Configuring a SAML 2.0-based identity provider for Integrated Cyber Defense Manager

If you use a SAML 2.0-based identity provider, follow these steps to configure it in Symantec Integrated Cyber Defense Manager and in your identity provider.

For a video tutorial on configuring SAML 2.0-based identity provider for Integrated Cyber Defense Manager:

See Configuring Integrated Cyber Defense Manager with a SAML 2.0-based identity provider

Before you begin

- Log on to Integrated Cyber Defense Manager and select **ICDm > Settings > Access and Authentication**.
- Log on to your identity provider's administration console.

To configure a SAML 2.0-based identity provider for Integrated Cyber Defense Manager

- Table: Add and configure a new application for Integrated Cyber Defense Manager in the identity provider describes providing information from Integrated Cyber Defense Manager to the identity provider.
- Table: Configure the identity provider in Integrated Cyber Defense Manager details providing information from the identity provider to Integrated Cyber Defense Manager.

  Note the reverse order of the columns.

Table: Add and configure a new application for Integrated Cyber Defense Manager in the identity provider

Step	In Integrated Cyber Defense Manager	In the identity provider console
1	From the drop-down menu, select **SAML 2.0-based Identity Provider.**	Create a new SAML 2.0 application and enter an application name that reflects the access that you want to allow.
2	Copy the Relay State URL. This URL is the landing URL for the Symantec cloud console.	Paste the Relay State value into the **Relay State** field, which is sometimes called **Default Relay State**. SAML protocol considers this field as optional, but here, the Relay State URL is required.
3	Copy the single sign-on URL. URL values are also listed for **Audience URI**, **Service provider (SP) ID**, **Service provider (SP) ID**, **Single logout URL**, and **SP issuer**. If any of these values vary from the single sign-in URL, use it instead.	Paste the URL into the following fields for single sign-on: • **Single sign-in** • **Audience URI** This field is sometimes called **Reply URL** or **ACS URL**. • **Service provider (SP) ID** This field is sometimes called **Entity ID**. Paste the URL into the following fields for single sign-out: • **Single logout URL** This field is sometimes called **Logout URL**. • **SP issuer** Not all field names exist on all identity providers.

4	Copy the required assertion attributes that display on the screen.	Add the required assertion attributes: • **Name**: PartnerUserId **Value**: user.email This value may also be any unique value on the identity provider side. For example, it can be object_id for Azure. • **Name**: Email **Value**: user.email • **Name**: FirstName **Value**: user.firstName • **Name**: LastName **Value**: user.lastName
5	Copy the required group assertion attributes that display on the screen.	Add the required group assertion attributes: • **Name**: Groups **Filter**: Matches regex .* Azure administrators should follow Microsoft's instructions and set **groupMembershipClaims** to **All** or **SecurityGroup**. For details, see the section "Configure group claims for SAML applications using SSO configuration" on the following webpage: Configure group claims for applications with Azure Active Directory
6	Next to **Signature Certificate**, select **Download**. Save the file to your device.	This certificate is required for encryption and single sign-out. You may need to upload it under a field or property such as **SP Certificate**. Browse to the signature certificate file on your device, and then upload the certificate.
7		Add groups and users to the application.
8		Save your configuration.

The following table reverses the columns for an easier workflow.

Table: Configure the identity provider in Integrated Cyber Defense Manager

Step	In the identity provider console	In Integrated Cyber Defense Manager
1	Copy the URL for the identity provider's single sign-on URL. This URL is sometimes called **Login URL**.	Under **Sign-in URL,** paste the identity provider's single sign-on URL.
2	Copy the URL for the identity provider's single sign-out URL. This URL is sometimes called **Logout URL**.	Under **Sign-out URL**, paste the identity provider's single sign-out URL.
3	Copy the value for the **Identity Provider Issuer**. This URL is sometimes called **Identity Provider ID**.	Under **IDP Identity ID**, paste the identity provider's issuer ID.
4	Download the identity provider's verification certificate and save the file to your device. The certificate must be in the X.509 Base64 format.	Under **Verification Certificate**, select the upload icon to browse to the certificate file on your device, and then upload the certificate.
5	Copy the name from the group assertion attribute that you previously added.	Under **Assertion Attribute for the User Group Value**, paste the group assertion attribute name or the URI.

6	Locate the group name or group identifier (GUID) for your group. For example, use the group name in Okta, but use the GUID for Azure. To obtain the GUID for the group for Azure, see: Edit your group information using Azure Active Directory	Under **Portal Access Control**, select **Add**. Under **Group Name**, add the group name exactly as it appears in the identity provider. The group name is case-sensitive. For Azure, add the GUID for the group. Select the role that the users of this group have in Integrated Cyber Defense Manager, and then select **Add**. You can add more than one group. From the action menu, you can move up a group's priority or down, or you can edit or delete a group. The order of the groups represents the priority of roles, in instances where a user appears in more than one group.
7		Select **Save** and then select **Yes**.

You should then be able to log on to Integrated Cyber Defense Manager using your identity provider credentials. When you log on to Integrated Cyber Defense Manager for the first time, your account is created.

Once the users are created in Integrated Cyber Defense Manager, synchronization through SAML 2.0 does not further affect their assigned roles. To adjust the assigned roles for existing users in Integrated Cyber Defense Manager, go to **Endpoint > Settings > Administrators and Roles**.

See Changing identity providers in Integrated Cyber Defense Manager

See Configuring an identity provider