server information. This is so GenoType's SAML server can authenticate E*nsure's SAML server for transmitting users and credentials to it.

Before beginning

Before running the Setup Tool, you consult with E*nsure and perform these initial tasks:

- Synchronize the clock settings between the two SAML server host computers.

 Both the sending and receiving SAML servers must ensure that clock settings at both sites not differ by more than a few minutes.

- Confirm the actual URL of E*nsure's SAML server so you configure the right value and ensure their URL alias for it works correctly.
- Determine the authentication method that E*nsure's SAML server uses to authenticate GenoType's SAML server. Together, they must choose between certificate or password authentication:
 - If they decide to use certificates, GenoType must get E*nsure's SSL client certificate for this purpose.



The client certificate must also contain either a `CN` or `UID` value (which must be unique). Otherwise, the server does not accept the certificate. GenoType must also check that the `CN` and `UID` values are valid on each other's directory servers.

- If they decide to use passwords, E*nsure must provide a password so GenoType can configure the corresponding parameter correctly.
- Check that the user attributes are LDAP v3.0-compliant attributes and ensure that names (in this case, `title` and `employeeNumber`) and values are valid on E*nsure's directory server. For example, GenoType had an attribute called `EmpType`, which they changed to `employeeType` to be compatible.
- Ensure that you have received a text file that contains E*nsure's exported values for your server's **Partner ID**, **Security Domain**, and **Issuer** properties. These values must match exactly; otherwise, the server cannot successfully transfer users.

Once you have taken these preliminary steps, you can be confident that you can easily configure your server. For details, see *To configure a SAML server so it transfers users to a partner*. These instructions assume you are the GenoType administrator.

To configure a SAML server so it transfers users to a partner

1. Run the Setup Tool as described in *To configure Select Access with the Setup Tool of the HP OpenView Select Access v5.2 Installation Guide*.
2. Click **Next** to reach the Setup Tool's **SAML server** setup screen where you click the **Configure** button.
3. On the **Contact the Administration server** setup screen, enter the contact information for your Administration server and click **Next**.
4. On the **ID** setup screen, enter a descriptive ID string for your SAML server: `fortress.genotype.com:SAML server`. Click **Next**.

- On the **General** setup screen, configure the general contact and functional parameters for your SAML server as shown in Table 2.

Table 2: GenoType's General SAML server configuration values

For this parameter...	Enter this value...
Host	fortress.genotype.com
SSL Port	9985, which is Select Access's default value The SAML server runs on two ports: <ul style="list-style-type: none"> The default port value you enter. This port is used for all communications that occur after the partner is authenticated. The default port minus 1 (in this example, 9984). This port is used for authentication only. Both port numbers become part of the SAML server's service entry properties that are automatically created when you finish the server's configuration. For details, see step 17.
Select the location of the SSL certificate	d:\ssl\pkcs#12 certs\fortress_saml.p12
SSL Server Certificate Password	BeamMeUpSco77y!
The server will transfer users to known SAML single sign-on partners	Box is checked.

When GenoType completes the configuration of this screen, it appears like the one shown in Figure 2.

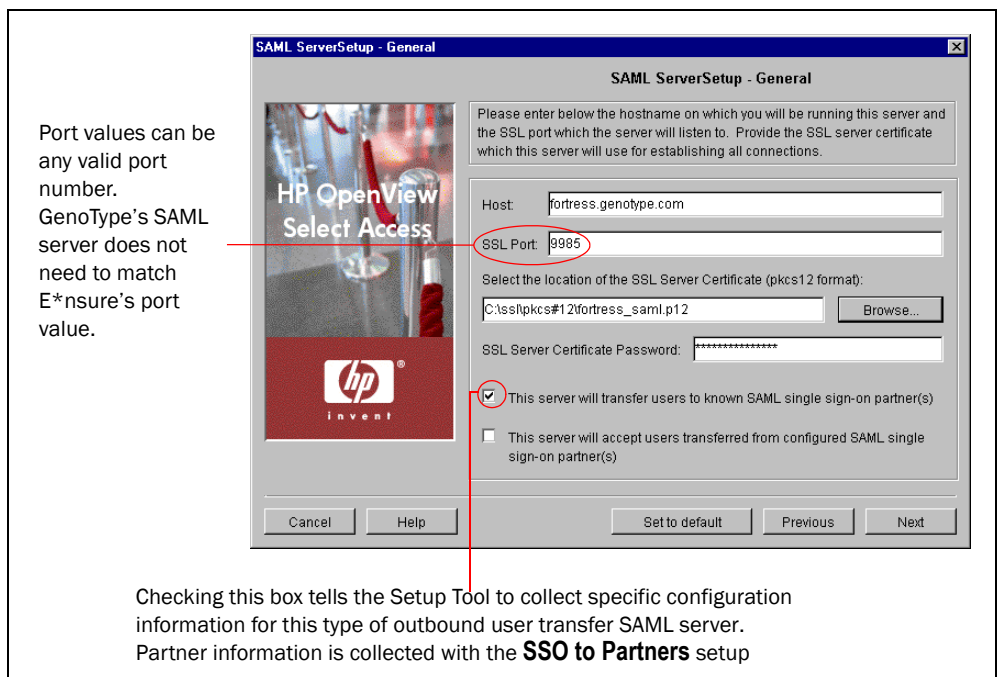


Figure 2: GenoType's General setup screen

- Click **Next**, and the **Setup SAML Server's Assertion Properties** screen appears. Configure the parameters that the SAML server uses to assert its identity, as highlighted in Table 3. E*nsure's SAML server verifies GenoType's assertions by verifying the tags in them with the information contained in E*nsure's locally stored configuration file for its server, which contains these same values.



E*nsure will already have authenticated GenoType's SAML server before receiving the first SAML assertion. They authenticate GenoType's server with E*nsure's CA certificate.

Table 3: GenoType's SAML Server's Assertion Properties values

For this parameter...	They enter this value...
Location in LDAP where all partners will be stored	Browse to ou=SAML partners, o=genotype.com
Server's Source ID*	GenoType SAML server
Issuer*	GT Admin
Security Domain*	www.genotype.com
Attribute Assertion Lifetime	7 days (10800)
Authentication Assertion Lifetime	5 minutes
Retrieval Timeout	5 minutes



Fields marked with an asterisk (*) in Table 3 indicate the properties the Setup Tool can export to file (see step 11). Note that the Source ID property is the same value that the E*nsure administrator must enter in his **Partner ID** field.

When GenoType completes the configuration of this screen, it appears like the one shown in Figure 3.

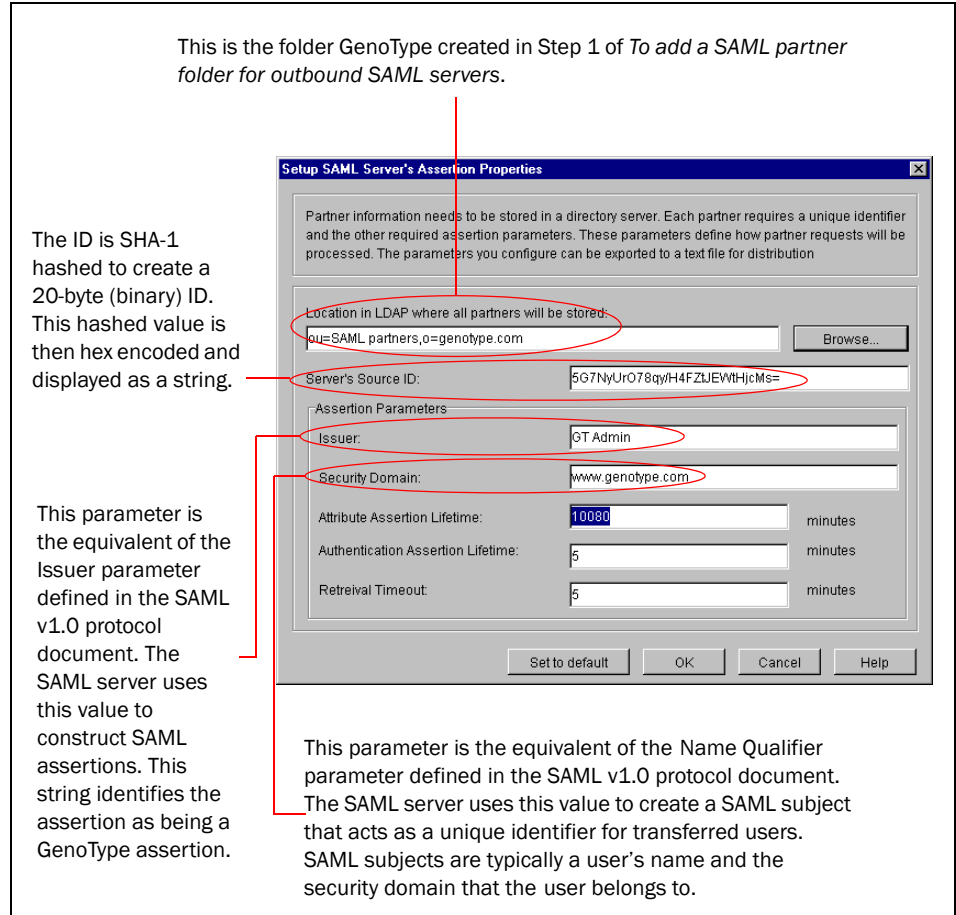


Figure 3: GenoType's Setup SAML Server's Assertion Properties screen

7. When finished, click **OK**. This displays the **SSO to Partners** setup screen.
8. Click the **Add** button to add E*nsure as their SAML partner.
9. On the **Setup SAML Destination Partner** screen, configure the values outlined in Table 4.




Fields marked with an asterisk (*) in Table 4 indicate the properties that you configure with information that comes from E*nsure's administrator. These values must match exactly with what E*nsure uses with its SAML server.

Table 4: GenoType's configured partner properties for E*nsure

For this parameter...	Enter this value...
Partner Name	E*nsure
URL Alias	to-ensure.com
Partner's SAML URL*	https://saml.ensure.com:9985/saml_in

Table 4: GenoType’s configured partner properties for E*nsure (Continued)

For this parameter...	Enter this value...
Attribute Namespace	<p>GenoType_Employee</p> <p>Note: When GenoType’s SAML server sends an activated attribute to E*nsure’s SAML server, GenoType’s server prepends the attribute with this namespace as follows:</p> <p>GenoType_Employee:title, VP Biogenetic Research</p> <p>This makes all attribute names unique across a group of partners, even if another partner uses the same attribute name. The namespace prevents the wrong set of users from accessing content they do not have permissions for.</p>
Partner’s SSL Client Certificate*	<p>Enable this option and paste in the client certificate counterpart to the CA certificate that will be forwarded to E*nsure.</p> <p>Note: The certificate must include a PEM-format client certificate in it.</p>

 GenoType uses the **URL Alias** in the transfer link that appears on the HR landing page. This way, they do not need to write a link that uses the full **Partner’s SAML URL**. For example:

```
https://saml.genotype.com:9985/saml_out/  
https://saml.ensure.com:9985/saml_in?TARGET=http://  
extranet.ensure.com:81/MyPages.asp
```

Instead, you can write a shorter version of it. For example:

```
https://saml.genotype.com:9985/saml_out/  
to-ensure.com?TARGET=http://extranet.ensure.com:81/  
MyPages.asp
```

This also has the added benefit of obscuring the real SAML URL and thereby minimizing the risk of attack.

When GenoType completes the configuration of this screen, it appears like the one shown in Figure 4.

The SAML server uses this name to display the partner in the Policy Builder's Users Tree and to create a CN attribute for that partner. It also uses the CN to construct the DN of user entries that the server adds to the User Tree for the partner.

Because GenoType's SAML server is performing outbound transfers only, they can only create one namespace. Each namespace is unique to a given partner. **Note:** Like other SAML properties, the SAML server drops namespaces before Select Access can record user information to the partner's directory server.

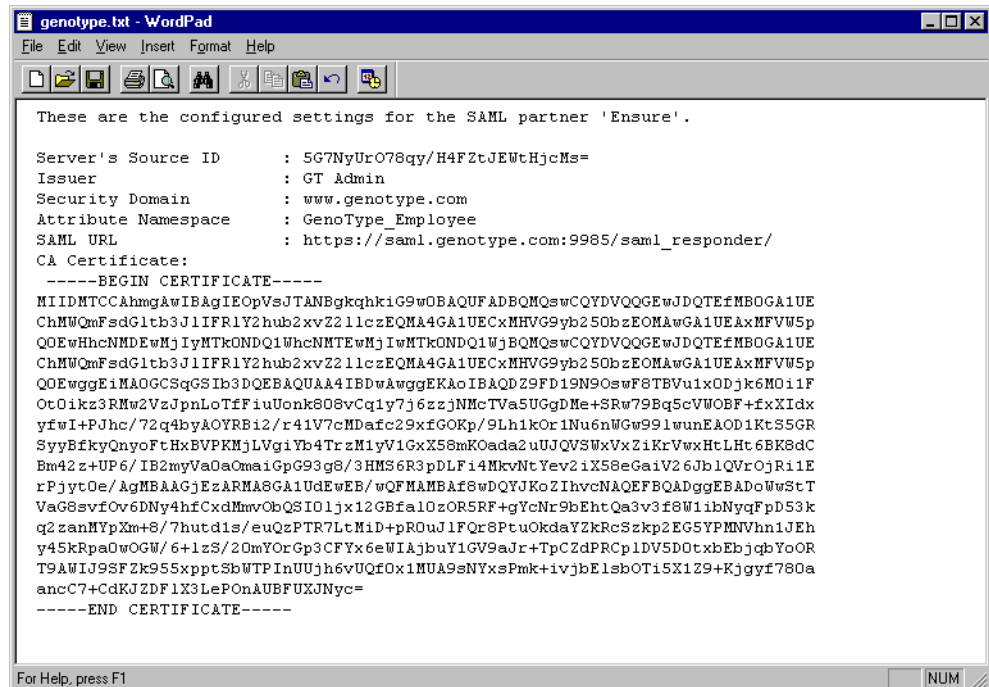
The SAML server extracts the UID and the CN in the client certificate from the certificate and adds them as attribute values in E*nsure's partner entry for GenoType on the Users Tree. If the UID or the CN values are not valid on E*nsure's directory server, it does not create the entry.

Figure 4: GenoType's Setup SAML Destination Partner setup screen

10. Click **OK** to return to the **SSO to Partners** setup screen.
11. Click the **Save to File** button so you can easily share your server information with E*nsure. The file you create is `genotype.txt`, which you email to the E*nsure administrator. Figure 5 shows this text file when opened in WordPad.



If GenoType's and E*nsure's assertion properties do not match (that is, one party misconfigures a value), SAML exchanges cannot occur. To minimize this risk, export this information to a text file as explained in step 11. Exporting this information guarantees that E*nsure configures its server using the exact values you configured with this setup screen.



```

These are the configured settings for the SAML partner 'Ensure'.

Server's Source ID      : 5G7NyUrO78qy/H4FZtJEWtHjcMs=
Issuer                  : GT Admin
Security Domain         : www.genotype.com
Attribute Namespace     : GenoType_Employee
SAML URL                : https://saml.genotype.com:9985/saml_responder/
CA Certificate:
-----BEGIN CERTIFICATE-----
MIIDMTCCAhmgAwIBAgIEOpVsJTANBgkqhkiG9w0BAQUFADBQMQuwCQYDVQQGEwJDQTEfMBOGA1UE
ChMwQmFsdG1tb3JlIFRlY2hub2xvZ211c2EQA4GA1UECXMHVGV9yb250bzEOMAwGA1UEAxMFVW5p
Q0EwHhcNMDEwMjIyMjEwMTk0NDQ1WzBQMA4GA1UECXMHVGV9yb250bzEOMAwGA1UEAxMFVW5p
ChMwQmFsdG1tb3JlIFRlY2hub2xvZ211c2EQA4GA1UECXMHVGV9yb250bzEOMAwGA1UEAxMFVW5p
Q0EwggEiMA0GCgsqSIs3DQEBAAQA4IBDwAwggEKAAIBAQDZ9FD19N9OswF8TBVU1xODjk6MOi1F
Ot01kz3RmW2VzJpnLoTfIUonk808vCq1y7j6zzjNMcTVa5UGgDMe+SRw79Bq5cVW0EF+fxXIdx
yfwI+PJhc/72q4byAOYRBi2/r41V7cMDaFc29xfGOKp/9Lh1kOr1Nu6nWgW991wunEA0D1KtS5GR
SyyEfyQnyoFtHxBVPKMjLVgiYb4TrzM1yV1GxX58mK0ada2uUJQVSWxVxZiKrVwxHtLHt6BK8dC
Bm42z+UP6/IB2myVaOaCmaiGpG93g8/3HMS6R3pDLF14MkvNtYev21X58eGaiV26Jb1QVrOjR11E
rPjytOe/AgMBAAGjEzARMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBADoWwStT
VaG8svfOv6Dny4hfCxdMmvObQSI01jx12GBfa10zOR5RF+gYcNr9bEhtQa3v3E8W11bNyqFpD53k
q2zanMYpXm+8/7hutd1s/euQzPTR7LtmID+pR0uJ1FR8PtUOkdaYZkRcSzkp2EG5YPMVhn1JEOR
y45kRpaOwOGW/6+1zS/2OmYOrGp3CFYx6eWIAjbuY1GV9aJr+TpC2dPRCpLDVSD0txbEbjqbYoOR
T9AWIJ9SFZk955xpptSbWTPInUUjh6vUQf0x1MUA9sNYxsPmk+1vjbE1sbOTi5X1Z9+Kjgyf780a
ancC7+CdKJZDF1X3LePonAUBUFUXJNyc=
-----END CERTIFICATE-----

```

Figure 5: GenoType's exported file with configuration parameters

12. Configure your SAML Enforcer plugin with the subsequent screens. These screens are the same screens that appear in the Enforcer plugin's setup wizard. Because you need the SAML Enforcer plugin to forward log messages to the Secure Audit server, choose the **Custom** configuration option on the SAML Enforcer plugin's **General** setup screen.
13. Click **Next** until the **Audit Settings** screen appears.
14. Click **Add** to create a new audit entry. This entry consists of an **Audit Trail** using your Secure Audit server as the output destination and an **Audit Policy** that includes the following **Component/Level** combinations:
 - SAML Out/INFO
 - SAML Responder/ERROR
 - SAML Action/ERROR



Because you configured audit policies to the lowest severity, the SAML server logs and forwards all messages of all severities to the Secure Audit server automatically.

For more information on audit policies, see *Available SAML-specific audit policies* on page 31.

15. On the **New Audit Entry** dialog, click **OK**.

16. Click **Next** until the **Finish** setup screen appears, informing you that you have completed all setup tasks for the SAML server and its Enforcer plugin.



You can modify the SAML server and the SAML Enforcer plugin's configuration with the Component Configuration tool, which is available from the Policy Builder. However, unlike with the Setup Tool, the Component Configuration tool cannot export the certificate to a text file, because it cannot access the certificate from its location. For the SAML server, changes only take effect after you or the Setup Tool restarts it.

For details, see Chapter 15, *Modifying components' central configuration parameters*, in the *HP OpenView Select Access v5.2 Policy Builder Guide*.

17. Keep the **Start now** box checked and then click **Finish** to commit your configuration to the Policy Store. The Setup Tool creates the following entries on the Resources Tree:
 - An HTTPS service entry for the SAML server. By default, this entry appears in the following location:
`ou=Network,nxResource=https,nxResource=<hostname>:SAML Server`
 - Two resource entries below the SAML server service entries:
 - saml_out is the script that initiates the transfer to E*nsure's SAML server.
 - saml_responder is the URL path that E*nsure's SAML server uses to query GenoType's SAML server for user information. The saml_responder communicates with E*nsure's saml_in script.



This URL is the same URL E*nsure configures in the **Partner's SAML URL*** field of the **SAML Partner Properties** dialog.

Setting SAML-specific policy

Once you have configured GenoType's SAML server, you need to set up the Policy Builder so it is equipped to handle outbound SAML

transfers. Outbound SAML transfers require that you configure the following:

- *Authentication and authorization:* Configure and choose not just what method of authentication SelectID is to use, but also which users can access specific SAML server components.



Because Select Access's implementation of the SAML server only supports either the certificate-based or password-based method, you need to set up SelectID authentication. This ensures it works with the SAML server GenoType has just configured.

- *Personalization:* Activate user attributes and configure personalization for outbound employees. Any SAML server that performs outbound transfers must enable personalization so SAML attribute assertions can be well-formed.

The corresponding subsections explain these requirements in greater detail.

Configuring SAML authentication and authorization policy

Configuring authentication and authorization for GenoType's newly configured SAML server requires that you manually add the components of this service along the Resources Tree axis. This allows authentication and authorization to be set up accordingly.

Table 5 summarizes how GenoType sets up SelectID, and assumes you are GenoType's administrator. This table describes the high-level steps as well as provides more granular detail on how you accomplish each step.



This procedure assumes that you have already added GenoType's Sun ONE Web server as a service and added the corresponding Web content resources below it (for example, the employee benefits landing page). It further assumes that the employee benefits landing page has an allow policy set against it for GenoType's employees.

Table 5: GenoType’s authentication methods and access policies

Setup task...	Instructions to accomplish...
<p>Step 1: GenoType sets the following access policies for:</p> <ul style="list-style-type: none"> • All users that GenoType’s server transfers to E*nsure’s SAML server. • E*nsure’s User Tree entry. 	<ol style="list-style-type: none"> 1. Where GenoType’s users folder (“Employees”) and the saml_out resource intersect on the grid, set an allow policy. All users in this folder automatically inherit this policy. Users need access to this script; otherwise, their server cannot initiate a transfer. 2. Where E*nsure’s User Tree entry and the saml_responder resource intersect on the grid, set an allow policy. E*nsure needs access to the saml_responder servlet. Otherwise, the saml_responder cannot send assertions to E*nsure’s saml_in script, which results in a 403:forbidden HTTP status message.
<p>Step 2: Realizing that they require certificate-based authentication, GenoType uploads the root CA certificate.</p> <p>This root certificate validates connections between GenoType’s and E*nsure’s SAML server.</p>	<ol style="list-style-type: none"> 1. On the directory server, create a Certificates folder, that is, ou=Certificates, o=GenoType.com. 2. They upload the certificate to this location. <p>Note: The directory server entry must use a <code>certificationAuthority</code> object class and a <code>caCertificate</code> attribute. Otherwise, GenoType will receive a message indicating that a certification authority policy cannot be found.</p>

Table 5: GenoType’s authentication methods and access policies (Continued)

Setup task...	Instructions to accomplish...
<p>Step 3: With the certificate uploaded to their directory server, GenoType configures a certificate server.</p>	<ol style="list-style-type: none"> 1. In the Policy Builder, click Tools>Authentication Servers. 2. In the Authentication Server dialog, click the Add button. 3. In the Authentication Method dialog, configure the following properties: <ul style="list-style-type: none"> – Name=CertSAML – Authentication Method=Certificate 4. In the New Certificate Server dialog, configure the following properties: <ul style="list-style-type: none"> – Specify location for user lookups=Known Users – Specify policy location for newly authenticated users without user entry=o=SAML Partners,o=GenoType.com <p>Note: This folder is the folder they created in Step 1 of <i>To add a SAML partner folder for outbound SAML servers</i> on page 13.</p> <ul style="list-style-type: none"> – Specify root certificate location=o=Certificates,o=GenoType.com <p>Note: This folder is the folder you created in Step 1 of this table.</p> <ul style="list-style-type: none"> – Require certificates to be stored on the directory server=checked (enabled). <p>Caution! Failure to check this box can result in unauthorized access to GenoType’s SAML server. By not enabling this option, the certificate authentication server only checks the <i>signature</i> of the certificate that was sent. It does not compare the certificate it receives with the partner’s certificate in the directory server. This means that the server considers any certificate signed by the configured CA as a valid certificate.</p> <ul style="list-style-type: none"> – Allow unknown CA=unchecked (disabled). 5. Click OK to write these configuration details to the Policy Store. <p>For details on how to configure a certificate server, see <i>To configure a new or existing certificate server</i> in the <i>HP OpenView Select Access v5.2 Policy Builder Guide</i>.</p>

Table 5: GenoType’s authentication methods and access policies (Continued)

Setup task...	Instructions to accomplish...
<p>Step 4: In case they ever need to use password authentication with another future SAML partner, GenoType also configures a password server.</p>	<ol style="list-style-type: none"> 1. In the Policy Builder, click Tools>Authentication Servers. 2. In the Authentication Server dialog, click the Add button. 3. In the Authentication Method dialog, configure the following properties: <ul style="list-style-type: none"> – Name=PassSAML – Authentication Method=Password 4. In the New Password Server dialog, configure the following properties: <ul style="list-style-type: none"> – Specify location for user lookups=Known Users – Enter filename of password login form =the default form, login_form.html. 5. Click OK to write these configuration details to the Policy Store. <p>For details on how to configure a password server, see <i>To configure a new or existing password server</i> on page 120 in the <i>HP OpenView Select Access v5.2 Policy Builder Guide</i>.</p>

Table 5: GenoType’s authentication methods and access policies (Continued)

Setup task...	Instructions to accomplish...
<p>Step 5: GenoType enables SelectID against the following resources:</p> <ul style="list-style-type: none"> • saml_out • saml_responder 	<ol style="list-style-type: none"> 1. For the saml_out resource, enable SelectID. Do this by: <ul style="list-style-type: none"> – Right-clicking the cell where the SelectID column and the saml_out resource intersect and click Enable SelectID. – In the Authentication Method dialog, selecting the same authentication method for their employee benefits landing page (as well as its graphic resources). In this case they choose PassEmp as the server. <p>Note: The saml_out resource also requires that GenoType configure personalization for it. Because details are extensive, we discuss them in a separate topic. For details, see <i>Activating attributes for SAML personalization</i> on page 28.</p> 2. For the saml_responder, GenoType also enables SelectID. Do this by: <ul style="list-style-type: none"> – Right-clicking the cell where the SelectID column and the saml_out resource intersect and clicking Enable SelectID. – In the Authentication Method dialog, selecting CertSAML as the authentication method for this script. In the future, they might opt to choose PassSAML.

What GenoType’s configured Policy Matrix looks like

When GenoType has successfully configured their Policy Matrix, they see:

- A populated SAML Partners folder, which holds only Ensure’s entry.
- SAML-specific resources.
- A certificate folder with a CA certificate uploaded to this location.
- A variety of explicitly set allow and deny policies, as well as inherited ones.
- A variety of explicitly set authentication/SelectID policies, as well as inherited ones.

Figure 6 summarizes all of these changes.

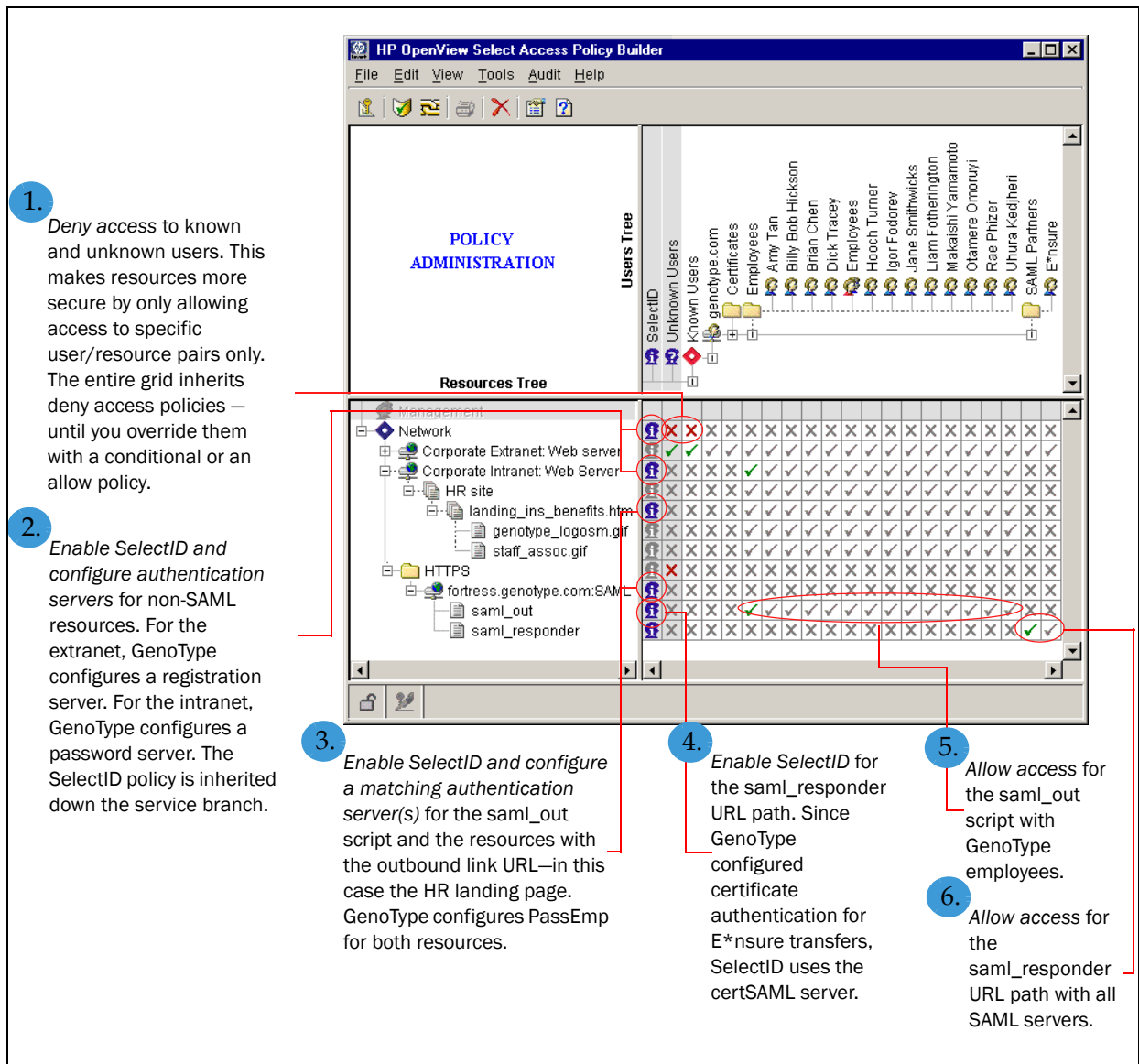



Figure 6: GenoType’s SAML-enabled Policy Matrix

Activating attributes for SAML personalization

Because each employee’s benefit package varies depending on their pension plan investments and current insurance items being processed, GenoType also needs to activate attributes. The SAML server then includes these attributes in the transfer, which allows E*nsure to configure personalization accordingly.



Partners must always agree upon which attributes the outbound partner must activate. GenoType and E*nsure met early on in their partnership and already concluded which attributes are a) the most useful, and b) supported by both directory servers. If you do not ensure attribute names and values are valid, the “To partner” ignores them, and personalization cannot occur.

 If you sending users that have a CN that is longer than 20 characters to a SAML partner that is using an Active Directory server, and you do not export the UID as a personalization attribute, the SAML authentication fails. In this case, always export the UID attribute to avoid this problem.

Personalization consists of three distinct steps, as summarized by Table 6. These instructions assume you are the GenoType administrator.

Table 6: Configuring personalization attributes

Step...	For details, see...
1. Activate personalization attributes. Attributes determine how a Web server deploys resources for personalization, once the partner receives the inbound user transfer. For example, E*nsure's Policy Validator will evaluate which network resource to display, depending on the attributes GenoType selects.	<i>To activate attributes on page 29</i>
2. Set up personalization. GenoType uses activated attributes to send additional user information to E*nsure. The Web server uses attributes to determine what content the user sees.	<i>To enable SAML-based personalization on page 31</i>

To activate attributes

1. In the Policy Builder, click **Tools>Activate Directory Attributes**.
2. In the **Activate Directory Attributes** dialog, activate all the attributes they require. Do this by:
 - a. Selecting one or more attributes in the **Available Attributes** list. Of the available attributes used for SAML-based personalization, GenoType activates the `title` and `employeeNumber` attributes only. These attribute names exactly match the attribute names supported by E*nsure's directory server.



Use the UID attribute selectively. Since Select Access requires that UIDs on the Users Tree be unique, two partners can have conflicting user entries.

- b. Clicking the **Add** button to move them into the **Activated Attributes** list. The “To partner” uses these attributes to determine how their Web server displays personalized content.



The Policy Builder reads which attributes are available from GenoType’s directory server schema.

Because two Select Access SAML server are exchanging attributes, GenoType can only enable the supported attributes for Select Access’s implementation of SAML. “To partner” Select Access SAML servers automatically discard unsupported attributes. Table 7 lists all supported SAML personalization attributes.



Not all directory servers support all of these attributes. Check your directory server’s documentation and see which subset of these attributes are available to you and your partner(s).

Table 7: Supported SAML personalization attributes

Available attributes by name (listed alphabetically)			
audio	businessCategory	carLicense	cn
departmentNumber	description	destinationIndicator	displayName
employeeNumber	employeeType	facsimileTelephoneNumber	givenName
homePhone	homePostalAddress	initials	internationaliSDNNumber
jpegPhoto	l	labeledURI	mail
manager	mobile	o	ou
pager	photo	physicalDeliveryOfficeName	postalAddress
postalCode	postOfficeBox	preferredDeliveryMethod	preferredLanguage
registeredAddress	roomNumber	secretary	seeAlso
sn	st	street	telephoneNumber
teletexTerminalIdentifier	telexNumber	title	uid
userCertificate	userPassword	userPKCS12	userSMIMECertificate
x121Address	x500uniqueIdentifier		

3. GenoType does not need to reorder these attributes, so leave them in the order they appear.
4. To commit these attributes, click the **OK** button.

To enable SAML-based personalization

1. In the Policy Builder, right-click the cell where the SelectID column and the saml_out resource intersect and choose **SelectID Properties**.
2. In the **Authentication Method** dialog, click the **Personalization** tab.
3. Click the **User Data** tab to configure the attributes used to personalize the user's Web content. Do this by:
 - a. Selecting the **Store user attributes in** check box.
 - b. Entering the `title` and `employeeNumber` attributes in the **Directory Attributes** column.
 - c. Defining the corresponding environment variable that the server exports the attribute to in the **Environment Variable Name** column. In this case, the environment variable names match the user attribute names.
4. Click **OK** to commit these changes to the Policy Store.



GenoType must take extreme care when setting up personalization, especially if their number of partners increases. Each additional partner creates additional risk that personalization could fail due to human error. Since each partner could conceivably have different directory servers that have different name/value requirements, all stakeholders must ensure that attribute names/values are not just supported by SAML, but that partners synchronize them with environment variables, as well as meet directory server restrictions.

Configuring the Secure Audit server to record SAML events

To monitor SAML transactions with E*nsure, GenoType reconfigures their Secure Audit server to specifically track SAML server messages and runtime events forwarded by the SAML Enforcer plugin. GenoType's Secure Audit server outputs all Select Access component messages to their Oracle database.

Available SAML-specific audit policies

Like other audit policies configured with the Secure Audit server, a SAML-specific **Audit Policy** consists of a component and an event level

pairing. Table 8 summarizes the possible component/event level pairings you can have.

Table 8: Audit policy combinations for “from” SAML servers

Set these SAML components...	With any of these event levels...
SAML Out: records events and messages that relate to outgoing transfers of users from your saml_out script.	INFO: monitors transactions in the component.
SAML Responder: records other events and messages logged by your SAML server.	WARNING: records warnings that occur in the component.
SAML Action: a multipurpose channel for recording messages logged by other subcomponent(s) of the SAML server.	ERROR: records all exceptions that occur in the component.
	FATAL: records all fatal exceptions that occur in the component.
	<p>DEBUG: Only use this option when testing SAML deployments or at the request of the HP OpenView Select Access Support team.</p> <p>Note: When you no longer need this event level, remove it. Otherwise, your log files become filled very quickly.</p>

To add SAML audit policies to the Secure Audit server’s configuration

1. As the administrator for GenoType, launch the Setup Tool and click **Next** until the setup wizard for the Secure Audit server appears.
2. Click **Next** in the setup wizard for the server until the **Audit Settings** setup screen appears.
3. To record SAML messages, add a new audit entry by clicking the **Add** button.
4. In the **Audit Entry** dialog, configure the details of this new entry. Do this by:
 - a. Clicking the **Audit Trail** tab and choosing **Database** as the output destination for SAML messages. For details on how to set up a JDBC-compliant database, see *To configure a database* in the *HP OpenView Select Access v5.2 Installation Guide*.

- b. Clicking the **Audit Policy** tab and configuring the following combinations:

Table 9: GenoType's SAML audit policy combinations

To record this data...	Set this component...	With this level...
The GenoType employees transferred to E*nsure's Select Access SAML server.	SAML Out	INFO
SAML-specific data (for example, assertion artifacts, namespaces, and so on) associated with the outbound user transfer.	SAML Responder	ERROR
SAML-specific transactions or events (for example, whether a connection was successful or not).	SAML Action	ERROR

5. Click **OK** to commit these changes and click **Next** until you exit the Setup Tool.

Preparing Web servers and Web content for SAML-enablement

Like other organizations that SAML-enable their Web site, GenoType assess their intranet site and determine what they need to do to transfer users to E*nsure. After reviewing the HR site's architecture, they conclude that they need to:

1. Delete all content files that used to appear on the HR site – except the *Employee Health Benefits and Corporate Pension Plan* HTML landing page (`landing_ins_benefits.html`).
2. Create a new folder on the Sun ONE Web server's host computer called "SAML transfers." That way, if GenoType decides to partner with other SAML partners in the future, the server can store all SAML-specific content together for easy reference.
3. Copy the landing page to this new folder. They modify the landing page to redirect users to E*nsure's SAML server by using a specific SAML-encoded hyperlink with very specific redirect syntax. For details on this syntax, see *Understanding SAML's redirect syntax*.
4. Ensure that `title` and `employeeNumber` environment variables that you defined in step 4c in *To enable SAML-based personalization on*

page 31 match the personalization attribute names used in user entries on E*nsure’s directory server.



GenoType’s environment variable names must match E*nsure’s user attribute names on their directory server. When they match, E*nsure’s SAML server can create the user entry on their directory server exactly as the information was transferred—provided that the values in them are also valid.

Understanding SAML’s redirect syntax

When a GenoType employee clicks on the landing page with the SAML transfer link, the SAML server becomes initiated and generates the redirect syntax for that link. However GenoType must first decode the redirect syntax in the transfer link. For example:

```
https://saml.genotype.com:9985/saml_out/
to-ensure.com?TARGET=http://extranet.ensure.com:81/
MyPages.asp
```

The transfer link is broken down into the following elements, as described by Table 10.

Table 10: Elements of the outbound SAML transfer link

This SAML-encoded link element...	Does this...
https://saml.genotype.com:9985/saml_out/	Identifies the location of GenoType’s SAML server, and names the script (saml_out) that it needs to initiate the conversation with E*nsure’s SAML server.
to-ensure.com	Is the URL alias used to keep E*nsure’s real SAML URL from being exposed, thereby minimizing the risk of unauthorized access to their SAML server. The SAML server substitutes the alias with the actual URL (both of which GenoType will configure with the Setup Tool). Note: For details on how to configure the real URL, see <i>Configuring the Select Access SAML server for outbound user transfers</i> on page 14.
?TARGET=http://extranet.ensure.com:81/MyPages.asp	Is the actual user destination on E*nsure’s Web server – in this case, E*nsure’s home page for GenoType employees.



Redirect links are mapped to the alias and the URL that you define when you configure your SAML server. When you write or in some cases, rewrite the URL(s) on your site, think of the redirect syntax like this:

```
https://www.mycompany.com:<port>/saml_out/  
<URL alias>?TARGET=<USER_DESTINATION>
```

Deploying an inbound SAML server

This chapter discusses how to set up a Select Access SAML server on a network with other Select Access components. It uses the scenario introduced in *What is a typical deployment scenario?* on page 6. Please read this scenario before continuing.



If you are configuring your own inbound SAML server, you can follow the examples discussed in this chapter. For each step where we use a E*nsure value to illustrate the scenario described at the outset of this guide, simply substitute your own value.

Table 11 summarizes what high-level steps E*nsure needs to perform to ensure their Select Access SAML server runs smoothly with GenoType's SAML server equivalent. These instructions assume you are the E*nsure administrator.

Table 11: "To partner" setup overview

Step...	For details, see...
1. Install the correct combination of Select Access components.	<i>Select Access components for a SAML-enabled network on page 38</i>
2. Create SAML-specific folders in the Policy Builder so you can set the SAML server up smoothly.	<i>Adding SAML-specific folders to the Policy Matrix on page 39</i>
3. Set up the Select Access SAML server.	<i>Configuring the Select Access SAML server as a "to partner" server on page 40</i>
4. Set the corresponding policies in the Policy Builder for the SAML resources required for inbound transfers.	<i>Setting SAML-specific policy on page 48</i>

Table 11: “To partner” setup overview (Continued)

Step...	For details, see...
5. Activate personalization attributes, so Select Access can process those received by the SAML server.	<i>Activating attributes for personalization on page 50</i>
6. Set up roles as needed.	<i>Taking advantage of roles with SAML on page 52</i>
7. Ensure the server captures the correct SAML messages.	<i>Configuring the Secure Audit server to record SAML events on page 55</i>

Once Ensure have successfully configured their SAML server, users are dynamically created according to the SAML specification document. For details on this process, see *Successful user transfers* on page 64.

Select Access components for a SAML-enabled network

As an organization that accepts inbound user transfers, the first step in SAML-enabling a network is to first assess what Select Access component combinations Ensure needs for this type of deployment.

Ensure ascertains that, at minimum for a company their size, they need to install and configure the following Select Access components:

- One SAML server to accept authenticated employees from GenoType’s SAML server, as well as to make content decisions with any additional personalization information sent with the user data. They install the SAML server on the same host machine as the Apache Web server that serves extranet content. For details, see *To configure a “to partner” SAML server* on page 41.



Ensure installs their SAML server on their De-Militarized Zone (DMZ) network so that GenoType can contact it.



The actual URL to the `saml_in` script component of their inbound SAML server always uses this syntax:

```
HTTPS://<hostname>.<domain>:<port>/saml_in
```

When GenoType configures the **Actual URL** parameter in the **Setup SAML Destination Partner** setup screen, they enter this value:

```
HTTPS://saml.ensure.com:9985/saml_in.
```

- Two Policy Validators for load balancing and high availability, which ensures faster throughput of users.

- Four Enforcer plugins:
 - Three to enforce access decisions on all Web servers (Internet, non-SAML extranet, and intranet). E*nsure actively installs these Enforcer plugins with the InstallAnywhere wizard.
 - One to Select Access-protect the SAML server specifically. The Setup Tool automatically installs this Enforcer plugin when E*nsure configures their SAML server. For details, see *To configure a “to partner” SAML server* on page 41.
- One Administration server to manage and coordinate Select Access components.
- One Secure Audit server to monitor Select Access components as well as record SAML transactions.

Adding SAML-specific folders to the Policy Matrix

E*nsure adds folders to the Policy Matrix before setting up their SAML server. This preliminary step avoids an interruption in the setup process.

The impact on the SAML server setup

E*nsure needs to create two folders on the Users Tree:

- One to hold all users transferred from their SAML partners (GenoType is only the first of others).



A single SAML user location makes relationship maintenance easier: as the number of partnerships increase, the entries for them are centrally located.

- One for GenoType’s employees.

Table 12 summarizes how E*nsure modifies their Policy Matrix. This table describes the high-level steps as well as provides more granular

detail on how they accomplished that step. This table assumes that you are the E*nsure administrator.

Table 12: Adding SAML-specific folders for in-bound user transfers

Setup task...	Instructions to accomplish...
<p>Step 1: E*nsure adds a new folder below the Known Users branch called “SAML transfers.” This folder location holds all current and future partner-specific folders. They create these partner-specific folders by configuring their SAML server.</p> <p>For additional details on how to create a new folder, see Chapter 5, <i>Organizing users and resources</i>, of the <i>HP OpenView Select Access v5.2 Policy Builder Guide</i>.</p>	<ol style="list-style-type: none"> In the Policy Builder, right-click the Known Users branch on the Users Tree and then click New>Folder. In the New Folder dialog, configure the following folder properties: <ul style="list-style-type: none"> Folder Name=SAML transfers Description=This folder holds all subfolders of SAML partner user transfers. <p>Note: The Folder Name value becomes the RDN of the entry. It is the name that appears on the Users Tree.</p> Click OK to commit these changes to the E*nsure directory server.
<p>Step 2: To allow E*nsure to set access policies against GenoType’s transferred employees, they create a folder below the Known Users branch called “GenoType Employees.”</p> <p>Note: The entries in this folder are temporary entries. For details, see <i>Assertion time restrictions and how they affect user entries</i> on page 66.</p> <p>Note: If E*nsure were to partner with other organizations, they can create a new folder for each partner. That way, Select Access can easily create a new SAML authentication server for each corresponding partner. For details, see step 12 in <i>To configure a “to partner” SAML server</i>.</p>	<ol style="list-style-type: none"> In the Policy Builder, right-click the Known Users branch on the Users Tree and then click New>Folder. In the New Folder dialog, configure the following folder properties: <ul style="list-style-type: none"> Folder Name=GenoType Employees Description=This folder holds all authenticated GenoType Employees. Users in this folder have temporary LDAP entries. <p>Note: The Folder Name value becomes the RDN of the entry. It is the name that appears on the Users Tree.</p> Click OK to commit these changes to the E*nsure directory server.

Configuring the Select Access SAML server as a “to partner” server

Having installed the SAML server, E*nsure now needs to go about configuring it for their needs. Because E*nsure is only going to need the SAML server to perform inbound user transfers, they follow the wizard in the Setup Tool to configure it as a “to partner” server.

Configuring a SAML server to receive inbound user transfers involves these basic steps:

- Providing the Administration server's contact information. This is so the SAML server can register with it and can retrieve configuration details from it.
- Configuring the basic setup parameters for the host machine of the SAML server and determining the kind of SAML server it needs to be. This enables E*nsure to set up the host machine as a SAML server.
- Adding and configuring GenoType as a SAML partner, which also creates a SAML authentication server for that partner. This involves setting up:
 - GenoType's SAML properties, including their source ID, security domain, and attribute namespaces
 - GenoType's CA certificate
 - E*nsure's directory server location for GenoType users

Before beginning

Before running the Setup Tool, E*nsure consults with GenoType and:

- Synchronizes the clock settings between the two SAML server host computers.



Both the sending and receiving SAML servers must make a reasonable effort to ensure that clock settings at both sites not differ by more than a few minutes.

- Obtains a copy of GenoType's CA certificate to authenticate the SAML connection with it.
- Checks that the user attributes used are LDAP v3.0-compliant attributes and ensures that names (in this case `title` and `employeeNumber`) and values are valid on E*nsure's directory server. For example, GenoType had an attribute called `EmpType`, which they changed to `employeeType` to be compatible.

Once they have taken these steps, E*nsure can easily configure their server. For details, see *To configure a "to partner" SAML server*. These instructions assume you are the E*nsure administrator.

To configure a "to partner" SAML server

1. Run the Setup Tool as described in *To configure Select Access with the Setup Tool of the HP OpenView Select Access v5.2 Installation Guide*.
2. Click **Next** to reach the Setup Tool's **SAML server** setup screen where you click the **Configure** button.
3. On the **Contact the Administration server** setup screen, you:

- Enter the contact information for the E*nsure Administration server.
 - Click **Next**.
4. On the **ID** setup screen, enter a descriptive ID string for the E*nsure SAML server: `extranet.ensure.com:SAML server`.
 5. On the **General** setup screen, configure the general contact and functional parameters for the E*nsure SAML server as shown in Table 13.

Table 13: GenoType’s General SAML server configuration values

For this parameter...	Enter this value...
Host	<code>saml.ensure.com</code>
SSL Port	<p>9985, which is Select Access’s default value</p> <p>The SAML server runs on two ports:</p> <ul style="list-style-type: none"> • The default port value you enter. This port is used for all communications that occur after the partner is authenticated. • The default port minus 1 (in this example, 9984). This port is used for authentication only. <p>Both port numbers become part of the SAML server’s service entry properties that are automatically created when you finish the server’s configuration.</p>
Select the location of the SSL certificate	<code>c:\\certs\saml.p12</code>
SSL Server Certificate Password	<code>B3astMa&ter?</code>
The server will accept users transferred from SAML single sign-on partner(s)	Box is checked.

When E*nsure completes the configuration of this screen, it appears like the one shown in Figure 7.

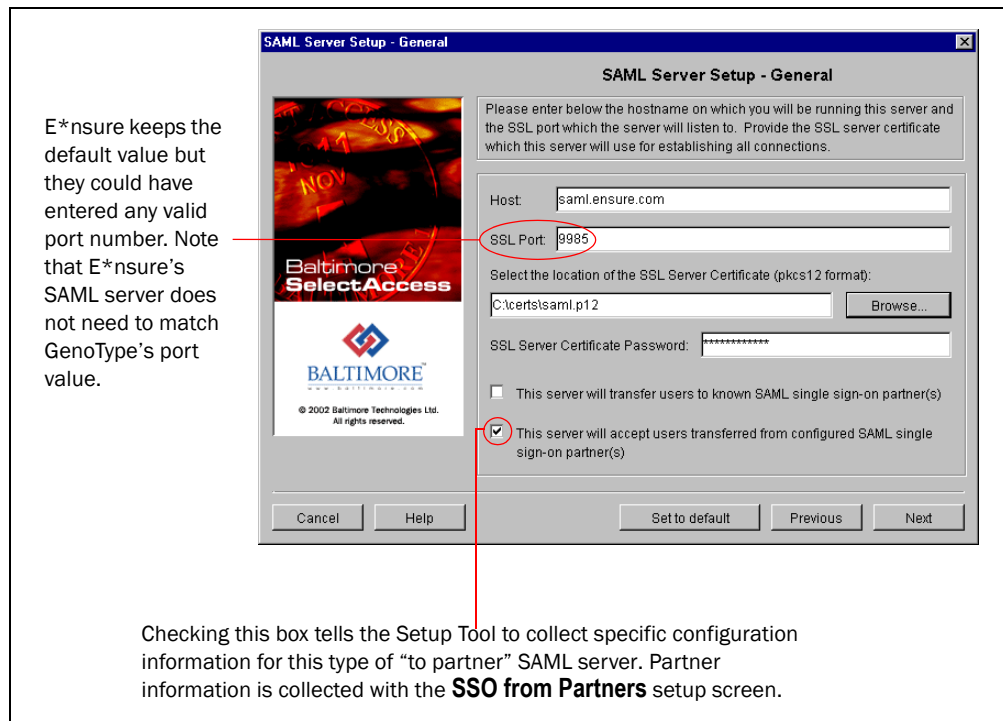


Figure 7: E*nsure's General setup screen

6. Click **Next** and the **SSO from Partners** setup screen appears.
7. After clicking **Add**, the **New SAML Authentication server** setup screen appears. Enter `GenoType_Auth` in the **Enter the name of the new SAML authentication server** field.

This screen allows you to define a single instance of an authentication server that will receive GenoType's SAML server's transfer request. Select Access dynamically adds this server's name to your list of configured authentication methods in the Policy Builder.



The information you exchange is of a sensitive nature. To avoid compromising this data with another partner, Select Access requires that you use a new authentication server for each partner. Each authentication server, therefore, only authenticates on one specific user location.

- Click **Next**, and the **SAML Partner Properties** setup screen appears displaying the **SAML Properties** tab. Configure the partner properties accordingly, as outlined in Table 14.



Fields marked with an asterisk (*) indicate properties that GenoType exported to file when they configured their Select Access SAML server and subsequently shared with E*nsure. E*nsure takes these values and pastes them in the subsequent fields. If you enter any of these values incorrectly, SAML fails. For an example of this exported file, see Figure 5 in *To configure a SAML server so it transfers users to a partner*.

Table 14: E*nsure’s SAML Partner Properties values

For this parameter...	Enter this value...
Partner Name	GenoType
Partner Source ID*	GenoType SAML server
Partner’s SAML URL*	https://saml.genotype.com:9985
Issuer*	GT Admin

When you complete the configuration of this tab for E*nsure, it appears like the one shown in Figure 8.

The Setup Tool SHA-1 hashes the ID to create a 20-byte (binary) ID. It then either base-64 encodes or hex encodes this SHA-1 hashed value and displays it as a string.

This parameter is the equivalent of the Issuer parameter defined in the SAML v1.0 protocol document. E*nsure’s server uses it to deconstruct GenoType’s SAML assertions. This string identifies the assertion as being a GenoType assertion.

Figure 8: E*nsure’s SAML Properties tab

9. In the **Security Domains** tab, enter `genotype.com` as the security domain for the authentication server you are configuring.



Typically, a security domain is the same as the domain of the Web site that authenticated and transferred the user. Therefore, most partners only send you one. However, depending on their SAML deployment, they can forward more to you.

10. In the **Attribute Namespaces** tab, enter the name of the attribute namespace `GenoType` defined when they configured their SAML server (that is, `GenoType_Employee`).

This namespace prepends the attributes that `GenoType` sends with the users it transfers (that is, either `title` or `employeeNumber`). For example, when `GenoType`'s server transfers John Smith, his attributes appear as follows:

```
GenoType_Employee:employeeNumber, JSmith_EX_123456  
GenoType_Employee:title, VP Biogenetic Research
```



While the SAML v1.0 protocol document allows multiple attribute namespaces, HP has simplified the SAML specification by allowing only one per outbound SAML server. Consequently, E*nsure will only configure one for `GenoType`. However, if they add other partners who are using SAML implementation from different vendors, they must then configure all attribute namespaces for non-Select Access partners.

11. In the **CA Certificate** tab, E*nsure pastes `GenoType`'s CA certificate in the window provided. In order to validate the identity of `GenoType`'s server, E*nsure's SAML server checks the signature on `GenoType`'s server's client certificate against the signature in this CA certificate.
12. In the **Directory Server** tab, E*nsure configures the partner properties accordingly, as outlined in Table 15.

The SAML authentication server uses the information in this tab to name the data location to which the Select Access temporarily adds transferred users. The location can either be:

- A folder – as the number of partners increase, you can add parallel folders to the directory server.
- A user data location – where you create a separate directory server branch, either on the same or different directory server. For details on how to create a new user location, see Chapter 4,

Building your Users and Resources Trees, in the HP OpenView Select Access v5.2 Policy Builder Guide.



If are configuring a folder that requires you to browse to a folder that contains a large number of entries that exceed the Tree threshold you have set, the **Quick Search** dialog box appears. For details, see *To perform a quick search* on page 68. For details on how to change the Tree threshold, see *To set Tree thresholds* on page 74.

The SAML authentication server only authenticates users in this user location. This is why Select Access requires that you to create a new user location for each new partner a company has.



Once the SAML authentication server authenticates the user, the Policy Validator can create a cookie for that individual.



If are configuring an user location that requires you to browse to a folder that contains a large number of entries that exceed the Tree threshold you have set, the **Quick Search** dialog box appears. For details, see *To perform a quick search* on page 68. For details on how to change the Tree threshold, see *To set Tree thresholds* on page 74.

Table 15: E*nsure's Directory Server values

For this parameter...	Enter this value...
Specify location to store all user information received from this partner	o=ensure.com, ou=GenoType Employees
Delete SAML users after	1440 minutes (approximately 1 day)

When E*nsure completes the configuration of this tab, it appears like the one shown in Figure 9.

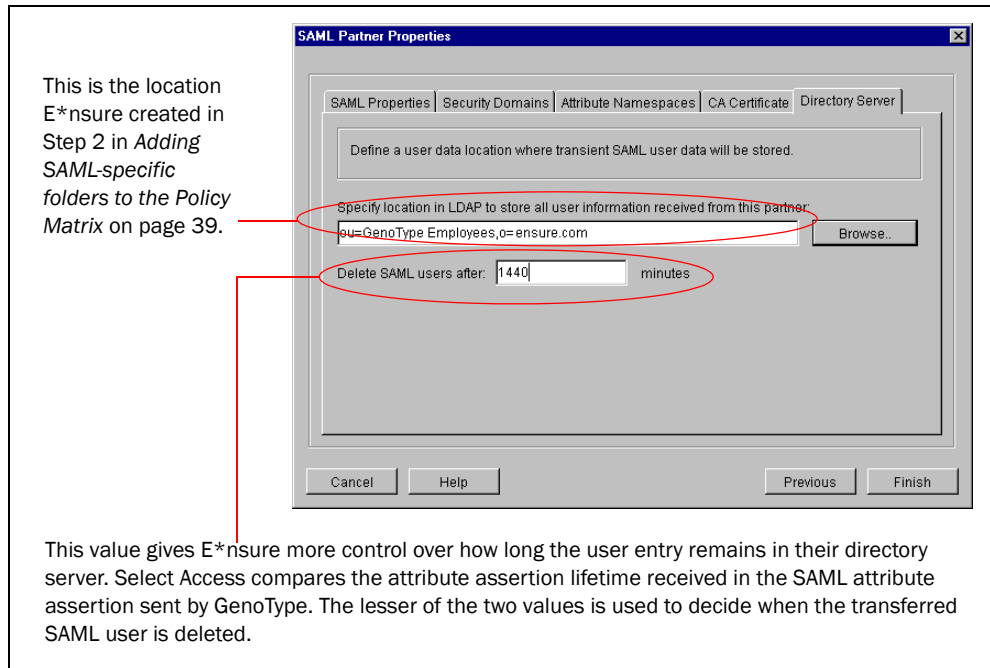


Figure 9: E*nsure's Directory Server tab

13. To proceed to the next configuration step, click:
 - **Finish** on the **SAML Partner Properties** setup screen. This creates the SAML authentication server and makes it available in the Policy Builder.
 - **Next** on the **SSO from Partners** setup screen.
14. Configure the SAML Enforcer plugin with the subsequent screens. These screens are the same screens that appear in the Enforcer plugin's setup wizard. Unlike the GenoType administrator, as the E*nsure administrator, you:
 - Choose the **Custom** configuration option on the SAML Enforcer plugin's **General** setup screen.
 - Configure the **Single DNS domain SSO** setup screen by entering `genotype.com` as the **Cookie Domain**. This value must match the local domain on which the partner's SAML server and Apache Web server are present.
 - Creates a new audit entry with the **Audit Settings** setup screen. This entry consists of an **Audit Trail** using their Secure Audit server as the output destination and an **Audit Policy** that includes the following **Component/Level** combinations: SAML In/INFO, SAML Responder/ERROR, SAML Action/ERROR. For more

information on audit policies, see *Available SAML-specific audit policies* on page 56.



Because GenoType configured audit policies to the lowest level, the SAML server records and forwards all messages of all severities to the Secure Audit server.

15. On the last Enforcer plugin setup screen, click **Next**. The **Finish** setup screen appears informing you that you have completed all setup tasks for the SAML server and its Enforcer plugin.



You can modify the SAML server and the SAML Enforcer plugin's configuration with the Component Configuration tool, which is available from the Policy Builder. Note that for the SAML server, changes only take effect after you or the Setup Tool has restarted the server.

For details, see Chapter 15, *Modifying components' central configuration parameters*, in the *HP OpenView Select Access v5.2 Policy Builder Guide*.

16. Click the **Start now** box, before clicking **Finish** to commit your configuration to the Policy Store. The Setup Tool creates the following entries on the Resources Tree:
 - An HTTPS service entry for the SAML server. By default, this entry appears in the following location:


```
ou=Network, nxResource=https, nxResource=
<hostname>:SAML Server
```
 - A `saml_in` resource entry below the SAML server service entries. `saml_in` is the script that receives and processes GenoType's authenticated employees, which GenoType's SAML server transfers.

Setting SAML-specific policy

Once you have configured the E*nsure SAML server, you need to set up their Policy Builder so it can handle inbound SAML transfers. Inbound SAML transfers require that they configure the following:

- *Authentication*: Configure and choose just what method of authentication SelectID is to use for SAML.
- *Authorization*: Configure which users transferred from the SAML partner can access SAML server components – as well as other local (non-SAML) resources.

Configuring SAML authentication and authorization policy

Configuring authentication and authorization for E*nsure's newly configured SAML server requires that you manually add the components of this service along the Resources Tree axis. This allows E*nsure to set up authentication and authorization accordingly.

Table 16 summarizes how E*nsure sets up SelectID. This table describes the high-level steps as well as provides more granular detail on how to accomplish that step.



This procedure assumes that E*nsure has already added their Apache Web server as a service (that is, extranet.ensure.com on port 81).

Table 16: E*nsure's authentication methods and access policies

Setup task...	Instructions to accomplish...
<p>Step 1: E*nsure adds all specific GenoType resources under the service branch for their Apache Web server, including the landing page (<code>MyPages.cgi</code>).</p>	<p>Re-scan the E*nsure Apache server for any changes to the resources below this service. For details on how to scan for resources, see <i>Automatically generating a list with a discovery plugin</i> in Chapter 4, <i>Building your Users and Resources Trees</i>, of the <i>HP OpenView Select Access v5.2 Policy Builder Guide</i>.</p>
<p>Step 2: To prevent all users from accessing any content inadvertently, E*nsure sets a deny policy at the root of both the Users Tree and Resources Tree. Now, only explicitly set allow or conditional policies determine access.</p>	<ol style="list-style-type: none"> 1. Scan the Policy Matrix to see where E*nsure's Known Users branch and the Network branch intersect. 2. Set a deny policy. All users automatically inherit this policy, and it secures resources until an allow policy or conditional policy overrides resource/user pairings in the grid.

Table 16: E*nsure’s authentication methods and access policies (Continued)

Setup task...	Instructions to accomplish...
<p>Step 3: E*nsure sets the access policies for all users that their SAML server receives from GenoType’s SAML server.</p> <p>Note: They will also need to set corresponding access policies for non-personalized content. To help them with this, E*nsure decides to implement roles. For details, see <i>Taking advantage of roles with SAML</i> on page 52.</p>	<ol style="list-style-type: none"> 1. Scan the Policy Matrix to see where E*nsure’s users folder for GenoType (“GenoType Employees”) and the saml_in resource intersect. 2. Set an allow policy. This policy automatically overrides the top-level deny. All users in this folder automatically inherit this policy: Users need access to reach this page before being able to proceed to their personalized content, as well as nonuser specific/communication type of content.
<p>Step 4: Enable SelectID against the saml_in resource and the landing page (MyPages.cgi).</p> <p>Note: If E*nsure adds new partners in the future, they need to configure SelectID so that they use a SAML authentication servers (that is, one unique server for each partner) with saml_in resource. Conversely, for any partner-specific resource (like the landing page), E*nsure needs to configure SelectID so that it only uses the partner-specific authentication server.</p>	<p>For the saml_in resource, E*nsure enables SelectID. You do this by:</p> <ol style="list-style-type: none"> 1. Right-clicking the cells where the SelectID column and the saml_in and MyPages.cgi resources intersect and selecting Enable SelectID. 2. In the Authentication Method dialog, selecting the authentication server created for GenoType (that is, GenoType_Auth). This authentication server was created when E*nsure set up their SAML server.

Activating attributes for personalization

Attributes determine how the Web server is to deploy personalized resources. The Policy Validator evaluates which network resource to display, depending on the attributes E*nsure receives from GenoType.

How it works

The partner whose SAML server is sending outbound user transfers activates the same user attributes agreed upon early on in the deployment cycle. Additionally they also activate attributes and configure personalization so that they encode the correct attributes as environment variables that the Web server can interpret. These instructions assume you are the E*nsure administrator.

To activate attributes

1. In the Policy Builder, click **Tools>Activate Directory Attributes**.
2. In the **Activate Directory Attributes** dialog, activate all the attributes E*nsure require. Do this by:

- a. Selecting one or more attributes in the **Available Attributes** list. Of the available attributes used for SAML-based personalization, activates the `title` and `employeeNumber` attributes only, since these are the ones that E*nsure plan to receive from GenoType.
- b. Clicking the **Add** button to move them into the **Activated Attributes** list.



The Policy Builder reads available attributes from E*nsure's directory server schema.



If E*nsure had created a conditional rule with an attribute logic point that uses an attribute that is unavailable for their directory server, the attribute logic decision point always denies access to all users.

Because two Select Access SAML server exchange attributes, E*nsure can only enable the supported attributes for Select Access implementation (see Table 17). Their SAML server automatically discards unsupported attributes.

3. Since the `employeeNumber` attribute is the most important personalization attribute, reorder the priority of the activated attributes. Do this by:
 - a. Selecting the `employeeNumber` attribute.
 - b. Using the up arrow to shift the position of it relative to the `title` attribute.
4. To commit these attributes, click the **OK** button.

Table 17: Supported SAML personalization attributes

Available attributes by name (listed alphabetically)			
audio	businessCategory	carLicense	cn
departmentNumber	description	destinationIndicator	displayName
employeeNumber	employeeType	facsimileTelephoneNumber	givenName
homePhone	homePostalAddress	initials	internationaliSDNNumber
jpegPhoto	l	labeledURI	mail
manager	mobile	o	ou
pager	photo	physicalDeliveryOfficeName	postalAddress
postalCode	postOfficeBox	preferredDeliveryMethod	preferredLanguage

Table 17: Supported SAML personalization attributes (Continued)

Available attributes by name (listed alphabetically)			
registeredAddress	roomNumber	secretary	seeAlso
sn	st	street	telephoneNumber
teletexTerminal Identifier	telexNumber	title	uid
userCertificate	userPassword	userPKCS12	userSMIME Certificate
x121Address	x500unique Identifier		

Taking advantage of roles with SAML

To maximize the power of SAML, E*nsure decides to create roles that categorize users within a specific category based on the attributes they receive from GenoType’s assertion. Select Access determines membership by user or group attributes defined via a search expression. Depending on how Select Access evaluates the expression, assignment is dynamic. Therefore, E*nsure cannot manually add a user to or delete a user from a role.



Roles are intrinsic to a user location. This means that users must be in the same user location in which you have created the role.

Creating roles and setting policy dynamically

Roles facilitate the way you control access to content and resources, and vary based on your business requirements. This allows E*nsure’s administrators to set access quickly and easily.



While all members of a role inherit the access policies created for the role, you can override the access policy for a specific role member if necessary.

Table 18 summarizes how E*nsure sets up roles and applies access rules accordingly. This table describes the high-level steps as well as provides more granular detail on how they accomplished that step.

Table 18: E*nsure’s dynamic role creation

Setup task...	Instructions to accomplish...
<p>Step 1: Based on preliminary meetings with GenoType, E*nsure determines they need the roles listed below. Because GenoType prepends employee numbers with a designation that corresponds to one of these roles, E*nsure can easily create the required search expression that sorts users into one of these roles.</p> <ul style="list-style-type: none"> • An executive role whose users have restricted access to forums and/or documents that describe possible changes to employee benefits. • A management role whose users have restricted access to memo and/communi-ques that explain benefit changes and how to communicate them to teams. • An employee role whose users have unre-stricted access to newsletters, memos, and so on. <p>For details on how to create a role, see Chapter 5, <i>Organizing users and resources</i>, of the <i>HP OpenView Select Access v5.2 Policy Builder Guide</i>.</p>	<ol style="list-style-type: none"> 1. Right-click the GenoType Employees folder and then click New>Role. 2. In the New Role dialog, configure the fol-lowing field combinations for each role: <ul style="list-style-type: none"> – Role Name = Executive OR Manager OR Employee – Search In = ou=GenoType Employees, ou=SAML transfers, o=Ensure.com – Include All Subfolders = unchecked (disabled) – Search expression (for Executive) = employeeNumber~=EXC* Search expression (for Manager) = employeeNumber~=MNG* Search expression (for Employee) = employeeNumber~=STF*

Table 18: E*nsure’s dynamic role creation (Continued)

Setup task...	Instructions to accomplish...
<p>Step 2: With these roles, E*nsure can quickly set policies for nonuser specific content – rather than needing to explicitly set one for each user. Note that they organize documents into three areas of GenoType’s site on E*nsure’s Apache Web server:</p> <ul style="list-style-type: none"> • Strategy and planning tools • Management and implementation tools • What’s new for GenoType 	<ol style="list-style-type: none"> 1. Against the folders holding resources previously described, keep the inherited deny policy for users in the GenoType Employees folder. 2. Where the Executive role and the folder for Strategy and planning tools intersect, set an allow policy. Only users in this role have access to these resources – even though the Policy Validator typically denies access to the user’s real user entry. The inherited allow overrides the deny in this case. 3. Where the Management role and the folder for Management and implementation tools intersect, set an allow policy. Only users in this role have access to these resources – even though the Policy Validator typically denies access to the user’s real user entry. The inherited allow overrides the deny in this case. 4. Where the Employee role and the folder for What’s new content intersect, set an allow policy. Only users in this role have access to these resources – even though the Policy Validator typically denies access to the user’s specific user entry. The inherited allow overrides the deny in this case.

What E*nsure’s configured Policy Matrix looks like

When you have successfully configured E*nsure’s Policy Matrix, you see:

- An empty GenoType Employees folder, which the SAML server will eventually populate with transferred users (For details, see Chapter 5, *Putting SAML deployment to the test.*)
- A roles folder populated with three roles: Executive, Management, and Employee
- SAML-specific resources
- User-specific/personalized resources
- Non-personalized resources

- A variety of explicitly set allow and deny policies, as well as inherited ones
- A variety of explicitly set authentication/SelectID policies, as well as inherited ones

Figure 10 summarizes all of these changes.

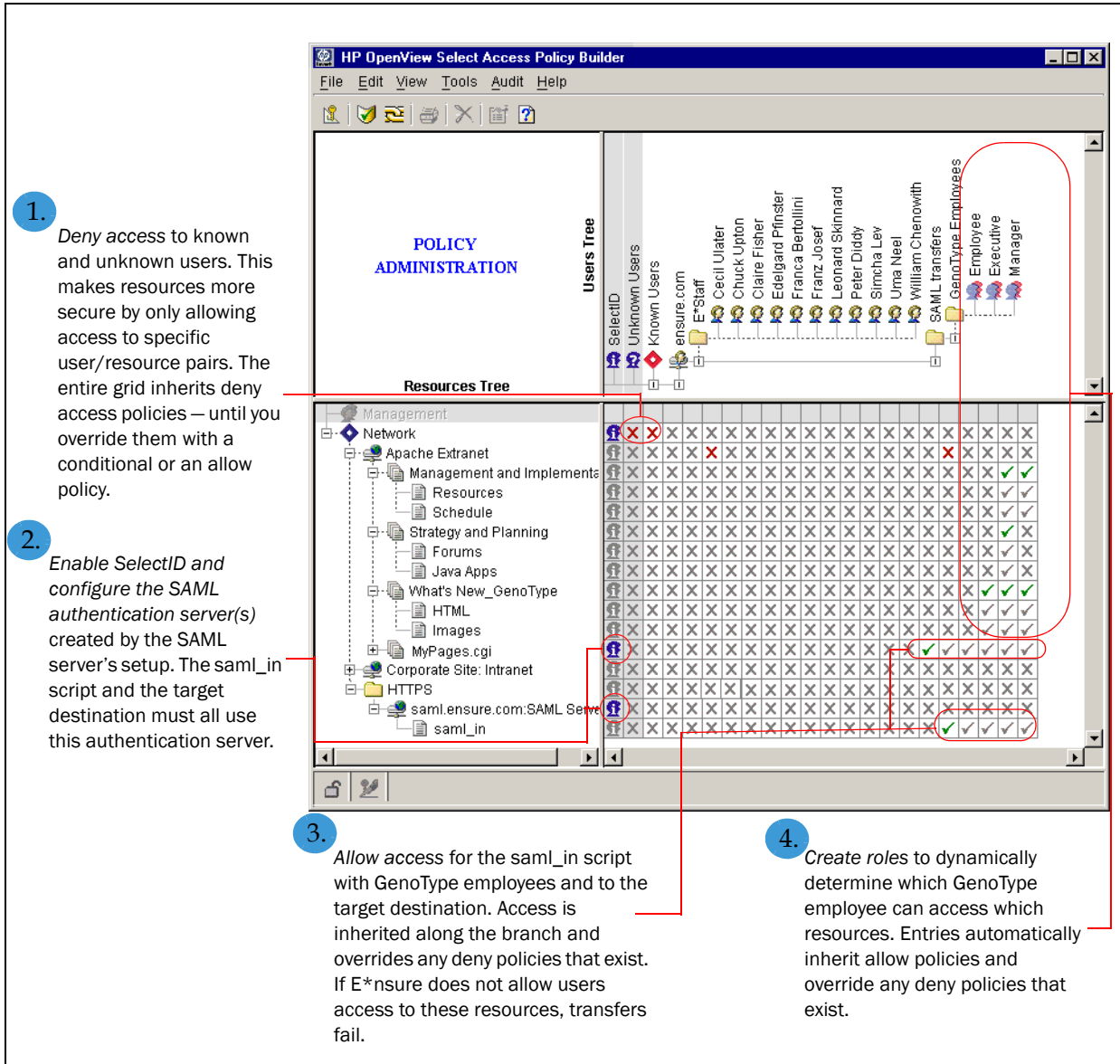


Figure 10: E*nsure's SAML-enabled Policy Matrix

Configuring the Secure Audit server to record SAML events

To monitor SAML transactions with GenoType, E*nsure reconfigures their Secure Audit server to specifically track SAML server messages and runtime events forwarded by the SAML Enforcer plugin.

E*nsure’s Secure Audit server outputs all Select Access component messages to their Oracle database.

Available SAML-specific audit policies

Like other audit policies configured with the Secure Audit server, a SAML-specific audit policy consists of a component and an event level pairing. Table 19 summarizes the possible component/event level pairings you can have. These instructions assume you are the E*nsure administrator.

Table 19: Audit policy combinations for “to” SAML servers

Set these SAML components...	With any of these event levels...
SAML In: records events and messages that relate to incoming transfers of users from GenosType’s <code>saml_in</code> script.	INFO: Monitors transactions in the component.
SAML Action: a multipurpose channel for recording messages logged by other subcomponent(s) of the SAML server.	WARNING: Records warnings that occur in the component.
	ERROR: Records all exceptions that occur in the component.
	FATAL: Records all fatal exceptions that occur in the component.
	<p>DEBUG: Only use this option when testing SAML deployments or at the request of HP OpenView Select Access Support team.</p> <p>Note: When you no longer need this event level, remove it. Otherwise, your log files are filled very quickly.</p>

To add SAML audit policies to the Secure Audit server’s configuration

1. Launch the Setup Tool and clicks **Next** until the setup wizard for the Secure Audit server appears.
2. Click **Next** in the setup wizard for the server until the **Audit Settings** setup screen appears.
3. To record SAML messages, add a new audit entry by clicking the **Add** button.

4. In the **Audit Entry** dialog, configure the details of this new entry. You do this by:
 - a. Clicking the **Audit Trail** tab and choosing **Database** as the output destination for SAML messages. For details on how to set up a JDBC compliant database, see *To configure a database* in the *HP OpenView Select Access v5.2 Installation Guide*.
 - b. Clicking the **Audit Policy** tab and configuring the combinations listed in Table 20.

Table 20: E*nsure's SAML audit policy combinations

To record this data...	Set this component...	With this level...
The GenoType employees transferred to E*nsure's Select Access SAML server	SAML In	INFO
SAML-specific transactions or events (for example, whether or not a connection was successful)	SAML Action	ERROR

5. Click **OK** to commit these changes and click **Next** until they exit the Setup Tool.

Putting SAML deployment to the test

Now that both parties have configured their SAML partnership information, the SAML system is ready to pass users and their necessary attributes. The final step in any SAML server deployment is to:

- Test user transfers and study the results of the exchange to determine if:
 - Data is being transferred correctly.
 - The needs of both organizations are being met. For details, see *Testing user transfers* on page 59.
- Tweak one or both SAML servers' configuration as needed. For details, see *Changing the SAML server's configuration* on page 66.

Testing user transfers

Before partnering organizations launch a full-scale deployment, HP recommends that you test your data exchanges and ensure that both Select Access SAML servers are communicating correctly.

What can typically go wrong

If either partner misconfigures their SAML servers, SAML transfers fail. Typical deployment errors include:

- Partners misenter values that they must synchronize. Check for inconsistencies in capitalization or spaces.
- SSL connections have failed. Check Select Access components to see that you have configured them correctly.
- Partners have not synchronized clocks between the two SAML server host, causing attribute assertions to timeout.
- If the inbound SAML server uses an Oracle directory server, ensure that you index `nxAccountDeleteTime` and `nxAccountAuthenticationMethod`. Run `catalog.sh` to correct this problem. For details, see *Cataloging attributes on Oracle* on page 13.

- Partners have not accounted for all roles or for or partners have not set up the attribute/environment variables to filter users correctly.
- Policies and/or authentication methods are not correctly configured, and the behavior is not what they are expecting.

To create a test user exchange

1. The outbound SAML server – in this case, GenoType – adds a fictional user:
 - a. On the branch of the user location branch that reads and writes employee data to the Oracle directory server, create the following folder: o=TestSAML, o=GenoType.com.
 - b. Right-click this new folder and choose **New>User**.
 - c. In the **New User** dialog, enter the properties described in Table 21.

Table 21: GenoType’s New User configuration values

For this parameter...	They enter this value...
First Name	Persona
Last Name	Non-Grata
Common Name	Persona Non-Grata
User ID	PNon-Grata
Password, Confirm Password	Test@123!
Employee Number	RD-001-12333
Title	Lead Researcher-Genetic Diseases

GenoType uses this user entry to test SAML transfers between the two SAML servers. For details on what the process for this transfer is, see *What happens when the user clicks the redirect link?* on page 61.

2. As the E*nsure administrator, create a mock set of Employee benefits and transactions. This allows E*nsure’s Web server to create a personalized page based on the attributes transferred with this mock user entry.
3. As the GenoType administrator, assume this identity and:
 - a. Log into the GenoType intranet site, and authenticates via the usual authentication server (that is, one of SecurID, RADIUS, registration, password, or certificate).
 - b. Browse to the *Employee Benefits* landing page.
 - c. Click the SAML link.

This transfers the administrator to E*nsure's site. Based on the `employeeNumber` (and `title`), the corresponding personalized page appears.

4. E*nsure monitors their Secure Audit server and corresponding directory server. Check to see that:
 - The inbound user transfer was handled correctly.
 - A temporary user entry was created successfully on the Oracle directory server.
 - Select Access has added the user to the corresponding role based on which characters prepend the `employeeNumber` attribute (that is, one of EXC, MGR, or STF).
 - The user entry has the correct attribute values stored with the entry on the directory server.
 - After the correct amount of time as specified in the SAML authentication server's configuration (that is, 24 hours), they see that Select Access has eventually deleted the user entry from the directory server. This requires that the Policy Validator re-authenticate the user by GenoType's Select Access-protected system.
5. GenoType, like E*nsure, also checks that they have configured their Secure Audit server logs to collect events and messages at the DEBUG level. They review logs closely to see that the outbound transfer was handled correctly.

If all things seem to be behaving as required by the two partners, both organizations can begin to roll out a full scale deployment of SAML. If any difficulties arise, both partners change elements of their deployment as needed. For details, see *Changing the SAML server's configuration* on page 66 below.

Successful SAML server communication

When the administrator pretending to be the test user clicks the redirect link, it initiates a series of events described by the following procedure.

What happens when the user clicks the redirect link?

1. The user is sent to `saml.genotype.com:9985`, which is GenoType's SAML server. In this case, GenoType is using the Select Access default port.
2. GenoType's SAML server constructs a Validator query with the information the server extracts from the HTTP redirect request.
3. GenoType's SAML server sends a query to the Policy Validator to:
 - Check the policy for the user for the `saml_out` resource.
 - Validate the user's cookie, so the Policy Validator can transfer it with the user.

4. With Policy Validator returning an allow, GenoType's SAML server extracts the following information from the response:
 - The DN of the authenticated user
 - The authentication method used
 - The user's login time
 - Any personalization attributes that were configured (in this case there are two: `title` and `employeeNumber`)
5. With the information extracted, GenoType's SAML server looks up the URL mapped to the alias, as well as checks all other partner information. GenoType's server uses this information to parse the remaining elements in the link to determine the complete URL on E*nsure's Web server:
 - a. The SAML server finds the URL alias, which GenoType encoded as being `to-ensure.com`.
 - b. The server looks up the correct, complete SAML URL from the configuration information it has stored locally. When GenoType configured the URL alias, they defined the actual SAML URL value as:


```
https://saml.ensure.com:9985/saml_in
```
6. GenoType's SAML server generates a random number. GenoType's server uses this number to:
 - Map the partner information.
 - Create an artifact, by combining with its **Source ID**.
7. With the artifact created, GenoTypes's SAML server can construct the complete redirect URL to E*nsure's site and redirect the user to E*nsure:


```
https://saml.ensure.com:9985/saml_in?saml_out=<random number>&TARGET=http://extranet.ensure.com/mypages.cgi
```
8. When E*nsure's SAML server gets the redirect request, it:
 - a. Extracts the artifact GenoType's server created in step 6.
 - b. Breaks up the artifact to obtain GenoType's contact information so it can contact GenoType's SAML server with future information requests (such as requesting the user's attributes):


```
https://saml.genotype.com:9985/saml_responder)
```
9. E*nsure's SAML server constructs its own artifact request and posts to this URL.
10. Both servers negotiate an SSL connection by exchanging certificates to prove their respective identities before continuing.
11. With the SSL connection opened, GenoType's SAML server receives the post and constructs another Policy Validator query using the original HTTP redirect request, so that the Policy Validator can authenticate E*nsure's SAML server and so that it

can check its access policy. Consequently, the new query contains E*nsure's server certificate.

12. Only if the Policy Validator reply is an allow, will GenoType's server check the DN to determine which partner is asking for information (currently, there is only one).
13. E*nsure's SAML server sends an artifact request.
14. When GenoType's SAML server receives the artifact, it:
 - a. Breaks up the artifact.
 - b. Extracts the random number generated for that server.
 - c. Looks up the corresponding user information in GenoType's directory server.
 - d. Constructs a new SAML assertion that contains the user's authentication and attribute information. For details on assertions, see *The things they need to agree upon* on page 7.
15. When E*nsure's SAML server receives this assertion it constructs a Policy Validator query from the data it contains.



If it does not find any attributes, E*nsure's SAML server sends an attribute request to specifically ask for them.

16. The SAML authentication plugin created specifically for GenoType then:
 - a. Checks the partner's name, to see if it is a recognized name.
 - b. If it is, it creates a user entry in the directory location configured for GenoType's employees, with the authentication and attribute values received in the query. For details, see *How Select Access creates user attributes* on page 65.



Between two Select Access SAML servers, all transferred SAML users have the following LDAP attributes: `nxAccountDeleteTime` describes when the Policy Validator deletes the user entry, and `nxAccountAuthenticationMethod` contains the authentication method used on the partner's system.



E*nsure's Policy Validator filters invalid/unknown attributes before adding them to the user entry. This is why both E*nsure and GenoType need to ensure important attribute names and values are valid.

17. E*nsure's Policy Validator returns an allow for the user in question when:
 - It creates the user entry successfully.
 - It determines that the policy assigned to the user target URL combination is an allow.

18. With the nonce received in the Policy Validator reply, the E*nsure SAML server sets the cookie in the user's browser, and finally redirects to the target URL (that is, `http://extranet.ensure.com/mypages.asp`).
19. The Web server receives the cookie and the policy for the user and resource combination, and gives user access to this resource – personalized for the user accordingly.

Successful user transfers

Incoming assertions contain all authentication information and attributes for the user. As the “to partner,” E*nsure's Select Access SAML server constructs a query with authentication and attribute data.

The importance of the NameIdentifier string

These incoming SAML assertions must contain a `NameIdentifier` string. This string takes the user's DN as its value, and therefore identifies the user that has authenticated on the assertion sending side, which in this case is GenoType's SAML server.



Because E*nsure's SAML server is a Select Access server, it can accept `NameIdentifier` strings that are either DN strings (where the server extracts the first RDN to create the user's DN on E*nsure's User Tree) or non-DN strings (where the server uses the string itself to create the user's DN on E*nsure's Users Tree).

Like any other Enforcer plugin, E*nsure's SAML server forwards a query to the Policy Validator. The only difference being that E*nsure's SAML query contains an element called `subject_name`, which it creates from the `NameIdentifier` string.

When Policy Validator receives the query, it attempts to identify the partner from whom the assertions were received. If it is successful, the Policy Validator creates a user entry in the user location configured for transferred users. Depending on the policy set at that location, the Policy Validator eventually returns an allow or deny access decision. In the case of GenoType's and E*nsure's partnership, the Policy Validator in this case allow access because of the policy E*nsure set for the target resource.



Directory servers do not permanently store transferred SAML user entries. For details, see *Assertion time restrictions and how they affect user entries* on page 66.

How Select Access creates user attributes

When creating the SAML user in LDAP, the Policy Validator creates the user's:

- CN with the `subject_name` value. It uses this CN to subsequently build the user's DN. If the SAML server also sends other CN attributes, the Policy Validator also adds these values.



Active Directory allows only a single CN attribute per entry. Active Directory uses `subject_name` to store the CN attribute. It then uses the CN to create the DN. The server discards any other CN attributes.

- UID with a UID attribute the SAML server sends. If the SAML server does not send a UID attribute, then the `subject_name` value becomes the UID's value. If the SAML server sends multiple UIDs, Policy Validator creates a random number and prepend it with `u_`. For example `u_123`.



Active Directory does not have UID attributes. Instead, it takes the CN and maps it to the `samlaccountname` attribute. For other directory servers, if the SAML server sends UID attribute(s), Active Directory uses the first one to store the `samlaccountname` attribute in the user entry and discards the remaining ones. If the CN on the sending side is longer than 20 characters and the SAML server does not export the UID, SAML authentication fails.



If a user entry with the same UID exists on E*nsure's directory server, the Policy Validator does not create the user entry. For additional details on how the Policy Validator creates user entries, see *Successful user transfers* on page 64.

- SN with an SN attribute that the SAML server sends. If the SAML server does not send an SN attribute, it uses the `subject_name` value as the SN value.



Active Directory allows only a single SN attribute per entry. If the SAML server sends an SN attribute, then it use the value for the user's SN attribute. Otherwise, the SAML server uses the `subject_name` attribute.

- User attributes when the SAML server sends attribute assertions. The server ignores any names or values that are invalid. It also drops SAML-specific elements to make the attributes LDAP compliant.

For a list of attributes you can use with SAML, see *Activating attributes for SAML personalization* on page 28.

Assertion time restrictions and how they affect user entries

Depending on the vendor of your partner's SAML server and their setup of that server, an attribute assertion can contain lifetime values. When the GenoType administrator configured their Select Access SAML server, she configured a value of 7 days. This lifetime controls how long a user entry remains in E*nsure's directory server. Consequently, partners must synchronize the clocks between the sending-side servers and the receiving-side servers, with no more than a two minute difference.



Because E*nsure wants to have more control over the lifetime of transferred users, they have configured a value for the **Delete SAML users after** parameter in the **Directory Server** tab of the **SAML Partner Properties** dialog. Because E*nsure's value of 1 day is the lesser of the two values, Select Access deletes GenoType's user entry from E*nsure's directory server after 1 day.

If no attribute assertion lifetime value exists, it uses the **Delete SAML users after** parameter.

Changing the SAML server's configuration

The following events require a change in a SAML server's configuration:

- The SAML server needs to send and receive users. Therefore, you need to add more configuration information.
- One or both of the SAML servers in the partnership fail the test. Therefore, the you must check the configuration to ensure you add the correct parameters.
- You are extending current relationships to include other partners. Therefore, each partner must correctly configure server information to ensure SSO transfers with them remain seamless.

There are two ways to change the SAML server's configuration:

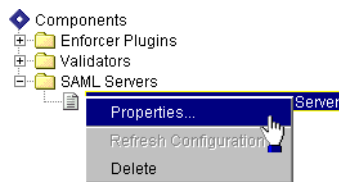
- The Setup Tool, using the SAML server setup wizard: You can modify all parameters of the SAML server you have set up, whether you have configured your server to send outbound transfers, receive inbound transfers, or both.
- The Policy Builder, using the Component Configuration wizard: You can only modify any of the centrally located parameters for a single instance of a server by editing the tabs that exist in the **Edit SAML server Settings** dialog. Centrally located parameters are those

that the Administration server stores in your Policy Store so it can more readily manage them.

i You can only change other configuration values with the Setup Tool.

Display this dialog by:

- Clicking **Tools>Component Configuration**.
- In the **HP OpenView Select Access Configuration** window, right-clicking the SAML server and then choosing **Properties** as shown below:



Index

A

- Access policies, 64
 - allow, 23, 24, 27, 49, 54, 62, 63, 64
 - deny, 27, 49, 51, 54, 64
 - inheritance, 24
 - setting for inbound SAML servers, 40, 50
 - setting for outbound SAML servers, 24
- Action, SAML, 32, 56
- Activating attributes, 23
- Administration server
 - configuring contact information for, 14, 15, 41
 - installing, 13, 39
 - managing configuration parameters, 66
- Administration, delegating. *See* Delegated Administration
- Alias, URL. *See* URL alias
- Allow policy. *See* Access policies
- Apache enforcer plugin. *See* Enforcer plugins
- Application servers, 4
- Architecture
 - SAML overview, 5
 - site, 33
- Artifacts, 62, 63
 - definition of, 8
 - how used, 62
 - sending request, 63
- Assertions
 - authentication and authorization, 8
 - configuring, 14, 17
 - deconstructing information sent, 44
 - description of, 4
 - example of, 4
 - exporting properties, 17, 44
 - lifetime of, 17, 66
 - partner name for, 18, 20
 - requesting, 63
- Attacks, 9
 - denial-of-service, 3, 4
 - impersonation, 9
 - preventing, 19
 - replay, 3, 4
 - types prevented, 3
- Attributes
 - activating, 23, 28
 - assertions for, 63
 - available for SAML, 30, 51

- decision point for, 51
- definition of, 8
- how created, 65
- LDAP v3.0 compliancy, 15, 41
- lifetime of, 17, 66
- namespaces, 19, 20, 41, 45
- nxAccountAuthenticationMethod, 59, 63
- nxAccountDeleteTime, 59, 63
- partner name for, 18, 20
- synchronizing, 31

- Audit policy
 - components, 32, 56
 - creating, 31, 33, 56, 57
 - event levels, 32, 56
- Audit server. *See* Secure Audit Server
- Audit trial, creating, 32, 57
- Authentication
 - assertions for, 63
 - certificates, 23, 24
 - lifetime of assertions, 17
 - passwords, 23, 26
- Authentication servers
 - adding, 43
 - multiple partners and SelectID setup, 50
 - SAML, 45
 - setting up, 23, 25, 26, 48
- Automating
 - attributes, discarding unsupported, 30
 - Enforcer plugin installation, 12
 - redirect syntax, 35

B

- Balancing, load, 12, 38
- Base64 encoding, 18, 44
- Binary, ID, 18, 44

C

- CA, 9, 19, 24, 41, 45
 - caCertificate attribute, 24
 - certificate, 17
 - certificationAuthority object class, 24
 - unknown, 25
- catalog.sh command, 13, 59
- Certificate
 - authenticating with, 23, 24
 - authority. *See* CA

- client, 9, 15, 19, 20
 - location of, 16, 42
 - password for, 16, 42
 - PEM, 19
 - server of, 25
 - unknown CAs, 25
 - uploading to directory server, 25
- Characteristics, user. See Attributes
- Clock, synchronizing, 14, 41
- CN, 15, 20, 30, 51, 65
- Communication, between two SAML servers, 5
- Component
 - configuration, 66
 - defining, 32, 56
 - SAML-specific options, 32, 56
- Conditional rules. See Rules
- Configuration
 - changing, 66
 - exporting, 20, 44
 - testing, 59
- Connection, authenticating, 41
- Content, Web, 23
- Cookies, 64
 - domain for SSO, 47
 - evaluating, 46

D

- Data
 - authentication and authorization, 3
 - avoiding excessive growth of, 3
 - binary, 5
 - compromising, 43
 - differences between partners, 6
 - exchanging, 3, 4, 6
 - logging components, 33, 57
 - maintaining consistency, 7
 - SAML-specific, 33, 64
 - securing, 4
 - testing, 38, 59
 - user attributes, 4, 8, 31
- Database, 32, 57
- DEBUG setting, event level, 32, 56
- Decision points
 - attribute logic, 51
- Delegated administration, 9
 - Enforcer plugins for, 13
 - introduction to guide, 1
 - setting up, 13
- Deleting
 - content files, 33

- SAML entries, 46, 47, 61, 66
- Denial-of-service attacks, 3, 4
- Deny policy. See Access policies
- Destination
 - for log output, 32, 57
 - partner name, 18, 38
- Directory attributes. See Attributes
- Directory servers
 - configuring SAML partner properties, 45
 - dropping SAML properties from, 20
 - location of partner entry, 17
 - location of partner's users, 41, 46
 - restrictions, 9
 - risks with multiple partners, 31
 - schema, reading, 30, 51
 - synchronizing attribute values, 34
 - uploading certificates, 25
 - validity of CN or UID values, 15
- DN, 20, 64, 65
- Domain
 - cookie, 47
 - DNS, 47
 - security, 8, 17, 41, 45

E

- EJB, 4
- Encoding
 - base64, 18, 44
 - hex, 44
 - hyperlinks, 33, 34, 35
- Enforcer plugins
 - configuring for inbound transfers, 47
 - configuring for outbound transfers, 21
 - cookie domain for SSO, 47
 - general setup, 21, 47
 - installing, 12, 39
 - modifying configuration, 22, 48
 - NameIdentifier string, 64
 - subject_name element, 64
- Environment variables
 - creating on Web server, 33, 34
 - defining, 31
- ERROR setting, event level, 32, 56
- Errors, SAML setup, 59
- Event level, 32
 - categories available, 56
 - pairing with component, 31, 32, 56
 - SAML examples, 34
- Exporting properties, 17, 20, 44

F

- Failover, 12, 38
- FATAL setting, event level, 32, 56
- Filtering attributes, 29, 50
- Folders
 - adding, 13, 23, 24, 33, 40, 48
 - copying files to, 33
 - creating test user in, 60
 - for certificates, 24
 - selecting, 18, 25
 - setting policies against, 49, 50
- Form-based login, password, 26
- From partner. See Outbound transfers

G

- General setup properties
 - Enforcer plugin, 21, 47
 - SAML server, 16, 42, 43

H

- Handles, 4
- Hashing, ID, 18, 44
- Hex, encoding, 44
- HP OpenView Select Access components
 - Administration server. See Administration server
 - Enforcer plugins. See Enforcer plugins
 - needed for inbound transfers, 38
 - needed for outbound transfers, 12
 - Policy Validator. See Policy Validator
 - SAML server. See SAML servers
 - Secure Audit server. See Secure Audit server
- HTTPS
 - example redirect link, 19, 34
 - selecting as protocol, 22, 48
 - service, adding, 22, 48
 - used as SAML URL, 18, 44, 62

Hyperlinks

- automating, 35
- encoding, 33, 34
- SAML elements of, 34

I**ID**

- hashing to create binary, 18, 44
- partner, 5, 17
- SAML server, 15, 42
- source, 17, 44
- why needed, 8

Impersonation attacks, 9**Inbound transfers**

- auditing events of, 55
- authentication, configuring, 48
- components to install, 38
- Policy Builder, configuring, 39
- SAML server, configuring, 37, 40, 41

INFO setting, event level, 32, 56**Inheritance, 24, 50, 52, 54****Issuer, 17, 44**

- authentication assertions, 8
- configuring, 8, 15
- description of, 8
- how used, 18, 44

J**JDBC, 32, 57****K****Known users, 13, 25, 26, 40, 49****L****LDAP v3.0 compliancy, 15, 41****Level, event, 32, 56**

- categories available, 56
- pairing with component, 31
- SAML examples, 33

Lifetime, 66

- assertion, 17
- authentication, 17

Links. See Hyperlinks**Load balancing, 12, 38****Location**

- certificates, 16, 42
- partners, 17
- users, 25, 26, 41, 46

Logging, events and messages, 31, 55**Logic, attribute decision point, 51****Login forms, password, 26****M****Matrix, Policy. See Policy Matrix****Membership, to role, 52****Messages, logging, 31, 55****Method, authentication. See Authentication servers****Multiple partners, configuring SelectID for, 50**

N

- Name Qualifier parameter, 18
- Namelfield parameter, 64
- Namespaces, 19, 20, 41, 45
 - definition of, 7
 - how used, 8
- Network architecture, 5
- nxAccountAuthenticationMethod, 59, 63
- nxAccountDeleteTime, 59, 63

O

- Object class
 - caCertificate, 24
 - certificationAuthority, 24
 - restrictions, 9
- Oracle
 - catalog.sh command, 13, 59
 - indexing attributes, 13
- Outbound transfers
 - auditing events of, 31
 - authentication, configuring, 23
 - components you need, 12
 - personalization attributes, configuring, 28
 - SAML server, configuring, 11, 14, 15

P

- parameter, 16
- Parameters
 - configuring, 15, 16, 17, 18, 41, 42, 44, 46, 60, 66
 - confirming values for, 66
 - modifying, 66
 - Name Qualifier, 18
 - Namelfield, 64
 - SAML server setup, 14
 - subject_name, 64, 65
 - testing, 66
- Partner
 - destination name, 18, 38
 - from, SAML servers. See Outbound transfers
 - ID, 5, 17
 - location on directory server, 17
 - name of, 18, 20
 - properties of server, 22, 44
 - risks with multiple, 31
 - sharing configuration, 20, 44
 - synchronizing clocks, 14, 41
 - testing, 59
 - to, SAML servers. See Inbound transfers
- Password
 - authenticating with, 23

- for certificate, 16, 42
- login form for, 26
- server, 26
- servers, 26
- synchronizing, 15
- PEM certificates, 19
- Personalization, 12, 38
 - activating user attributes for, 23
 - available SAML attributes for, 30, 51
 - configuring, overview, 24, 29
 - enabling, 29, 31
- PKCS#12 certificates, 16, 42
- Policies
 - access. See Access policies
 - audit. See Audit policy
- Policy Builder, 9
 - activating attributes, 29, 50
 - adding SAML authentication server in, 47
 - authentication methods, 43
 - configuring for SAML, 39
 - enabling SelectID, 27
 - modifying component's configuration from, 22, 48
 - personalization, 31
 - setting authentication methods, 27
- Policy Matrix, 23, 48
 - adding folders, 14, 40
 - adding partners, 20, 39
 - adding services, 22, 48
 - adding users, 23, 48
 - configured inbound server example, 54
 - inbound server example, 27
 - SAML entries, deleting, 46
 - saml_in, 48
 - saml_out, 22
 - saml_responder, 22
 - setting up overview, 13, 39
- Policy Validator
 - cookies, 46, 61
 - evaluating attributes, 29, 50
 - identifying partners, 64
 - installing, 12, 38
 - queries, 64
- Portal servers, 4
- POSTs, 62
- Properties, exporting, 17, 44
- Protocols
 - HTTPS, 22, 48
 - SAML. See SAML
 - SOAP. See SOAP

Q

Qualifier, of name, 18

Queries, 4, 64

- checking for partner name, 64
- checking policy, 61
- creating, 61, 62
- populating with SAML data, 64
- subject_name parameter, 64, 65
- user information, 22
- validating cookie, 61

R

RDN, 14, 40, 64

Recording transactions, 13, 39

Redirects, 5

- how they work, 61
- saml_out, 34
- syntax of, 33, 34, 35

Related references, 1

Replay attacks, 3, 4

Resources Tree. *See* Policy Matrix

Resources, adding, 22, 23, 48, 49

Retrieval timeout, 17

Roles

- adding users to, 52
- benefits of, 52
- creating, 38, 50, 52
- inheritance, 52
- testing, 60
- using for delegation of administration, 9

Rules

- conditional, creating, 51

Runtime events, recording, 31, 55

S

SAML

- action, auditing, 32, 56
- adjusting Web content, 33
- assertions, 4, 44
- attribute risk, 31
- authentication servers, 45
- available attributes for, 30, 51
- basic architecture of, 5
- communication overview, 5
- deployment scenario for, 6
- handles, 4
- how it works, 4
- hyperlinks, encoding, 33, 34
- Name Qualifier, 18
- properties, 41

redirects, 33, 34, 35, 61

security mechanisms, 3

server. *See* SAML servers

setting up with multiple partners, 31

testing, 59

to partner URL, 18, 22, 34, 38, 44

transactions, recording, 13, 39

users, creating, 64

users, deleting, 46

SAML servers

attributes, discarding, 30, 51

auditing, 31, 55

authenticating partners, 14

configuration, changing, 66

configuring Enforcer plugin for, 21, 47

configuring for inbound transfers, 37, 40, 41

configuring for outbound transfers, 11, 14, 15

configuring SelectID for multiple partners, 50

exporting configuration, 20, 44

failures caused by misconfiguring, 59

general setup, 16, 42, 43

ID, 15, 42

installing, 12, 38

setting access policies, 24, 40, 50

setup overview, 11, 37

synchronizing configuration values, 59

testing, 59

saml_in

auditing, 56

recording events of, 56

setting SelectID against, 50

URL path for, 38

saml_out

adding to Policy Matrix, 22, 48

auditing, 32

called from redirect, 34

recording events of, 32

setting SelectID against, 27

saml_responder

adding to Policy Matrix, 22

auditing, 32

recording events of, 32

setting SelectID against, 24, 27

Schemas

object class restrictions, 9

reading attributes from, 30, 51

SAML-specific attributes, 30

Script

saml_out. *See* saml_out

Search expression, 52

Secure Audit server

audit policy, creating, 31, 33, 56, 57

- audit trail, creating, 32, 57
 - auditing SAML, 31, 55
 - components to audit, 32, 56
 - event level, defining, 32, 56
 - installing, 13, 39
- Security Assertions Markup Language. See SAML
- Security domain, 47
- configuring partner value for, 41, 45
 - description of, 8
 - setting value for, 15, 17
 - used as Name Qualifier parameter, 18
- SelectID, 27, 55
- configuring authentication methods, 49, 53
 - configuring for inbound transfers, 50
 - configuring for multiple partners, 50
 - configuring for outbound transfers, 27
 - configuring for SAML, 48
 - enabling, 23, 48
 - enabling personalization with, 31
 - setting against SAML resources, 27, 50
- Servers
- Application, 4
 - authentication. See Authentication servers
 - certificate, 25
 - directory restrictions, 9
 - Directory. See Directory servers
 - messages, recording, 31, 55
 - password, 26
 - portal, 4
 - SAML. See SAML servers
 - Secure Audit. See Secure Audit server
 - SSL, 16
 - Web. See Web servers
- Services
- adding resources to, 22, 48
 - adding to Resources Tree, 22, 48
 - denial of, 3, 4
 - HTTPS, 22, 48
 - Web servers, adding as, 23, 49
- Servlet, saml_responder. See saml_responder
- Setup errors, 59
- SHA-1, 44
- Signatures, verifying, 45
- Simple Object Access Protocol. See SOAP
- Single sign-on. See SSO
- SN, 30, 52, 65
- SOAP, how used, 6
- Source ID, 17, 44, 62
- Sript
- saml_out. See saml_out
- SSL, 9, 16
- SSO
- cookie domain for, 47
 - DNS domain, single, 47
 - from partners, configuring, 43, 47
 - knowledge of, requirement, 1
 - to partners, configuring, 16, 18, 20
 - transfers, testing, 66
- subject_name parameter, 64, 65
- Sun ONE Enforcer plugin. See Enforcer plugins, 21
- Synchronizing
- attributes, 31
 - clocks, 14, 41
 - passwords, 15
 - SAML server configuration, 20, 44, 59
- Syntax
- SAML redirects, 33, 34, 35
 - URL path for saml_in, 38
- ## T
- Testing
- creating folder for, 60
 - creating user for, 60
 - deployment, 59
 - roles, 60
- Text file, exporting, 20
- Theft, of data, 3
- Timeout, retrieval, 17
- Time, synchronizing, 14, 41
- To partner. See Inbound transfers
- Trail, audit. See Audit trail
- Transactions
- recording, 13, 39
 - SAML, 31, 55
- Typical setup errors, 59

U

UID, 15, 20, 29, 30, 52, 65

URL

 - alias, 15, 18, 34, 62
 - for inbound SAML server, 22, 34, 38, 44

User, 32

 - attributes. See Attributes
 - credentials, sharing, 4
 - credentials, transmitting, 14
 - data, 4
 - entries, deleting, 46
 - lookups, defining location of, 25, 26
 - partner storage location, 41, 46

- redirects, 5
- roles. See Roles
- SAML, how created, 64
- transfers, configuring inbound servers, 40, 41
- transfers, configuring outbound servers, 14, 15
- transfers, setting up, 11, 37
- transfers, testing, 59

V

- Values, sharing with partners, 20, 44
- Variables, environment. See Environment variables

W

- WARNING setting, event level, 32, 56
- Web content, access policies for, 23
- Web servers
 - adding as a service, 23
 - creating environment variables, 33, 34
 - creating SAML content for, 33
 - redirect syntax, 33, 34, 35
 - Select Access-protecting, 12
 - setting up, 23, 49

X

- XML, 6

