



Juniper Networks Secure Access

Configuring a SAML Server Instance
Release 5.3R4

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 53B053006

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986–1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, The Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

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.

The following are trademarks of Juniper Networks, Inc.: ERX, E-series, ESP, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, T-series, and TX Matrix. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Copyright © 2006, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Juniper Networks Secure Access Administration Guide, Release 5.3
Writer: Mark Smallwood
Editor: Claudette Hobbart

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.

Year 2000 Notice

Juniper Networks hardware and software products are Year 2000 compliant. The JUNOS software has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

Software License

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

End User License Agreement

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

- 1. The Parties.** The parties to this Agreement are Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").
- 2. The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller.
- 3. License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:
 - a. Customer shall use the Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller, unless the applicable Juniper documentation expressly permits installation on non-Juniper equipment.
 - b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees.
 - c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use the Software on non-Juniper equipment where the Juniper documentation does not expressly permit installation on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; or (k) use the Software in any manner other than as expressly provided herein.

5. Audit. Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. Confidentiality. The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. Ownership. Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. Termination. Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. Taxes. All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. Commercial Computer Software. The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. Interface Information. To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. Third Party Software. Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language).)

Configuring a SAML Server instance



NOTE: The content in this supplemental document is valid for the 5.3R4 release. This content will be included in the Secure Access Administration Guide at the next major product release.

The IVE accepts authentication assertions generated by a SAML authority using either an artifact profile or a POST profile. This feature allows a user to sign in to a source site or portal without going through the IVE first, and then to access the IVE with single sign-on (SSO) through the SAML consumer service.

As a result, the user who authenticates elsewhere is able to access resources behind the IVE without signing in again.

Using the artifact profile and the POST profile

The two supported profiles provide different methods of accomplishing the same task. The end-user's goal is to sign in to all desired resources once, without experiencing multiple sign-in pages for different resources or applications. Although the end-user wants transparency, you, the administrator, want to ensure complete security across the resources on your system, regardless of the servers or sites represented.

The artifact profile requires that you construct an automated request-response HTTP message that the browser can retrieve based on an HTTP GET request. For details about this method, see "Using the artifact profile scenario" on page 210.

The POST profile requires that you construct an HTML form that can contain the SAML assertion, and which can be submitted by an end-user action or a script action, using an HTTP POST method. For more details about this method, see "Using the POST profile scenario" on page 211.

Using the artifact profile scenario

The SAML server generally supports the following artifact profile scenario:

1. The user accesses a source site via a browser. The source site might be a corporate portal using a non-IVE authentication access management system.
2. The source site challenges the user for username and password.
3. The user provides username and password, which the source site authenticates through a call to an LDAP directory or other authentication server.
4. The user then clicks on a link on the source site, which points to a resource on a server that is protected behind the IVE.

5. The link redirects the user to the Intersite Transfer Service URL on the source site. The source site pulls an authentication assertion message from its cache and encloses it in a SOAP message. The source site constructs a SAML artifact (a Base64 string) that it returns to the browser in a URI along with the destination and assertion address.
6. The destination site queries the authenticated assertion from the source site, based on the artifact it receives from the source site.
7. If the elapsed time falls within the allowable clock skew time, the IVE accepts the assertion as a valid authentication, and the user meets any other IVE policy restrictions, the IVE grants the user access to the requested resource.

The main tasks you are required to fulfill to support the IVE as the relying party with the artifact profile include:

- Implement the assertion consumer service, which:
 - Receives the redirect URL containing the artifact
 - Generates and sends the SAML request
 - Receives and processes the SAML response
- Integrate the assertion consumer service with the existing IVE process, which:
 - Maps the SAML assertion to a local user
 - Creates an IVE user session
 - Performs local authorization
 - Serves the resource or denies access

Using the POST profile scenario

The SAML server generally supports the POST profile scenario, as follows:

1. The end-user accesses the source Web site, hereafter known as the source site.
2. The source site verifies whether or not the user has a current session.
3. If not, the source site prompts the user to enter user credentials.
4. The user supplies credentials, for example, username and password.
5. If the authentication is successful, the source site authentication server creates a session for the user and displays the appropriate welcome page of the portal application.
6. The user then selects a menu option or link that points to a resource or application on a destination Web site.
7. The portal application directs the request to the local inter-site transfer service, which can be hosted on the source site. The request contains the URL of the resource on the destination site, in other words, the TARGET URL.

8. The inter-site transfer service sends an HTML form back to the browser. The HTML FORM contains a SAML response, within which is a SAML assertion. The response must be digitally signed. Typically the HTML FORM will contain an input or submit action that will result in an HTTP POST. This can be a user-clickable Submit button or a script that initiates the HTTP POST programmatically.
9. The browser, either due to a user action or by way of an auto-submit action, sends an HTTP POST containing the SAML response to the destination Web site's assertion consumer service.
10. The replying party's assertion consumer (in this case, on the destination Web site) validates the digital signature on the SAML Response.
11. If valid, the assertion consumer sends a redirect to the browser, causing the browser to access the TARGET resource.
12. The IVE, on the destination site, verifies that the user is authorized to access the destination site and the TARGET resource.
13. If the user is authorized to access the destination site and the TARGET resource, the IVE returns the TARGET resource to the browser.

The main tasks you are required to fulfill to support the IVE as the relying party with the POST profile include:

- Implement the assertion consumer service, which receives and processes the POST form
- Integrate the assertion consumer service with the existing IVE process, which:
 - Maps the SAML assertion to a local user
 - Creates an IVE user session
 - Performs local authorization
 - Serves the resource or denies access

Understanding Assertions

Each party in the request-response communication must adhere to certain requirements. The requirements provide a predictable infrastructure so that the assertions and artifacts can be processed correctly.

- The artifact is a Base64-encoded string of 40 bytes. An artifact acts as a token that references an assertion on the source site, so the artifact holder—the IVE—can authenticate a user who has signed in to the source site and who now wants to access a resource protected by the IVE. The source site sends the artifact to the IVE in a redirect, after the user attempts to access a resource protected by the IVE. The artifact contains:
 - **TypeCode**—2-byte hex code of 0x0001 that identifies the artifact type.

- **SourceID**—20-byte encrypted string that determines the source site identity and location. The IVE maintains a table of SourceID values and the URL for the corresponding SAML responder. The IVE and the source site communicate this information in a back channel. On receiving the SAML artifact, the IVE determines whether or not the SourceID belongs to a known source site, and, if it does, obtains the site location before sending a SAML request. The source site generates the SourceID by computing the SHA-1 hash of the source site's own URL.
- **AssertionHandle**—20-byte random value that identifies an assertion stored or generated by the source site. At least 8 bytes of this value should be obtained from a cryptographically secure RNG or PRNG.
- The inter-site transfer service is the identity provider URL on the source site (not the IVE). Your specification of this URL in the IVE Web console enables the IVE to construct an authentication request to the source site, which holds the user's credentials in cache. The request is similar to the following example:

```
GET http://<inter-site transfer host name and path>?TARGET=<Target>...<HTTP-Version><other HTTP 1.0 or 1.1 components>
```

In the preceding sample, <inter-site transfer host name and path> consists of the host name, port number, and path components of the inter-site transfer URL at the source and where Target = <Target > specifies the requested target resource at the destination (IVE protected) site. This request might look like:

```
GET http://10.56.1.123:8002/xferSvc?TARGET=http://www.dest.com/sales.htm
```

- The inter-site transfer service redirects the user's browser to the assertion consumer service at the destination site—in this case, the IVE. The HTTP response from the source site inter-site transfer service must be in the following format:

```
<HTTP-Version> 302 <Reason Phrase>
<other headers>
Location : http://<assertion consumer host name and path>?<SAML searchpart><other HTTP 1.0 or 1.1 components>
```

In the preceding sample, <assertion consumer host name and path> provides the host name, port number, and path components of an assertion consumer URL at the destination site and where <SAML searchpart>= ...TARGET=<Target> ...SAMLart=<SAML artifact>... consists of one target description, which must be included in the <SAML searchpart> component. At least one SAML artifact must be included in the SAML <SAML searchpart> component. The asserting party can include multiple SAML artifacts.

**NOTE:**

- You can use status code 302 to indicate that the requested resource resides temporarily under a different URI.
 - If <SAML searchpart> contains more than one artifact, all of the artifacts must share the same SourceID.
-

The redirect might look like:

HTTP/1.1 302 Found

Location:

<http://www.ive.com:5802/artifact?TARGET=/www.ive.com/&SAMLart=artifact>

- The user's browser accesses the assertion consumer service, with a SAML artifact representing the user's authentication information attached to the URL.

The HTTP request must appear as follows:

```
GET http://<assertion consumer host name and path>?<SAML searchpart>
<HTTP-Version><other HTTP 1.0 or 1.1 request components>
```

In the preceding sample, `<assertion consumer host name and path>` provides the host name, port number, and path components of an assertion consumer URL at the destination site.

```
<SAML searchpart>= ...TARGET=<Target>...SAMLart=<SAML artifact> ...
```

A single target description **MUST** be included in the `<SAML searchpart>` component. At least one SAML artifact **MUST** be included in the `<SAML searchpart>` component; multiple SAML artifacts **MAY** be included. If more than one artifact is carried within `<SAML searchpart>`, all the artifacts **MUST** have the same SourceID.

You should not expose the assertion consumer URL unless over SSL 3.0 or TLS 1.0. Otherwise, transmitted artifacts might be available in plain text to an attacker.

- The **issuer value** is typically the URL of the source site. You can specify the `<ISSUER>` variable which will return the issuer value from the assertion.
- The **user name template** is a reference to the SAML name identifier element, which allows the asserting party to provide a format for the user name. The SAML specification allows for values in the following formats:
 - **Unspecified**—indicates that interpretation of the content is left up to the individual implementations. In this case, you can use the variable `assertionName`.
 - **Email Address**—indicates that content is in the form of an email address. In this case, you can use the variable `assertionName`.
 - **X.509 Subject Name**—indicates that the content is in the form of an X.509 subject name. In this case, you can use the variable `assertionNameDN`. `<RDN>`.
 - **Windows Domain Qualified Name**—indicates that the content is a string in the form of `DomainName\Username`.

You should define the user name template to accept the type of user name your SAML assertion contains.

- To prevent eavesdropping on the SAML artifact, source and destination sites should synchronize their clocks as closely as possible. The IVE provides an **Allowed Clock Skew** attribute that dictates the maximum time difference allowed between the IVE and the source site. The IVE rejects any assertions whose timing exceeds the allowed clock skew.

Creating a new SAML Server instance

To create a new SAML server instance, and configure the common elements:

1. In the Web console, choose **Authentication > Auth. Servers**.
2. Select **SAML Server** from the **New** list, and then click **New Server**.
3. Specify a name to identify the server instance.
4. Under **Settings**, specify the **Source Site Inter-Site Transfer Service URL**.
5. Specify the **issuer value** for the source site. Typically the URI or hostname of the issuer of the assertion.
6. Specify the **user name template**, which is a mapping string from the SAML assertion to an IVE user realm. For example, enter `<assertionNameDN.CN>`, which derives the username from the CN value in the assertion. For more information about allowable values for this object, see “Configuring a SAML Server instance” on page 210.
7. Specify the **Allowed Clock Skew** value, in minutes. This value determines the maximum allowed difference in time between the IVE clock and the source site clock.
8. Proceed to define the configuration for either the artifact profile, as described in “Configure the SAML Server instance to use an artifact profile” on page 215 or for the POST profile as described in “Configure the SAML server instance to use the POST profile” on page 216.

Configure the SAML Server instance to use an artifact profile

To configure the SAML Server to use an artifact profile, continue the following procedure from the last step in “Creating a new SAML Server instance” on page 215.

1. On the **New SAML Server** page, enter the **Source ID**. The source ID is the 20-byte identifier that the IVE uses to recognize an assertion from a given source site.
2. Enter the **Source SOAP Responder Service URL**. You should specify this URL in the form of an HTTPS: protocol.
3. Choose the type of **SOAP Client Authentication**.
 - If you choose **HTTP Basic**, you must then enter the username and password, and confirm the password.

- If you choose **SSL Client Certificate**, choose an IVE certificate from the drop down menu.
4. Click **Save Changes**. If you are creating the server instance for the first time, the **Settings** and **Users** tabs appear.

The **Settings** tab allows you to modify any of the settings pertaining to the SAML Server instance and the artifact profile. The **Users** tab lists valid users of the server.

Configure the SAML server instance to use the POST profile

To configure the SAML Server to use a POST profile, continue the following procedure from the last step in “Creating a new SAML Server instance” on page 215.

1. On the **New SAML Server** page, select the **Post** option.
2. Enter the name of, or browse to locate, the Response Signing Certificate. This is the PEM-formatted signing certificate, which is loaded for the SAML response signature verification.

The certificate you select should be the same certificate used for signing the SAML response at the source site. The source site may send this certificate along with the SAML response, depending on the source site configuration. By default, the system performs signature verification of the SAML response first on the locally configured certificate. If a certificate is not configured locally in the SAML authentication server, then the system performs the signature verification on the certificate included in the SAML response from the source site.

3. Select the **Enable Signing Certificate status checking** option if you want the IVE to be able to check the validity of the signing certificate configured in the SAML authentication server POST profile. It is possible that the certificate has already expired or has been revoked.
4. If you already have a certificate loaded and want to use another, locate the certificate, then click **Delete**. You can then install another certificate.
5. Click **Save Changes**. If you are creating the server instance for the first time, the **Settings** and **Users** tabs appear.

The **Settings** tab allows you to modify any of the settings pertaining to the SAML Server instance and the artifact profile. The **Users** tab lists valid users of the server.