



Securonix Cloud Documentation

22 November 2023

Contents

Administration Guide.	3
Creating and Managing Users.	4
Creating and Managing Groups.	6
Enabling Granular Access Control.	7
Enabling Password Control.	11
Connection Types.	12
Adding a New Connection.	12
Downloading Files.	18
Uploading Files.	20
Register Connectors.	21
Creating a New Workflow.	23
Approve Unmasking Request.	24
Administering Spark Jobs using Command Line.	27
Email Templates.	37
Workflows.	39
Enabling/Disabling Autodiscovery of Syslog Datasources.	43
Enabling or Disabling Multi-Factor Authentication.	43
Monitoring Event Activity.	44
Configuring Log Settings.	48
Job Monitoring.	49
Enable/Configure Data Masking.	55
Managing Data Dictionary.	59

Administration Guide

The Administration Guide is designed to help you configure, manage, and maintain Unified Defense SIEM. It contains information about Unified Defense SIEM components and how they work, various features and configuration settings, and how to configure and use Unified Defense SIEM.

Who This Guide is For

This guide is for system administrators and service providers who need information about how to monitor and administer the platform at a systems level, and business managers and other users in a supervisory role who need information about how to use Unified Defense SIEM to grant employees and partners access to applications, check for policy violations, and manage cases.

How This Guide is Organized

This guide describes how to administer the Unified Defense SIEM application. By the end of this guide, you will know how to manage crucial Unified Defense SIEM application settings, configure access control for SNPR users, run reports, monitor and troubleshoot Hadoop and Unified Defense SIEM components, and understand disaster recovery options.

[Creating and Managing Users](#)

[Creating and Managing Groups](#)

[Enabling Granular Access Control](#)

[Enabling Password Control](#)

[Connection Types](#)

[Creating a New Workflow](#)

[Approve Unmasking Request](#)

[Administering Spark Jobs using Command Line](#)

[Email Templates](#)

Workflows

Enabling/Disabling Autodiscovery of Syslog Datasources

Enabling or Disabling Multi-Factor Authentication

Monitoring Event Activity

Configuring Log Settings

Job Monitoring

Enable/Configure Data Masking

Managing Data Dictionary

Creating and Managing Users

Users, in the context of Access Control, refer to all users interacting with the SNYPR application.

This can be:


- Systems administrators responsible for the maintaining the platform
- Analysts responsible for managing threats
- Content developers responsible for developing use cases
- Compliance officers responsible for ensuring compliance with regulations like GDPR

When you use access control to create a user, you grant them permissions that determine what they can and cannot do in SNYPR.

Note

SNYPR gives users with the role, `ROLE_PRIVACYMASTER`, the ability to unmask (not unencrypted) masked data. When creating users and groups, enable the role `ROLE_PRIVACYMASTER` to use this feature.

To create a user

1. Go to **Menu > Administration > Access Control > Manage Users**.
2. Click  [Add New User]. The Create User dialog appears.
3. Provide the requested information. See [Create User / User Details dialog](#) for details.

Multi-factor authentication (MFA) can be enabled for a user only when MFA is enabled on the tenant. See [Enabling or Disabling Multi-factor Authentication](#).

1. Click **Save and Next**.
2. Set the Role sliders to **Yes** for all roles the user should be assigned.
3. Click **Save and Next**.
4. (Optional) Set the Group slider to **Yes** to assign the user to a group.

Note

You must enable at least one group to continue to step 4: Assign Notifications.

5. To create a new group:
 - a. Click **Add New Group**.
 - b. Provide the requested information. See [Create Group dialog](#) for details.
 - c. Click **Save** to save the new Group definition.
6. Click **Save and Next**.
7. Set the Enable sliders to **Yes** for all role notifications that the user should receive.
8. Click **Save**. The user appears on the [Access Control screen](#).

To change an existing user

1. Go to **Menu > Administration > Access Control > Manage Users**.
2. Under the User Name column, click a User Name link. The User Details dialog appears.

See [Create User / User Details dialog](#) for details.

3. Follow steps under [To create a User](#) (starting with step 3), modifying the existing User settings.

Creating and Managing Groups

A *group* is a collection of users who share a set of permissions. For example, a group called "Administrators" would be assigned permissions such as creating new users, changing passwords, and configuring application settings. Any user added to the Administrator group automatically inherits the permissions assigned to that group.

The permissions of a group are determined by the roles enabled for the group. Creating groups can be viewed as a shortcut to assigning roles to users; rather than assigning each role individually to each user, you can assign all the roles to a group and add users to the group.


Groups also provide greater control over data-level access using the [Access Control - Granular Access Control screen](#).

Note

SNYPR gives users with the role `ROLE_PRIVACYMASTER` the ability to unmask (not unencrypted) masked data. When creating users and groups, enable the role `ROLE_PRIVACYMASTER` to use this feature.

To create a new group

1. Go to **Menu > Administration > Access Control > Manage Groups**. The [Access Control - Manage Groups screen](#) appears.

2. Click  **[Add New Group]**. The Create Group dialog appears.
3. On the Enter Group Details page, provide the basic group information, then click **Save and Next**.
4. Proceed with the group definition procedure, assigning tenants, users, roles, and notifications as required. See [Create Group / Group Details dialog](#) for details.
5. When finished, on the Assign Notification to Group page, click **Save**. You return to the Manage Groups screen. The new group has been added.

To change an existing group

1. Go to **Menu > Administration > Access Control > Manage Users**. The [Manage Groups screen](#) appears.
2. Under the User Name column, click a User Name link. The Edit Group dialog appears.
3. On the Enter Group Details page, provide the basic group information, then click **Save and Next**.
4. Proceed with the group definition procedure, assigning tenants, users, roles, and notifications as required. See [Create / Edit Group dialog](#) for details.
5. When finished, on the Assign Notification to Group page, click **Save**. You return to the Manage Groups screen. The group has been updated.

Enabling Granular Access Control

Granular access control is used to restrict access for users at a data level. When granular access control is enabled, Unified Defense SIEM users will only see the users, resources, policies, and threat models to which they have been granted access.

Before You Begin

Before you enable Granular Access Control, you need to create users, roles, and groups. See [Defining Roles](#), [Creating Groups](#), and [Creating Users](#) for details.

To Enable Granular Access Control for a Group

1. Go to **Menu > Administration > Access Control**.
2. Click **Granular Access Control** from the left pane.
3. Set **Enable Data level Access Control** to **YES**.
4. Click the drop-down and select a Sec group to view tenant configurations:

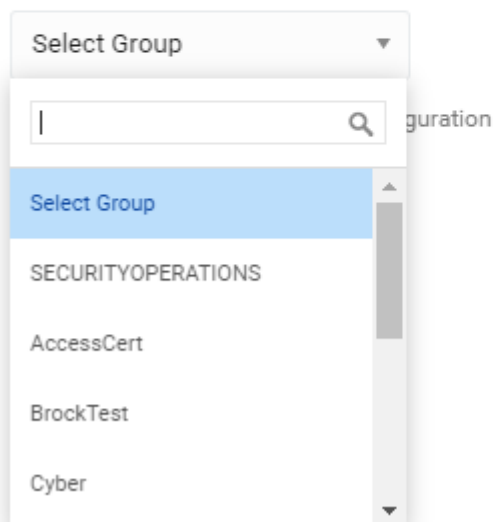
Granular Access Control

Enable Data level Access Control



Allow access control based on users, resources, policy categories and threat models.

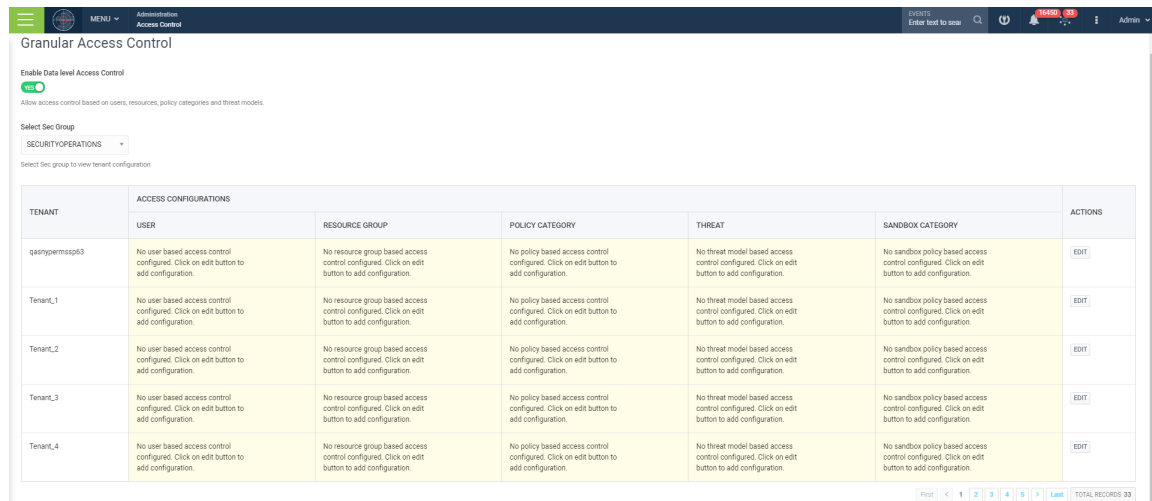
Select Sec Group



5. (Optional) You can edit the access configurations on this step. Do the following, depending on what action you want to take:

I want to edit access configurations

- a. Click **Edit** to modify access configurations for the selected Sec group.



The screenshot shows the 'Granular Access Control' interface. At the top, there's a header with 'Administration' and 'Access Control' tabs. Below the header, there's a section for 'Enable Data level Access Control' with a green 'ON' toggle. A dropdown menu for 'Select Sec Group' is set to 'SECURITYOPERATIONS'. Below this, a table displays access configurations for various tenants. Each row has columns for Tenant, User, Resource Group, Policy Category, Threat, Sandbox Category, and Actions. The 'Actions' column contains an 'EDIT' button for each row.

TENANT	ACCESS CONFIGURATIONS					ACTIONS
	USER	RESOURCE GROUP	POLICY CATEGORY	THREAT	SANDBOX CATEGORY	
qanyperrmsp3	No user based access control configured. Click on edit button to add configuration.	No resource group based access control configured. Click on edit button to add configuration.	No policy based access control configured. Click on edit button to add configuration.	No threat model based access control configured. Click on edit button to add configuration.	No sandbox policy based access control configured. Click on edit button to add configuration.	EDIT
Tenant_1	No user based access control configured. Click on edit button to add configuration.	No resource group based access control configured. Click on edit button to add configuration.	No policy based access control configured. Click on edit button to add configuration.	No threat model based access control configured. Click on edit button to add configuration.	No sandbox policy based access control configured. Click on edit button to add configuration.	EDIT
Tenant_2	No user based access control configured. Click on edit button to add configuration.	No resource group based access control configured. Click on edit button to add configuration.	No policy based access control configured. Click on edit button to add configuration.	No threat model based access control configured. Click on edit button to add configuration.	No sandbox policy based access control configured. Click on edit button to add configuration.	EDIT
Tenant_3	No user based access control configured. Click on edit button to add configuration.	No resource group based access control configured. Click on edit button to add configuration.	No policy based access control configured. Click on edit button to add configuration.	No threat model based access control configured. Click on edit button to add configuration.	No sandbox policy based access control configured. Click on edit button to add configuration.	EDIT
Tenant_4	No user based access control configured. Click on edit button to add configuration.	No resource group based access control configured. Click on edit button to add configuration.	No policy based access control configured. Click on edit button to add configuration.	No threat model based access control configured. Click on edit button to add configuration.	No sandbox policy based access control configured. Click on edit button to add configuration.	EDIT

You will be directed to the configuration screen.

- b. Set **Show only correlated data** to **YES** to enable a flag to see both correlated and uncorrelated data.
- c. Set **What users you want to grant access to?** to **YES** to select which users the group will be allowed to view.
- d. Provide the following information:
- **Search By:** Select a user attribute from the drop-down.
 - **Search Condition:** Select a condition from the drop-down.
 - **Provide Value:** Provide a value for the selected user attribute.
 - **Select Operator:** Select AND or OR.
 - **+/-:** Click to add/remove users.

Note

The group will only be able to see the users selected.

- e. Set **What resources you want to grant access to?** to **YES**.
- f. Check the box next to the resource(s) you want the group to be able to view.
Quickly search for the resource you want by typing in the **Type To Filter** bar.
- g. Set **What policy categories you want to grant access to?** to **YES**.
- h. Check the box next to the policy categories you want the group to be able to view.
- i. Set **What threat models you want to grant access to?** to **YES**.
- j. Check the box next to the threat model(s) you want the group to be able to view.
- k. Click **Save**.

I want to add access configurations

- a. Click **Add** in the **Actions** column.
- b. Complete the following information:

Granular Access Control

Enable Data level Access Control YES

Allow access control based on users, resources, policy categories and threat models.

Select Sec Group
DataXfiltrate

Select Sec group to view tenant configuration

TENANT	ACCESS CONFIGURATIONS					ACTIONS
	USER	RESOURCE GROUP	POLICY CATEGORY	THREAT	SANDBOX CATEGORY	
qtenpmsspg63	No user based access control configured. Click on edit button to add configuration.	No resource group based access control configured. Click on edit button to add configuration.	No policy based access control configured. Click on edit button to add configuration.	No threat model based access control configured. Click on edit button to add configuration.	No sandbox policy based access control configured. Click on edit button to add configuration.	[Add]
Tenant_1	No user based access control configured. Click on edit button to add configuration.	No resource group based access control configured. Click on edit button to add configuration.	No policy based access control configured. Click on edit button to add configuration.	No threat model based access control configured. Click on edit button to add configuration.	No sandbox policy based access control configured. Click on edit button to add configuration.	[Add]
Tenant_2	No user based access control configured. Click on edit button to add configuration.	No resource group based access control configured. Click on edit button to add configuration.	No policy based access control configured. Click on edit button to add configuration.	No threat model based access control configured. Click on edit button to add configuration.	No sandbox policy based access control configured. Click on edit button to add configuration.	[Add]
Tenant_3	No user based access control configured. Click on edit button to add configuration.	No resource group based access control configured. Click on edit button to add configuration.	No policy based access control configured. Click on edit button to add configuration.	No threat model based access control configured. Click on edit button to add configuration.	No sandbox policy based access control configured. Click on edit button to add configuration.	[Add]
Tenant_4	No user based access control configured. Click on edit button to add configuration.	No resource group based access control configured. Click on edit button to add configuration.	No policy based access control configured. Click on edit button to add configuration.	No threat model based access control configured. Click on edit button to add configuration.	No sandbox policy based access control configured. Click on edit button to add configuration.	[Add]

First 1 2 3 4 5 Last TOTAL RECORDS 33

- a. **Show only correlated data:** Disable this to see both correlated and uncorrelated data.

- b. **What users you want to grant access to?:** Enable to have all users visible.
- c. **What resources you want to grant access to?:** Enable to select which resources should be accessible.
- d. **What policy categories you want to grant access to?:** Enable to select which policy categories should be accessible.
- e. **What threat models you want to grant access to?:** Enable to select which threat models should be accessible.
- f. **What sandbox policy categories you want to grant access to?:** Enable to select which sandbox policy will be accessible.
- g. **Do you want to apply these categories only on incident?:** Select this option to display only incidents. If this option is not selected, then only the selected categories are displayed on SCC.

This option is only enabled when the **What sandbox policy categories you want to grant access to?** setting is enabled.

6. Click **Save Configuration**. Your changes appear on the Granular Access Control screen.

Enabling Password Control

For additional access control, you can enable password control options.

To Enable Password Control

1. Go to **Menu > Administrator > Access Control**.
2. Click **Password Control** from the left pane.
3. Set **Enable Password Control?** to **YES**.
4. Set the parameters required for passwords.

See [Password Control screen](#) for details.

5. Click **Save**.

Connection Types

Connection Types allow you to manage connections to third-party tools, and upload files to or download files from the Unified Defense SIEM directory, and register and edit existing connectors for data import. See [Connection Types screen](#).

You can add the following Connection Types:

- **Export Policy Violations:** Create a connection to export Unified Defense SIEM violation events as CEF to third-party applications including RSA Archer and RSA Netwitness. This option appears on the Actions for Violations screen when creating Policy Violations.
- **Threat Library:** Create a connection to the Threat Model Exchange database from which you can import new threat models and export threat models you created.
- **Response Connections:** Create connections to take actions on violations including export violations as CEF, to a database, to a remote server as a file, to a NPP (Nitro) tool, or to a syslog server.
- **Archival:** Create a connection to AWS to send archival data.

Next Steps

See [Adding a New Connection](#).

Connection Types

Adding a New Connection

You can add the following Connection Types:

Export Policy Violations

To configure a connection for CEF export, complete the following steps:

1. Navigate to **Menu > Administration > Connection Types**.
2. Click **+** from the left pane, then select **Add New Connection**.
3. Complete the following information:
 - **Connection Name:** Provide a unique name for the connection. Example: CEF Export.
 - **Connection Type for:** Select **Export Policy Violations** from dropdown.
 - **Connection Type:** Select **CEF Export** from dropdown.

Note

You may also select RSA Archer or RSA Netwitness to export CEF from Unified Defense SIEM. For information about integrating RSA Archer, see [Configuring RSA Archer GRC Platform](#). For information about integrating RSA Netwitness, see [Configuring RSA Netwitness](#).

4. Complete the following information in the **Connection Details** section:
 - **Protocol:** Enter connection protocol. Example: UDP.
 - **Host:** Enter the IP address to which you will export CEF data.
 - **Port:** Enter the port for the IP address to which you will export CEF data.
 - **Generate token:** Enable slider to **YES** to generate a token.

This will create a user called **siemuser** and a role called **ROLE_siemrole** under **Administration > Access Control**. This will also create a token that can be used to access the Unified Defense SIEM application from CEF Syslog.

You can create a device URL in CEF Syslog using this token.

```
https://<hostname>:<port>/Snypr/manageData/showUserSearch?token=${generated-token}&accountid=${destinationUserName}
```

Replace **<hostname>** with appropriate network address/domain name and **<port>** with port number.

5. Click **Save**. This new connection type becomes available in the left pane from which you can edit or delete connections.

Threat Library

To configure a connection for Threat Library, complete the following steps:

1. Navigate to **Menu > Administration > Connection Types**.
2. Click **+** from the left pane, then select **Add New Connection**.
3. Complete the following information:
 - a. **Connection Name**: Provide a unique name for the connection.

Example

Threat Model Exchange.

- b. **Connection Type for**: Select **Threat Library** from drop-down.
 - c. **Connection Type**: Select **Database** from drop-down.
4. Complete the following details in the **Connection Details** section:
 - a. **Database Type**: Select the database type from the dropdown.
Example: MySQL.
 - b. **JDBC URL**: Specify the JDBC URL.
 - c. **Driver Class**: Specify the driver class.
 - d. **Database Username**: Specify the username.
 - e. **Database Password**: Specify the password.
 5. **Test Connection** to ensure connection is successful.
 6. Click **Save**. This new connection type becomes available in the left pane from which you can edit or delete connections.

Response Connections

To configure a connection for response integrations, complete the following steps:

CEF Format

See instructions in [Export Policy Violations](#).

Database

See instructions in [Threat Library](#).

File

1. Navigate to **Menu > Administration > Connection Types**.
2. Click **+** from the left pane, then select **Add New Connection**.
3. Complete the following information:
 - **Connection Name:** Provide a unique name for the connection.
 - **Connection Type for:** Select **Response Connections** from drop-down.
 - **Connection Type:** Select **File** from drop-down.
4. Complete the following information in the **Connection Details** section:
 - **Import from Remote Server?:** Toggle to **YES** and complete the following fields to import from a remote server location:
 - **Remote Connection Type**
 - **Host IP Address**
 - **Port Number**
 - **Username**
 - **Password**
 - **Source Directory**
 - **Proxy Server?**
 - **Test Remote Connection**

- **Source Folder:** Provide the source folder from which to import the file. Default: \$Securonix_home/import/in.
- **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default: \$securonix_home/import/success/
- **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default: \$securonix_home/import/failed/
- Click **Save**. This new connection type becomes available in the left pane from which you can edit or delete connections.

NPP (Nitro)

1. Navigate to **Menu > Administration > Connection Types**.
2. Click + from the left pane, then select **Add New Connection**.
3. Complete the following information:
 - **Connection Name:** Provide a unique name for the connection.
 - **Connection Type for:** Select **Response Connections** from drop-down.
 - **Connection Type:** Select **NPP Nitro** from drop-down.
4. Complete the following information in the **Connection Details** section:
 - **Nitro Receiver Host:** Provide the host URL of the Nitro receiver.
 - **Nitro Receiver Port:** Provide the port for the Nitro receiver.
 - Securonix **Source IP Address:** Provide the IP Address of the Unified Defense SIEM application.

Note

You must first create a device type for Unified Defense SIEM on McAfee ESM with the application IP address to use this feature.

5. Click **Save**. This new connection type becomes available in the left pane from which you can edit or delete connections.

Syslog

1. Navigate to **Menu > Administration > Connection Types**.
2. Click **+** from the left pane, then select **Add New Connection**.
3. Complete the following information:
 - **Connection Name:** Provide a unique name for the connection.
 - **Connection Type for:** Select **Response Connections** from drop-down.
 - **Connection Type:** Select **Syslog** from drop-down.
4. Complete the following information in the **Connection Details** section:
 - **Protocol:** Enter connection protocol.
 - **Host:** Enter the IP address to which you will export syslog events.
 - **Port:** Enter the port for the IP address to which you will export syslog events. Default: 514.
 - **Facility:** Select from the dropdown. Example: Security/authorization messages.
5. Click **Save**. This new connection type becomes available in the left pane from which you can edit or delete connections.

Archival

To configure a connection to send archival data to AWS, complete the following steps:

1. Navigate to **Menu > Administration > Connection Types**.
2. Click **+** from the left pane, then select **Add New Connection**.
3. Complete the following information:
 - **Connection Name:** Provide a unique name for the connection.
 - **Connection Type for:** Select **Archival** from drop-down.

- **Connection Type:** Select **AWS** from drop-down.

4. Complete the following information in the **Connection Details** section:

- **Access Key:** Provide the alphanumeric key that uniquely identifies the user who owns the AWS account.
- **Secret Key:** Provide the alphanumeric secret key for the AWS account.
- **Bucket:** Click Test Connection & get buckets to get the AWS Bucket list.

5. Complete the following information:

- **Source Folder:** Provide the source folder where the file is located. **Default:** \$Securonix_home/import/in.
- **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. **Default:** \$securonix_home/import/success/
- **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. **Default:** \$securonix_home/import/failed/
- **Incremental Field:** Enable to allow incremental updates.
- **Prefix:** Specify the path within the bucket from which the logs must be extracted. You can use this to limit the response to folders that begin with the specified prefix.

Example

aws/AWSLogs/853268358782/CloudTrail/us-east-1/2017 limits the search to logs from 2017.

Next Steps

See [Downloading Files](#).

[Adding a New Connection](#)

Downloading Files

Use the this function to download files from Unified Defense SIEM directories to remote FTP, SFTP, or SCP remote host.

Download a properties file from "securonix/tenants/<tenantname>/securonix_home/response/activedirectory" to edit connection details.

To download a file, do the following:

1. Navigate to **Menu > Administration > Connection Types**.
2. Click **+** from the left pane, then select **Download File**.
3. Complete the following information:

Type text to filter

Total: 1

CEExport

No more results to display

Remote Connection Type*

FTP

Host IP Address*

<host>

Port Number*

21

Username

Password

Source directory*

File Name *

Download

- a. **Remote Connection Type:** Click the drop-down and select a remote connection type.
 - b. **Host IP Address:** Select the Host IP address to which to download the file.
 - c. **Port Number:** Provide the port number. Default: 21 of the host IP address.
 - d. (Optional) **Username:** Provide the username for the server.
 - e. (Optional) **Password:** Provide the password for the server.
 - f. **Source directory:** Provide the source directory from which to download the file.

securonix/tenants/<tenantname>/securonix_home/response/activedirectory.
 - g. **File Name:** Provide the file name to download.
4. Click **Download**.

Next Steps

See [Uploading Files](#).

Downloading Files

Uploading Files

Upload files from an FTP, SFPT, or SCP host into your Securonix_home directory. For example, you can add data files to your "\$securonix_home/import/in" folder to import from **Add Data > Activity**.

To upload a file, do the following:

1. Navigate to **Menu > Administration > Connection Types**.
2. Click **+** from the left pane, then select **Upload File**.
3. Complete the following information:

The screenshot shows the 'Upload File' form in the Securonix Administration interface. The form is titled 'Type text to filter' and has a search bar. Below the search bar is a list of items, including 'CEFEExport' and 'No more results to display'. The main form area contains fields for 'File' (with a 'Browse' button), 'Remote Connection Type' (a dropdown menu set to 'FTP'), 'Host IP Address' (a text field with a placeholder '<host>'), 'Port Number' (a text field with the value '21'), 'Username' (a text field), 'Password' (a text field with a password icon), and 'Destination directory' (a text field). An 'Upload' button is located at the bottom right of the form.

- **File:** Specify the file name and path or click **Browse** to select from local machine.
- **Remote Connection Type:** Click the drop-down and select a remote connection type.
- **Host IP Address:** Select the Host IP address from which to upload the file.
- **Port Number:** Provide the port number. Default: 21 of the host IP address.
- (Optional) **Username:** Provide the username for the server.

- (Optional) **Password**: Provide the password for the server.
- (Optional) **Destination directory**: Provide the destination directory into which to upload the file.

Example

```
securonix/tenants/<tenantname>/securonix_home/import/in
```

4. Click **Upload**.

Next Steps

See [Register Connectors](#).

Register Connectors

You can register a new connection in SNYPR to import data, or edit details about existing connections.

To import data, use the **Add Data** module of the Main Menu.

To register connectors, do the following:

1. Navigate to **Menu > Administration > Connection Types**.
2. Click **+** from the left pane, then select **Register connectors**.
3. Complete the following information:

The screenshot shows a web form for configuring a connector. It includes the following fields and controls:

- Connector Type***: A dropdown menu with a downward arrow and the text "-Select-". Below it is a small text instruction: "Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources."
- Connector description**: A text input field with a small edit icon on the right. Below it is a label: "Enter connector description".
- Connector Class***: A text input field with a small icon on the right. Below it is a label: "Enter connector class".
- Import Type***: A dropdown menu with a downward arrow and the text "-Select-".
- Enable Connector**: A toggle switch currently set to "No". Below it is a label: "Enable to make connection visible".

At the bottom right of the form, there are two buttons: "Cancel" and "Save".

- **Connector Type:** Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources.
- (Optional) **Connector description:** Enter connector description.
- **Connector Class:** Enter the connector class.
- **Import Type:** Click the drop-down and select an import type.
- (Optional) **Enable Connector:** Enable to make connection available for Unified Defense SIEM.

By default, the class files for connectors are present in the folder [Custom Location]/webapps/Snypr/WEB-INF/classes.

4. Click **Save**.

Towards the bottom of the screen, you can view the list of connectors available in Unified Defense SIEM. To edit default connectors, click the edit icon and complete the steps described above.



Enable to make connection visible


Cancel Save

Available Connectors

Connector type	Connector description	Connector class	Enabled	Actions
activedirectory	UserAD Connector	com.securonix.connector.user.ad.UserADConnector	true	
activedirectory	AD for ACCESS	com.securonix.connector.access.ad.AccessADConnector	true	
activedirectory	AD for User	com.securonix.connector.user.ad.UserADConnector	true	
akamai	Akamai Connector	com.securonix.connector.akamai.AkamaiConnector	true	
aws	AWS cloudtrail connector	com.securonix.connector.awscloudtrail.AWSCloudTrailConnector	true	
azurereport	Azure Report API Connector	com.securonix.connector.azurereport.AzureReportAPIConnector	true	
boxcontent	Box Content connector	com.securonix.connector.boxcontent.BoxConnector	true	
carbonblack	Carbon Black Json	com.securonix.connector.carbonblack.CarbonBlackConnector	true	
citrixapi	Citrix Monitor API	com.securonix.connector.citrix.CitrixAPIConnector	true	
clouderaaudit	Cloudera Audit Connector	com.securonix.connector.cloudera.ClouderaAuditConnector	true	

Creating a New Workflow

How to Get There

1. Go to **Menu > Administration > Workflows**.
2. Click  **Create new workflow**.

What it Does

Allows you configure a workflow to determine what actions a case analyst can take when an incident is created for a policy or threat violation.


Options

To create a new workflow

This section lists the minimum requirements necessary to configure workflows:

- [Import User Data](#)

- [Configure Access Control to create users](#)
- [Configure Access Control to create roles](#)
- [Configure Access Control to create groups](#)

1. Click  **Create new workflow**.
2. On the General Details screen, provide the basic information. See [Workflows Screen](#) for more information.
3. Click **Save & Next**.
4. Click **Add Action** to add an action for this step in the workflow. See [Add Action Dialogue](#).

Note

The Open case step for this workflow is already created by default You can customize or remove this step.

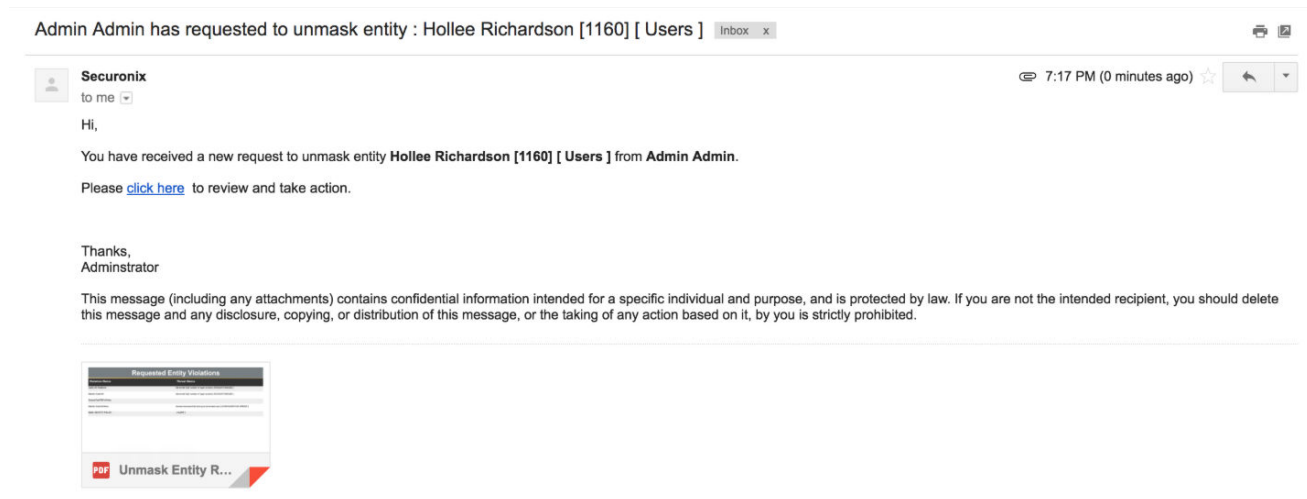
5. (Optional) Click the **Action Name** to open the [Edit Action dialog](#) where you can edit the actions properties.
6. Click **Add Workflow Step** to open the [Add Workflow Step dialog](#) where you can add step(s) to the workflow.
7. Click **Remove Action(s)** to open the [Remove Action\(s\) dialog](#) where you can remove steps from the workflow.
8. Click **Finish**.

Approve Unmasking Request

The **Unmasking Approval** option allows an approver to accept or reject data masking requests. Security analysts can request to unmask entities for a limited time period from **Security Command Center** by clicking **Take Action > Request to unmask entity**.

When an analyst sends a request to unmask an entity, (Undefined variable: General.SNYPR) displays a **Notification** and sends an email to the approver with the entity's violation details. The approver can open the approval interface and view unmasking requests pending approval, add comments to requests, and approve or deny requests.

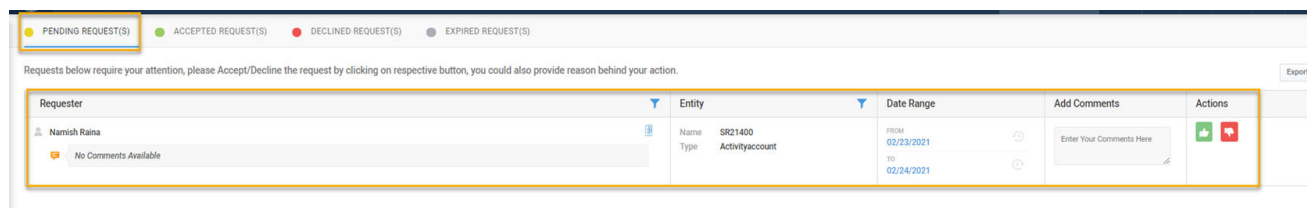
The **Unmasking Approval** screen can be accessed from **Menu > Administrator > Unmasking Approval**.



The Approver can click the link in the email to open the approval interface from which they can view unmaking requests pending approval, add comments to requests, and approve or deny requests.

Note

The Approver UI is accessible only to the Approver through the **Click Here** link in the email and an additional option on the Unified Defense SIEM Main Menu.



When an Approver approves the request, they can select the date range during which the analyst will have access to the unmasked entity, after which the entity will appear masked to the analyst.

● PENDING REQUEST(S) ● ACCEPTED REQUEST(S) ● DECLINED REQUEST(S) ● EXPIRED REQUEST(S)

Requests below require your attention, please Accept/Decline the request by clicking on respective button, you could also provide reason behind your action.

Requester	Entity	Date Range	Add Comments	Actions
[Redacted] unmask	Name: Kyla Douglas [1151] Type: Users	FROM: 05/10/2018 TO: 05/11/2018	<input type="text"/>	
[Redacted] Please unmask entity to remediate violation	Name: [Redacted] Type: Activityaccount	FROM: 05/10/2018 TO: 05/11/2018	<input type="text"/>	

The Approver can click to revoke the request at any time before the expiration date.

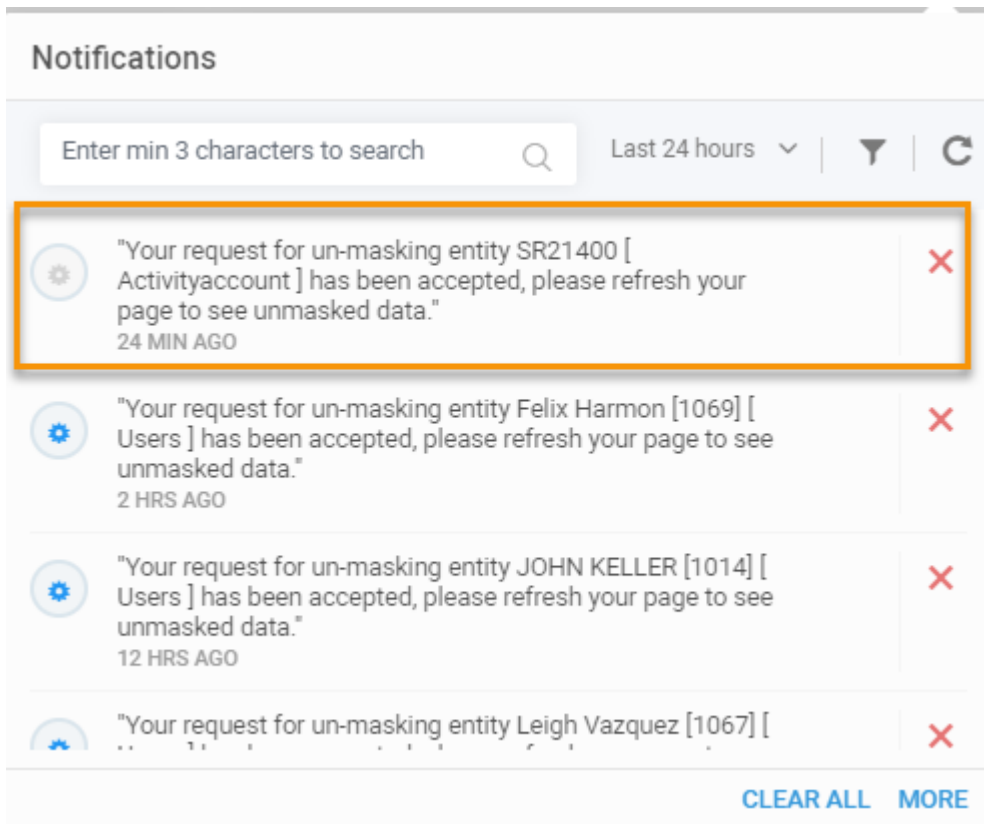
● PENDING REQUEST(S) ● ACCEPTED REQUEST(S) ● DECLINED REQUEST(S) ● EXPIRED REQUEST(S)

Requests below have been already accepted, requires no action.

Requester	Entity	Accepted By	Date Range	Actions
Admin Admin requesting access	Name: Elaina Lowe [1503] Type: Users	[Redacted] No Comments Available	FROM: 04/19/2018 TO: 04/20/2018	
Admin Admin Requesting unmasking of entity for investigation	Name: Hollee Richardson [1160] Type: Users	[Redacted] Approving this request for further analysis	FROM: 04/20/2018 TO: 04/21/2018	

Click to revoke

When the request is approved, Unified Defense SIEM sends an email, a notification appears in the security analyst's **Notifications**, and the violation record is unmasked.



Administering Spark Jobs using Command Line

To make changes to the Spark Job properties and run the Spark jobs:

1. Go to the installation folder designated during Installation.

Example

`"/Securonix/tenants/snypr/Sparkjobs/".`

2. (Optional) Edit Spark jobs parameters in the "snypr_apps.properties" file in `"/Securonix/tenants/snypr/Sparkjobs/conf/snypr_apps.properties"`.

`snypr_apps.properties`

The scripts to run each Spark job are converted to accept the configurations as arguments.

Configurable parameters:

- Name `(name)`
- Driver memory `(driver-memory)`
- Number of executors `(num-executors)`
- Executor Memory `(executor-memory)`
- Drive cores `(driver-cores)`
- Executor cores `(executor-cores)`
- Consumer group `(cg)`
- Max rate per partition `(mrpp)`
- Duration `(d)`
- HDFS user having access permission to HDFS
- Unique identifier to distinguish your jobs, attached as prefix to the name of each spark job initiated (tenant.id)

Example

If `tenant.id =CS` , the jobs runs as “CS_Event_Enrichment”

- Queue name

These configurations are maintained in the following file: “snypr_apps.properties”. You can edit this file to run your custom configurations for each job.

3. Execute the following command to run all Spark jobs at once: `sh`

```
snypr_apps.sh -a all
```

```
snypr_apps.sh
```

- Utility script to start the spark application by reading from the properties file, “snypr_apps.properties”.
- The script will start each application, wait for 20 seconds and check the status of the application. If it is in a **Running** state, then it generates a `<jobname.pid>` file with the applicationId of the application.

Example

```
jobname=CS_Event_Enrichment , then
CS_Event_Enrichment.pid will have the applicationId for
CS_Event_Enrichment
```

- If it is not in a **Running** state, then the `<Jobname=applicationId>` is stored in a file `<tenant.id_pending_apps.txt>`.

Example

```
CS_pending_apps.txt
```

- This file is checked again after 30 seconds to check if the application moved to a **Running** or **Failed** state. The logs for status check for pending applications are maintained in `< tenant.id_pending_apps.log>`.

Example

```
CS_pending_apps.log
```

- Following are the ways the script can start the spark application:

o -r (or) range: Series of applications at once. To start jobs from enrichment through behavior analytics, use:

```
sh snypr_apps.sh -r <from_number-to_number>
```

Example

- `sh snypr_apps.sh -r 1-4`
- `sh snypr_apps.sh -range 1-4`

o -i (or) initiate: Start individual jobs or a list of discontinuous jobs:

```
sh snypr_apps.sh -i <job_number>
```

Example

- `sh snypr_apps.sh -i 1`
- `sh snypr_apps.sh -i 1,5,9`
- `sh snypr_apps.sh -initiate 1,5,9`

o -a (or) alias: By alias:

```
sh snypr_apps.sh -a <alias_name>
```

Example

- `sh snypr_apps.sh -a enrichment`
- `sh snypr_apps.sh -alias enrichment`

- To start all applications:

```
sh snypr_apps.sh -a all
```

Example

```
[root@10-0-0-90 sparkjobs]# sh snypr_apps.sh -a all 17/05/18
12:11:12 INFO client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 CS_Event_Enrichment running
successfully, CS_Event_Enrichment.pid generated in /Securonix/
props_sparkjobs/logs 17/05/18 12:11:34 INFO client.RMPProxy:
Connecting to ResourceManager at 10-0-0-90.securonix.com/
10.0.0.90:8032 CS_Event_Ingestion running successfully,
CS_Event_Ingestion.pid generated in /Securonix/props_sparkjobs/
logs 17/05/18 12:11:55 INFO client.RMPProxy: Connecting to
ResourceManager at 10-0-0-90.securonix.com/10.0.0.90:8032
CS_Event_Indexer running successfully, CS_Event_Indexer.pid
generated in /Securonix/props_sparkjobs/logs 17/05/18 12:12:16
INFO client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 Warning:
CS_Behaviour_Analytics not running, appended to /Securonix/
```

```

props_sparkjobs/logs/CS_pending_app.txt 17/05/18 12:12:37 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 CS_Policy_Engine_IEE
running successfully, CS_Policy_Engine_IEE.pid generated in /
Securonix/props_sparkjobs/logs 17/05/18 12:12:58 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 CS_Policy_Engine_AEE
running successfully, CS_Policy_Engine_AEE.pid generated in /
Securonix/props_sparkjobs/logs 17/05/18 12:13:20 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032
CS_ThreatModel_RiskScoring_App running successfully,
CS_ThreatModel_RiskScoring_App.pid generated in /Securonix/
props_sparkjobs/logs 17/05/18 12:13:41 INFO client.RMPProxy:
Connecting to ResourceManager at 10-0-0-90.securonix.com/
10.0.0.90:8032 Warning: CS_Analytics_App not running, appended
to /Securonix/props_sparkjobs/logs/CS_pending_app.txt 17/05/18
12:14:02 INFO client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 CS_Behaviour_Profile running
successfully, CS_Behaviour_Profile.pid generated in /Securonix/
props_sparkjobs/logs Checking all pending app status, check /
Securonix/tenants/snypr/Sparkjobs/logs/CS_pending_app.log for any
further errors

```

- Execute the following command to terminate all Spark jobs at once: `sh snypr_apps.sh -t all CS`

-t (or) -terminate: To terminate a particular application, you can pass by range, one job number/list of jobs, alias, or kill all jobs for a particular tenant:

```
sh snypr_apps.sh -t <option> <tenantId>
```

Option 1: Terminate a continuous range of jobs:

```
sh snypr_apps.sh -t <start_job_num>-<end_job_num> <tenantId>
```

Example

```
sh snypr_apps.sh -t 1-4 CS
```

Option 2: Kill one job:

Example

- `sh snypr_apps.sh -t <job_num> <tenantId>`
- `sh snypr_apps.sh -t 4 CS`

Option 3: Kill a list of discontinuous jobs:

```
sh snypr_apps.sh -t <job_num1>,<job_num2>,<job_num3>.. <tenantId>
```

Example

```
sh snypr_apps.sh -t 1,5,8 CS
```

Option 4: Kill using an alias:

```
sh snypr_apps.sh -t <job_alias_name> <tenantId>
```

Example

```
sh snypr_apps.sh -t enrichment CS
```

Option 5: Kill all applications for a tenant:

```
sh snypr_apps.sh -t all <tenantId>
```

Example

- `sh snypr_apps.sh -t all CS`
- `sh snypr_apps.sh -terminate all CS`

Example

```
[root@10-0-0-90 sparkjobs]# sh snypr_apps.sh -t all CS 17/05/18
12:41:20 INFO client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 No such yarn application
with name = CS_Analytics_App present 17/05/18 12:41:21 INFO
```



```
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 No such yarn application
with name = CS_Behaviour_Profile present 17/05/18 12:41:22 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 killing CS_Event_Enrichment
17/05/18 12:41:23 INFO client.RMPProxy: Connecting to
ResourceManager at 10-0-0-90.securonix.com/10.0.0.90:8032 17/05/18
12:41:24 INFO client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 Killing application
application_1494916983246_0199 17/05/18 12:41:25 INFO
impl.YarnClientImpl: Killed application
application_1494916983246_0199 17/05/18 12:41:26 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 killing CS_Event_Indexer
17/05/18 12:41:27 INFO client.RMPProxy: Connecting to
ResourceManager at 10-0-0-90.securonix.com/10.0.0.90:8032 17/05/18
12:41:28 INFO client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 Killing application
application_1494916983246_0201 17/05/18 12:41:29 INFO
impl.YarnClientImpl: Killed application
application_1494916983246_0201 17/05/18 12:41:29 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 killing CS_Event_Ingestion
17/05/18 12:41:30 INFO client.RMPProxy: Connecting to
ResourceManager at 10-0-0-90.securonix.com/10.0.0.90:8032 17/05/18
12:41:32 INFO client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 Killing application
application_1494916983246_0200 17/05/18 12:41:32 INFO
impl.YarnClientImpl: Killed application
application_1494916983246_0200 17/05/18 12:41:33 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 killing
CS_Policy_Engine_AEE 17/05/18 12:41:34 INFO client.RMPProxy:
Connecting to ResourceManager at 10-0-0-90.securonix.com/
10.0.0.90:8032 17/05/18 12:41:35 INFO client.RMPProxy: Connecting
to ResourceManager at 10-0-0-90.securonix.com/10.0.0.90:8032
Killing application application_1494916983246_0204 17/05/18
12:41:36 INFO impl.YarnClientImpl: Killed application
application_1494916983246_0204 17/05/18 12:41:37 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 killing
CS_Policy_Engine_IEE 17/05/18 12:41:38 INFO client.RMPProxy:
Connecting to ResourceManager at 10-0-0-90.securonix.com/
10.0.0.90:8032 17/05/18 12:41:39 INFO client.RMPProxy: Connecting
```

```
to ResourceManager at 10-0-0-90.securonix.com/10.0.0.90:8032
Killing application application_1494916983246_0203 17/05/18
12:41:39 INFO impl.YarnClientImpl: Killed application
application_1494916983246_0203 17/05/18 12:41:40 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 killing
CS_ThreatModel_RiskScoring_App 17/05/18 12:41:41 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 17/05/18 12:41:42 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 Killing application
application_1494916983246_0205 17/05/18 12:41:43 INFO
impl.YarnClientImpl: Killed application
application_1494916983246_0205
```

- Execute the following command to check the status of all pending Spark jobs:
`snypr_check-pending-apps.sh`
 - Checks if the applications started by the `snypr_apps.sh` has moved to **“Running”** state and if in running state, generates `<jobname.pid>` file containing the applicationId of the application
 - Argument required:
 - File containing the jobname & applicationId `<tenant.id_pending_apps.txt>`

Example

```
CS_pending_apps.txt Usage: sh snypr_check-pending-apps.sh
CS_pending_apps.txt
```

Example

```
[root@10-0-0-90 sparkjobs]# cat logs/CS_pending_app.log 17/05/18
12:14:54 INFO client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 CS_Behaviour_Analytics
failed, try re-initiating
```

- Execute the following command to check the status of all Spark jobs: `sh snypr_apps.sh -s 1 CS`

-s (or) -status: To get status a particular application by specifying the jobnum or alias name:

```
sh snypr_apps.sh -s <job_num> <tenantId>
```

Example

- `sh snypr_apps.sh -s 1 CS`
- `sh snypr_apps.sh -s <alias_name> <tenantId>`

```
sh snypr_apps.sh -s enrichment <tenantId>
```

Example

```
[root@10-0-0-90 sparkjobs]# sh snypr_apps.sh -s 1 CS 17/05/18
12:21:32 INFO client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 17/05/18 12:21:33 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 17/05/18 12:21:34 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 Application Report :
Application-Id : application_1494916983246_0199 Application-Name :
CS_Event_Enrichment Application-Type : SPARK User : securonix
Queue : root.root Start-Time : 1495127477673 Finish-Time : 0
Progress : 10% State : RUNNING Final-State : UNDEFINED Tracking-
URL : http://10.0.0.90:43713 RPC Port : 0 AM Host : 10.0.0.90
Aggregate Resource Allocation : 2500214 MB-seconds, 1220 vcore-
seconds Log Aggregation Status : NOT_START Diagnostics :
[root@10-0-0-90 sparkjobs]# sh snypr_apps.sh -s 2 CS 17/05/18
12:21:54 INFO client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 17/05/18 12:21:56 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 17/05/18 12:21:57 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 Application Report :
Application-Id : application_1494916983246_0200 Application-Name :
CS_Event_Ingestion Application-Type : SPARK User : securonix
Queue : root.root Start-Time : 1495127498602 Finish-Time : 0
Progress : 10% State : RUNNING Final-State : UNDEFINED Tracking-
URL : http://10.0.0.94:34406 RPC Port : 0 AM Host : 10.0.0.94
```

```
Aggregate Resource Allocation : 2510521 MB-seconds, 1225 vcore-
seconds Log Aggregation Status : NOT_START Diagnostics :
[root@10-0-0-90 sparkjobs]# sh snypr_apps.sh -s 3 CS 17/05/18
12:22:11 INFO client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 17/05/18 12:22:12 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 17/05/18 12:22:14 INFO
client.RMPProxy: Connecting to ResourceManager at
10-0-0-90.securonix.com/10.0.0.90:8032 Application Report :
Application-Id : application_1494916983246_0201 Application-Name :
CS_Event_Indexer Application-Type : SPARK User : securonix Queue :
root.root Start-Time : 1495127520070 Finish-Time : 0 Progress :
10% State : RUNNING Final-State : UNDEFINED Tracking-URL : http://
10.0.0.91:43255 RPC Port : 0 AM Host : 10.0.0.91 Aggregate
Resource Allocation : 2489124 MB-seconds, 1214 vcore-seconds Log
Aggregation Status : NOT_START Diagnostics :
```

- Execute the following script to get logs for a particular application: `sh snypr_apps.sh -l <application_name>`

-l (or) -logs: To get logs a particular application:

```
sh snypr_apps.sh -l <application_name>
```

Example

- `sh snypr_apps.sh -l CS_Event_Enrichment`
- `sh snypr_apps.sh -logs CS_Event_Enrichment`

- Execute the following script to run the Spark applications in either multitenant mode or single mode: `sh snypr_apps.sh <script intializing parameters> -m <mode>`

-m (or) -mode: To run the spark applications in either "multi-tenant" mode to pass the dynamic parameters or "**single**" mode:

```
sh snypr_apps.sh <script intializing parameters> -m <mode>
```

Example

- `sh snypr_apps.sh -a all -m multitenant`
- `sh snypr_apps.sh -i 1 -m single`
- `sh snypr_apps.sh -r 1-9 -m multitenant`

Note

If the mode is not mentioned in the parameters, the applications will be initiated with mode specified in the properties file.

Tip

Files starting with **mt** are used to run the scripts in multi-tenant mode.

Email Templates


Email templates are used by administrators to send standardized responses and notifications via email. You can customize your own or use a default email template to build a notification email that best suits the needs of your organization. You can also add variables, which allow you to personalize these communications and include additional relevant information.

You can create new email templates to use in place of default templates for each type of activity.

Note

You will only be able to create templates for activity within modules that are already configured to send notifications.

To Create or Edit an Email Template

1. Go to **Menu > Administration > Email Templates**. To create a new email template, click  > **Create New Email Template**. To edit an existing email template, click the template link under the **Template Name** column.

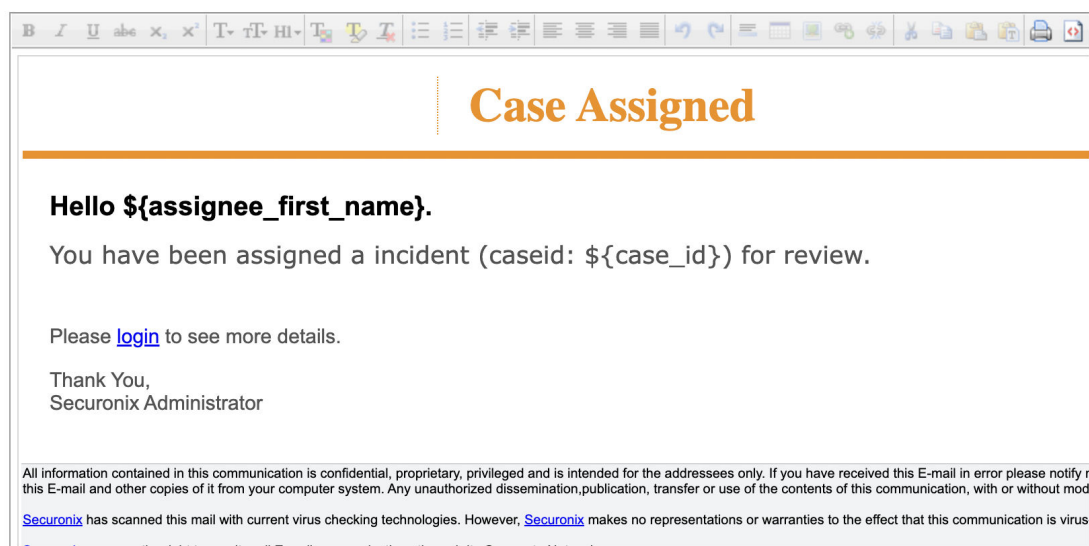
Tip

To filter the list of available templates by module, click the module name in the left panel.

Alternatively, select **Create New Email Template** while importing data, such as peer groups or watch lists, to open the **Create New Email Template dialog**, which contains the same options.

2. Add or edit the information requested on the [Enter Email Template Information screen](#) to define the template information.
 - The template must have a unique name.
 - Separate multiple email addresses with commas.
 - The module you select for the template will determine the variables that you can use in the email template. You will only be able to use variables for the module you select.
 - Click **Add Email Template Variables** to select from a list of variables to use as placeholders to populate the body of the email message with relevant personalized information. For example, the following template includes variables for the assignee's first name and case ID.

Add Email Template Variables



The main part of an email message containing the actual, arbitrary data such as text or images.

See [Email Template Variables](#) for a list of available variables.

3. Click **Save**. The updated email template is used, for example, when an incident is assigned for review.

Workflows

Unified Defense SIEM provides several default workflows to handle incidents and case management. Workflows determine the actions case analysts can take during each stage of the case management process.

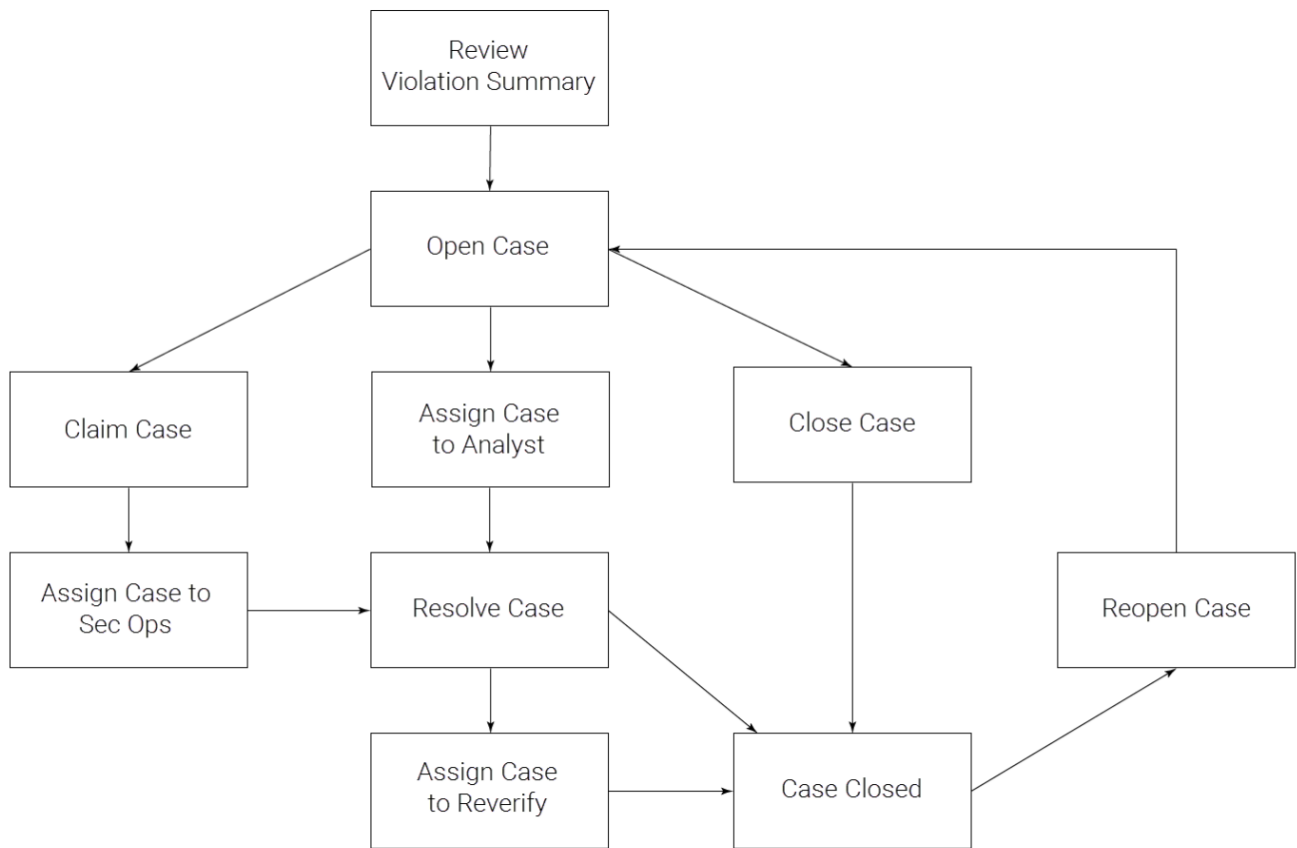
You can create custom workflows to take specific actions on cases, or you can make changes to the existing workflows. Workflows are invoked in the following screens within the application:

- Security Command Center (SCC): Workflows are invoked when an incident is created by an analyst for a policy or threat violation.
- Policy Violations: Workflows are invoked when a policy is configured to automatically generate an incident in the event of a violation.

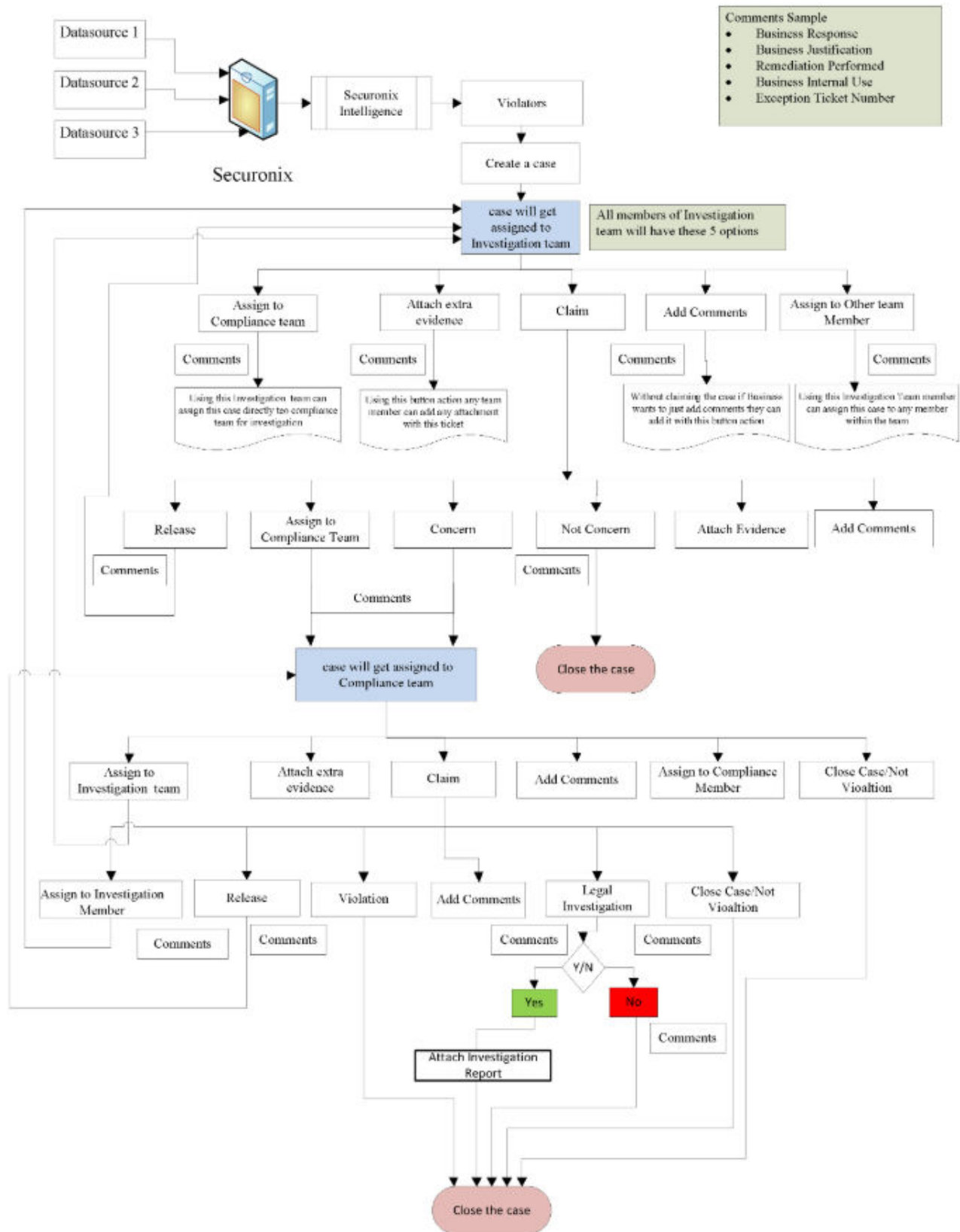
Sample Workflow

The diagram displays the following sample workflow:

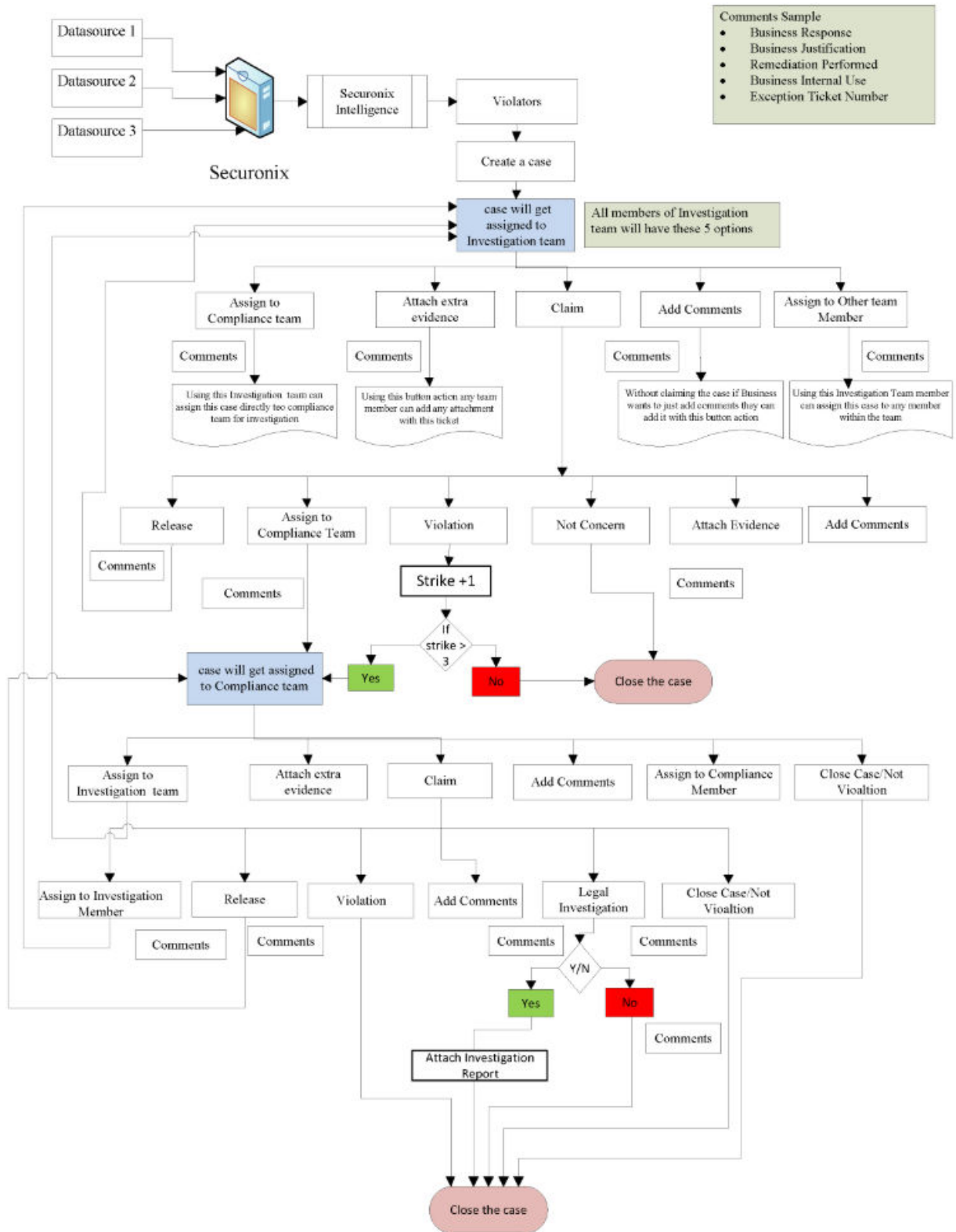
1. The user begins the case workflow by creating a case from the Security Command Center.
2. The user takes action to claim the case, assign the case to another analyst, or close the case.
3. The analyst to whom the case is assigned takes appropriate action to resolve the case.
4. The case is closed or assigned to another analyst to re-verify the resolution, or the user can reopen the closed case for further investigation. See [Incident Management](#) for more information about cases.



Example 1: Workflow for Investigation



Example 2: Workflow for Investigation With 3 Strike Rule

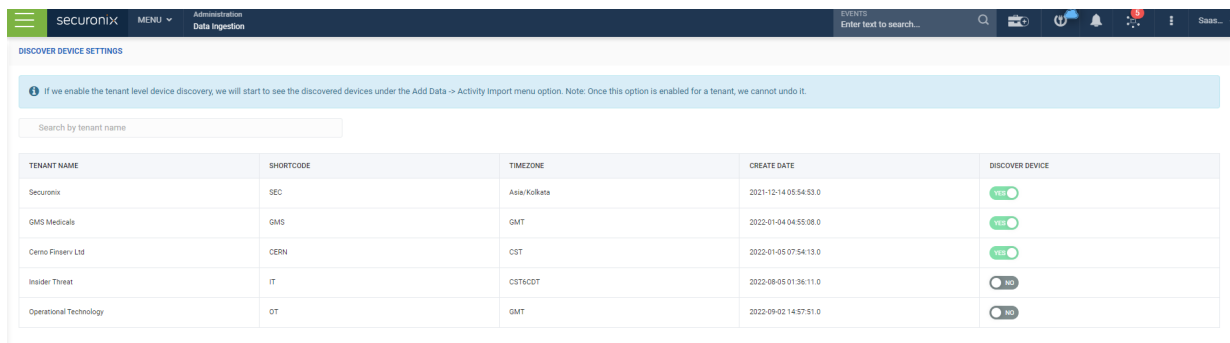


Enabling/Disabling Autodiscovery of Syslog Datasources

You can enable or disable autodiscovery of syslog based datasources.

To Enable/Disable Autodiscovery of Syslog Datasources

1. Navigate to **Menu > Administration > Settings**.
2. Click **Data Ingestion** from the left pane.



DISCOVER DEVICE SETTINGS

If we enable the tenant level device discovery, we will start to see the discovered devices under the Add Data → Activity Import menu option. Note: Once this option is enabled for a tenant, we cannot undo it.

Search by tenant name

TENANT NAME	SHORTCODE	TIMEZONE	CREATE DATE	DISCOVER DEVICE
Securonix	SEC	Asia/Kolkata	2021-12-14 05:54:53.0	YES
GMS Medicals	GMS	GMT	2022-01-04 04:55:08.0	YES
Cerno FinServ Ltd	CERN	CST	2022-01-05 07:54:13.0	YES
Insider Threat	IT	CST6CDT	2022-08-05 01:36:11.0	NO
Operational Technology	OT	GMT	2022-09-02 14:57:51.0	NO

3. Toggle to enable or disable the **Discover Device**. By default, the **Discover Device** is enabled.

Enabling or Disabling Multi-Factor Authentication

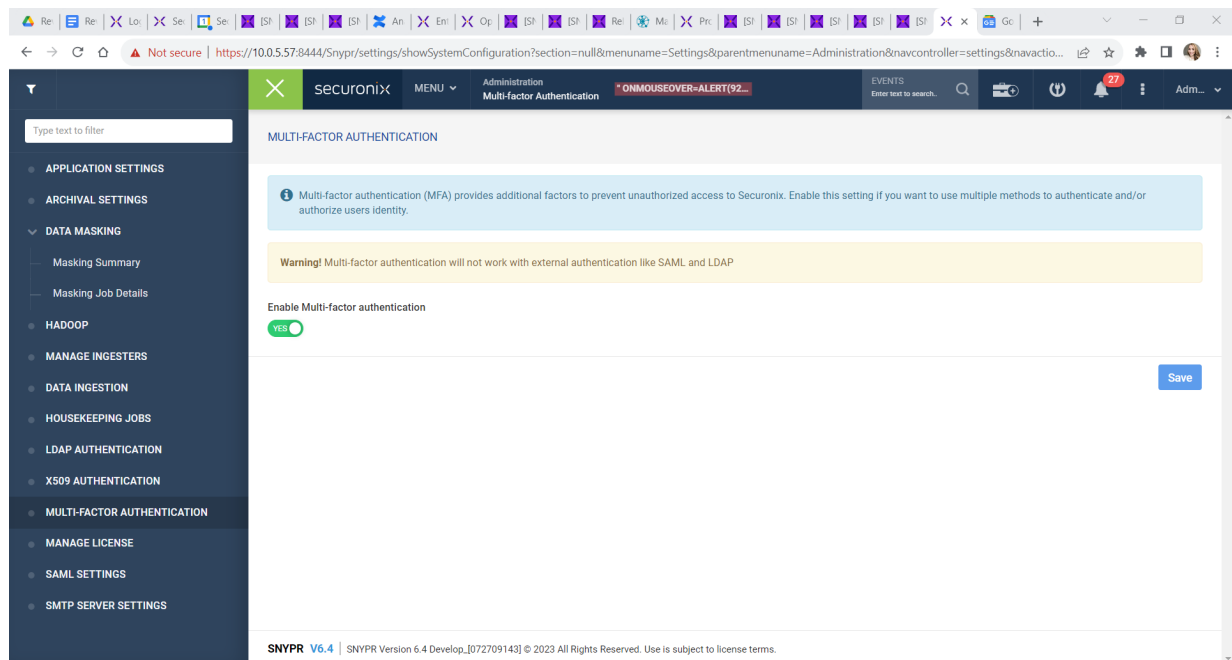
You can enable or disable multi-factor authentication (MFA) on the tenant. You can assign or reset multi-factor authentication for users in your organization only when multi-factor authentication is enabled. See [Manage Users](#).

Note

The Unified Defense SIEM application manages auditing for multi-factor authentication activity. See [Auditing your Unified Defense SIEM Environment](#).

To Enable or Disable MFA

1. Navigate to **Menu > Administration > Settings**.
2. Click **Multi-Factor Authentication** from the left pane.



3. Toggle to enable or disable the **Enable Multi-factor authentication**. By default, multi-factor authentication is not enabled.

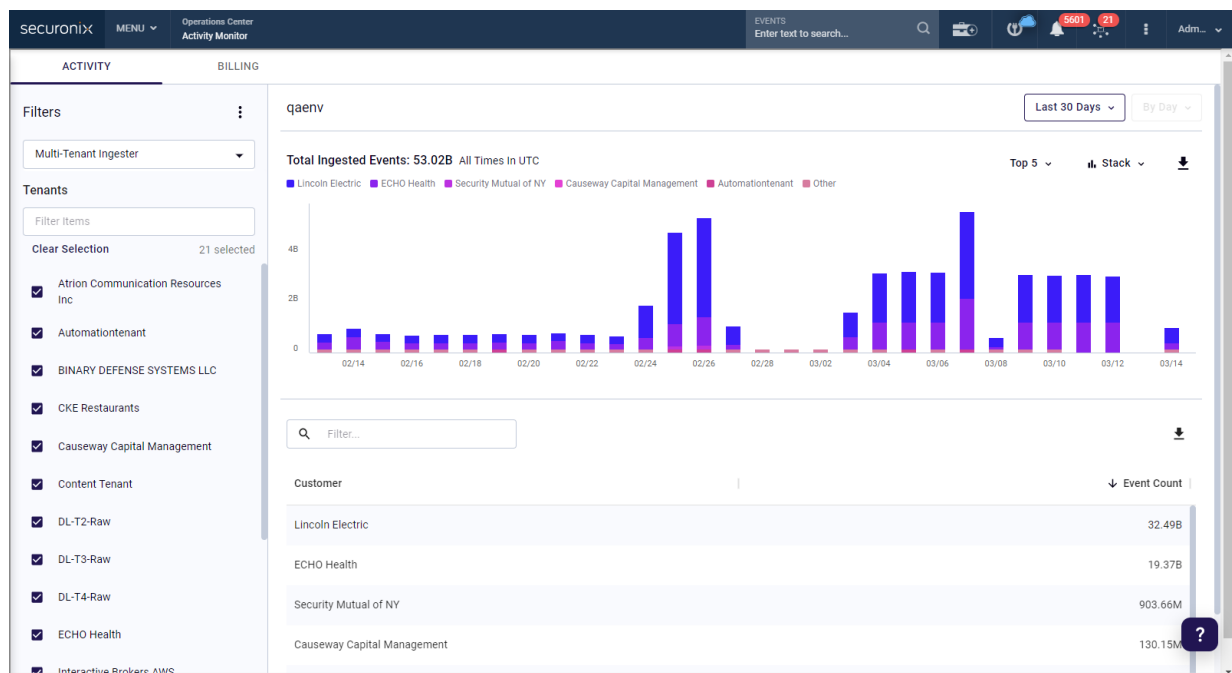
Monitoring Event Activity

Activity Monitor provides a crucial, real-time view of events ingested by SNYPR. Administrators can use this information to identify ingestion delays, interruptions, and sudden increases in number of events. You can filter events by tenant, datasource, ingester, time period, and graphical output type.

To Monitor Event Activity

1. Go to **Menu > Operations Center > Activity Monitor**.
2. Under **Filters**, select the Multi-Tenant Ingester and Tenants.
3. Click **Apply**.
4. Use the interactive dashboard to view the activity.

For example, the following image shows an example for **30 days** time period with **Top 5** datasources:




In the above image, events from ten datasources were ingested during the selected time period. The graph displays the first five datasources in different colors and provides the aggregate of the other five datasources in the green color. Additionally, the graph displays events by datasource in a table.

You can refer to **Time Since Last Event** to see how long ago data was ingested from a datasource. This information is important for administrator to investigate any delays during ingestion.

You can select a datasource from the **Graphical Data Display** section to view specific event details.

You can analyze events to determine if there are any unusual spikes or delays.

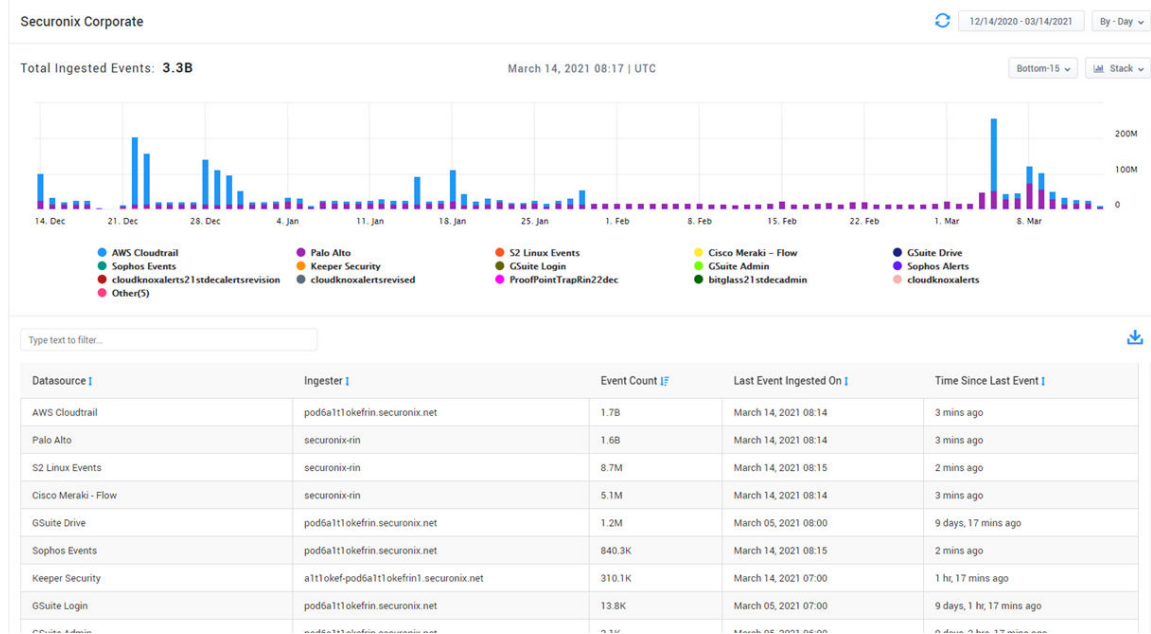
If required, you can download the summary in PDF and CSV format, and detailed report in the CSV format by clicking  .

See [Activity Monitor](#) for more details.

Filtering Events

Perform the following to sort events:

1. Go to **Menu > Operations Center > Activity Monitor**.
2. Select a tenant from **Customer**. The **Datasources** section displays the datasources available for that tenant.
3. Select any number of datasources or all datasources .
4. Click **Include** or **Exclude** selected datasources.
5. Select any or all ingesters.
6. Click **Include** or **Exclude** selected ingesters. By default, the screen displays top 5 records for the last 24 hours.
7. Select the following to view bottom 15 events:
 - Click the time period drop-down list to select the duration. In this scenario, **3 Months** is selected.
 - Select **By Day**.
 - Click **Bottom 15**.



8. Click  and select **Detail-CSV**. A report is downloaded.

A sample Detail CSV Report

	A	B	C	D	E	F	G	H	I	J	K	L
1	Securonix Corporate											
2	Report generated: December 14 2020 00:00 to March 14 2021 08:17											
3												
4	Date	AWS Clou	Palo Alto	S2 Linux E	Cisco Mer	GSuite Dri	Sophos Ev	Keeper Se	GSuite Log	GSuite Ad	Sophos Al	cloud
5	14-Dec-20	75878956	24399506	91796	51955	17903	6924		905	39	16	
6	15-Dec-20	18472213	14966552	90474	42198	41211	6278		734	30	15	
7	16-Dec-20	6909454	14869832	91379	96262	19075	6052		206	27	15	
8	17-Dec-20	8962393	15348497	92078	120240	14833	5441		188	29	13	
9	18-Dec-20	9182074	15197288	91264	84942	13186	5588		150	78	11	
10	19-Dec-20	1115052	2725767	16522	7494	2336	918		15		1	
11	21-Dec-20	4938626	7692257	47091	21880	5191	4034	1087	89	3	11	
12	22-Dec-20	1.9E+08	15047761	91226	46416	9697	8868	3818	169	17	18	
13	23-Dec-20	1.44E+08	14979323	91421	50408	21148	8945	20332	137	3	15	
14	24-Dec-20	6687135	14744887	91178	51553	3668	5192	1016	86	4	7	
15	25-Dec-20	5672482	14285534	91100	54946	412	3036	547	33		8	
16	26-Dec-20	5578920	14312989	90542	44461	251	64756	460	35		12	
17	27-Dec-20	5541439	14404232	90557	40242	4588	63610	400	28	3	7	
18	28-Dec-20	1.27E+08	14558167	91087	41253	21177	55709	1680	212	64	15	
19	29-Dec-20	99732629	12797098	80321	35841	3934	5846	805	153	50	10	
20	30-Dec-20	82303254	14711098	90117	74230	7615	8155	1883	165	6	7	
21	31-Dec-20	37836045	15111501	90485	41208	3365	35783	1901	116	28	8	
22	1-Jan-21	6517981	14949878	88563	40997	787	2087	388	41		3	
23	2-Jan-21	6017625	15120100	88503	42162	10321	11587	218	31	1	8	
24	3-Jan-21	5427919	17018306	87950	43210	681	80634	205	59		9	
25	4-Jan-21	10429839	23462445	90265	73035	21511	48974	1561	360	116	20	
26	5-Jan-21	14490172	16339831	92585	44017	15351	6128	1842	239	30	13	
27	6-Jan-21	3665830	5548081	32148	14594	2226	3216	319	51	3	5	

Configuring Log Settings

The Unified Defense SIEM application logs both errors and debug statements to a log file. The securonix.log file is located in the <TOMCAT_HOME>/logs directory. You can change the location of the securonix.log file to any desired folder.

To Log the securonix.log File

To specify the location of the log file:

1. Go to `<TOMCAT_HOME>/WEB-INF/classes`.
2. Search for a file named, "log4j.properties".
3. Open the file with a text editor.
4. To specify the location of the logs file, search for the following line under the # File Appender heading:


```
log4j.appender.file.file=.../securonix.log
```

5. Restart the application to begin logging to the new location.

To Change the Log Format

By default, the log file does not include the date on which the log was written. This is because of the following directive in log4j.properties:

```
log4j.appender.file.layout.ConversionPattern=%d{ABSOLUTE} %-5p [%c{1}] %m%n
```

Example

From securonix.log: 09:37:26,744 DEBUG [LoginController] auth. Getting license information

If you want to change this setting to include the date, use the following format:

```
log4j.appender.file.layout.ConversionPattern=%d{dd MMM yyyy HH:mm:ss,SSS} %-4r [%t] %-5p %c{1} %x - %m%n
```

Job Monitoring

Monitor the status of all jobs in SNYPR from the **Job Monitor** page. This page has various elements to help you view, filter, and configure your data import jobs.

To Monitor Jobs

1. Go to **Menu > Operations Center > Job Monitor**.

The latest Jobs by Connection appear. See [Job Monitor](#).

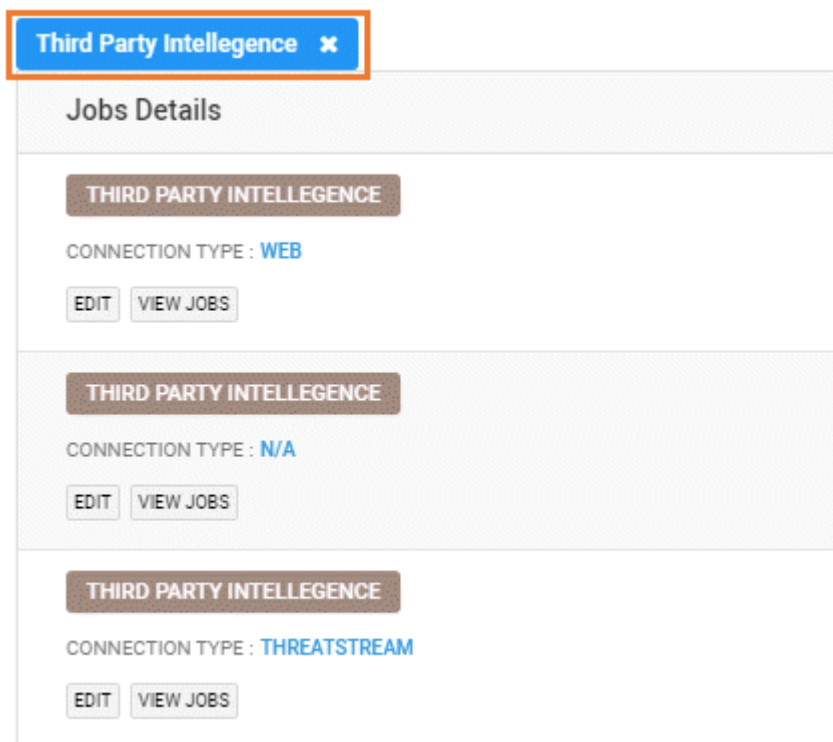
2. (Optional) You can take many actions in the **Job Details** column, all of which are listed below. Do the following, depending on what action you want to take:

Filter jobs by data import type

You can filter jobs by the selected data import type. For this example, the data import type is **Third Party Intelligence**. Click the data import type you want to view.

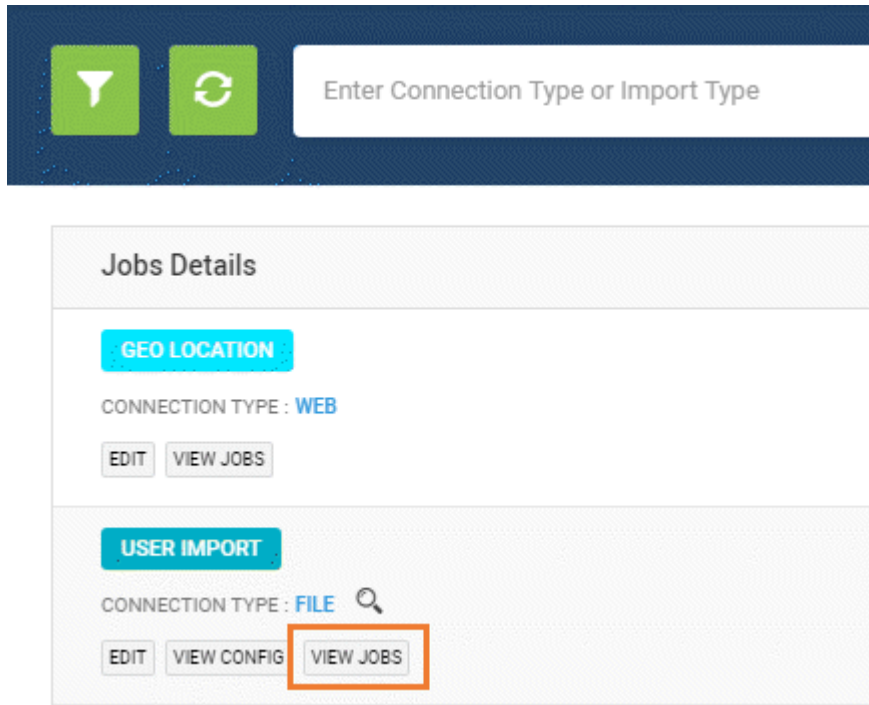
The page will update and only display results for the **Third Party Intelligence** data import type.

The data import type will display as a filter above the table. To delete this filter or go back to the list of jobs, click the 'X'.



Filter jobs by job type

You can filter jobs by job type. For this example, the job type is **User Import**. Click **View Jobs** to filter your list.



The **All Jobs** page appears and displays every job with the job type: **User Import**.
E To go back to the list of latest jobs, click **Back to Job by All Types** in the top right corner.

See [Job Monitor](#).

View today's statistics for my datasource.

Click the blue link next to **Datasource Name**.

ACTIVITY IMPORT

DATASOURCE NAME: **DIGITAL GUARDIAN USB** 🔍

TODAY'S STATICS	
PUBLISHED	542
PARSED	297
UNPARSED	245
INDEXED	297
STORED	297
CORRELATED	297
VIOLATIONS	10

Note

The **Datasource Name** only displays for certain jobs.

View configurations for my data import job

- Click **View Config** to view and edit the configuration for the data import job.

Jobs Details

GEO LOCATION

CONNECTION TYPE : **WEB**

EDIT **VIEW JOBS**

USER IMPORT

CONNECTION TYPE : **FILE** 🔍

EDIT **VIEW CONFIG** **VIEW JOBS**

- A pop-up appears with the configuration summary. Details on this screen include:

Configuration

✕

Activity Import Summary

DEVICE TYPE INFORMATION

Datasource Name ControlDS-21	IP Address Or Host Name
Vendor Securonix	Functionality TestCaseGroup2
Resource Type ControlDS2	

COLLECTION METHOD

Method
file

All Files Matching Condition
Prefix : TrafficAna

[Show more](#)

LINE FILTERS

POLICIES

SxTestCase10 - Beaconing-44 Available Through Datasource : ControlDS-21
SxTestCase11 - Randomly generated domains-44 Available Through Datasource : ControlDS-21
SxTestCase7 - Rare domain visits by an account-44 Available Through Datasource : ControlDS-21
SxTestCase8 - Rare user agent used by an account-44 Available Through Datasource : ControlDS-21
SxTestCase9 - Grouping customstrings by destinationhostname-44 Available Through Datasource : ControlDS-21
SxTestCase-New-Beaconing-43 Available Through Datasource : ControlDS-21

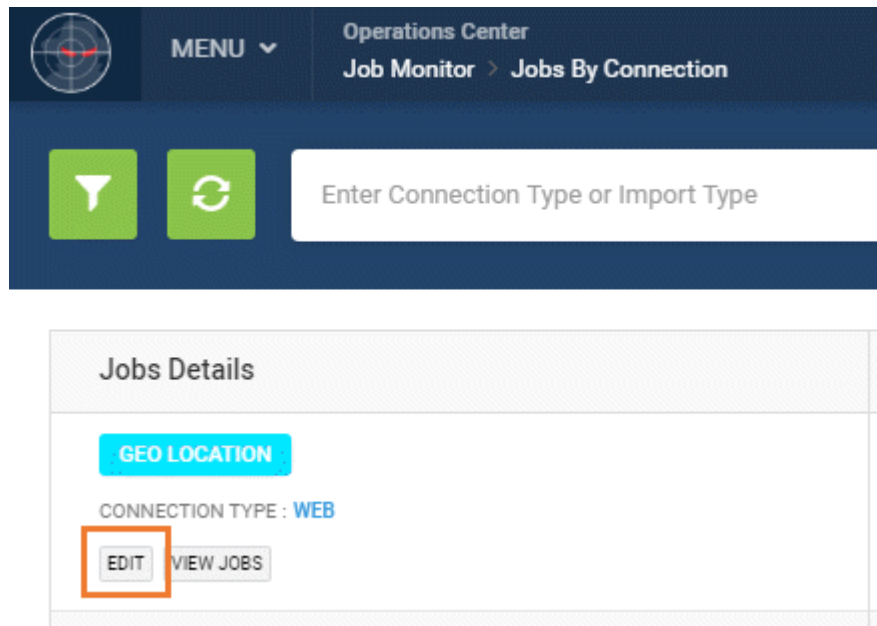
THREAT MODELS

i No Threat Models Available to configure Policy

- Device type information
- Collection method
- Line filters
- Correlation Rules
- Action filters
- Policies
- Threat Models

Edit my data import job

- a. Click the **Edit** button to edit information for the data import job.



- b. The **Activity Import** screen appears, where you can edit your existing data import configuration.

1 Datasource Parsing & Normalization Conditional Actions Identity Attribution Summary

Import activities from files, applications, databases, security products, network devices & other sources.

PREVIEW INPUT

← BACK TO DATASOURCES

DEVICE TYPE INFORMATION

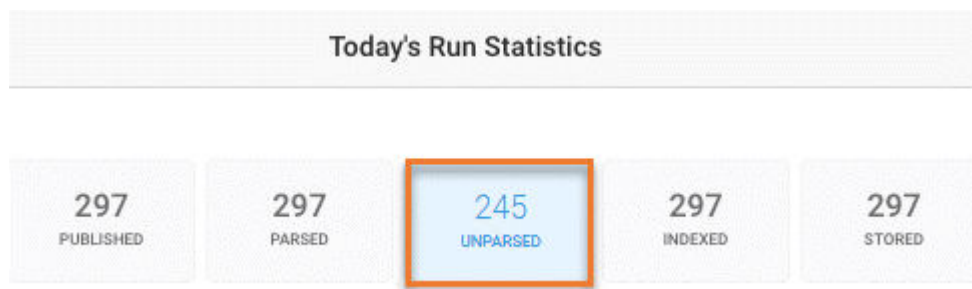
Vendor	Securonix
Functionality	TestCaseGroup2
Resource Type	ControlsDS2
Collection Method	Delimited-pipe [file]

CHOOSE IMPORT TYPE

Console

The actions you can take and information that displays in this column will vary per job.

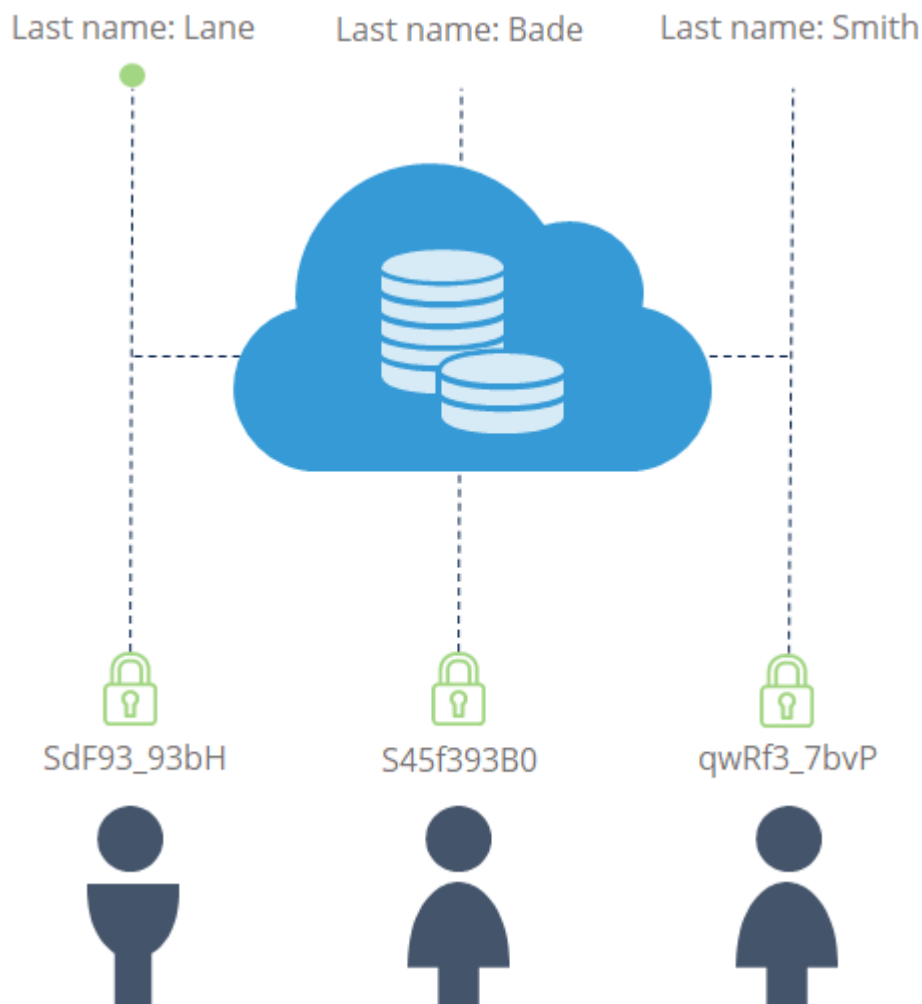
3. (Optional) There is only one button (**Unparsed**) in the **Today's Run Statistics** column that lets you view/modify additional information. Click **Unparsed** to view unparsed events for your datasource.



A popup allows you to **Select the Date, Download Events**, and shows you **Error Message Counts**.

Enable/Configure Data Masking

Data masking allows you to hide original data to protect sensitive information for users and entities, including activity and access accounts, resource names, IP Addresses, and other event attributes that could contain personally identifiable information (PII).



To mask data, do the following;

1. Navigate to **Menu > Administration > Settings**.
2. Click **Data Masking** from the left pane, then click **Masking Summary**.
3. By default, data masking is disabled. To enable and configure data masking, click **Edit**.

4. Complete the following information in the **Select Entities** section:

- a. **Mask Users Attributes:** Set to **YES** to mask attributes for all users.

The left panel lists the available user attributes that can be masked. To mask a user attribute, click the attribute name, then click the right arrow (>) to move the selected attribute to the right panel.

The example above masked **lastname** and **employeeid**. When you save and run the job, those user attributes will be masked as seen in the following image:

Enter your search criteria						
Employee ID ⓘ			First Name	Last Name	Manager Employee ID	Email
<input type="checkbox"/>						
<input type="checkbox"/>		EAF02F10BBAC26C0D2937ECAEAE29C17	HARRY	E54FD1C1AF47B2209EA5C37862DE36	1012	HARRY.OGWA@scnx.com
<input type="checkbox"/>		747875EF7C7E8BFA810E8C2E064C592	HOMER	85128E4B90B36CAA5D0E3F68750976F4	1001	HOMER.OGWAL@scnx.com
<input type="checkbox"/>		6936CD89E579E09DE4CD34A633A4A290	HILLARY	1E54FD1C1AF47B2209EA5C37862DE365	1001	HILLARY.OGWA@scnx.com

- b. **Do you want to enable conditional masking?:** Set to **YES** to mask all users data with conditional masking. When you set this field to **YES**, the following table will display:

The previous image is configured to mask all users whose **Department = Engineering**. When you run the job after enabling conditional masking on department= "engineering", all users who belong to the engineering department are masked as shown below:

Employee ID ⓘ			First Name	Last Name	Manager Employee ID	Email	Department	Division	Title
<input type="checkbox"/>									
<input type="checkbox"/>		73A7320F40621D5CA8B453D550CDB8D9	SEAN	706EC732AA71ABC56B43C3A7EB6E7026	1013	SEAN.connery@scnx.com	673885E37626A8C1D8954633AA0D1028	Global Technology	Associate-Data Services

c. **Mask Activity Account:** Set to **YES** to mask all the activity account names globally.

d. **Mask IP Address:** Set to **YES** to masks the IP address for all the datasources.

TUE, 22 AUG 2017 @ 02:59:37 PM resourcegroupname: Test-Cisco

accountname = JDOE@COMPANY.COM , transactionstring1 = IPSEC: Received a packet that failed anti-replay checking ,
ipaddress = 3B00F2C7C9166F95D2532C5E5879F9B8 resourcegroupname = Test-Cisco , rg_functionality = VPN , rg_vendor = Cisco System ,

e. **Mask Resource Name:** Masks all the resource names globally. The following figures shows an example a masked resourcename.

TUE, 22 AUG 2017 @ 02:59:37 PM resourcegroupname: Test-Cisco

accountname = JDOE@COMPANY.COM , transactionstring1 = Error processing payload , ipaddress = 192.168.1.57 , resourcegroupname = Test-Cisco ,
rg_functionality = VPN , rg_vendor = Cisco System , resourcename = 7E53866F69173F3531054F8D2353F06D

f. **Mask Access Account:** Masks all the access account names globally. If access accounts are enabled for masking, the access account names are masked for all datasources globally as shown:

TUE, 22 AUG 2017 @ 02:59:37 PM resourcegroupname: Test-Cisco

accountname = 09A6201E66DE56D3B1202555EB61FE93FACFDE94B25D6A58DB74DFE14A1B354B transactionstring1 = Error processing payload ,
ipaddress = 192.168.1.57 , resourcegroupname = Test-Cisco , rg_functionality = VPN , rg_vendor = Cisco System , resourcename = Test-Cisco

5. Click **Next**.

6. (Optional) Click **Add Datasource Attributes** to add the datasource attributes.

7. (Optional) Complete the following information in the **Add Datasource Attributes** pop-up:

a. **Select Datasource:** Click the drop-down and select a datasource.

b. **Datasource attributes to mask event data:** Click the datasource attribute(s) you want to mask from the left panel, and move them to the right panel by clicking the right arrow (>).

8. (Optional) Click **Add** to add the datasource attributes.

9. (Optional) Click **Add** to add the datasource attributes.
10. Click **Next**.
11. (Optional) Click **Add Datasource Attributes** to add the datasource attributes.

Note

The **Global Mode** settings for masking event attributes override the **Datasource Mode** settings.

12. (Optional) Do the following in the **Add Datasource Attributes** pop-up:
 - a. **Select Datasource:** Click the drop-down and select a datasource.
 - b. **Datasource attributes to mask event data:** Click the datasource attribute(s) you want to mask from the left panel, and move them to the right panel by clicking the right arrow (>).
13. Click **Save** run the job to enable masking in the user interface.

To read more about how to view the masking job summary, see [Masking Job Details](#) .

Managing Data Dictionary

Data Dictionary simplifies the ingestion process by providing easy to understand labels. All datasources of a functionality will have same labels. These labels provide uniformity to data ingested from multiple datasources of same functionality. Content developers can use these mapped labels to perform data ingestion and create policies.

As part of out-of-box content, Securonix provides functionalities with new labels mapped to Unified Defense SIEM attributes. You can view and edit these labels from the **Data Dictionary** screen.

Only users with role as **ROLE_CONTENT_ADMIN** can access the **Data Dictionary** screen. The role can be assigned from **Menu > Administrator > Access Control > User**.

User Details ✕

2 Enter User Information Assign roles Assign Tenants Assign groups Assign Notifications Prev Save & Next

ROLE_CONTENT_ADMIN Content Administrator	<input checked="" type="checkbox"/> YES
ROLE_CONTENT_ADMIN Content Administrator	<input type="checkbox"/> NO
ROLE_CONTENT_ADMIN Content Administrator	<input type="checkbox"/> NO
ROLE_CONTENT_ADMIN Content Administrator	<input type="checkbox"/> NO
ROLE_CONTENT_ADMIN Content Administrator	<input type="checkbox"/> NO

To edit labels for an existing functionality

1. Go to **Menu > Administration > Settings**.
2. Click **Data Dictionary** from the left pane. The **Data Dictionary** screen appears.
3. Select any functionality. The screen shows the Unified Defense SIEM attributes and mapped labels.



DATA DICTIONARY

Select Functionality

Securonix Application ▼

EVENT MESSAGE

Mapped Attributes Label	Label
transactionstring1	Transaction
customnumber16	
customnumber15	
customnumber14	
customnumber13	

4. Hover the mouse on a label. The  (edit) button appears.
5. Click  next to the label.

6. Modify the label name and click **Save**. The label is saved.

These labels provide meaningful context to content developers. It reduces the time to create policies as labels are informative and clear. For example, in the **Policy Violation** screen, the content developer can select the labels from the **Select Event Attribute** field to create new rules.

Note

You cannot create labels for a new functionality from this screen. You can create and map labels for a new functionality while configuring data ingestion from **Activity**.