ServiceNow Email Integration with Apex Central / Control Manager

ServiceNow email integration with Apex Central / Control Manager allows you to send Apex Central / Control Manager threat detection notifications to your ServiceNow instance and automatically create new Security Incident Response activities. Apex Central / Control Manager sends email messages for event notifications to the ServiceNow email gateway, which parses the inbound email messages and creates corresponding Security Incident Response activities on your ServiceNow instance.

ServiceNow email integration involves the following:

Activating the Security Incident Response Plugin

ServiceNow email integration with Apex Central / Control Manager uses the **Security Operations** application, which is enabled by activating the **Security Incident Response** plugin.

Note

- You may skip this procedure if the **Security Operations** application is already enabled on your ServiceNow instance.
- For more information about configuring or troubleshooting your ServiceNow instance, refer to the ServiceNow documentation at:

  https://docs.servicenow.com/

Procedure

1. Log on to the ServiceNow console.
2. Go to **System Definition** > **Plugins**.
3. Find and click the **Security Incident Response** plugin.
4. On the **System Plugin** form, review the plugin details and then click the **Activate/Upgrade** related link.

   Note

   - If the plugin depends on other plugins, these plugins are listed along with their activation status.
   - If the plugin has optional features that depend on other plugins, those plugins are listed under **Some files will not be loaded because these plugins are inactive**. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).

5. (Optional) If available, select the **Load demo data** check box.

   Note

   - Some plugins include demo data—Sample records that are designed to illustrate plugin features for common use cases. Loading demo data is a good practice when you first activate the plugin on a development or test instance.
   - You can also load demo data after the plugin is activated by clicking the **Load Demo Data Only** related link on the **System Plugin** form.

6. Click **Activate**.

Importing and Committing the Email Parser Update Set

ServiceNow uses the Apex Central / Control Manager email parser update set to parse inbound Apex Central / Control Manager email notifications and create corresponding security incident entries.

Procedure

1. Download the Apex Central / Control Manager email parser update set from the following link:

   https://success.trendmicro.com/solution/1120090

2. Extract the XML file of the email parser update set.

3. Log on to the ServiceNow console.

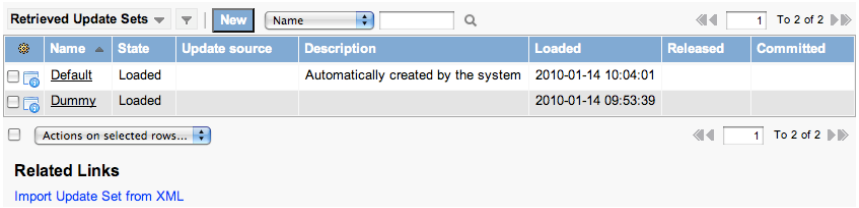
4. Elevate privileges to the **security_admin** role.

5. Go to **System Update Sets** > **Retrieved Update Sets**.

6. Click **Choose File** and select the extracted XML file of the Apex Central / Control Manager email parser update set.

7. Click **Upload**.

   The customization is now available as a retrieved update set with the **State** column displaying "Loaded".



8. Commit the update set:

   a. Go to **System Update Sets** > **Retrieved Update Sets**.

   b. Resolve any problems.

   Note

   You cannot commit an update set until all problems are resolved.

   c. Click **Commit Update Set**.

- Click **Cancel** to return to the preview and reevaluate the change.

  None of the updates are committed.

- Click **OK** to skip reevaluating the change and continue committing the changes marked as **Commit**.

A confirmation screen appears when ServiceNow successfully commits the update set.

Note

- If the update set contains one or more `DELETE`s for the schema, ServiceNow displays a warning. The warning lists up to five updates that may contain problems.
- If more than five updates have potential problems, ServiceNow provides a reference link.

---

d. (Recommended) Click **Commit Log** on the confirmation page, or go to **System Update Sets** > **Update log** and filter for the update set name.

- Look for warnings that contain the text **unsafe edit**. The system automatically skips any changes that results in data loss, such as changing the type of a field that contains data. You must manually make any of these changes, if necessary. Use caution when making changes that affect production data.
- Look for errors that indicate which records failed to commit and why. Create a new update set to address those failures, if necessary.

9. (Recommended) When you are no longer working on the update set, change the state to **Ignore**.

Important

For a completed update set on the production instance, always change the state to **Ignore**.

---

a. Go to **System Update Sets** > **Local Update Sets**.

b. Open the local update set record.

c. Change the **State** to **Ignore**.

The update set is not committed again when cloning the instance.

Configuring ServiceNow Email Integration

Important

Before configuring ServiceNow email integration with Apex Central / Control Manager, ensure you have completed the following prerequisites:

- *Activating the Security Incident Response Plugin on page 1*
- *Importing and Committing the Email Parser Update Set on page 2*

For more information about configuring or troubleshooting your ServiceNow instance, refer to the ServiceNow documentation at:

https://docs.servicenow.com/

Procedure

1. Prepare the ServiceNow email gateway:

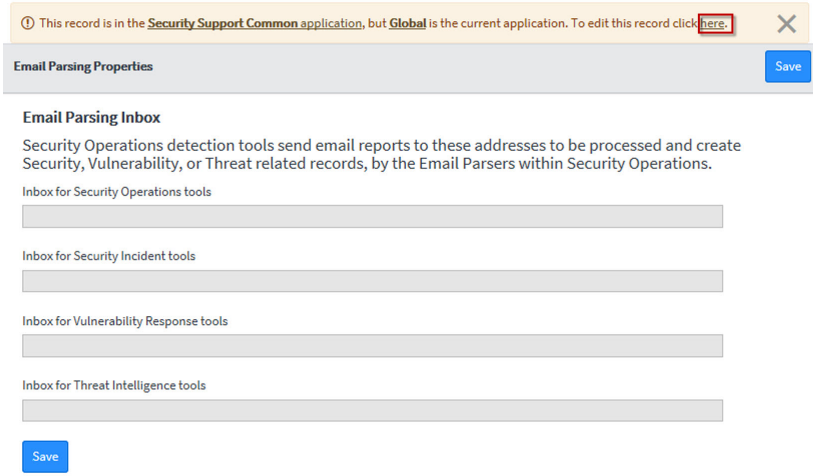
   a. On the ServiceNow console, go to **System Mailboxes** > **Administration** > **Email Accounts** > **ServiceNow SMTP**.

   b. Copy or write down the ServiceNow email gateway address displayed in the **User name** field.

   c. Go to **Security Operations** > **Email Processing** > **Properties**.

   The **Email Parsing Properties** form appears.

   d. Click the **here** link at the top of the **Email Parsing Properties** form to edit the record.



The current application switches to the **Security Support Common application** and the **Email Parsing Inbox** record becomes editable.

e. In the **Inbox for Vulnerability Response tools** field, provide the ServiceNow email gateway address obtained from the **ServiceNow SMTP** form.

f. Click **Save**.

2. Enable email receiving on the ServiceNow instance:

   a. On the ServiceNow console, go to **System Mailboxes** > **Administration** > **Email Properties**.

   b. In the **Inbound Email Configuration** section, select the **Yes** check box for the **Email receiving enabled** field.

3. Create a new ServiceNow contact group for Apex Central / Control Manager event notifications:

   a. Go to the **Contact Groups** screen.

      - On the Apex Central console, go to **Detections** > **Notifications** > **Contact Groups**.

- On the Control Manager console, go to **Notifications** > **Contact Groups**.

b. Click **Add**.

c. In the **Name** field, specify the name for the new ServiceNow contact group.

d. In the **Additional recipients** field, type the email address of your ServiceNow instance.

e. Click **Save**.

4. Assign the ServiceNow contact group to Apex Central / Control Manager event notifications:

a. Go to the **Event Notifications** screen.

- On the Apex Central console, go to **Detections** > **Notifications** > **Event Notifications**.
- On the Control Manager console, go to **Notifications** > **Event Notifications**.

b. Go to the event notification that you want to configure.

A new screen appears for the selected event notification.

c. In the **Recipients** section, select the newly created contact group from the **Available Users and Groups** list and add the group to the **Selected Users and Groups** list.

d. In the **Notification Methods** section, select the **Email message** check box.

Important

Do not customize the email subject or message content, or use a language other than English. Currently, ServiceNow email integration only supports English language email notifications and might not accept Apex Central / Control Manager email notifications containing modified email subjects or message contents.

e. (Optional) Click **Test** to verify the connection between the Apex Central / Control Manager server and ServiceNow email gateway.

f. Click **Save**.

5. On the ServiceNow console, go to **System Logs** > **Emails**.

   - If the **Emails** form displays the Apex Central / Control Manager test message or new Apex Central / Control Manager notifications, then the ServiceNow email integration completed successfully.
   - If the **Emails** form does not display any messages or notifications from Apex Central / Control Manager, check the SMTP server settings on the Apex Central / Control Manager console.

Viewing Security Incident Response Activities

Use the **Security Incidents** form to view Security Incident Response activities created for inbound Apex Central / Control Manager event notifications.

Note

For more information about responding to Security Incident Response activities, refer to the ServiceNow documentation at:

https://docs.servicenow.com/

Procedure

1. On the ServiceNow console, go to **Security Incident** > **Incidents** > **Show All Incidents**.

   The **Security Incidents** form displays all the new Security Incident Response activities.

2. In the **Short description** search box, type `Apex Central` or `Control Manager`.

3. Press `ENTER` to filter for Security Incident Response activities created for inbound Apex Central / Control Manager event notifications.

- The **Security Incidents** form only displays Security Incident Response activities created for inbound Apex Central / Control Manager event notifications.
- The **Short description** field displays the Apex Central / Control Manager event notification email subject.