



Security Access Markup Language (SAML)

Integration

Release 4.1 Beta

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 100504, Revision B

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, Neoteris, Neoteris-Secure Access, Neoteris-Secure Meeting, NetScreen-SA 1000, NetScreen-SA 3000, NetScreen-SA 5000, IVEGigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Copyright © 2001 D. J. Bernstein. Copyright © 1985-2003 by the Massachusetts Institute of Technology. All rights reserved. Copyright © 2000 by Zero-Knowledge Systems, Inc. Copyright © 2001, Dr Brian Gladman <brg@gladman.uk.net>, Worcester, UK. All rights reserved. Copyright © 1989, 1991 Free Software Foundation, Inc. Copyright © 1989, 1991, 1992 by Carnegie Mellon University. Derivative Work - 1996, 1998-2000. Copyright © 1996, 1998-2000 The Regents of the University of California. All Rights Reserved. Copyright © 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted. Copyright © 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland. All rights reserved. Copyright © 1986 Gary S. Brown. Copyright © 1998 CORE SDI S.A., Buenos Aires, Argentina. Copyright © 1995, 1996 by David Mazieres <dm@lcs.mit.edu>. Copyright © 1998-2002. The OpenSSL Project. All rights reserved. Copyright © 1989-2001, Larry Wall. All rights reserved. Copyright © 1989, 1991 Free Software Foundation, Inc. Copyright © 1996-2002 Andy Wardley. All Rights Reserved. Copyright © 1998-2002. Canon Research Centre Europe Ltd. Copyright © 1995-1998. Jean-loup Gailly and Mark Adler.

Security Access Markup Language (SAML) Integration, Release 4.1 Beta

Copyright © 2004, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Writer: Claudette deGiere

Editor: Anchal Jain

Revision History

10 May 2004 — Beta draft

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Contents

- SAML overview1**

- Creating a trust relationship between SAML-enabled systems3**
 - Trusted application URLs3**
 - Issuer3**
 - Certificates4**
 - User Identity6**

- Enabling and configuring SAML transactions7**
 - Single sign-on (SSO) transactions7**
 - Access control transactions14**

- Glossary17**

SAML overview

The SAML feature enables you to pass user and session state information between the IVE and another trusted access management system that supports the Secure Access Markup Language (SAML). **SAML** provides a mechanism for two disparate systems to create and exchange authentication and authorization information using an XML framework, minimizing the need for users to re-enter their credentials when accessing multiple applications or domains¹. The IVE uses SAML version 1.1.

SAML exchanges are dependent upon a trusted relationship between two systems or domains. In the exchanges, one system acts as a **SAML authority** (also called an asserting party or SAML responder) that asserts information about the user. The other system acts as a **relying party** (also called a SAML receiver) that relies on the statement (also called an assertion) provided by the SAML authority. If it chooses to trust the SAML authority, the relying party authenticates or authorizes the user based on the information provided by the SAML authority.

For example, an authenticated IVE user named John Smith may try to access a resource protected by an access management system. When he does, the IVE acts as a SAML authority and declares "This user is John Smith. He was authenticated using a password mechanism." The access management system (the relying party) receives this statement and chooses to trust the IVE (and therefore trust that the IVE has properly identified the user). The access management system may still choose to deny the user access to the requested resource (for instance, because John Smith has insufficient access privileges on the system), while trusting the information sent by the IVE.

For information about configuring a trust relationship, see "Creating a trust relationship between SAML-enabled systems" on page 3.

When configuring the IVE, you can use SAML for:

- **Single sign-on (SSO) authentication**

In a SAML SSO transaction, an authenticated IVE user is seamlessly signed into another system without re-submitting his credentials. In this type of transaction, the IVE is the SAML authority. It makes an **authentication statement**, which declares the user's username and how he was authenticated. If the relying party (called an **assertion consumer service** in SAML SSO transactions) chooses to trust the IVE, the user is seamlessly signed into the assertion consumer service using the username contained in the statement. For more information, see the *IVE Administration Guide*.

- **Access control authorization**

In a SAML access control transaction, the IVE asks an access management system whether the user has access. In this type of transaction, the IVE is the relying party (also called a policy enforcement point in access control transactions). It consumes and enforces an **authorization decision statement** provided by the access management system (SAML authority), which declares what the user is allowed to access. If the SAML authority (also called a policy decision point in access control transactions) declares that the IVE user has sufficient access privileges, the user may access the requested resource. For more information, see the *IVE Administration Guide*.

To configure SAML through the IVE, you must configure a Web resource policy for a URL. Within the policy, you must provide information about the IVE, the trusted access management system, and the mechanism they should use to share information. Then, you must give IVE users within a role access to the resource policy. For more information, see "Single sign-on (SSO) transactions" on page 7 or "Access control transactions" on page 14.

1. The Secure Access Markup Language is developed by Security Services Technical Committee (SSTC) of the OASIS standards organization. For a technical overview of SAML, see the OASIS web site:
<http://www.oasis-open.org/committees/download.php/5836/sstc-saml-tech-overview-1.1-draft-03.pdf>

Important:

- The IVE does not support **attribute statements**, which declare specific details about the user (such as “John Smith is a member of the gold group”).
- The IVE does not accept authentication statements from other SAML authorities. In a SAML SSO transaction, the user must sign into the IVE first.
- The IVE does not generate authorization decision statements—it only consumes them.
- In addition to providing users access to a URL based on the authorization decision statement returned by a SAML authority, the IVE also allows you to define users’ access rights to a URL using IVE-only mechanisms (**Resource Policies > Web > Access** tab). If you define access controls through the IVE as well as through a SAML authority, both sources must grant access to a URL in order for a user to access it. For example, you may configure an IVE access policy that denies members of the “Users” role access to www.google.com, but configure another SAML policy that bases a user’s access rights on an attribute in an access management system. Even if the access management system permits users access to www.google.com, users are still denied access based on the IVE access policy.
- When asked if a user may access a resource, access management systems that support SAML may return a response of permit, deny, or indeterminate. If the IVE receives an indeterminate response, it denies the user access.
- The session timeouts on the IVE and your access management system may not coordinate with one another. If a user’s access management system session cookie times out before his IVE cookie (DSIDcookie) times out, then single sign-on between the two systems is lost. The user is forced to sign in again when he times out of the access management system.

Creating a trust relationship between SAML-enabled systems

In order to ensure that SAML-enabled systems are only passing information between trusted sources, you must create a trust relationship between the applications that are sending and receiving information. To create a trust relationship between the IVE and another SAML-enabled application, you must configure the following types of information on each system:

Trusted application URLs	3
Issuer.....	3
Certificates	4
User Identity	6

Trusted application URLs

In a trust relationship, you must provide the SAML-enabled systems with the URLs they need to contact each other. In some transactions, only the system that initiates the transaction (the IVE) needs to know the URL of the other system. (The IVE uses the URL to initiate the transaction.) In other transactions (SSO transactions using artifact profiles), you need to configure each system with the URL of the other.

Listed below are the different transaction types and the URLs you must configure for each:

- **SSO transactions: Artifact profile**

On the IVE, you must enter the URL of the assertion consumer service. For example:
https://hostname/acs

Also, you must enter the following URL for the IVE on the assertion consumer service:
https://<IVEhostname>/dana-ws/saml.ws

- **SSO transactions: POST profile**

On the IVE, you must enter the URL of the assertion consumer service. For example:
https://hostname/acs

- **Access control transactions**

On the IVE, you must enter the URL of the SAML Web service. For example:
https://hostname/ws

Issuer

Before accepting a statement from another system, a SAML-enabled entity must trust the issuer of the statement. You can control which issuers a system trusts by specifying the unique strings of the trusted issuers during the system's configuration. (When sending a statement, an issuer identifies itself by including its unique string in the statement. SAML-enabled applications generally use hostnames to identify issuers, but the SAML standard allows applications to use any string.) If you do not configure a system to recognize an issuer's unique string, the system will not accept that issuer's statements.

Listed below are the different transaction types and the issuers you must configure for each:

- **SSO transactions**

You must specify a unique string on the IVE (typically its hostname) that it can use to identify itself and then configure the access management system to recognize that string.

- **Access control transactions**

You must specify a unique string on the access management system (typically its hostname) that it can use to identify itself and then configure the IVE to recognize that string.

Certificates

Within SSL transactions, the server must present a certificate to the client, and then the client must verify (at minimum) that it trusts the certificate authority who issued the server's certificate before accepting the information. You can configure all of the IVE's SAML transactions to use SSL (HTTPS). The following sections list different transaction types and the certificate requirements for each.

SSO transactions: Artifact profile

Artifact profile transactions involve numerous communications back and forth between the IVE and access management system. The methods you use to pass data and authenticate the two systems effect which certificates you must install and configure. Listed below are the different artifact profile configuration options that require special certificate configurations:

- **All artifact profile transactions**

Regardless of your artifact profile configuration, you must install the certificate of the CA that signed the IVE Web server's certificate on the access management system. (The IVE requires the access management system to use an SSL connection when requesting an authentication statement. In an SSL connection, the initiator must trust the system to which it is connecting. By installing the CA certificate on the access management system, you ensure that the access management system will trust the CA that issued the IVE's certificate.)

- **Sending artifacts over an SSL connection (HTTPS GET requests)**

If you choose to send artifacts to the access management system using an SSL connection, you must install the access management system's root CA certificate on the IVE. (In an SSL connection, the initiator must trust the system to which it is connecting. By installing the access management system's CA certificate on the IVE, you ensure that the IVE will trust the CA that issued the access management system's certificate.) You can install the root CA from the **System > Configuration > Certificates > CA Certificates** page in the Web console. If you do not want to send artifacts over an SSL connection, you do not need to install any additional certificates.

To enable SSL-based communications from the IVE to the access management system, enter a URL that begins with HTTPS in the **SAML Assertion Consumer Service URL** field during IVE configuration. You may also need to enable SSL on the access management system.

- **Transactions using certificate authentication**

If you choose to authenticate the access management system using a certificate, you must:

- Install the access management system's root CA certificate on the IVE. You can install the root CA from the **System > Configuration > Certificates > CA Certificates** page in the Web console.
- Specify which certificate values the IVE should use to validate the access management system. You must use values that match the values contained in the access management server's certificate.

If you do not choose to authenticate the access management system, or if you choose to use username/password authentication, you do not need to install any additional certificates.

SSO transactions: POST profile

In a POST profile transaction, the IVE may send signed authentication statements to the access management system. Generally, it sends them over an SSL connection (recommended), but in some configurations, the IVE may send statements via a standard HTTP connection. Listed below are the different POST profile configuration options that require special certificate configurations:

- **All POST profile transactions**

Regardless of your POST profile configuration, you must specify which certificate the IVE should use to sign its statements. You can choose a certificate in the **Resource Policies > Web > SAML > SSO > [Policy] > General** page in the Web console (page 7). Then, you must install the IVE's certificate on the access management system. You can download the IVE's certificate from the **System > Configuration > Certificates > Server Certificates > [Certificate] > Certificate Details** page.

- **Sending POST data over an SSL connection (HTTPS)**

If you choose to send statements to the access management system using an SSL connection, you must install the access management system's root CA certificate on the IVE. (In an SSL connection, the initiator must trust the system to which it is connecting. By installing the access management system's certificate on the IVE, you ensure that the IVE will trust the CA that issued the access management system's certificate.) You can install the root CA from the **System > Configuration > Certificates > CA Certificates** page in the Web console. If you do not want to post statements over an SSL connection, you do not need to install any additional certificates.

To enable SSL-based communications from the IVE to the access management system, enter a URL that begins with HTTPS in the **SAML Assertion Consumer Service URL** field during IVE configuration. You may also need to enable SSL on the access management system.

Access control transactions

In an access control transaction, the IVE posts an authorization decision query to the access management system. To ensure that the access management system responds to the query, you must determine which certificate options are required by your configuration. Listed below are the different access control configuration options that require special certificate configurations:

- **Sending authorization data over an SSL connection**

If you choose to connect to the access management system using an SSL connection, you must install the access management system's root CA on the IVE. (In an SSL connection, the initiator must trust the system to which it is connecting. By installing the access management system's certificate on the IVE, you ensure that the IVE will trust the CA that issued the access management system's certificate.) You can install the root CA from the **System > Configuration > Certificates > CA Certificates** page in the Web console.

- **Transactions using certificate authentication**

If you choose to use certificate authentication, you must configure the access management system to trust the CA that issued the IVE's certificate. Optionally, you may also choose to accept the certificate based on the following additional options:

- Upload the IVE certificate's public key to the access management system.
- Validate the IVE using specific certificate attributes.

These options require that you specify which certificate the IVE should pass to the access management system. You can choose a certificate in the **Resource Policies > Web > SAML > Access Control > [Policy] > General** page in the Web console (page 14).

To determine how to configure your access management system to validate the IVE's certificate, see your access management system's documentation. If your access management system does not require certificate authentication, or if it uses

username/password authentication, you do not need to configure the IVE to pass the access management server a certificate. If you do not specify a trust method, your access management system may accept authorization requests from any system.

User Identity

In a trust relationship, the two entities must agree on a way to identify users. You may choose to share a username across systems, select an LDAP or certificate user attribute to share across systems, or hard-code a user ID. (For example, you may choose to set the Subject Name field to "guest" to easily allow access across systems.)

To ensure that the two systems are passing common information about users, you must specify which information the IVE should pass using options in the **User Identity** section of the **Resource Policies > Web > SAML > SSO > [Policy] > General** page (page 7) and the **Resource Policies > Web > SAML > Access Control > [Policy] > General** page (page 14) of the Web console. Choose a username or attribute that the access management system will recognize.

Enabling and configuring SAML transactions

This section includes the following instructions for enabling and configuring SAML transactions through the IVE's Web console:

Write a SAML SSO artifact profile resource policy	7
Write a SAML SSO POST profile resource policy	11
Write a SAML Access Control resource policy	14

Single sign-on (SSO) transactions

Use the **SAML > SSO** tab in the IVE's Web console to write a Web resource policy that specifies SAML-aware access management systems with which the IVE interacts (as explained in "SAML overview" on page 1). The IVE supports SAML single sign-on to multiple assertion consumer services, which may include applications or domains. To configure SAML SSO policies to multiple assertion consumer services, define a separate resource policy for each.

Write a SAML SSO artifact profile resource policy

When you choose to communicate using the artifact profile, the trusted access management server "pulls" authentication information from the IVE, as explained in the *IVE Administration Guide*.

Important: If you configure the IVE to use artifact profiles, you must install the IVE's Web server certificate on the assertion consumer service (as explained in "Certificates" on page 4).

To write a SAML SSO artifact profile resource policy:

1. In the Web console, choose **Resource Policies > Web > SAML > SSO**.
2. On the **Web Policies** page, click **New Policy**.
3. On the **SAML SSO Policy** page, enter:
 - 1 A name to label this policy.
 - 2 A description of the policy. (optional)
4. In the **Resources** section, specify the resources to which this policy applies. See the *IVE Administration Guide* for more information.
5. In the **Roles** section, specify:
 - **Policy applies to ALL roles**
To apply this policy to all users.
 - **Policy applies to SELECTED roles**
To apply this policy only to users who are mapped to roles in the **Selected roles** list. Make sure to add roles to this list from the **Available roles** list.
 - **Policy applies to all roles OTHER THAN those selected below**
To apply this policy to all users *except* for those who map to the roles in the **Selected roles** list. Make sure to add roles to this list from the **Available roles** list.

6. In the **Action** section, specify:
 - **Use the SAML SSO defined below**
The IVE performs a single-sign on (SSO) request to the specified URL using the data specified in the **SAML SSO details** section. The IVE makes the SSO request when a user tries to access to a SAML resource specified in the **Resources** list.
 - **Do NOT use SAML**
The IVE does not perform a SSO request.
 - **Use Detailed Rules**
To specify one or more detailed rules for this policy. See *IVE Administration Guide* for more information.
7. In the **SAML SSO Details** section, specify:
 - **SAML Assertion Consumer Service URL**
Enter the URL that the IVE should use to contact the assertion consumer service (that is, the access management server). For example, `https://hostname/acs`. (Note that the IVE also uses this field to determine the SAML recipient for its assertions.)

Important: If you enter a URL that begins with HTTPS, you must install the assertion consumer service's root CA on the IVE (as explained in "Certificates" on page 4).

 - **Profile**
Select **Artifact** to indicate that the assertion consumer service should "pull" information from the IVE during SSO transactions.
 - **Source ID**
Enter the source ID for the IVE. If you enter a:
 - Plain text string—The IVE converts, pads, or truncates it to a 20-byte string.
 - Base-64 encoded string—The IVE unencodes it and ensures that it is 20 bytes.
 If your access management system requires base-64 encoded source IDs, you can create a 20 byte string and then use a tool such as OpenSSL to base-64 encode it.

Important: The IVE identifier (that is, the source ID) must map to the following URL on the assertion consumer service (as explained in "Trusted application URLs" on page 3):
`https://<IVEhostname>/dana-ws/saml.ws`

 - **Issuer**
Enter a unique string that the IVE can use to identify itself when it generates assertions (typically its hostname).

Important: You must configure the assertion consumer service to recognize the IVE's unique string (as explained in "Issuer" on page 3).

8. In the **User Identity** section, specify how the IVE and the assertion consumer service should identify the user:
 - **Subject Name Type**
Specify which method the IVE and assertion consumer service should use to identify the user:
 - **DN**—Send the username in the format of a DN (distinguished name) attribute.
 - **Email Address**—Send the username in the format of an email address.
 - **Windows**—Send the username in the format of a Windows domain qualified username.

- **Other**—Send the username in another format agreed upon by the IVE and the assertion consumer service.
- **Subject Name**
Use the variables described in the *IVE Administration Guide* to specify the username that the IVE should pass to the assertion consumer service. Or, enter static text.

Important: You must send a username or attribute that the assertion consumer service will recognize (as explained in “User Identity” on page 6).

9. In the **Web Service Authentication** section, specify the authentication method that the IVE should use to authenticate the assertion consumer service:

- **None**
Do not authenticate the assertion consumer service.
- **Username**
Authenticate the assertion consumer service using a username and password. Enter the username and password that the assertion consumer service must send the IVE.
- **Certificate Attribute**
Authenticate the assertion consumer service using certificate attributes. Enter the attributes that the assertion consumer service must send the IVE (one attribute per line). For example, cn=sales. You must use values that match the values contained in the assertion consumer service’s certificate.

Important: If you select this option, you must install the assertion consumer service’s root CA on the IVE (as explained in “Certificates” on page 4).

10. **Cookie Domain**—Enter a comma-separated list of domains to which we send the SSO cookie.

11. Click **Save Changes**.

12. On the **SAML SSO Policies** page, order the policies according to how you want the IVE to evaluate them. Keep in mind that once the IVE matches the resource requested by the user to a resource in a policy’s (or a detailed rule’s) **Resource** list, it performs the specified action and stops processing policies.

For an example Web resource policy, see the figures in the *IVE Administration Guide*.

The screenshot displays the 'SAML SSO Policies > artifact transaction' configuration page in the Juniper Central Manager. The interface is divided into several sections:

- General:**
 - Name:** artifact transaction (Required: Label to reference this policy.)
 - Description:** (Empty text area)
- Resources:**
 - Specify the resources for which this policy applies, one per line.
 - * Resources:** https://10.10.10.10:443/* (Examples: http://*.domain.com/public/*, https://www.domain.com:443/*, 10.10.10.10/255.255.255.0:80,443/public/*, 10.10.10.10/24:8000-9000/*)
- Roles:**
 - Policy applies to ALL roles
 - Policy applies to SELECTED roles
 - Policy applies to all roles OTHER THAN those selected below
 - Available roles:** Test
 - Selected roles:** Users
 - Buttons: Add ->, Remove
- Action:**
 - Use the SAML SSO defined below
 - Do not use SAML
 - Use Detailed Rules (see Detailed Rules page)
- SAML SSO Details:**
 - SAML Assertion Consumer Service URL:** https://yourcompany.com/acs (Example: http://hostname/acs)
 - Profile:** Artifact POST
 - Source ID:** samplesourceid (20-byte IVE identifier that maps to https://<IVEhostname>/dana-ws/saml.ws on the assertion consumer service)
 - Issuer:** https://iveserver.com (Hostname of the IVE)
 - User Identity:**
 - Subject Name Type:** DN
 - Subject Name:** <userAttr.distinguishedName> (Example: <userAttr.distinguishedName>)
 - Web Service Authentication:**
 - Authentication Type:** None, Username/Password, Certificate
 - Values:** cn=sales, cn=engineering, cn=partners (One value per line. Example: cn=sales)
 - Cookie Domain(s):** yourcompany.com (Comma-separated list of domains to which the SSO cookie is sent. For example, company.com.)
- Save changes?**
 - Buttons: Save Changes, Save as Copy

Figure 1: Resource Policies > Web > SAML > SSO (artifact)

This figure shows the Policies page for SAML SSO resource policies with the artifact profile option enabled.

☑ Write a SAML SSO POST profile resource policy

When you choose to communicate using the artifact profile, the IVE “pushes” authentication information from the access management system, as explained in the *IVE Administration Guide*.

Important: If you configure the IVE to use POST profiles, you must install the assertion consumer service’s root CA on the IVE and determine which method the assertion consumer service uses to trust the certificate (as explained in “Certificates” on page 4).

To write a SAML SSO POST profile resource policy:

1. In the Web console, choose **Resource Policies > Web > SAML > SSO**.
2. On the **Web Policies** page, click **New Policy**.
3. On the **SAML SSO Policy** page, enter:
 - 1 A name to label this policy.
 - 2 A description of the policy. (optional)
4. In the **Resources** section, specify the resources to which this policy applies. See the *IVE Administration Guide* for more information.
5. In the **Roles** section, specify:
 - **Policy applies to ALL roles**
To apply this policy to all users.
 - **Policy applies to SELECTED roles**
To apply this policy only to users who are mapped to roles in the **Selected roles** list. Make sure to add roles to this list from the **Available roles** list.
 - **Policy applies to all roles OTHER THAN those selected below**
To apply this policy to all users *except* for those who map to the roles in the **Selected roles** list. Make sure to add roles to this list from the **Available roles** list.
6. In the **Action** section, specify:
 - **Use the SAML SSO defined below**
The IVE performs a single-sign on (SSO) request to the specified URL using the data specified in the **SAML SSO details** section. The IVE makes the SSO request when a user tries to access to a SAML resource specified in the **Resources** list.
 - **Do NOT use SAML**
The IVE does not perform a SSO request.
 - **Use Detailed Rules**
To specify one or more detailed rules for this policy. See the *IVE Administration Guide* for more information.
7. In the **SAML SSO Details** section, specify:
 - **SAML Assertion Consumer Service URL**
Enter the URL that the IVE should use to contact the assertion consumer service (that is, the access management server). For example, `https://hostname/acs`.
 - **Profile**
Select **POST** to indicate that the IVE should “push” information to the assertion consumer service during SSO transactions.
 - **Issuer**
Enter a unique string that the IVE can use to identify itself when it generates

assertions (typically its hostname).

Important: You must configure the assertion consumer service to recognize the IVE's unique string (as explained in "Issuer" on page 3).

- **Signing Certificate**

Specify which certificate the IVE should use to sign its assertions.

8. In the **User Identity** section, specify how the IVE and the assertion consumer service should identify the user:

- **Subject Name Type**

Specify which method the IVE and assertion consumer service should use to identify the user:

- **DN**—Send the username in the format of a DN (distinguished name) attribute.
- **Email Address**—Send the username in the format of an email address.
- **Windows**—Send the username in the format of a Windows domain qualified username.
- **Other**—Send the username in another format agreed upon by the IVE and the assertion consumer service.

- **Subject Name**

Use the variables described in the *IVE Administration Guide* to specify the username that the IVE should pass to the assertion consumer service. Or, enter static text.

Important: You must send a username or attribute that the assertion consumer service will recognize (as explained in "User Identity" on page 6).

9. Cookie Domain—Enter a comma-separated list of domains to which we send the SSO cookie.

10. Click **Save Changes**.

11. On the **SAML SSO Policies** page, order the policies according to how you want the IVE to evaluate them. Keep in mind that once the IVE matches the resource requested by the user to a resource in a policy's (or a detailed rule's) **Resource** list, it performs the specified action and stops processing policies.

For an example Web resource policy, see the figures in the *IVE Administration Guide*.

NETSCREEN

Central Manager Help | Sign Out

SAML SSO Policies > **POST transaction**

General Detailed Rules

* Name: Required: Label to reference this policy.

Description:

Resources

Specify the resources for which this policy applies, one per line.

* Resources: Examples:
http://*.domain.com/public/*
https://www.domain.com:443/*
10.10.10.10/255.255.0:80,443/public/*
10.10.10.10/24:8000-9000/*

Roles

Policy applies to ALL roles
 Policy applies to SELECTED roles
 Policy applies to all roles OTHER THAN those selected below

Available roles: Selected roles:

Action

Use the SAML SSO defined below
 Do not use SAML
 Use Detailed Rules (see [Detailed Rules](#) page)

SAML SSO Details

SAML Assertion Consumer Service URL: Example: http://hostname/acs

Profile: Artifact POST

Issuer: Hostname of the IVE

Signing Certificate: Select certificate used to sign the assertion.

User Identity

Subject Name Type:

Subject Name: Example: <userAttr.distinguishedName>

Cookie Domain(s): Comma-separated list of domains to which the SSO cookie is sent. For example, company.com.

Save changes?

Figure 2: Resource Policies > Web > SAML > SSO (POST)

This figure shows the Policies page for SAML SSO resource policies with the POST profile option enabled.

Access control transactions

Use the **SAML > Access Control** tab in the IVE's Web console to write a Web resource policy that specifies SAML-aware access management systems with which the IVE interacts. For more information on this feature, see "SAML overview" on page 1. The IVE supports SAML access control authorization to multiple access management systems. To configure SAML access control policies to multiple applications, define a separate resource policy for each.

Write a SAML Access Control resource policy

When you choose to enable access control transactions, the IVE queries the SAML Web service for authorization decisions (as explained in the *IVE Administration Guide*).

Important: If you configure the IVE to use access control transactions, you must install the SAML Web service's root CA on the IVE (as explained in "Certificates" on page 4).

To write a SAML Access Control resource policy:

1. In the Web console, choose **Resource Policies > Web > SAML Access Control**.
2. On the **SAML Access Control Policies** page, click **New Policy**.
3. On the **New Policy** page, enter:
 - 1 A name to label this policy.
 - 2 A description of the policy. (optional)
4. In the **Resources** section, specify the resources to which this policy applies. See the *IVE Administration Guide* for more information.
5. In the **Roles** section, specify:
 - **Policy applies to ALL roles**
To apply this policy to all users.
 - **Policy applies to SELECTED roles**
To apply this policy only to users who are mapped to roles in the **Selected roles** list. Make sure to add roles to this list from the **Available roles** list.
 - **Policy applies to all roles OTHER THAN those selected below**
To apply this policy to all users *except* for those who map to the roles in the **Selected roles** list. Make sure to add roles to this list from the **Available roles** list.
6. In the **Action** section, specify:
 - **Use the SAML Access Control checks defined below**
The IVE performs an access control check to the specified URL using the data specified in the **SAML Access Control Details** section.
 - **Do not use SAML Access**
The IVE does not perform an access control check.
 - **Use Detailed Rules**
To specify one or more detailed rules for this policy. See the *IVE Administration Guide* for more information.
7. In the **SAML Access Control Details** section, specify:
 - **SAML Web Service URL**
Enter the URL of the access management system's SAML server. For example, `https://hostname/ws`.

- **Issuer**

Enter the hostname of the issuer, which in most cases is the hostname of the access management system.

Important: You must enter unique string that the SAML Web service uses to identify itself in authorization assertions (as explained in “Issuer” on page 3).

8. In the **User Identity** section, specify how the IVE and the SAML Web service should identify the user:

- **Subject Name Type**

Specify which method the IVE and SAML Web service should use to identify the user:

- **DN**—Send the username in the format of a DN (distinguished name) attribute.
- **Email Address**—Send the username in the format of an email address.
- **Windows**—Send the username in the format of a Windows domain qualified username.
- **Other**—Send the username in another format agreed upon by the IVE and the SAML Web service.

- **Subject Name**

Use the variables described in the *IVE Administration Guide* to specify the username that the IVE should pass to the SAML Web service. Or, enter static text.

Important: You must send a username or attribute that the SAML Web service will recognize (as explained in “User Identity” on page 6).

9. In the **Web Service Authentication** section, specify the authentication method that the SAML Web service should use to authenticate the IVE:

- **None**

Do not authenticate the IVE.

- **Username**

Authenticate the IVE using a username and password. Enter the username and password that the IVE must send the Web service.

- **Certificate Attribute**

Authenticate the IVE using a certificate signed by a trusted certificate authority. If you have more than one certificate installed on the IVE, use the drop-down list to select which certificate to send to the Web service.

Important: If you select this option, you must install the IVE Web server’s certificate on the access management system’s Web server and determine which method the SAML Web service uses to trust the certificate (as explained in “Certificates” on page 4).

10. In the **Options** section, specify:

- **Maximum Cache Time**

You can eliminate the overhead of generating an authorization decision each time the user request the same URL by indicating that the IVE must cache the access management system’s authorization responses. Enter the amount of time the IVE should cache the responses (in seconds).

- **Ignore Query Data**

By default, when a user requests a resource, the IVE sends the entire URL for that resource (including the query parameter) to the SAML Web service and caches the URL. You can specify that the IVE should remove the query string from the URL before requesting authorization or caching the authorization response.

11. Click **Save Changes**.

12. On the **SAML Access Control Policies** page, order the policies according to how you want the IVE to evaluate them. Keep in mind that once the IVE matches the resource requested by the user to a resource in a policy's (or a detailed rule's) **Resource** list, it performs the specified action and stops processing policies.

For an example Web resource policy, see the figures in the *IVE Administration Guide*.

The screenshot displays the 'access control transaction' configuration page in the Juniper Central Manager. The interface includes a left-hand navigation menu with categories like System, Administrators, Users, Resource Policies, and Maintenance. The main content area is titled 'SAML Access Control Policies > access control transaction' and has two tabs: 'General' (selected) and 'Detailed Rules'.

General Tab Configuration:

- Name:** 'access control transaction' (Required: Label to reference this policy.)
- Description:** (Empty text area)
- Resources:** 'Specify the resources for which this policy applies, one per line.' The field contains 'https://10.10.10.10:443/*'. Examples listed include 'http://*.domain.com/public/*', 'https://www.domain.com:443/*', '10.10.10.10/255.255.255.0:80,443/public/*', and '10.10.10.10/24:8000-9000/*'.
- Roles:**
 - Policy applies to ALL roles
 - Policy applies to SELECTED roles
 - Policy applies to all roles OTHER THAN those selected below
- Available roles:** 'Test' (in a list box)
- Selected roles:** 'Users' (in a list box)
- Action:**
 - Use the SAML Access Control checks defined below
 - Do not use SAML Access
 - Use Detailed Rules (see [Detailed Rules](#) page)
- SAML Access Control Details:**
 - SAML Web Service URL:** 'https://yourcompany.com/ws' (Example: http://hostname/ws)
 - SAML Web Service Issuer:** 'https://yourcompany.com' (SAML authority that issues the assertion (generally the hostname of the access management system))
 - Web Service Authentication:**
 - Authentication Type:**
 - None
 - Username/Password
 - Certificate
 - Field: 'yourcompany.com' (Method used to authenticate the IVE against the SAML Web service)
 - User Identity:**
 - Subject Name Type:** 'DN' (dropdown)
 - Subject Name:** '<userAttr.distinguishedName>' (Example: <userAttr.distinguishedName>)
 - IVE Issuer:** 'samplestring' (String that identifies the SAML authority. For example, the hostname of the IVE.)
 - Options:**
 - Maximum Cache Time (seconds):** '20' (Amount of time the authorization response is cached)
 - Ignore Query Data (Ignore the query string for authorization requests)

Figure 3: Resource Policies > Web > SAML > Access Control

This figure shows the Policies page for SAML access control resource policies.

Glossary

Artifact: An encoded string passed from the IVE to an assertion consumer service. The string identifies the IVE's SAML web service and the authentication statement that the assertion consumer service must retrieve from the IVE for SSO.

Artifact profile: SAML SSO transaction method that two trusted entities use to transfer a SAML statement. With the artifact profile method, the assertion consumer service (access management server) "pulls" authentication information from the SAML authority (IVE). (Synonymous term: Browser/Artifact profile.)

Asserting party: In a SAML exchange, the asserting party is the entity that asserts information about the user. (Synonymous terms: SAML authority, SAML responder.)

Assertion consumer service: The relying party in SAML SSO transactions. An assertion consumer service depends on the authentication statement provided by a SAML authority.

Attribute statement: Statement made by a SAML authority that declares specific details about the user (such as "John Smith is a member of the gold group"). Not supported by the IVE.

Authentication statement: Statement made by a SAML authority that declares the user's username and how he was authenticated.

Authorization decision statement: Statement made by a SAML authority that declares what a user is allowed to access.

Browser/Artifact profile: SAML SSO transaction method that two trusted entities use to transfer a SAML statement. With the Browser/Artifact profile method, the assertion consumer service (access management server) "pulls" authentication information from the SAML authority (IVE). (Synonymous term: Artifact profile.)

Browser/POST profile: SAML SSO transaction method that two trusted entities use to transfer a SAML statement. With the Browser/POST profile method, the SAML authority (IVE) "pushes" information to the assertion consumer service (access management server). (Synonymous term: POST profile.)

Issuer: Identity of the entity that sends a statement.

Policy decision point: The SAML authority in SAML access control transactions. The policy decision point asserts what the user is authorized to access.

Policy enforcement point: The relying party in SAML access control transactions. The policy enforcement point depends on the authorization decision statement provided by a SAML authority (policy decision point).

POST profile: SAML SSO transaction method that two trusted entities use to transfer a SAML statement. With the POST profile method, the SAML authority (IVE) "pushes" information to the assertion consumer service (access management server). (Synonymous term: Browser/POST profile.)

Profile: SAML SSO transaction method that two trusted entities use to transfer a SAML statement. Profile types include artifact profiles and POST profiles.

Relying party: In a SAML exchange, the relying party is the entity that depends upon the statement provided by the other entity (that is, the SAML authority). (Synonymous term: SAML receiver.)

SAML: A mechanism based on a XML framework that two disparate systems can use to create and exchange authentication and authorization information. SAML minimizes the

need for users to re-enter their credentials when accessing multiple applications or domains.

SAML access control transaction: Exchange in which a relying party asks a SAML authority whether the user has access to a resource.

SAML authority: In a SAML exchange, the SAML authority is the entity that asserts information about the user. (Synonymous terms: asserting party, SAML responder.)

SAML receiver: In a SAML exchange, the SAML receiver is the entity that depends upon the statement provided by the other entity (that is, the SAML authority). (Synonymous term: relying party.)

SAML responder: In a SAML exchange, the SAML responder is the entity that asserts information about the user. (Synonymous terms: SAML authority, asserting party.)

SAML SSO transaction: Exchange in which an authenticated user is seamlessly signed into another system without re-submitting his credentials.