IMPLEMENTING SINGLE SIGN-ON USING SAML 2.0 ON JUNIPER NETWORKS MAG SERIES JUNOS PULSE GATEWAYS

SAML 2.0 combines encryption and digital signature verification across resources for a more secure and robust single sign-on mechanism across network boundaries
Table of Contents

Introduction ................................................................. 4
Scope .............................................................................. 4
Design Considerations .................................................. 5
  Advantages of SAML ..................................................... 5
  Components of SAML 2.0.............................................. 5
  Features of SAML 2.0 ..................................................... 5
  Supported Scenarios ..................................................... 6
MAG Series as Identity Provider (IdP) .............................. 6
  Flow Diagram ............................................................. 6
  Setting Up IdP Configuration ......................................... 7
  Setting Up the SP Information ....................................... 9
  Configuring the Bookmark ........................................... 11
  Configuring Resource Policies for SSO ....................... 12
MAG Series as IdP Summary ........................................... 13
MAG Series SSL VPN as Service Provider ....................... 13
  Flow Diagram ............................................................ 13
  Install Certificates ....................................................... 14
  Setting Up the Authentication Server ......................... 16
  Setting Up the Sign-In Page ....................................... 17
MAG Series as Service Provider Summary ..................... 20
Summary ................................................................. 20
Appendix A ............................................................... 21
References ............................................................... 22
About Juniper Networks ............................................... 22
List of Figures

Figure 1: MAG Series as an IdP ................................................................. 7
Figure 2: Sign-in SAML—metadata provider .................................................. 7
Figure 3: Sign-in SAML—identity provider settings ......................................... 8
Figure 4: Adding SP information .................................................................. 9
Figure 5: SAML global configuration .......................................................... 9
Figure 6: Uploading the metadata file of an SP on the MAG Series .................. 9
Figure 7: Configuring SP on the MAG Series using metadata ......................... 10
Figure 8: Configuring SP on the MAG Series manually ................................ 10
Figure 9: Setting up the SP on the MAG Series and specifying details .......... 11
Figure 10: Setting up bookmarks and user roles .......................................... 11
Figure 11: Roles -> Web -> Bookmark ....................................................... 12
Figure 12: Bookmark details ...................................................................... 12
Figure 13: Resource Policies -> SSO -> SAML External Apps ...................... 12
Figure 14: SAML external apps configuration ............................................. 13
Figure 15: MAG Series as an SP ............................................................... 14
Figure 16: Installing a Trusted Server CA .................................................... 15
Figure 17: Installing a certificate for encryption ........................................... 15
Figure 18: Setting up SAML Auth Server .................................................... 16
Figure 19: SAML Auth Server configuration – 1 ......................................... 16
Figure 20: SAML Auth Server configuration – 2 ......................................... 17
Figure 21: SAML Auth Server configuration – 3 ......................................... 17
Figure 22: Sign-In pages ......................................................................... 18
Figure 23: Custom Sign-In page creation .................................................... 18
Figure 24: Sign-In policy ....................................................................... 19
Figure 25: Sign-In page ....................................................................... 19
Figure 26: SAML error displayed when URL is missing .............................. 20
Figure 27: Role Mapping Rule for a custom expression ............................... 21
Figure 28: Creating a custom expression .................................................. 21

List of Tables

Table 1. MAG Series as IdP and SP .......................................................... 6
Table 2. Modes for MAG Series as IdP ...................................................... 6
**Introduction**

As enterprises and other organizations increasingly move their sensitive business information, applications, and other resources to public, private, or hybrid clouds, security becomes paramount. One of the essential steps toward a more secure environment is to establish and ratify user credentials before allowing them access to resources. While the importance of password protection cannot be emphasized enough, it can prove challenging for users to remember and enter multiple user names and passwords for the various resources they use during their workday.

Single sign-on (SSO) is a methodology that allows a user to enter credentials just once in order to access multiple cloud-based resources. While the concept helps to ease the burden on users, it is useful only if it can guarantee a secure means of communication with every other application once the credentials have been entered.

Security Assertion Markup Language (SAML) 2.0 can achieve a secure method of verifying user credentials before granting access to cloud-based resources. Perhaps the biggest advantage of SAML 2.0 is the ability to cross-reference beyond borders—across clouds, applications, and other resources. By spanning these resources and combining encryption and digital signature verification, SAML 2.0 offers a more secure and robust mechanism to achieve SSO for organizations.

While moving data, applications, and other resources to the cloud can have a positive impact on business efficiency and costs, the user experience—and productivity—often suffer by requiring multiple logins to diverse resources. Of course, the need to verify login credentials before granting access is the first line of defense in network security. Therefore, if a mechanism can maintain the same level of security while easing the burden on the end user, it will achieve dual objectives. To that end, SSO allows users to enter their credentials only once in order to access multiple end applications.

There are a variety of ways in which SSO can be implemented, but most of them impose constraints and thus offer less flexibility. While traditional SSO works well in an environment confined within an intranet, expanding the scope of the network (as to the cloud) exposes severe limitations. SAML 2.0 combines the features of a variety of mechanisms including Shibboleth and Liberty Alliance's Identity Federation Framework (ID-FF), thus federating the identity and removing many of the constraints of other methods.

SAML, developed by Organization for the Advancement of Structured Information Standards (OASIS), was designed primarily to implement web-based SSO and enable businesses to leverage an identity-based security system. It is an XML-based framework that is used for communicating user information. The standard defines the XML-based assertions, protocols, bindings, and profiles used in communication between SAML entities. OASIS-standard SAML offers security and scalability that has been field proven in production deployments worldwide. With the increasing adoption of cloud-based applications, SAML 2.0 can help alleviate a significant user burden by eliminating the need to enter credentials more than once.

**Scope**

This document provides a discussion of the two essential components of the SAML realm—the Identity Provider (IdP) and the Service Provider (SP). It includes details of how Juniper Networks MAG Series Junos Pulse Gateways running Junos Pulse Secure Access Service (SSL VPN) can be set up to function as either an IdP or an SP. It also provides specific configuration examples that network engineers can use to set up the MAG Series as either an IdP or SP, depending upon the use case.
Design Considerations

Advantages of SAML

The benefits of SAML include:

- **Platform neutrality**—SAML abstracts the security framework from platform architectures and particular vendor implementations. This offers increased interoperability across different IdP and SP implementations.
- **Loose coupling of directories**—SAML does not require user information to be maintained and synchronized between directories.
- **Improved online experience for end users**—SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication. In addition, identity federation (linking of multiple identities) with SAML allows for a better and more customized user experience at each service while still promoting privacy.
- **Reduced administrative costs for service providers**—Using SAML to “reuse” a single act of authentication (such as logging in with a user name and password) multiple times across multiple services can reduce the cost of maintaining account information. This burden is transferred to the identity provider.
- **Risk transference**—SAML can act to push responsibility for proper management of identities to the identity provider, which is more often compatible with its business model than that of a service provider.

Components of SAML 2.0

SAML 2.0 uses the following components:

- **Assertions** – A package of information that supplies one or more statements made by an SAML authority.
- **Protocol** – Defines the request/response protocols to enable communication between the SP and IdP.
- **Bindings** – Called SAML protocol bindings, these are mappings from SAML request-response message exchanges into standard messaging or communication protocols. For instance, the SAML SOAP binding defines how SAML protocol messages can be communicated within SOAP messages, while the HTTP Redirect binding defines how to pass protocol messages through HTTP redirection.
- **Profiles** – Constraints and/or extensions in support of the use of SAML for a particular application. The goal of profiles is to enhance interoperability by removing some of the flexibility inevitable in a general use standard. It describes how and which protocol bindings and assertions to use to solve any specific use case.

Features of SAML 2.0

SAML 2.0 is not backward compatible with SAML 1.0 or SAML 1.1. New features implemented in SAML 2.0 include:

- **Metadata** – The Service Provider and Identity Provider can generate metadata that contains information about themselves, including URLs, certificates, keys and supported profiles. The metadata from the IdP, for example, can then be used to set up the correct information on the SP, making SAML 2.0 deployment easier.
- **Encryption** – SAML 2.0 permits the communication of user information between the Identity Provider and the Service Provider to be encrypted, ensuring end-to-end confidentiality.
- **Identity Provider discovery** – This helps the SP discover the correct identity provider when there are multiple IdPs.
- **Devices** – This provides the ability to support mobile devices and smartphones.
- **Pseudonyms** – SAML 2.0 defines how an opaque pseudo random identifier with no discernible correspondence with meaningful identifiers (for example, e-mails or account names) can be used between providers to represent principals. Pseudonyms are a key privacy-enabling technology because they inhibit collusion between multiple providers (as would be possible with a global identifier such as an e-mail address).
- **Identifier management** – This determines how two providers can establish and manage the principals.
- **Attribute profiles** – These are the formats in which attribute profiles can be exchanged.
- **Session management** – This is a mechanism by which all sessions can be terminated by a session authority at the same time, e.g., single logout.

Juniper Networks MAG Series Junos Pulse Gateways running Junos Pulse Secure Access Service can be deployed as an IdP or an SP. The following sections examine specific use cases where the MAG Series has been deployed for SSO.
Supported Scenarios
The following implementations are supported on MAG Series today.

Table 1. MAG Series as IdP and SP

<table>
<thead>
<tr>
<th>IdP-Initiated SSO</th>
<th>SP-Initiated SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAG Series as IdP</td>
<td>Supported</td>
</tr>
<tr>
<td>MAG Series as SP</td>
<td>Supported</td>
</tr>
</tbody>
</table>

MAG Series as IdP supports two modes:
- Gateway
- Peer SAML Entity

Table 2. Modes for MAG Series as IdP

<table>
<thead>
<tr>
<th>MAG Series as IdP in Gateway Mode</th>
<th>IdP-initiated SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>- SAML SSO policies are used.</td>
<td></td>
</tr>
<tr>
<td>- MAG Series acts as an IdP as well as the end user. When the MAG Series is in gateway mode, it is the IdP and the SP is a protected resource which the end user cannot access directly. As the end user cannot contact the SP directly, the MAG Series will act on behalf of the end user, performing the dual role of being the IdP and forwarding the SAML Assertion on behalf of the end user's browser.</td>
<td></td>
</tr>
<tr>
<td>- Only an IdP-initiated scenario is supported.</td>
<td></td>
</tr>
<tr>
<td>- The session with the SP is maintained at the MAG Series. User does not receive any cookies from the SP. All cookies are stored in the MAG Series device.</td>
<td></td>
</tr>
<tr>
<td>- All user traffic passes through the rewriting engine on the MAG Series.</td>
<td></td>
</tr>
<tr>
<td>- Since the session is maintained at the MAG Series, access to the session with the SP will be lost when the user logs out of the MAG Series, even though the session will still exist on the SP.</td>
<td></td>
</tr>
</tbody>
</table>

- This is the standard SAML deployment and both IdP-initiated and SP-initiated are supported.
- For IdP-initiated SAML external apps, SSO policies are used.
- For SP-initiated, just IdP and SP configuration under Sign-In are sufficient. No resource policy is required.
- The session with the SP is maintained at the end user browser.
- This mode requires direct access (i.e., without going through the rewriting engine) to the resource from the end user browser. The resource can be on the Internet, on a cloud, or in a protected corporate environment. In the case of a protected resource, a Network Connect/Windows Secure Application Manager (NC/WSAM) tunnel is required.
- In this case, users will continue to have access to the session at the SP even after logging out of the MAG Series, provided the resource is still reachable by the user.

The single logout feature is currently supported only when the MAG Series is set up as an SP.

MAG Series as an SP supports:
- Consumption (IdP initiated) where the MAG Series can consume the Single Logout generated by the IdP.
- Generation (SP initiated) of a Single Logout request, where the MAG Series generates a single logout.

MAG Series as Identity Provider (IdP)
Following is a case study of how MAG Series Junos Pulse Gateways running Junos Pulse Secure Access Service can be successfully set up as a SAML IdP to achieve SSO for users.

Flow Diagram
The diagram is a logical representation and explains the process a customer would follow in order to single sign-on users to one application. This method can be replicated for multiple applications, with each having a distinct Service Provider (SP) configured. The steps involved are as follows:
1. User goes to the login page hosted by the IdP.
2. User enters credentials to log in.
3. The password is verified by the authentication server. Authorization is also completed at this stage.
4. Upon successful authentication, the MAG Series launches a Network Connect (NC or VPN Connection) that gives the user an IP address from a pool while disabling split tunneling.
5. After obtaining an IP address, the user is presented with a page which has a bookmark for the application they want to access. The user then clicks on the bookmark.
6. Clicking on the bookmark triggers a SAML Assertion to be generated by the MAG Series, which acts as the Identity Provider (IdP). The SAML Assertion is sent to the corresponding Service Provider (SP). The SAML response is sent to the SP via HTTP POST through the user's browser. The SP consumes the SAML Assertion, and obtains the username to verify who is trying to access the application.
7. The SP then grants the user access to the application.
The following steps need to be completed when configuring the MAG Series to function as an IdP:

- Configure the IdP
- Set up the Service Provider information with which the IdP should communicate
- Configure the bookmark
- Configure the SSO information for the bookmark

**Setting Up IdP Configuration**

The Entity Id represents the IdP entity information and is auto populated based upon the host name configured on the device. The metadata validity indicates the number of days a peer SAML entity (SP for example) can cache this information. This metadata can be downloaded and imported by the SP as the IdP metadata information.

To set up the IdP further, go to: Authentication -> Signing In -> Sign-in SAML -> Identity Provider. The application uses POST mode for communication. Select the Signing Certificate. This certificate will be used to verify that the information sent is indeed sent by this IdP. This is the digitally signed certificate and the IdP provides the public key with which the SP can verify it. Do not select any Decryption Certificates.
In the “Other Configurations” section, check both of these boxes:

- Reuse Existing NC (Pulse) Session (which will aid in SP-initiated SSO)
- Accept Unsigned AuthnRequest

The “Service-Provider-related IdP Configuration” can be left at the default settings, as this will be overridden by the individual SP settings that will be configured later.

- Relay State—Leave this blank
- Session Lifetime—Configure it to be “Role Based”
- Sign-In Policy—Choose “*/”
- Force Authentication Behavior—Choose “Reject AuthnRequest”

User Identity

- Subject Name Format—Choose “Other”
- Subject Name—Configure “USERNAME”

Web Service Authentication

- Authentication Type—Choose “None”

Artifact Configuration

- Source ID—This field is auto populated
- Uncheck the box for “Enable Artifact Response for Signing and Encryption”

Figure 3: Sign-in SAML—identity provider settings
Setting Up the SP Information

Each SP can be added by clicking on the “Add SP” button tab under the “Peer Service Provider Configuration.” The Service Provider information can be configured manually or by using the information in the metadata file uploaded to the IdP.

![Figure 4: Adding SP information](image)

The metadata file can be uploaded under the section: System –> Configuration –> SAML.

![Figure 5: SAML global configuration](image)

Click on the “New Metadata Provider” to add the metadata file from any SP. When uploading the metadata file for the SP, the following options were chosen in this example:

- Specify location as “Local” and assign the location where the metadata file can be found
- Check the box for “Accept Unsigned Metadata”
- Select roles: “Service Provider”

![Figure 6: Uploading the metadata file of an SP on the MAG Series](image)
Once the metadata file has been uploaded, the SP can be configured as shown below. Select the Configuration Mode to be “Metadata” and then select the appropriate Entity Id from the drop-down menu. The metadata file will also have information on the method of communication—Artifact/POST.

![Figure 7: Configuring SP on the MAG Series using metadata](image)

When the “Manual” Configuration Mode option is chosen, the configuration will change as shown in Figure 8.

![Figure 8: Configuring SP on the MAG Series manually](image)

Carefully populate the Entity Id field and the Assertion Consumer Service URL information. Most SAML failures are related to an improper assertion consumer service (ACS) configuration URL.

The Relay state is used to identify the SAML Auth Server to which the user needs to authenticate. It contains the sign-in URL (or the relative path of the sign-in URL) of the MAG Series. RelayState in the case of an IdP-initiated scenario is a value that is agreed upon between the SP and IdP. In the case of a third-party SP, this information needs to be identified from the SP vendor and configured here. This field is SP specific, and some SPs may not require this information, in which case it can be left blank. In the case of SP-initiated SSO, the value from this configuration field is not used at all. In an SP-initiated case, the RelayState is dictated by the AuthnRequest sent by the SP. The RelayState is sometimes essential to configure (in some IdP-initiated SSO) but can be left blank most of the time.
The rest of the tabs can be configured as shown in the figure below.

**Figure 9: Setting up the SP on the MAG Series and specifying details**

**Configuring the Bookmark**

The bookmark can be configured under the User Roles or through Resource Profiles. The bookmark might need a Web ACL and Rewriting policy.

**Figure 10: Setting up bookmarks and user roles**
Configuring Resource Policies for SSO


Then choose the SAML External Apps instead of SAML (available under Web –> SSO) because the application does not need the MAG Series to be a gateway, and users can access the resource directly.
The policy is configured by clicking on the “New Policy” button. The Resources field is where the URL for the target resource is specified, while the specific SP with which to communicate is configured from the drop-down menu under: SAML SSO Details → Service Provider Entity Id. Select the appropriate role that should have access.

Since the end resources are in a protected environment and will be accessed via Network Connect only, the SSO policies are configured under SAML External Apps. The access to the end resource is through the NC tunnel and the resource is not rewritten via the rewrite engine.

**MAG Series as IdP Summary**

With this setup, when users log in with their credentials and click on the bookmark that is presented on their screen, they are able to Single Sign-On into the application via SAML 2.0. This setup supports both IdP-initiated SSO as well as SP-initiated SSO.

Single logout is not currently supported in this mode. If the user logs out of the SP, the session is not automatically terminated on the IdP and vice versa.

**MAG Series SSL VPN as Service Provider**

Following is a case study of how MAG Series Junos Pulse Gateways, running Junos Pulse Secure Access Service (SSL VPN), can be successfully set up as a SAML SP to achieve SSO for users.

**Flow Diagram**

The diagram below explains the process a customer would follow to allow or deny users access to the end application. A logical representation of the workflow is as follows:

1. User wants to access a protected application and therefore must log into the site. After clicking on login, the user is redirected to the Service Provider (SP) via a browser redirect.
2. The SP then redirects the request to the associated Identity Provider (IdP).
3. The IdP presents a login screen to the user in which the user enters login credentials.
4. The IdP performs an authentication against an authentication server and provides a response of either success or failure.
5. Upon successful authentication, the IdP then sends an SAML response with the SAML Assertion to the SP. This response is digitally signed in order to verify that the SP is indeed getting the information from the correct IdP. The response is also encrypted and only the SP has the private key to decrypt this information. This ensures a secure communication channel between the IdP and SP.

6. The SAML response is sent to the SP via HTTP POST through the user’s browser.

7. Host Checker verification is performed via the MAG Series at this point.

8. A response is provided depending upon whether the user meets the defined criteria.

9. On successfully passing the above preconditions, the MAG Series redirects the user to a MAG Series starter/landing page. The MAG Series also simultaneously launches a Network Connect (VPN connection) that gives the user an IP address from a pool while disabling split tunneling.

The following steps should be performed when configuring the MAG Series to function as an SP:

- Install the certificates to be used
- Configure the Authentication/Authorization Server
- Set up the Sign-In page

**Install Certificates**

There will be two certificates required to enable secure communication between the IdP (Identity Provider) and SP (Service Provider) within the realm of SAML 2.0. In this scenario, the MAG Series gateway will be the SP. The purpose of the two certificates are as follows:

1. One certificate is used to verify that the information sent is indeed sent by the corresponding IdP. This is the digitally signed certificate, and the IdP provides the public key. This information can either be part of the metadata file provided by the IdP or a separate certificate that can be uploaded to the MAG Series.

2. The second certificate is used to encrypt the SAML response with the assertion. The public key is provided to the IdP while the private key is stored on the MAG Series.
Installing the certificates for encryption involves the following steps:

1) Installing the Trusted Server CA to trust the self-signed certificate
2) Installing the self-signed certificate

Install the certificate authority (CA) information under the Trusted Server CA under: System –> Configuration –> Certificates –> Trusted Server CAs.

Figures 16 and 17 outline the details as to how this is accomplished.

![Figure 16: Installing a Trusted Server CA](image)

Once this is installed, the next step is to generate and install the self-signed certificate. Install the CA information under: Device Certificates. The path is: System –> Configuration –> Certificates –> Device Certificates.

The generated certificate should match the hostname or the fully qualified domain name (FQDN) for the MAG Series.

![Figure 17: Installing a certificate for encryption](image)

The public key for the self-signed certificate is installed on the IdP.

Installation of the public key that is used to verify the digitally signed certificate with the SAML response is shown in the next section, which describes set up steps for the SAML Auth Server.
Setting Up the Authentication Server

The next step is to configure the SAML Authentication Server. In order to configure the Authentication Server, go to: Authentication –> Auth Server, and then select SAML Server from the list as shown in Figure 18.

The following steps were used to populate the numerous fields under the SAML Server:

- Entity Id is automatically populated with the FQDN of the MAG Series gateway (from Network Overview) and the SAML endpoint.
  - https://rr-mdf-xxxxxxxxxxxxxxxx.net/dana-na/auth/saml-endpoint.cgi?p=sp1
- Enter the FQDN of the IdP Entity Id.
  - https://zit8665.development.xxxxxxxxxxxx.net/
- Enter the Identity Provider Single Sign-On Service URL. This is the URL at which the IdP accepts the SAML AuthnRequest.
  - https://zit8665.development.xxxxxxxxxxxx.net/JuniperSAMLTest/Login.aspx
- Ensure that the appropriate clock skew is set. Ideally the SP and IdP should be configured to use the same Network Time Protocol (NTP) server. The recommended value is 5 minutes. The reason the example was configured as 20 in Figure 19 was because the time difference was over 10 minutes.

The IdP information could also be set up using the metadata file. The metadata file from the IdP can be imported onto the MAG Series under: System –> Configuration –> SAML.

You can then select “New Metadata Provider.” This is similar to how it was set up in the previous scenario, but in this case the option Identity Provider needs to be checked instead of Service Provider.

The section below highlights the installation of the IdP certificate or the public key that is used for verifying the digitally signed SAML response:

- Upload the IdP certificate
  - zit8665.development.xxxxxxxxxxxx.net
- Check “Enable Signing Certificate Status Checking”
- Mark “Select Device Certificate for Signing” as “Not Applicable”
- “Select Device Certificate for Encryption” is the certificate for the FQDN of the MAG Series
  - Select “rr-mdf-xxxxxxxxxxx.net” from the drop-down menu
Use the Download Metadata button for a reference of SAML settings needed for the IdP.

Setting Up the Sign-In Page
The final step involves creating a Sign-In page. This is essential in order to map users to the realm and Authentication Server. The Sign-In policy maps to the realm and the realm maps to the Authentication Server. Therefore, a new realm will need to be created or any existing realm can be mapped to the SAML Auth server.

- Go to: Authentication –> Signing In –> Sign-in Policies and create a new Sign-In URL as “*/saml/”.
- The Sign-in page can be customized (please see the Custom Sign-In Page Solutions Guide).
- Create a Sign-In page as SAML Test by modifying the sample.zip file.
- Fill in the realm to which the user should be mapped and the “Sign-In SAML” for the Sign-In page.
- Add the path for the Sign-In page for SAML communication as shown in Figure 22.
Figure 22: Sign-In pages

Figure 23: Custom Sign-In page creation
APPLICATION NOTE - Implementing Single Sign-On Using SAML 2.0 on Juniper Networks MAG Series Junos Pulse Gateways

Figure 24: Sign-In policy

Figure 25: Sign-In page
Configuring the Sign-In URL is an essential step in setting up SAML communication. The message shown in Figure 26 is displayed if the Sign-In URL is not configured when posting the SAML assertion.

Figure 26: SAML error displayed when URL is missing

A Missing/Invalid sign-in URL error is shown when the RelayState does not map to a configured Sign-In URL, or it maps to a Sign-In URL that is not configured with a realm that has an SAML Server. It is important to note that for SAML authentication, there cannot be more than one realm mapped to the same Sign-In URL being used.

**MAG Series as Service Provider Summary**

With this setup, when the user logs in with credentials and succeeds against all levels of security checks, including authentication and Host Checker, SAML 2.0 allows that user to go directly to the cloud-based end application. The user experience is seamless, as SSO is achieved via browser redirects, which are completely transparent to the user. All communication happens on the back end in a secure yet nonintrusive manner. This setup supports both IdP-initiated SSO as well as SP-initiated SSO.

Single Logout is supported in this mode. If the user logs out of the SP, user credentials will need to be reentered before accessing the end application at a later time.

**Summary**

With the increasing adoption of cloud-based applications, SAML 2.0 helps alleviate a significant user burden by eliminating the need to enter credentials more than once. At the same time, it helps secure access to applications and other valuable resources in public, private, or hybrid clouds, ensuring the validity of user credentials before allowing access to resources. SSO allows users to enter their credentials only once in order to access multiple end applications, and it enables businesses to leverage an effective, identity-based security system.

Being able to deploy the Juniper MAG Series as an IdP or an SP provides an organization with added flexibility. The ability to combine encryption along with digital signatures ensures confidentiality and integrity of the user information along with guaranteeing non-repudiation – aspects that are critical to the success of cloud-based applications.
Appendix A

While the MAG Series running Junos Pulse Secure Access Service (SSL VPN) cannot generate SAML attributes, currently it can read simple attributes that are sent to it. Therefore, if the IdP sends attributes for the SP to filter along with the username, the MAG Series functioning as an SP is capable of performing this action.

The attributes are usually sent in “userAttr” format. In order to learn specifics of the sent attribute, use the policy trace feature. Once the attribute has been identified, it can be incorporated under the Role Mapping and filtered accordingly. Select Custom Expressions and click on Update. Then click on the tab “Expressions.” This will open another window as shown in Figure 27 below. Create a custom expression and save the changes. Map the user role for the role mapping rule created and save changes.

Figure 27: Role Mapping Rule for a custom expression

Figure 28: Creating a custom expression
References

About Juniper Networks
Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.