DEPLOYMENT GUIDE

Fortinet FortiSIEM and Entrust IDaaS Integration

FortiSIEM is an advanced security information and event management (SIEM) solution that combines advanced log and traffic analysis with performance and availability monitoring, change analysis, and accurate infrastructure knowledge to provide accurate threat detection, remediation, incident response, and compliance reporting. You can protect access to FortiSIEM by integrating it with **Identity-as-a-Service (IDaaS)**. Once integrated, users can use single sign-on to log in to their FortiSIEM account through IDaaS.

Note: This integration was tested using IDaaS version 5.33 and FortiSIEM version 7.0.2. Other versions of FortiSIEM may require integration and configuration steps that differ from those documented in this procedure. In the event of other issues, contact support@entrust.com for assistance.

To integrate FortiSIEM with IDaaS, you must do the following:

Step 1: Copy the SAML configuration from IDaaS.

Copy the SAML Configuration from IDaaS

1. Log in to your IDaaS administrator account.
2. Click ☰ **> Resources > Applications**. The **Applications Lists** page appears.
3. Under **SAML Cloud Integrations**, click **SAML Configuration**. The **SAML Configuration** dialog box appears.
   This dialog box contains the information you need to configure your SAML application for IDaaS authentication.
4. Do one of the following:
   - Leave this dialog box open for reference later in this procedure.
   - Copy the Entity ID, Single Sign-on URL, and Single Logout URL to a text file and save it for reference later in this procedure.

Note: Depending on the integration you are performing, you may not need all three of these SAML configuration values.

Step 2: Copy the SAML configuration from IDaaS

Copy a SAML signing certificate

1. Log in to your Identity as a Service administrator account.
2. Click ☰ **> Resources > Applications**. The **Applications List** page appears.
3. Under **SAML Cloud Integrations**, click **Signing Certificate**. The **Signing Certificates** page appears.
4. Click 📄 next to the certificate to copy it to the clipboard.
5. Open a text editor like Notepad and paste the certificate's contents into the text file.
6. Save the file.

Step 3: Configure FortiSIEM for IDaaS authentication

1. Log in to FortiSIEM as an Admin User.
2. Go to **ADMIN > Settings > General > External Authentication**.
3. Click **New**.
4. Under **Name**, give the name of the profile. Example: EntrustSAMLProfile
5. Under **Protocol**, select **SAML**.
   a. In the **Issuer** field, enter the Entity ID URL you copied in *Step 1: Copy the SAML configurations from IDaaS*.
   b. In the **Certificate** field, paste the certificate you copied in *Step 2: Copy the SAML signing certificate from IDaaS*.
   c. Leave the rest as default.

6. Click **Save**.
7. Go **to ADMIN > Settings > Role > SAML Role**
8. Click **New**.
9. In the Add SAML Role, enter the following information:
    a. From the **SAML Auth profile**, select the SAML profile created in step 5. Example: EntrustSAMLProfile
    b. In the **SAML Role** field, enter the SAML Role Example: Super
    c. In the **SAML Organization** field, enter the SAML Organization Example: Entrust
    d. From the **Mapped Role** drop-down list, select an existing role. Example: Executive
    e. From the **Mapped Organization** drop-down list, select an organization. Example: Super / Local
    f. (Optional) In the **Comments** field, enter any information you wish to reference at a future date.
    g. Click **Save**.
10. Go to **CMDB > Users**.
    a. If the SAML user is absent, click New to create a new user.
    Note: You may need to navigate to CMDB > Users > FortiSIEM Users.
    b. In the User Name field, enter the name.
    c. Click System Admin and set the Role.
        A. Under **Mode**, select External.
        B. Under **Profiles**, select Profile Create in Step 5. Example: EntrustSAMLProfile
        C. Under **Default** Role, select a role. Example: Executive
        D. Under **Contact** info, fill in required parameters like Email.
    d. When done, click **Save**.

Step 4: Add FortiSIEM as an application to IDaaS

Add FortiSIEM as an application to IDaaS

1. Log in to your IDaaS administrator account.
2. Click ☰ **> Resources > Applications**. The **Applications Lists** page appears.
3. Click **Add**. The **Select an Application Template** page appears.
4. Under **SAML Cloud Integrations**, click **FortiSIEM**. The **Add FortiSIEM** page appears.
5. Enter an **Application Name**.
6. Enter an **Application Description**.
7. Optional. Add a custom application logo.
    a. Click ⊕ next to the **Application Logo**. The **Upload Logo** dialog box appears.
    b. Click to select an image file to upload.
    c. Browse to select your file and click **Open**. The **Upload Logo** dialog box reappears, showing your image.
    d. If required, resize your image.
    e. Click **OK**.
8. Select the **Authentication Flow** that appears to users during login.
9. Click **Next**. The **General** page appears.
10. In the **Assertion Consumer Service URL** field, enter
    https://super_ip/phoenix/sso/saml/ExternalAuthenticationProfileName

Example: https://10.10.10.10/ phoenix/sso/saml/EntrustSAMLProfile

super_ip represents the FortiSIEM IP address you want to log into, and ExternalAuthenticationProfileName will need to be configured in FortiSIEM by a total Admin creating an SAML External Authentication Profile via **ADMIN > Settings > General > External Authentication** as in *Step 3, Configure FortiSIEM for Identity as a Service authentication*.

11. In the **Service Provider Entity ID** field, enter your organization name, for example, "Super."
12. Leave the **Single Logout Service URL** field empty.
13. Enter the **SAML Session Timeout** to the time when the SAML Assertion times out. The maximum is 720 minutes.
14. From the **SAML NameID Attribute** drop-down list, select User ID.
15. From the **SAML NameID Encoding Format** drop-down list, select UNSPECIFIED.
16. From the **SAML Signing Certificate** drop-down list, select the signing certificate you copied into FortiSIEM in *Step 3: Configure FortiSIEM for Identity as a Service authentication*
17. Deselect **Enable Go Back Button** if you do not want users to be able to go back to the FortiSIEM Enterprise login page to log in.
18. Add **SAML Attributes** as follows (you need to add two attributes):
    Add the First Name attribute as follows:

    f. Under **SAML Attributes**, click **Add**. The **SAML Attributes** dialog box appears.

    g. In the **Name** field, enter Email

    h. Click **Add** next to Value(s).

    i. In the **Values** field, type **<** and select **Email**.

    j. Click **Add**.
19. Leave the remaining settings at the default values.
20. Click **Submit**.

Step 5: Create a resource rule to protect access to FortiSIEM

Limitation: Resource rules for SAML applications cannot have resource rules with **External Authentication** set as the **First Authentication Step**.

Create a resource rule to protect access to a SAML application

1. Log in to your Identity as a Service administrator account.
2. Click ☰ **> Resources > Resource Rule**. The **Resource Rules List** page appears.
3. Click **+** next to the application you want to protect with a resource rule. The **Add Resource Rules** page appears.
4. Enter a **Rule Name** and **Rule Description** for the resource rule.
5. In the **Groups** list, select the group or groups of users restricted by the resource rule.
   These are the groups to which the resource rule applies. If you do not select any groups, the resource rule applies to all groups by default.
6. Click **Next**. The **Authentication Conditions Settings** page appears.
7. Optional: Select **Disable Single Sign-On for Application** to force users to re-authenticate when they attempt a new login.
8. Select **Enable Advanced Risk Factors** to add additional risk factors to the resource rule. The **Risk Factors** appear.
9. Do one of the following:
   - If you enable Risk Factors, follow **steps 10–17** to configure the risk factors.
   - If you do not need to configure risk factors, skip to **step 18**.

10. Click **Date/Time** to set the conditions as follows:

    a. Select one of the following:

    - **Allow Date/Time** to set when a user can access the application.

    - **Deny Date/Time** to set when the user cannot access the application.
      The **Date/Time Context Condition Settings** appear.

    b. Select the **Condition Type:**

    - **Specific Date Range Condition**—Allows or denies access to the application during a select period of days.

    - **Time-of-day and/or Day-of-Week Recurring Conditions**—Allows or denies access to the application on a specific time of day, day of the week, or both. Recurring times selected only apply to days not denied.

    - **Clear Selection**—Clears existing Date and Time conditions.

    c. Set the **Condition Type** settings as follows:

    i) Select **Use local time zone to use the local time zone** or deselect **Use local time zone to use the local time zone**, begin typing the time zone in the Begin Typing Time zone name field, and select the time zone from the drop-down list.

    ii) If you selected **Specific Date Range Condition**, click **Start Date** to select a start date from the pop-up calendar. Optionally, select the **End Date**.

    iii) If you selected **Time-of-Day and Day-of-Week**, click **Start Time** and select the start time from the pop-up clock. Optionally set the **End Time**. You must also choose the days of the week for the condition.

    d. Click **Save** to return to the **Authentication Conditions Settings** page.

11. Click **Geolocation** to set the **Location Condition Settings** as follows:

    a. Select **Allow** or **Deny** to create an allowed or denied country list.

    b. From the **Selected Countries** drop-down list, select the countries to add or deny access to the application. Repeat until you have added all the desired countries to the list.

    c. Select **Allow Anonymous IP Address** to increase the risk of users authenticating from an anonymous IP.

    d. Click **Save** to save to return to the **Authentication Conditions Settings** page.

> **Note:** Identity as a Service uses GeoLite2 data created by MaxMind, available from http://www.maxmind.com.

12. Click **Source IP Address.** The **IP Address Risk Setting** dialog box appears. Do one of the following:

    a. Select **Custom** and add the required **IP Allowed Addresses** and **IP Denied Addresses**.

    b. Select the **IP List Address** and select the IP List to allow or deny.

    c. Select **None** to not restrict any IP addresses.

    d. Click **OK** to return to the **Authentication Conditions Settings**.

13. Click **Machine Authentication** to set the **Machine Authentication Condition Settings** as follows:

    a. Set the **Machine Authentication Risk is less than or equal** to the value that the machine authenticator's total risk score must be less than during authentication to pass this condition.

The risk score is based on the attribute differences between a user's Machine Authentication information and that recorded on Identity as a Service before the condition fails. If an attribute does not match, the attribute incurs the number of risk points shown in **Non-Matching Risk Points** for that attribute. The **Non-Matching Risk Points** values of each non-matching attribute are added together, resulting in a total risk score. This score is normalized to be out of 100 as follows:

```
Total Risk Score = (Total Risk Points of Failing Attributes / Maximum Risk Points of All Enabled
Attributes) * 100
```

The resource rule condition fails when the number of non-matching risk points exceeds the Machine Authentication Risk value defined in this step. A value of 0 means that a single attribute difference causes the **Device Fingerprint** condition to fail. The default value is 3. The value between 0-50 can be entered.

The **Machine Risk Limit** defines the default value. See Manage machine authenticator settings.

b. Click **Save**.

14. Define the **Location History / Known Locations** and **Travel Velocity** conditions. The Risk-Based Authentication (RBA) settings of your Identity as a Service account define the location history and travel velocity conditions. See Manage risk-based authentication settings for more information.
15. Set the **risk score** for application conditions by clicking the dot next to the condition setting and sliding the risk scale to the risk percentage a user receives if they fail to meet the condition. The default setting is 0%. The Risk percentage determines the authentication requirements as set by the **Authentication Decisions**. When a user attempts to authenticate to an application, the final risk percentage is the sum of all failed conditions.
16. Set the risk threshold for **Medium Risk** and **High Risk** as follows:

    a. Click the risk threshold percentage to the right of **Medium Risk** or **High Risk**. The **Risk Threshold** dialog box appears.

    b. Enter the risk percentage.

    c. Click **OK**.
17. Set the **Authentication Decisions** for low, medium, and high risk as follows:

    a. Select the **first factor** from the drop-down list.
    The type of authenticator selected is the first authentication challenge a user must complete to access the application—the list of **Second Factors** authenticators available updates based on the type of **first-factor** authenticator selected.

    b. Click the checkboxes to select the Second Factor.

    The authenticators you select can be used to complete the authentication challenge.

    c. Click and drag the **Second Factors** authenticators for the risk level so they are ordered from top to bottom in order of preference.

    d. Repeat these steps for Medium Risk and High Risk.

> **Note:** You cannot add second factors to medium and high risk if you select **Deny Access** as the first factor.

18. If you do not enable advanced risk factors, select the **Authentication Settings** as follows:

    a. Select Skip Password or Password for the **First Factor** authentication method.

    b. Click and drag the **Second Factors** authenticators for second-factor authentication in order of preference.
19. Enable **Smart Login**. Smart Login is available only if your account has been enabled to allow Smart Login. Smart Login can authenticate to the Identity as a Service Admin Portal, User Portal, OIDC, and SAML applications integrated with Identity as a Service. See Protect applications with a resource rule for more information.

    a. Select **Enable Smart Login**.
    When you enable Smart Login, **first-factor**, and **second-factor** Authenticators are used for fallback authentication.

b. Select the **first-factor** authentication method used for fallback.
Entrust recommends using **Skip Password** for first-factor. If you do not want to enable fallback authentication, select **Deny Access** from the first-factor drop-down list.

c. Click the checkboxes to select the **Second Factors** used for Fallback authentication.
Entrust recommends selecting **Mobile Smart Credential Push** as the second-factor fallback authentication method. The authenticators you choose can be used to complete the authentication challenge.

d. Click and drag the **Second Factors** authenticators for the risk level so they are ordered from top to bottom in order of preference.

e. Repeat these steps for Medium Risk and High Risk.

> **Note:** You cannot add second factors to medium and high risk if you select **Deny Access** as the first-factor.

20. Optional: Select **Disable Single Sign-On for Application** to force users to re-authenticate when they attempt a new login.

> **Note:** This setting is only available for resource rules protecting IDaaS Administrator, User Portals, and SAML applications.

21. Optional: Click **Show KBA Advanced Settings** to modify the **Q&A challenge size** and **Number of Wrong Answers Allowed** for the resource rule. This setting is visible only if you select KBA for second-factor authentication and modify the Identity as a Service default settings for Knowledge-based authentication (see Modify knowledge-based authentication settings).
22. Click **Submit** to create your resource rule.

Step 6: Testing the integration

Testing IDaaS **redirect login**

1. Log in to your Identity as a Service account.
2. Go to your **My Profile** page.
3. Under **Applications**, click **FortiSIEM** Logo.
4. Respond to the second-factor authentication challenge. If you respond successfully, you are redirected to FortiSIEM.

www.fortinet.com

February 23, 2024 11:02 AM
2569617-0-0-EN