



Securonix Cloud Documentation

22 November 2023

Contents

Data Integration Guide.	4
Importing User Data.	5
Connecting to User Data.	6
Importing User Data From a File.	7
Importing User Data From a Database.	8
Importing User Data Using LDAP.	9
Importing User Data From Active Directory.	10
Importing User Data From Azure Active Directory.	12
Importing User Data From Bamboo HR.	14
Importing User Data From Google Directory.	15
Importing User Data From Google BigQuery.	16
Importing User Data From Okta.	17
Importing User Data From One Login.	18
Importing User Data From Oracle IDM.	19
Importing User Data From Oracle Identity Analytics (OIA).	20
Importing User Data From Salesforce.	22
Importing User Data From Saviynt.	23
Importing User Data From Sailpoint.	24
Importing User Data From Splunk.	25
Importing User Data From Waveset IDM.	26
Importing User Data From Workday.	27
Configuring the User Import.	28
Running the User Data Import Job.	29
Reviewing and Managing Imported User Data.	31
Importing Activity Data.	31
Configuring the Datasource.	34

Managing Parsers, Normalizing, and Adding Conditional Action Filters.	44
Adding Identity Attribution Rules.	48
Detecting Policy Violations.	52
Reviewing the Summary and Running the Job.	52
Importing Entity Metadata.	55
Importing Watch Lists.	63
Lookup Tables.	65
Importing Lookup Data.	66
Third Party Intelligence.	74
Geolocation Network Map Data.	87
Import Geolocation.	88
Importing a Network Map.	94
Search Geolocation Using Spotter.	98

Data Integration Guide

The Securonix platform depends on connections to your organization's activity data and enrichment data. It must be configured with connector libraries to ingest this data from various sources, including antivirus tools, data loss prevention tools, identity and access management tools, SIEMs, third-party intelligence and other data sources to support the out-of-the-box and custom use cases in your environment. The Data Integrator establishes and maintains these connections.

A senior security professional, such as a SOC Manager or Security Architect, must manage ongoing operations and maintain the health of the SNYPR platform and Hadoop cluster (infrastructure). This guide describes how to determine the SNYPR deployment options in a Hadoop cluster, install SNYPR on Hadoop cluster, configure Hadoop components, configure the SNYPR application, configure datasources, ingest data, grant role-based access to the application, define business continuity and disaster recovery capabilities, and use SNYPR eye and monitoring capabilities of the platform to identify and troubleshoot common issues.

Who This Guide is For

This guide is for data integrators and deployment engineers responsible for implementing the Securonix platform within an organization.

How This Guide is Organized

This guide describes the process of ingesting and enriching data, and setting up datasources.

[Importing User Data](#)

[Importing Activity Data](#)

[Importing Entity Metadata](#)

[Importing Watch Lists](#)

[Lookup Tables](#)

[Third Party Intelligence](#)

Geolocation Network Map Data

Importing User Data

User identity data is information about the user such as first name, last name, department, division, title, manager. Unified Defense SIEM uses the user identity data to add context to events and activities. Additionally, this information is used during analytics to identify suspicious activities. User details from one or more identity data sources can be fed to the application.

Unified Defense SIEM ingests user identity data, correlates it, and detects anomalies indicative of different types of threats. Data ingested by the application is normalized and correlated to enable context-aware monitoring and analysis using advanced algorithms to identify threats.

Unified Defense SIEM provides connections to several different identity stores including directories, databases, delimited files, identity management systems, and identity governance technologies.

To Import User Data

1. **Configure the connection method for the tenant:** You can use an existing connection or create a custom connection. See [Connecting to User Data](#).
2. **Configure the User Import:** This requires:
 - Mapping the event data attributes with corresponding Unified Defense SIEM attributes.
 - Setting conditional actions for user life cycle changes, white listing, and pre/post actions on identity data.

See [Configuring the User Import](#).

3. **Run the job:** See [Running the User Data Import Job](#).
4. **Review the user data (optional):** Review the job status to ensure the data was uploaded successfully. See [Reviewing the Imported User Data](#).

Next Steps

See [Connecting to User Data](#).

Importing User Data

Connecting to User Data

Unified Defense SIEM imports user data using collection methods such as files, databases, or LDAP, as well as out-of-the-box premium connectors like Active Directory, Okta, and others.

Next Steps

See the following instructions for the collection method or connector you are using to learn how to connect it to Unified Defense SIEM for data import.

[Importing User Data From a File](#)

[Importing User Data From a Database](#)

[Importing User Data Using LDAP](#)

[Importing User Data From Active Directory](#)

[Importing User Data From Azure Active Directory](#)

[Importing User Data From Bamboo HR](#)

[Importing User Data From Google Directory](#)

[Importing User Data From Google BigQuery](#)

[Importing User Data From Okta](#)

[Importing User Data From One Login](#)

[Importing User Data From Oracle IDM](#)

[Importing User Data From Oracle Identity Analytics \(OIA\)](#)

[Importing User Data From Salesforce](#)

[Importing User Data From Saviynt](#)

[Importing User Data From Sailpoint](#)

[Importing User Data From Splunk](#)

[Importing User Data From Waveset IDM](#)

[Importing User Data From Workday](#)

[Connecting to User Data](#)

Importing User Data From a File

This topic describes how to import data to SNYPR from a delimited (comma or pipe separated) file.

Before You Begin

Prior to importing data from a file, ensure you have the following information:

- File Name, location, type (fixed length), file delimiter
- The connection method, host IP address, port number, credentials, and source directory if the file is located on a remote server
- The URL and credentials for the proxy server if the remote server is a proxy server

To Import User Data from a File

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **File**.
 - b. For Connection Name, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose the Remote Ingester name.

Note

The Console option is used only for file uploads from the browser for testing purposes.

4. Complete the requested information in the Connection Properties section. See [Connection Settings - File](#) for additional details.
5. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding SNYPR attributes and set conditional actions.

Connecting to User Data

Importing User Data From a Database

This section describes how to import data from a database, such as MySQL, MSSQL Server, and Oracle.

Before You Begin

Prior to importing data from Database ensure you have the following information:

- JDBC URL to connect to the Database (IP Address or host name, port number, Database name and type)
- Credentials to establish the connection

To Import User Data from a Database

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **Database**.

- b. For Connection Name, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.
4. Complete the requested information in the Connection Properties section. For example:
 - a. For **Database Type**, select **MySQL**.
 - b. For **JDBC URL**, enter the connection URL to connect your database.

Example

```
jdbc:mysql://hostname:port/database_name
```

- c. For **Driver Class** Enter the database specific class.
 - d. For **Database Username**, enter the user name for the database.
 - e. For **Database Password**, enter the password for the database.
 - f. For **SQL Query**, enter the SQL query for the data import.

Example

```
select  
employeeid,firstname,lastname,department,workemail from  
users
```

See [Select Connection - Database](#) for additional details.

5. Click **Save & Next**. the Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding Unified Defense SIEM attributes and set conditional actions.

Connecting to User Data

Importing User Data From LDAP

This section describes how to import data into SNYPR using LDAP (Lightweight Directory Access Protocol). SNYPR can connect using an LDAP or LDAP over SSL connection. The application uses an LDAP search to query the directory for the appropriate data. It requires an account with read permissions to perform the search. Follow the steps below to establish a connection, and import user identity data.

Before You Begin

Prior to importing data using LDAP, make sure to have the following information:

- Host name
- Credentials to establish LDAP connection (username and password)
- Domain

To Import User Data From LDAP

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **LDAP**.
 - b. For Connection Name, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.
4. Complete the requested information in the Connection Properties section. See [Connection Settings - LDAP](#) for additional details.
5. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding SNYPR attributes and set conditional actions.

Connecting to User Data

Importing User Data From Active Directory

This section describes how to import data from Active Directory.

Before You Begin

Prior to importing data from Active Directory, ensure you have the following information:

- IP address of the server that holds the LDAP accounts
- Credentials to establish the connection
- The Active Directory Base Context

To Import User Data from Active Directory

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **Active Directory**.
 - b. For **Connection Name**, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.
4. Complete the requested information in the Connection Properties section.
 - a. To enable SSL connections by adding Certificates to the Java Keystore, do the following (if SSL is not being enabled skip to the next step):
 - a. Set **SSL?** to **Yes**.
 - b. From the terminal, get the location of JAVA_HOME using the command `echo $JAVA_HOME`. Invoke the key tool utility (found in the

\$JAVA_HOME/bin/ folder) to import the new certificate to the existing keystore.

- c. To import the new CA certificate, run the following command:

```
sudo $JAVA_HOME/bin/keytool -import -alias [alias]  
-file [file location of the new certificate] -keystore  
$JAVA_HOME/jre/lib/security/cacerts
```

- d. The default password for the keystore is changeit. Type **Yes** to the question Trust this certificate?.

- e. The Certificate was added to keystore message indicates the successful import of the new certificate. Restart Tomcat to reflect the changes.

- b. For **Hostname**, enter the LDAP username with privileges to search the OU structure where the user records are present. The default format is the domain\username.

- c. The **Base Context** is usually the location in the Active Directory tree structure where the search starts. The search is always down the tree structure; not upwards. For example, Base context can be **DC=securonix,DC=com**).

5. Click **Test Connection** to ensure the credentials are correct and you are able to connect to **Active Directory** without any issues.

6. (Optional) Before moving to the next screen, the solution provides an option to use **Active Directory** as the source for Access Entitlements. If you want to evaluate **Active Directory** group memberships, click **Yes**. If you do not want to import group memberships, click **No**.

7. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding SNYPR attributes and set conditional actions.

Connecting to User Data

Importing User Data From Azure Active Directory

This section describes how to import data from Microsoft Azure Active Directory. For complete instructions to configure the Microsoft Azure Active Directory, see [Configuring Azure Active Directory for SNYPR](#).

Before You Begin

Prior to importing data using Azure Active Directory, make sure to have the following information:

- Microsoft Azure Client ID
- Microsoft Azure Client Secret
- Microsoft Azure Tenant ID

To Import User Data From Azure Active Directory

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For **Connection Method**, choose **Azure AD**.
 - b. For **Connection Name**, provide a unique name to identify this connection.
 - c. For **Import Using**, choose **Console** or remote ingester name from the drop-down.
4. Complete the following information in the **Connection Properties** section:
 - a. **Client ID**: Enter the client ID generated from Microsoft Azure AD.
 - b. **Client Secret**: Enter the client secret generated from Microsoft Azure AD.
 - c. **Tenant ID**: Enter the tenant ID generated from Microsoft Azure AD.
 - d. **Attributes**: Add the following attributes:

```
accountEnabled,city,companyName,country,department,displayName,employeeId,givenName,id,jobTitle,mail,postalCode,state,surname,userPrincipalName,userType
```

e. **Filter Statements:** Enter * for all users.

See [Connection Settings - Azure Active Directory](#) for additional details.

5. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding SNYPR attributes and set conditional actions.

Connecting to User Data

Importing User Data From Bamboo HR

This section describes how to import data from Bamboo HR.

Before You Begin

Prior to importing data using Bamboo HR, make sure to have the following information:

- Company Domain
- API Key

To Import User Data From Bamboo HR

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **Bamboo HR**.
 - b. For **Connection Name**, provide a unique name so the connection can be easily identified.

- c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.
4. Complete the requested information in the Connection Properties section. See [Connection Settings - Bamboo HR](#).

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding SNYPR attributes and set conditional actions.

Connecting to User Data

Importing User Data From Google Directory

This section describes how to import data from Google Directory.

For complete instructions to configure the Google Console API, see [Configuring Google for Unified Defense SIEM](#).

Before You Begin

SNYPR uses a .p12 File or open authentication (OAuth) to connect to Google Directory to import data. Ensure you have the following information prior to setting up the connection, depending on the authentication type:

.p12

- The .p12 file generated from the Google API Console.

The file must be present in /Securonix/tenants/<tenantname>/Console/securonix_home/conf/google/ or uploaded from the local machine.

- The service account email used to provision the project.
- The domain from where the data is to be imported.
- The admin email address used to generate the service email account.

OAuth

- Name of the project that holds SNYPR related information to connect to Google.
- The service account email used to provision the project.

- The domain from where the data is to be imported.
- The Client ID generated from the Google Console API.
- The Client Secret generated from the Google Console API.

To Import User Data From Google Directory

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **Google Directory**.
 - b. For **Connection Name**, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.
4. Enter the project and authentication information in the **Connection Properties** section. See [Connection Settings - Google Directory](#) for additional details.
5. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding Unified Defense SIEM attributes and set conditional actions.

Connecting to User Data

Importing User Data From Google BigQuery

This section describes how to import data from Google Directory.

Before You Begin

Prior to importing data from Google BigQuery, make sure to have the following information:

- Path to the Credentials file

To Import User Data From Google Directory

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **Google BigQuery**.
 - b. For **Connection Name**, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose the Remote Ingester name.

Note

This connector can be run through Ingester only.

4. Enter the project and authentication information in the **Connection Properties** section. See [Connection Settings - Google BigQuery](#) for additional details.
5. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding Unified Defense SIEM attributes and set conditional actions.

Connecting to User Data

Importing User Data From Okta

This section describes how to import data from Okta.

Before You Begin

Prior to importing data from Okta, make sure to have the following information:

- URL of the Okta API
- Token generated from the Okta API

For information about how to generate a Token from the Okta API, see the [Okta Authentication Deployment Guide](#).

To Import User Data from Okta

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **Okta**.
 - b. For **Connection Name**, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.
4. Provide the **URL**, **Token**, and additional information. See [Connection Settings - Okta](#) for additional details.
5. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding Unified Defense SIEM attributes and set conditional actions.

Connecting to User Data

Importing User Data From One Login

This section describes how to import data from One Login.

Before You Begin

Prior to importing data from Okta, make sure to have the following information:

- One Login client ID
- One Login client secret

To Import User Data from One Login

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **OneLogin**.
 - b. For **Connection Name**, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.
4. Provide the requested information including the client ID and client secret.

For Filter Secret, enter an appropriate filter:

Example

```
firstname=Abc&email=*@xyz.com
```

Use * in case of no filter.

See [Get Users](#) in the One Login documentation for more information.

5. See [Connection Settings - One Login](#) for additional details.
6. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding Unified Defense SIEM attributes and set conditional actions.

Connecting to User Data

Importing User Data from Oracle IDM

This section describes how to import user data from Oracle IDM.

Before You Begin

Prior to importing data from Oracle IDM, make sure to have the following information:

- OIM Host Name
- OIM Port
- Credentials to establish the connection

To Import User Data from Oracle IDM

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **Oracle IDM**.
 - b. For **Connection Name**, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.
4. Submit the requested information in the **Connection Properties** section. See [Connection Settings - Oracle IDM](#) for additional details.
5. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding Unified Defense SIEM attributes and set conditional actions.

[Connecting to User Data](#)

Importing Oracle Identity Analytics (OIA)

This section describes how to import from OIA. Oracle Identity Analytics provides enterprises with the ability to define and manage roles and automate critical identity-based controls. Unified Defense SIEM integrates directly with OIA to collect identity and access privileges, and analyze the access privileges to detect abnormal privileges assigned to users. Additionally, customers can use OIA to perform access certifications only on the suspicious access detected by the Unified Defense SIEM application.

Before You Begin

Prior to importing data from OIA, make sure to have the following information:

- JDBC URL to connect to the Database application (IP Address or host name, port number, Database name and type)
- Credentials to establish the connection

To Import Oracle Identity Analytics (OIA)

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **Oracle Identity Analytics**.
 - b. For **Connection Name**, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.
4. Provide the requested information. See [Connection Settings - Oracle Identity Analytics](#) for additional details.
5. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding Unified Defense SIEM attributes and set conditional actions.

Connecting to User Data

Importing User Data From Salesforce

This section describes how to import data from Salesforce:

Before You Begin

Prior to importing data from Salesforce, make sure you have the following information:

- Consumer Key and Secret of your Salesforce application
- URL to access the Salesforce application
- File Source from which to import users

To Import User Data From Salesforce

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **Salesforce**.
 - b. For Connection Name, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.
4. Enter the Salesforce Instance Domain. For Production Environments use "login.salesforce.com" and for Sandbox(Test) Environments use "test.salesforce.com".
5. Enter the Key and Secret, then click **Generate Tokens**.
6. Enter the requested information and click **Grant Access**.
7. Click **Populate Tokens** to retrieve access and refresh tokens.

See [Connection Settings - Salesforce](#) for additional details.

8. Click **Save & Next**. the Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding Unified Defense SIEM attributes and set conditional actions.

Connecting to User Data

Importing User Data From Saviynt

This section describes how to import user data from Saviynt.

Before You Begin

Prior to importing data from Splunk, make sure you have the following information:

- URL to connect to the application
- Credentials to establish the connection

To Import User Data From Splunk

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **Saviynt**.
 - b. For Connection Name, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.
4. Provide the requested information. See [Connection Settings - Saviynt](#) for additional details.
5. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding Unified Defense SIEM attributes and set conditional actions.

Connecting to User Data

Importing User Data From SailPoint

SailPoint provides streamlined access reviews, improves audit performance, and reduces the cost of compliance. It also provides access certification, centralized IAM certification across all systems and acts as an access provisioning engine.

Unified Defense SIEM has the ability to detect and score rogue access privileges using advanced peer group-analysis techniques. It also reduces the burden and rubber stamping during access certifications by providing only high risk access privileges for review. Unified Defense SIEM improves the access request process by ensuring appropriate approvals for high risk access.

Before You Begin

Prior to importing data from SailPoint, make sure to have the following information:

- JDBC URL to connect to the Database application (IP Address or host name, port number, Database name and type)
- Credentials to establish the connection
- File Source from which to import users

To Import User Data From SailPoint

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **Sailpoint**.
 - b. For Connection Name, provide a unique name so the connection can be easily identified.

- c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.
4. Provide the requested information. See [Connection Settings - Sailpoint](#) for additional details.
5. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding Unified Defense SIEM attributes and set conditional actions.

Connecting to User Data

Importing User Data From Splunk

This section describes how to import data from Splunk.

Before You Begin

Prior to importing data from Splunk, make sure you have the following information:

- URL to connect to the application (host name and port number)
- Credentials to establish the connection

To Import User Data From Splunk

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **Splunk**.
 - b. For Connection Name, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.

4. Provide the requested information. See [Connection Settings - Splunk](#) for additional details.
5. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding Unified Defense SIEM attributes and set conditional actions.

Connecting to User Data

Importing User Data From Waveset IDM

This section describes how to import from Oracle Waveset IDM.

Before You Begin

Prior to importing data from Waveset IDM, make sure to have the following information:

- URL of the Waveset IDM database
- Credentials to establish the connection

To Import User Data From Waveset IDM

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **WavesetIDM**.
 - b. For Connection Name, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.
4. Provide the requested information. See [Connection Settings - WavesetIDM](#) for additional details.

5. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding Unified Defense SIEM attributes and set conditional actions.

Connecting to User Data

Importing User Data From Workday

This section describes how to import user data from Workday.

Before You Begin

Prior to importing data from Workday, make sure you have the following information:

- URL to connect to the Workday application
- Credentials to establish the connection

To Import User Data From Workday

1. Go to **Menu > Add Data > User**. The User Import screen appears.
2. Click **New Connection** to create a new connection.
3. Complete the following information in the **Connection Method** section:
 - a. For Connection Method, choose **Workday**.
 - b. For Connection Name, provide a unique name so the connection can be easily identified.
 - c. From the Import Using drop-down, choose **Console** or the Remote Ingester name.
4. Provide the requested information. See [Connection Settings - Workday](#) for additional details.
5. Click **Save & Next**. The Configure User Import screen appears.

Next Steps

See [Configuring the User Import](#) to map event attributes with corresponding Unified Defense SIEM attributes and set conditional actions.

Connecting to User Data

Configuring the User Import

After you have connected SNYPR to your user data (see [Creating the Connection](#)), use the following procedure to map each event attributes with the corresponding Unified Defense SIEM attribute and set conditional actions.

To Configure the User Import

1. Scroll down to the **Preview** section to view the input before mapping the column numbers to the available attributes in the application.
 - a. Under **Input File Column Position**, enter the number for each row that corresponds to the column number in the Preview table. You can map fields such as **employeeid**, **firstname**, **department**, **division**, **manageremployeeid**, and **hiredate**.

Example

Column 1 Employeeid to Input File Column Position 1.

- b. Under **Mapped to Securonix Field**, select the corresponding Unified Defense SIEM attribute from the drop-down menu to match to the input file field.

Example

Mapped to Securonix Field Position 1: Employeeid to Securonix Field: employeeid.

- c. Under **Maintain Change History**, select **Yes** for fields that you want to track in the Maintain Change History column. The application can maintain old values for user identity attributes when they change.

Note

Date formatted fields (hiredate, sunrise, sunset, terminationdate) expect a date format. Select the date format from the dropdown. (Example: MM/dd/YY = 10/25/13, MM/dd/yyyy = 10/25/2013, MMM dd, yyyy for Oct 25, 2013), or type the date format you prefer to use.

2. Adjust the following options, depending on what **Additional Settings** you want to modify (Optional):

- Under **User Lifestyle Changes**, select conditions to indicate user termination and user transfer. See [User Lifestyle Changes](#).
- Under **Whitelist**, specify which users will get added to a whitelist, and on which condition. See [Whitelist](#).
- Under **Pre and Post Actions**, run custom pre-processors or post-processors that execute before or after user import. It can be custom class or SQL query.
- Under **Merge Data with Existing User Identity**, you can merge data from multiple data sources.
- Under **Notifications/Alerts**, send email notifications for certain conditions.
- Under **Allow Duplicate Employee ID**, to manage user updates from multiple data sources. Fields mapped to the Employee ID field is used by Securonix to identify the user identity. When updated information is available for the same employee id, the default behavior is to update the information for the user matching the employee id. This behavior can be updated with the settings below.

Next Steps

See [Running the User Data Import Job](#).

Configuring the User Import

Running the User Data Import Job

You have the flexibility to choose when to run import jobs. You can choose to run the job once or on a recurring schedule. If the job runs successfully, the status shows as completed, and you can review the user data that was imported.

To run the job, follow the steps below:

1. Complete the following information in the **Job Details** section:

- a. **Job Name:** Enter a job name.
- b. (Optional) **Job Description:** Describe the job.

Note

By default, these are already filled in the text box based on date-time.

c. **Enable Job Related Notifications:** Set to **YES** to enable notifications, then complete the following settings:

- **On Success:** Set up the details for the **On Success** email by selecting **Create New Email Template** or by selecting an existing email template.
- **On Failure:** Set up the details for the **On Failure** email, either by selecting **Create New Email Template** or by selecting an existing email template.
- **On Completed With Errors:** Set up the details for the **On Completed With Errors** email, either by selecting **Create New Email Template** or by selecting an existing email template.

2. Complete the following information in the **Job Schedule Information** section:

a. **Run Job:** Select one of the following options:

- **Do you want to run job Once?:** Select if you only want to run this job one time.
- **Do you want to schedule this job for future?:** Select how often you want to run the job.

b. **Start Job At:** Type when you want to start the job.

c. **Run Every:** How often you want the job to run in seconds.

d. **Stop after:** Leave this field blank if you want the job to run all the time.

3. Click **Save** to save your information.

4. Click **Run** to run the job.

If the job runs successfully, the status shows as completed, and you can review the data that was imported. Click the refresh icon at the top left corner (as indicated by the orange box) to see the job update on the screen. You can also run the import job by clicking the **Update Ingestor** button on the top right of the screen.

Click **View Jobs** to see the status of the job.

The job details show the user information, such as the number of records imported, the total number of users, and the total number of new users. These details only appear if the job import was successful.

To monitor jobs at a later time, Go to **Menu > Operations Center > Job Monitor**. Click the filter icon to view the **Jobs List** or **Jobs by Datasource**.

Next Steps

See [Reviewing and Managing Imported User Data](#).

[Running the User Data Import Job](#)

Reviewing and Managing Imported User Data

To review and manage imported user data, complete the following steps:

1. Go to **Menu > Views > User**.
2. Click an Employee ID to view and manage details about users.

See [Views](#) for more information on actions you can perform from the Users view screen.

Search using Spotter

Upon successful import, the user data will be available for searching in Spotter. To search users in Spotter, complete the following steps:

1. Go to **Menu > Security Center > Spotter**.
2. In the search bar, type `index=users` , then click the search icon.

For more detailed information, see [Spotter](#).

Importing Activity Data

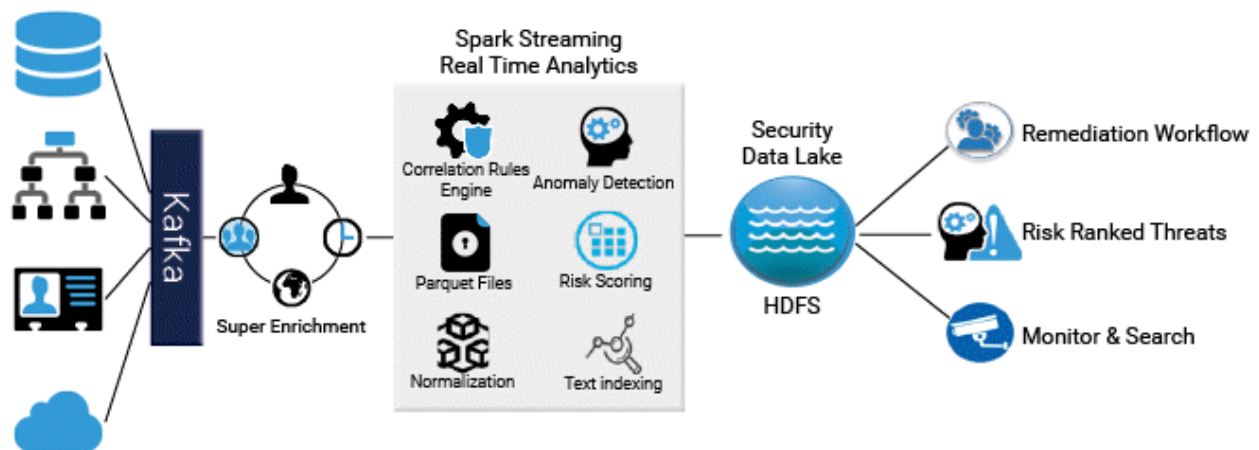
Unified Defense SIEM uses out-of-the-box and custom connectors to ingest security log event data from a variety of structured and unstructured data sources. Some data sources include enterprise applications, endpoint monitoring, perimeter security, and identity systems. There are also non-technical data sources such as badge readers and social media that are not supported by typical log management solutions.

During ingestion, Unified Defense SIEM super enriches event data with meaningful context including entity metadata, threat intelligence, geolocation, lookup data, and user identity information (job function, access privileges, location, and peer groups). This makes raw event data easy to understand, search, and investigate, as in the following illustration:



The enriched data is normalized, run through Unified Defense SIEM's correlation rules engine, analyzed using policy evaluators and anomaly detection, risk scored, indexed for quick searching, and converted to Parquet. The enriched data is then stored in Unified Defense SIEM Security Data Lake for long-term compliance. You can view risk ranked results on the Security Dashboard, take action on threats for remediation, and hunt threats using Spotter natural language search engine.

Unified Defense SIEM can ingest data from both on-prem and remote ingester nodes.



Note

Unified Defense SIEM supports the import of both structured and unstructured log formats. For a complete list of connectors, see [Activity Import Connectors](#).

To Import Activity Data

You can select from existing connection methods or create a custom connection. The following steps are required to configure non-syslog based activity data import:

1. Configure the resource type from an existing resource type or create a custom connection.

For out-of-the-box APIs, configure the resource type from an existing resource type. See [Configuring the Datasource](#).

2. Map event data attributes with corresponding Unified Defense SIEM attributes. Set conditional actions using enrichment data such as user identity data, entity metadata, geolocation, and third party intelligence. See [Managing Parsers, Normalizing, and Adding Conditional Action Filters](#).

3. Apply identity correlation rules to attribute user identity to events. See [Adding Identity Attribution Rules](#).

4. Select policies that you can run on the ingested data. This provides a comprehensive view of policies and threat models with their statuses. See [Detect policy violation](#).

5. Review the import summary, save configuration template, and create behavior profiles to apply to the datasource. See [Reviewing the Summary and Running the Job](#).

Next Steps

See [Configuring the Datasource](#).

[Configuring the Datasource](#)

[Managing Parsers, Normalizing, and Adding Conditional Action Filters](#)

[Adding Identity Attribution Rules](#)

[Detecting Policy Violations](#)

[Reviewing the Summary and Running the Job](#)

Configuring the Datasource

The following steps describe how to configure datasources.

To Configure a New Datasource

1. Go to **Menu > Add Data > Activity**. The [Activity Import screen](#) appears, showing the production datasources, representing existing connections.

Note

To edit an existing connection click .

2. To add a datasource for an existing device type, click **Add Data > Add Data for Existing Device Type**. Submit the requested information for resource type.

For **Resource Type Information**, use the Vendor drop-down to search by organization, or the Functionality drop-down to search by functionality (for example, web proxy, antivirus, or data warehouse).

3. To add a datasource for a custom device type, click **Add Data > Create Custom Device Type**. Submit the requested information for and resource type.

- (Optional) **Duplicate Parser and Policies From:** Click to indicate how Unified Defense SIEM should parse the incoming data.

The **Resource Type Information** section displays the information based on your selection.

- **Vendor:** Click the drop-down and select **Create New Vendor**. The **Add New Vendor** popup appears, which allows you to provide a unique vendor name. Type the vendor name and click **Save**.
 - **Functionality:** Click the drop-down and select **Create New Functionality**. The **Add New Functionality** popup appears, which allows you to provide a unique functionality name. Type the functionality name and click **Save**.
 - **Resource Type:** Specify the resource type based on the vendor or functionality.
 - **Collection Method:** Click the drop-down and select a collection method.
4. Select an ingester from the **Console or Ingester** drop-down list.
 5. Provide the requested information in the **Resource Group Information** section. The fields that display in this section will vary by collection method. See [Resource Group Information](#) for additional details.

Examples

This section provides example configurations for traditional collection methods and out-of-the-box API connectors.

JSON (Key Value Pair)

1. Go to **Menu > Add Data > Activity**.
2. Click **+ Add Data**.

Create Custom Device Type


- a. Provide the following information in the **Resource Group Information** section:

- a. **Vendor:** Select the **Vendor** name. from the dropdown or select Create New Vendor to specify a custom vendor name.
- b. **Functionality:** Select the **Functionality** from the dropdown.
- c. **Resource Type:** Specify the resource type based on the vendor or functionality.
- d. **Collection Method:** Select **JSON** from the dropdown.

Add Data for Existing Device Type

- a. Enter the following information in the **Device Type Information** section:
 - a. **Vendor:** Select the **Vendor** name.
 - OR
 - b. **Functionality:** Select the **Functionality**.
 - c. **Device Type:** Specify the resource type based on the vendor or functionality.
 - d. **Collection Method:** Select **Syslog [file]**.
- 3. Select an **ingester** from the **Console or Ingestor** dropdown list.

Select only an ingester from the **Console or Ingestor** drop-down list.
- 4. Provide the following information in the **Resource Group Information** section:
 - a. **Datasource Name:** Specify a unique datasource name.
 - b. **IP Address:** Not required.
 - c. **Specify timezone for activity logs:** Click the drop-down and select a time zone.
- 5. Provide the following information in the **Collection Method** section:
 - a. **Folder Location:** Provide the import folder. Default is \$Securonix_home/import/in, but you can specify another path if needed.
 - b. **Prefix:** Provide the file prefix. Example: samplelog.json.

- c. **Parsing Technique:** Key Value Pair.
 - d. **Delimiter:** Select the delimiter used in the file. Example: | (pipe).
 - e. **Column Identifier:** Specify the symbol used to enclose columns in the file. Example: " (double quotes).
 - f. **Parse Header with Regex?:** Toggle to **YES** to provide a Regex to parse the first line of the file.
6. Provide the following information in the **More Settings** section:
- a. **Action Taken on Unparsed Events:** Click the drop-down and select one of the following options:
 - **Save in unprocessed folder on HDFS**
 - **Drop Events**
 - **Ingest as unparsed events**
 - b. **Batch Size:** Specify a batch size. The default is 50,000.
 - c. **Include Header:** Enable to include the header during import.
 - d. **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default: /Securonix/tenants/four/snypr6/securonix_home/import/success/
 - e. **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default: /Securonix/tenants/four/snypr6/securonix_home/import/failed/
 - f. **Staging Folder:** Specify the staging folder (required for data requiring preprocessing). Default: /Securonix/tenants/four/snypr6/securonix_home/import/in
7. Click the Refresh button  in the top-right corner of the screen to preview the input and ensure the data has uploaded successfully.
8. Click **Save & Next**.

XML (Key Value Pair)

1. Go to **Menu > Add Data > Activity**.

2. Click **+ Add Data**.

Create Custom Device Type

a. Provide the following information in the **Resource Group Information** section:

a. **Vendor:** Select the **Vendor** name. from the dropdown or select Create New Vendor to specify a custom vendor name.

Functionality: Select the **Functionality** from the dropdown.

b. **Resource Type:** Specify the resource type based on the vendor or functionality.

c. **Collection Method:** Select **JSON** from the dropdown.

3. Select an **ingester** from the **Console or Ingestor** dropdown list.

Select only an ingester from the **Console or Ingestor** drop-down list.

4. Provide the following information in the **Device Information** section:

a. **Datasource Name:** Specify a unique datasource name.

b. **IP Address:** Not required.

c. **Specify timezone for activity logs:** Click the drop-down and select a time zone.


5. Complete the following information in the **Collection Method** section:

a. **Folder Location:** Click to upload a file from the local machine or specify the complete path to the folder in which the file to be imported is located.
Default: \$Securonix_home/import/in.

b. **Import Files Matching Conditions:** Specify a condition to upload multiple files with the same prefix or postfix.

c. **Root Element Tag Name:** Specify the root element tag name from the XML file.

d. **Event Element Tag Name:** Specify the event element tag name from the XML file.

- e. **Parsing Technique:** Key Value Pair.
6. Complete the following information in the **More Settings** section:
 - a. **Action Taken on Unparsed Events:** Click the drop-down and select one of the following options:
 - **Save in unprocessed folder on HDFS**
 - **Drop Events**
 - **Ingest as unparsed events**
 - b. **Batch Size:** Specify a batch size. The default is 50,000.
 - c. **Include Header:** Enable to include the header during import.
 - d. **Record Element:** Enter the XML record element.
 - e. **Record Attribute:** Enter the XML record attribute.
 - f. **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default: /Securonix/tenants/four/snypr6/securonix_home/import/success/
 - g. **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default: /Securonix/tenants/four/snypr6/securonix_home/import/failed/
 - h. **Staging Folder:** Specify the staging folder (required for data requiring preprocessing). Default: /Securonix/tenants/four/snypr6/securonix_home/import/in/
7. Click the Refresh button  in the top-right corner of the screen to preview the input and ensure the data has uploaded successfully.
8. Click **Save & Next**.

File Import

To import data from Delimited or Regex files, complete the following steps:

1. Go to **Menu > Add Data > Activity**.
2. Click **+ Add Data**.

Add Data for Existing Device Type

a. Enter the following information in the **Device Type Information** section:

a. **Vendor:** Select the **Vendor** name.

OR

b. **Functionality:** Select the **Functionality**.

c. **Device Type:** Specify the resource type based on the vendor or functionality.

d. **Collection Method:** Select **Syslog [file]**.

Create Custom Device Type

a. Provide the following information in the **Device Type Information** section:

a. **Vendor:** Select the **Vendor** name. from the dropdown or select Create New Vendor to specify a custom vendor name.

b. **Functionality:** Select the **Functionality** from the dropdown.

c. **Resource Type:** Specify the resource type based on the vendor or functionality.

d. **Collection Method:** Select **File Import** from the dropdown.

3. Select an **ingester** from the **Console or Ingester** dropdown list.

Select only an ingester from the **Console or Ingester** drop-down list.

4. Provide the following information in the **Device Information** section:


a. **Datasource Name:** Specify a unique datasource name.

b. **IP Address:** Not required.

c. **Specify timezone for activity logs:** Click the drop-down and select a time zone.

5. Complete the following information in the **Collection Method** section:

- a. **Folder Location:** Select one of the following two options:
 - Specify the folder location of the file(s) you want to import. Default: /Securonix/tenants/four/snypr6/securonix_home/import/in
 - Click to upload file and browse for file on your local machine.
 - b. **Import Files Matching Condition:** Specify the prefix or postfix and supply a condition to upload multiple files.
 - c. **Parsing Technique:** Click the drop-down to select the way Unified Defense SIEM will parse the fields in the input file. Example: Delimited Fields or Capturing Groups (Regex).
 - d. **Delimiter:** Click the drop-down and select a delimiter if required by **Parsing Technique**. Example | (pipe).
6. (Optional) Click the **More Settings** section and complete the following information:
- a. **Action Taken On Unparsed Events:** Click the drop-down and select any of the following options:
 - **Save in unprocessed folder on HDFS**
 - **Drop Events**
 - **Ingest as unparsed events**
 - b. **Success Folder:** Provide the folder used to store files that have been successfully imported.
 - c. **Failed Folder:** Provide the folder used to store files that have been failed to import.
 - d. (Optional) **Staging Folder:** Provide the folder to be used to store files that will be processed with a preprocessor prior to being imported.
 - e. **Enable Preprocessor:**
 - a. **Yes:** Provide a Preprocessor Class.
 - b. **No:** Proceed to next step.
 - f. (Optional) **Incomplete Folder:** Provide the folder to be used by preprocessors to store intermediate or incomplete files.

7. Click the Refresh button  in the top-right corner of the screen to preview the input and ensure the data has uploaded successfully.
8. Click **Save & Next**.

Database

1. Go to **Menu > Add Data > Activity**.
2. Click **+ Add Data**.

Add Data for Existing Device Type

- a. Enter the following information in the **Device Type Information** section:
 - a. **Vendor**: Select the **Vendor** name.

OR
 - b. **Functionality**: Select the **Functionality**.
 - c. **Device Types**: Specify the device based on the vendor or functionality.
 - d. **Collection Method**: Select **database**.

Create Custom Device Type

- a. Provide the following information in the **Device Type Information** section:
 - a. **Vendor**: Select the **Vendor** name. from the dropdown or select Create New Vendor to specify a custom vendor name.
 - b. **Functionality**: Select the **Functionality** from the dropdown.
 - c. **Resource Type**: Specify the device name.
 - d. **Collection Method**: Select **Database** from the dropdown.
3. Select an **ingester** from the **Console or Ingestor** dropdown list.

Select only an ingester from the **Console or Ingestor** drop-down list.

4. Complete the following information in the **Collection Method** section:

- a. **Database Type:** Click the drop-down and select the database type.
- 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.
- f. **Query:** Enter a query to extract information from the database.
- g. **Incremental:** Do the following, depending on what you set this option to:

YES

Complete the following fields:

- a. **Incremental Field:** Click the drop-down and select an attribute to retrieve incremental events. The query sent to the database is appended with this field.
- b. **Type:** Select the data type for this field.
- c. **Format:** Provide format for the field.
- d. **Incremental Condition Created:** This field will auto-populate based on the information entered in the previous steps.
- e. **Force Ascending Order:** Set to **YES** to force ascending order.
- f. **Parsing Technique:** This is set to **Delimited Fields**.
- g. **Delimiter:** This is set to | (pipe).


NO

Skip to the next step.

5. Complete the following information in the **More Settings** section:

- a. **Action Taken on Unparsed Events:** Click the drop-down and select from the following options:
 - **Save in unprocessed folder on HDFS**

- **Drop Events**
- **Ingest as unparsed events**

6. Click the Refresh button  in the top-right corner of the screen to preview the input and ensure the data has uploaded successfully.
7. Click **Save & Next**.

Out of Box API Connectors

You can import data using API connections, including Google, Box, Office365, CrowdStrike, and more.

For a complete list and instructions to integrate available connectors, see [Activity Import Connectors](#).

Next Steps

See [Managing Parsers, Normalizing, and Adding Conditional Action Filters](#).

[Configuring the Datasource](#)

Managing Parsers, Normalizing, and Adding Conditional Action Filters

To parse and normalize data in Unified Defense SIEM, complete the following steps:

For existing connections, this step has been completed for you, and you may skip this step. To map attributes for a custom datasource or edit mapping for existing datasources, complete the following steps.

1. From this page, you can add a new line filter or edit an existing line filter. Do the following, depending on which action you want to take:

To Add a New Line Filter

Line filters parse the data (using the selected parsing technique from step 1) so you can map each attribute to the corresponding attribute in Unified Defense SIEM. Depending on the parsing technique, you can create multiple line filters.

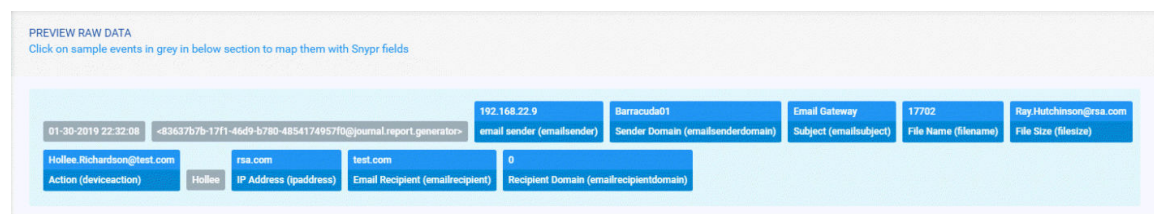
- a. Click **+ Add line filter** to create a new line filter.

- b. Enter a name for the line filter in the **Line Filter Name** text box.
Example: SNX_AccessLogFormat2.

For most parsing techniques, you will only be able to create a single line filter. You can create multiple line filters using the **Regex** parsing technique.

- c. Provide the **Regular Expression** to parse the fields extracted to fields to corresponding Unified Defense SIEM attributes.
- d. Click **Extract Fields** to map the attributes to corresponding Unified Defense SIEM attributes.

When you have created a line filter, the mapped attributes will display in blue and the attributes that have not been mapped will appear in gray.



- e. (Optional) Click + again if you want to extract additional fields with another Line Filter.

This option is not available for all parsing techniques.

To Edit an Existing Line Filter

- a. From the left side of the screen, choose an existing filter then click the edit icon.
 - b. Edit any information that displays in the **Edit Line Filter** section.
 - c. Click **Extract Fields** to map the attributes to corresponding Unified Defense SIEM attributes.
2. (Optional) Click an attribute to map to Unified Defense SIEM fields, then complete the following information:
 - a. **Attribute Name:** Specify the name of the attribute in the datasource.

- b. **Map With:** Click the drop-down and select a corresponding Unified Defense SIEM attribute.
- c. **Description:** Enter a brief a description of the attribute.
- d. **Populate Using Function:** Click **Select Function** to view and select available functions/formulas to perform operations on attribute values. Functions include:

- a. **Logical Functions**

- b. **Math Functions**

- c. **Other Functions**

- d. **String Functions:** Click this function to extract only the specified string, within a field, to appear in the search and dashboard results. If you select this function, do the following:

Extract a specified string to appear in the search and dashboard results

- a. Click **FILE_EXTENSION_EXTRACTOR**.

Information will auto-populate in the text box.

- b. Click **Field** in the text box.
- c. Click the drop-down and select an activity attribute or type a constant in the text box, then click **Add**.
- d. Click **Add** from the **Populate Using Function** pop-up.
- e. Click **Save** from the **Attribute Mapping** window.

To clear mapping from the attribute window and start over, click **Remove Mapping**.

Unified Defense SIEM will extract only the file extension from this field in the indexed results and on the UI (if enabled).

e. **Formula**

(Optional) Click the name of the function, then click **Save** to save your information and go back to the **Parsing & Normalization** screen.

e. **Indexed?:** There are two options, including:

- **YES:** Indexes the attribute in Solr to be available in Spotter search results.
- **NO:** Excludes the field from Spotter search results.

f. **Display on UI?:** This field has two options, including:

- **YES:** Displays the attribute in results on the user interface (UI).
- **NO:** Excludes the field from results on the UI.

For a complete list of functions, see [Functions](#).

3. Click **Save**.

4. Review results to ensure the attributes are mapped correctly.

To Add a Conditional Action Filter

The **Conditional Actions** section allows you to create action filters to specify what actions should be performed when conditions are met. in imported events.

First you add a condition(s); then specify an action(s) that should happen if events meet that condition.

1. Click **+** to add a condition.

2. Specify the following information for your new condition:

- a. **Attribute:** Click the drop-down and select the attribute you want to apply the condition to.
- b. **Operator:** Click the drop-down and select the operator:
 - **Equal To**
 - **Contains**

- **Does Not Contain**
 - **Not Equal To**
 - **Ends With**
 - **Starts With**
 - **Is Not Null**
 - **Greater Than**
 - **Less Than**
- c. **Value:** Specify the value of the attribute.
- d. **Condition:** Click the drop-down and select **AND** or **OR**.
- e. **Add/Remove:** Click + to add conditions, or click - to remove conditions.
- f. **Do you want to drop Events that do not get correlated?:** Set to **YES** if you want the above conditions to be evaluated after the correlation of event data.
3. In the **Select Actions for Above Conditions** section, click + to add actions to the conditions you just created. A list of actions appears

See [Select Actions for Above Conditions](#) for details.

Next Steps

See [Adding Identity Attribution Rules](#).

[Managing Parsers, Normalizing, and Adding Conditional Action Filters](#)

Adding Identity Attribution Rules

Unified Defense SIEM provides a comprehensive and feature-rich correlation engine to associate user identities with security log events. The correlation engine features the following:

- **Ability to specify multiple correlation rules:** You can specify multiple correlation rules to account for different conventions used to create account IDs for different users on datasource. The correlation rules are evaluated in the order in which they are specified. When the account ID is matched to a user identity within the organization, the correlation rule engine stops processing the other rules.

- **Ability to specify multiple operations on the identity data:** The correlation engine will perform the following operations on any identity attribute. The identity attribute generated after the operator is applied can be concatenated with other identity attributes.
 - Trim Left
 - Trim Right
 - Prefix
 - Postfix
 - Substring
 - Prefix and Postfix
- **Ability to prioritize rules:** You can assign weights to rules to prioritize them. Rules are processed based on the weight assigned to them.
- **Ability to request suggested matches:** Unified Defense SIEM utilizes special comparators that perform the following types of matches:
 - **Phonetics:** The comparator provides results for words that sound like each other.
 - **Character Swapping:** The comparator provides results by swapping characters (Sean misspelled to Saen will match).
 - **Closest Match:** jsmith01 and jsmith02 will match to jsmith.
- **Ability to filter users:** You can select all users for correlation or filter users by specifying user selection for correlation.

Example

An application uses the convention first initial of first name + first initial of lastname + employeeid for the account ID, so Harry Ogwa, employeeid 1001, owns the account name HO1001.

To construct this rule:

Correlation Rule Name: Select Event Field:

Correlate Events To: ☒ Users ☐ Access Account

CORRELATE EVENTS TO USER USING RULE

User Attribute	Operation	Parameter	Condition	Separator
<input type="text" value="firstname"/>	<input type="text" value="Substring"/>	<input type="text" value="1"/> <input type="text" value="1"/>	<input type="text" value="AND"/>	<input type="checkbox"/>
<input type="text" value="lastname"/>	<input type="text" value="Substring"/>	<input type="text" value="1"/> <input type="text" value="1"/>	<input type="text" value="AND"/>	<input type="checkbox"/>
<input type="text" value="employeeid"/>	<input type="text" value="None"/>		<input type="text" value="Select an Option"/>	<input type="checkbox"/>

1. Perform substring operation on first name with 1,1 (start from first character and extract the first character).
2. Perform substring operation on last name with 1,1 (start from first character and extract the first character).
3. Concatenate with Employee ID.

To Create Correlation Rules to Attribute Identities to Events

1. Click **Add Condition** to add a correlation rule. A list appears with the following options:

+ Add New Correlation Rule

OR

CHOOSE FROM EXISTING RULES

- LastnameFirstname-2
- firstnamedotlastname-1
- AccountnameLanID
- Email-workemail-1
- Networkid
- FnameDotLname-1-1

2. Choose **+ Add New Correlation Rule** to add a new rule, or one of the existing rules to edit it. The Correlation Rule section appears on the right side of the screen with additional options.

See [Identity Attribution](#).



3. Correlate Event To:

- **Users:** This option will display the **Correlate Events to User Using Rule** section.
- **Access Account:** This option will hide the **Correlate Events to User Using Rule** section.

Users

Complete the following information in the **Correlate Events to User Using Rule** section:

CORRELATE EVENTS TO USER USING RULE

User Attribute	Operation	Parameter	Condition	Separator	Add/Delete
employeeid	None		AND		 

- **User Attribute:** Click the drop-down and select a user attribute.

- **Operation:** Click the drop-down and select an operation.
- **Condition:** Click the drop-down and select a condition.
- **Separator:** Check the box to specify a separator. Once you check the box, a text box will display where you will specify the separator value.
- **Add/Delete:** Click + to add another rule or click - to remove a rule.

Click **Save**.

Access Account

If you choose Access Account, the correlation rule is automatically synchronized and stored in HBase. Click **Save**.

Next Steps

See [Detecting Policy Violations](#).

[Adding Identity Attribution Rules](#)

Detecting Policy Violations

Next, select policies and threat models you want to run on the ingested data, or create new policy.

A threat model is only valid when all prerequisites required to run that threat model are available. A threat model requires data from various datasources and if data is not available, then the threat model status is invalid.

To Enable a Policy:

1. You can select **Yes** for **Enabled**, and to disable a policy toggle **No**.
2. Click **Save & Next** to review the datasource configuration.

For information on how to configure policies for datasources, see [Creating Policies](#).

Next Steps

See [Reviewing the Summary and Running the Job](#).

Detecting Policy Violations

Reviewing the Summary and Running the Job

The Import Summary screen provides a summary of the job you are about to import. From this screen, you can review and edit your information to ensure the line filters and correlation rules are correct.

From this screen, you can perform the following:

1. Review and edit the resource information.
2. Review and edit the parser Information.
3. Review and edit policy & threat Models.
4. Review and edit Identity Attribution.
5. Save a Template.
6. Sync Content Changes.
7. Setup Job Scheduling Information.

Saving the Import Template

1. Click **Save Template**.

A pop-up appears asking if you want to save the template.

2. Click **Save**.

Run the Job

You have the flexibility to choose when to run import jobs. You can choose to run the job once or on a recurring schedule. If the job runs successfully, the status shows as completed, and you can review the Activity data that was imported.

To run the job, follow the steps below:

1. Complete the following information in the **Job Scheduling Information** section:
 - a. **Do you want to run job Once?:** Runs the job right now.

- b. **Do you want to run this job every seconds?:** Specify when you want to run the job, in seconds.
- c. **Do you want to schedule this job for future?:** Choose how often you want to run the job.

2. Complete the following information in the **Job Details** section:

- a. **Job Name:** Enter a unique name for the job or use the default name that appears in the text box.
- b. **Incremental Import:** Set to **YES** to run the job increments.

3. (Optional) Do the following in the **Notifications** section:

a. **Enable Notifications:** Select one of the following options:

- **YES:** You will receive email notifications when the job is run.
- **NO:** You will not receive email notifications when the job is run.

b. Do the following, depending on what option you selected above:

YES

a. Complete the following information:

b. **Notification Type:** Select **Email** or **Application Alert**.

Email

- **Email Address:** Enter the email address that will receive notifications.
- **Email Template:** Select the email template you want to use to send email notifications.

To create a new template, see Email Templates.

- **Interval between Notifications (In Seconds):** Specify the interval between notifications in seconds.

- **No Data Notification Interval (In Minutes):** If there is no data imported within specified interval (in minutes), then send notification.

Application Alert

- **Group:** Select the group that will receive alerts within the application.

OR

- **User:** Select the user that will receive alerts within the application.
- **Interval between Notifications (In Seconds):** Specify the interval between notifications in seconds.
- **No Data Notification Interval (In Minutes):** If there is no data imported within specified interval (in minutes), then send notification.

NO

Skip to the next step.

4. Click **Save & Run**.

You will be redirected to the [Job Monitor screen](#). From here, you can ensure data was loaded successfully.

5. (Optional) Upon successful import, the event data will be available for searching in Spotter. To search events in Spotter, complete the following steps:
 - a. Go to **Menu > Security Center > Spotter**.
 - b. Click the datasource name on the **Spotter** summary screen. See [Spotter](#).

Importing Entity Metadata

Metadata summarizes basic information about other data, which can make it easier to find and work with other data. Entity metadata, and asset metadata, are used at the

time of ingestion to transform raw events into meaningful information that is easy to understand, search, and investigate.

Raw event:

2017-09-03 20:32:56, 218.107.132.66, download, Creditors2017.xls,
22786,h.ogwa, Finance_docs, scnx_fin_srv, yes

Enrichment context:

User context: h.ogwa = Harry Ogwa, IT admin, contractor, Technology

Asset context: scnx_fin_srv = Prod, Restricted Asset, PCI/SOX

Geo-location: 218.107.132.66 = Shenghai, China

Threat Intelligence: N.A

You can import entity metadata to super enrich events for the following resources:

- **Resources:** The assets on your network such as workstations, laptops and servers.
- **IP addresses:** The IP addresses of the assets on your network.
- **Activity Account:** The user accounts performing activity on your network.

The process of importing Entity Metadata must be completed in sequential order.

Ingesting Entity Metadata



Step 1: Create a Connection

1. Navigate to **Menu > Add Data > Entity Metadata**.
2. Click **New Connection** to create a new connection.
3. Click the **Connection Type** drop-down and select one of the following connection types:

- a. **File Import**
 - b. **Database**
 - c. **Qualys**
 - d. **Tanium**
 - e. **ServiceNow Asset Management**
4. Complete the following information in the **Connection Information** section:
- a. **Connection Name:** Enter a unique connection name or use the pre-populated default.
 - b. **MetaData Entity:** Click the drop-down and select one of the following options:
 - **Resources**
 - **IP Address**
 - **Activity Account**
5. Do the following, depending on the connection type you selected:

File Import

Complete the following in the **Connection Details** section:

- a. **Upload File?**
 - **YES:** Browse to upload a file on your local machine.
 - **NO:** Specify the complete path to the folder in which the file to be imported is located. Default: \$Securonix_home/import/in. Skip the next step.
- b. (Optional) **Select File to import:** This field will only display when **Upload File?** is set to **YES**. Select the file for importing user identity data. The file will be uploaded to : /Securonix/tenants/partnerdemo/securonix_home/import/in. You can also copy the file manually to the location.
- c. **File Prefix:** Prefix of the file containing data to import.
- d. **Column Delimiter:** Specify the delimiter between the fields in the input file.
- e. **Exclude Header**

- **YES:** Specify the number of lines to ignore.
 - **NO:** Does not exclude the header. Skip the next step.
- f. (Optional) **Number of lines to Ignore:** This field only displays when **Exclude Header** is set to **YES**.
- g. **Delete Old Entity Metadata**
- **YES:** Deletes the old data and replaces it with the new import.
 - **NO:** Keeps the old data and doesn't replace it with the new import.

Database

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

- a. **Delete Old Entity MetaData:** Select one of the following options:
- **YES:** Deletes the old data and replaces it with new metadata.
 - **NO:** Keeps the old data and doesn't replace it with new metadata.
- b. **SQL Query:** Enter the query.

Example

```
select id, resourcename, ownerid, ownertype,  
criticality from resources;
```

- c. **Database Type:** Click the drop-down and select a database type.
- d. **JDBC URL:** Enter the JDBC URL to connect to a particular database.

Example

```
jdbc:mysql://<host>:<3306>/<database>.
```

- e. **Driver Class:** Specify the database driver class.
- com.mysql.jdbc.Driver.
- f. **Database Username:** Enter the database username.
- g. **Database Password:** Enter the database password.

Qualys

To import Entity Metadata from Qualys, you must configure the required connection credentials:

- a. Navigate to "../securonix_home/connectorapis/qualys/scr" folder.
- b. Open **config.txt**.
- c. Enter connection credentials.

Tanium

Before You Begin

To import Entity Metadata from Tanium, you will need the following information for your Tanium server:

- **API Username:** User name to connect to the user interface (UI).
- **API Password:** Password associated with the API user name
- **API IP Address:** IP Address of the Server.

Instructions

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

- a. **API Username:** Specify the username to connect to the API.
 - b. **API Password:** Specify the password associated with the above username.
 - c. **API IP Address:** Provide the IP address of the server.
- Continue to step 7.

ServiceNow Asset Management

Before You Begin

To import Entity Metadata from ServiceNow, you will need the following information for your ServiceNow server:

- **ServiceNow URL:** URL to connect to ServiceNow.
- **ServiceNow Username:** User name to connect to ServiceNow .

- **ServiceNow Password:** Password associated with the ServiceNow user name.
- **ServiceNow Asset Management Table:** Table name from where the records are retrieved.

Instructions

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

- ServiceNow URL:** Specify the URL to connect to ServiceNow.
- ServiceNow Username:** Specify the username to connect to ServiceNow.
- ServiceNow Password:** Specify the password associated with the above username.
- ServiceNow Asset Management Table:** Specify the table name.
- Query String:** Enter the query to retrieve data from ServiceNow.
- Delete Old MetaData for Entity:** Enable to delete the data imported during the last import, or disable to retain the data.

6. Complete the following information in the **Connection Properties** section:

- Import From Remote Server?:** Do the following, depending on what option you select:

YES

Set this field to **YES** to use FTP/SFTP/SCP to ingest the file located in a remote location. There will be additional fields that display with this setting. Follow the instructions below to learn more about these settings:

Complete the following information:

- Remote Connection Type:** Click the drop-down and select a remote connection type.
- Host IP Address:** Specify the host IP address.
- Port Number:** Specify the port number.
- Username:** Specify the username.
- Password:** Specify the password.
- Source directory:** Specify the source directory.

g. **Proxy Server?:** This is the server that all computers on the local network have to go through before accessing information on the Internet. Select one of the following options:

- **YES:** Enter the **Proxy Server URL, Username, and Password.**
- **NO:** Continue to the next step.

h. **Test Remote Connection?:** Click if you want to test the remote connection.

NO

Skip to the next step.

- b. **Source Folder:** Specify the source folder in which the file is located. Default `${SECURONIX_HOME}/import/in`.
- c. **Success Folder:** Specify the success folder into which to move the file once the import is completed successfully. Default `${SECURONIX_HOME}/import/success`.
- d. **Failed Folder:** Specify the failed folder into which to move the file if the import job fails to complete. Default `${SECURONIX_HOME}/import/failed`.

7. Click **Save And Next**.

Step 2: Configure Attribute Mapping

Now that you have configured the connection, you will specify column positions in the in file that map to the entity metadata fields.

Complete the following information:

2
Select Connection
Configure Attribute Mapping
Run job
Prev
Save & Next

Specify column positions in file that map to Meta data Fields

Position	Value	Is indexed key	Action
<input type="text" value="2"/>	<input type="text" value="resourcename"/>	<input checked="" type="checkbox"/>	
<input type="text" value="3"/>	<input type="text" value="OS"/>	<input type="checkbox"/>	
<input type="text" value="4"/>	<input type="text" value="macaddress"/>	<input type="checkbox"/>	
<input type="text" value="5"/>	<input type="text" value="owner"/>	<input type="checkbox"/>	

PREVIEW

First 10 lines from input file are shown below. Headers in the table correspond to column positions. Enter the position number above and select corresponding field to map to. You can choose not to map columns you do not wish to import.

40	harryogwa's Macbook	Mac OS Sierra	19:46:48:65:1:72:21	harry.ogwa	10.1.5.95
69	homerogwal's Macbook	Mac OS Sierra	14:63:6B:36:6:37:53	homer.ogwal	10.1.1.96
157	hillary-ogwa-Laptop	Microsoft Windows	21:50:1B:95:23:86:0	hillary.ogwa	10.1.1.149
183	terrymeritt's Macbook	Mac OS Sierra	7:13:5B:30:19:88:27	terry.meritt	10.1.4.39

1. **Position:** Specify the column position in the file that maps to metadata fields.
2. **Value:** Specify the column value in the file that maps to metadata fields.
3. **Is indexed key:** Set to **YES** to specify the primary key for the table.

Before you can continue to step 3, you must set one attribute as the primary key for the table.

4. (Optional) **Action:** Click **+** to add an entry or click **-** to remove an entry.

Step 3: Run the Job

You have the flexibility to choose when to run import jobs. You can choose to run the job once or on a recurring schedule. If the job runs successfully, the status shows as completed, and you can review the entity metadata that was imported.

To Run the Job

Complete the following information in the **Job Details** section:

1. **Job Name:** Enter a job name.
2. (Optional) **Job Description:** Describe the job.

By default, this text box is auto-populated based on the date-time.

3. **Enable Job Related Notifications:** Set to **YES** to enable notifications, then complete the following settings:

- **On Success:** Set up the details for the **On Success** email by selecting **Create New Email Template** or by selecting an existing email template.
- **On Failure:** Set up the details for the **On Failure** email, either by selecting **Create New Email Template** or by selecting an existing email template.
- **On Completed With Errors:** Set up the details for the **On Completed With Errors** email, either by selecting **Create New Email Template** or by selecting an existing email template.

Complete the following information in the **Job Schedule Information** section:

1. **Run Job:** Select one of the following options:

- **Do you want to run job Once?:** Select if you only want to run this job one time.
- **Do you want to schedule this job for future?:** Select how often you want to run the job.

2. **Start Job At:** Type when you want to start the job.

3. **Run Every:** How often you want the job to run in seconds.

4. **Stop after:** Leave this field blank if you want the job to run all the time.

5. Click **Save** to save your information.

6. Click **Run** to run the job.

Importing Watch Lists

You can import a list of entities as a watchlist from files or databases. To import a watchlist, complete the following steps.

Step 1: Create a Connection

To create a connection, do the following:

1. Go to **Menu > Add Data > Watch List**. The [Select Connection page](#) appears.

2. Click **New Connection**.

3. For **Connection Type**:

- To import a file, click the drop-down menu and select **File Import**, then enter the information requested. See [Select Connection page - File](#) for details.
- To use a Spotter query, click the drop-down menu and choose **Spotter**, then enter the information requested. See [Select Connection page - Spotter](#) for details.

4. For **Connection Name**, enter a name for the Connection.

5. Click **Save And Next**. The Attribute Mapping page appears.

Step 2: Configure Attribute Mapping

Now that you have configured the connection, specify column positions in the input source that map to the Watch List fields.

1. Complete the following information in the table:

- a. **Position**: Enter the column position.
- b. **Mapped With**: Click the drop-down and select the item you want to map with.

To add or remove entries, click the + or - sign in the last column.

See also [Attribute Mapping](#).

2. Click **Save And Next**.

Step 3: Run the Job

You have the flexibility to choose when to run import jobs. You can choose to run the job once or on a recurring schedule. To run the job, follow the steps below:

1. Enter the **Job Name**. By default, the text box will auto-populate with a name. If you want to change the name, delete the default and enter your own unique job name.

- Optional: Enter a **Job Description** and indicate whether you want to enable notifications.
- Use the options under **Job Scheduling Information** to create a recurring schedule.

See [Run Job page](#) for more details.

- Click **Save** to save your changes.
- Click **Run** to run the job. The [Job Monitor](#) appears, where you can ensure data was loaded successfully.

Note

To find specific jobs, Go to **Menu > Operations Center > Job Monitor**.

Lookup Tables

Lookup tables are used to save any data needed for reference, such as critical keywords, competitors, non-business domains, malicious file extensions, job portals, etc. The contents of a lookup table are used to make comparisons in policies. They function like an index for faster processing, wherein the lookup function is used to find a one-row or one-column range for a value. The function then returns a value from the same position in a second one-row or one-column range.

The Unified Defense SIEM application includes lookup tables by default, but you must import the data into the tables. There are two types of lookup tables: User and System.


The User and System lookup tables are stored in Redis. However, the System lookup tables are loaded into memory and User lookup tables are not loaded into memory. We recommend you to use the System Lookup table.

Note

The User lookup table has known performance issues and few conditions are not supported such as Contain/Does not Contain/Starts With/Ends With. All conditions are supported in System lookup table.

This section describes how to create new lookup tables. To import existing lookup data, see [Importing Lookup Data](#).

To Edit a Lookup Table

1. Go to **Menu > Views > Lookup Tables**.
2. Click  [Edit] to edit the lookup table. The Edit Lookup Table dialog appears. See [Edit Lookup Table](#) for details.
3. Enable the **Restrict Access to this lookup table to your user groups?** setting to restrict access to the lookup table.
4. Select one or multiple user groups to select which users have access to the lookup table.
5. Click **Save**.

To Add Lookup Data

1. Go to **Menu > Views > Lookup Tables**.
2. Click **Add Lookup Records**.
3. Complete the required information in the Add Lookup Data dialog. See [Add Lookup Data](#) for details.
4. Click **Add**.

To Delete Lookup Data

1. Go to **Menu > Views > Lookup Tables**.
2. Check the box to the left of the lookup table you want to delete.
3. Click **Delete Lookup Records**.

Importing Lookup Data

The process of importing Lookup data includes three steps and must be completed in sequential order:

Step 1: Create a Connection

Configure the connection to import the lookup data. You can import lookup data from files and databases.

1. Navigate to **Menu > Add Data > Lookup Data**.
2. Click **New Connection**.
3. For **Connection Type**, choose Database, File Import, Splunk, AWS S3 using SQS, or another connection type.
 - a. **Create New Lookup Table**: Enter a unique name for the lookup table or keep the default name.
 - b. **Lookup Table Type**: Select user or system, depending on the type needed.
 - c. See also [Configure Connection](#).
4. Do the following, depending on the connection type selected.

Database

Submit the requested information in the **Connection Details** section:

- a. (Optional) **Delete Old Lookup Data**: Select one of the following settings:
 - **YES**: Allows you to remove previous data from the lookup table.
 - **NO**: Does not allow you to remove previous data for the lookup table.
- b. **SQL Query**: Enter the SQL query.

Example

Select domainname, domainkey from lookuptable10.

Under **Connection Properties** configure the following:

- **Database Type:** Select a database type.
- **JDBC URL:** Type a connection string to connect to a particular database.

Example

```
jdbc:mysql://hostname:port/database_name
```

- **Driver Class:** Specify the database specific driver class.

Example

```
com.mysql.jdbc.Driver.
```

- **Database Username:** Enter the database username.
- **Database Password:** Enter the database password.

File Import

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

- (Optional) **Upload a file?:** Do the following, depending on the setting you select:
 - **YES: Click Browse to select a file from your local machine. Skip the next step.**
 - **NO:** Continue to the next step.
- File Name:** Enter a name for the file.
- Delimiter:** Specify the delimiter that will be between the fields, such as comma ",", or semicolon ";".
- (Optional) **Exclude Header:** Specify if the column headers should be ignored from the input.

- e. **Number of lines to Ignore:** Specify the number of lines to ignore.
- f. (Optional) **Delete Old Lookup Data:** Select one of the following settings:
 - **YES:** Allows you to remove previous data from the lookup table.
 - **NO:** Does not allow you to remove previous data for the lookup table.

Splunk

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

- a. **Restrict Access to this lookup table to your user group:** Enable to restrict access to this lookup table to your group. Disable to allow all users to access this lookup table.
- b. (Optional) **Delete Old Lookup Data:** Select one of the following settings:
 - **YES:** Allows you to remove previous data from the lookup table.
 - **NO:** Does not allow you to remove previous data for the lookup table.

Complete the following information in the **Connection Properties** section:

- a. **URL:** Enter the URL to access the Splunk application.
- b. **Username:** Enter the Splunk username.
- c. **Password:** Enter the Splunk password.
- d. **Host:** Enter the ipaddress or the host name of the application.
- e. **Port:** Enter the port number for the Splunk application.
- f. **App:** Enter the application name to import the lookup table.
- g. **Available Splunk Search:** Select the search query to import lookup table.

AWS S3 using SQS

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

- a. **Restrict Access to this lookup table to your user group:** Enable to restrict access to this lookup table to your group. Disable to allow all users to access this lookup table.

- b. **Parsing Technique:** Select a parsing technique to parse the data.
- c. (Optional) **Delete Old Lookup Data:** Select one of the following settings:
 - **YES:** Allows you to remove previous data from the lookup table.
 - **NO:** Does not allow you to remove previous data for the lookup table.
- d. **Delimiter:** Specify the delimiter used in the file. For example, comma and pipe.
- e. **Exclude Header:** Enable to ignore the header row.
- f. **Number of Lines to ignore:** Specify the number of header lines that will be ignored during parsing.
- a. Complete the following information in the **Connection Properties** section:
 - a. **Select Access Type:** Enter the access type for AWS S3.
 - b. **SQS Queue URL:** Enter the URL to access the SQS Queue.
 - c. **SQS Access Key:** Enter the access key for SQS.
 - d. **SQS Secret Key:** Enter the secret key associated with the access key for SQS.
 - e. **S3 Region:** Enter the region where SQS is located.
 - f. **S3 Access Key:** Enter the access key for S3.
 - g. **S3 Secret Key:** Enter the secret key associated with the access key for S3.
 - h. **S3 Region:** Enter the region where S3 is located.

5. Click **Save And Next**.

Step 2: Configure Attribute Mapping

When you have configured the connection, you will specify column positions in the input source that map to the Lookup Fields.

1. Complete the following information in the table:

Configure Connection | **Attribute Mapping** | Run Job

Specify column positions in the input source that map to Lookup Fields

Position*	Mapped With*	Map as key*	Encryption	
1	Domain Name	YES	NO	+ -

Do you want to use operators to populate Geolocation information.
☐ YES ☒ NO
If yes then this will populate latitude and longitude in lookup table that can be used in policies.

PREVIEW

First 10 lines from input file are shown below. Headers in the table correspond to column positions. Enter the position number above and select corresponding field to map to. You can choose not to map columns you do not wish to import.

aol.com
att.com
comcast.net
eccouncil.org
e-fensive.net

- Position:** Enter the column position.
- Mapped With:** Enter the mapped with.
- Map as key:** Set to **YES** to specify the primary key.

Before you can continue to Step 3: Run the Job, you must map a primary key for the table.

- Encryption:** Select one of the following settings:

- **YES**
- **NO**

To add or remove entries, click the + or - sign in the last column.

- (Optional) Set **Do you want to use operators to populate Geolocation information** to **YES** to populate the latitude and longitude in the lookup table.

There will be a list of fields that display in a text box, as seen in the image below:

CONCATENATE(Street Name || City || State || Zip Code)

i "You can concatenate fields to form a valid street address. Street address will be used to calculate latitude and longitude. Ex: 2301 Peaceful Lane, Garfield Heights, Ohio, 44125."

When you click a field, a **Select Field** pop-up will display. From here, select a lookup attribute in the drop-down or enter a constant, then click **Add**.

Once you have completed the **Select Field** pop-up for each field in the text box, you can continue to step 3.

3. Click **Save & Next**.

Step 3: Run the Job

You have the flexibility to choose when to run import jobs. You can choose to run the job once or on a recurring schedule. If the job runs successfully, the status shows as completed, and you can review the Lookup Table data that was imported.

To run the job, complete the following information in the **Job Details** section:

1. **Job Name:** By default, the text box will auto-populate with a name. If you want to change the name, delete the default and enter your own unique job name.
2. (Optional) **Job Description:** Enter a job description.
3. (Optional) **Enable Job Related Notifications:** Select one of the following options:

YES

Towards the bottom of the screen, you can specify notification emails to be sent to you for when a job has successfully run, failed, or for when error messages have been received:

- **On Success**
- **On Failure**
- **On Completed with Errors**

ON SUCCESS	ON FAILURE	ON COMPLETED WITH ERRORS
Select Email Template to Use for Sending Notifications -Select- ▼ OR	Select Email Template to Use for Sending Notifications -Select- ▼ OR	Select Email Template to Use for Sending Notifications -Select- ▼ OR
Override email address from template <input type="text"/>	Override email address from template <input type="text"/>	Override email address from template <input type="text"/>
If we specify email address above then email addresses in email template will be overridden.	If we specify email address above then email addresses in email template will be overridden.	If we specify email address above then email addresses in email template will be overridden.

For this example, the **On Success** section is used. Click the drop-down and select one of the following options:

- **Create New Email Template**

- **Job Status**

Do the following, depending on which option you selected in the drop-down:

Create New Email Template

Complete the following information that displays in the pop **Create New Email Template** pop-up:

See [Email Templates](#).

- Sender Name:** Enter the name of the sender.
- Template Name:** Enter a unique name for the template.
- (Optional) **Description:** Enter a description of the template.
- To:** Enter the email address of the recipient.
- From:** This field will auto-populate with the sender address.
- (Optional) **CC:** Enter email addresses of the carbon copy recipients separated by commas.
- (Optional) **BCC:** Enter email address of the blind carbon copy recipients separated by commas.
- (Optional) **Subject:** Enter a subject for the email template.
- (Optional) **HTML Enabled:** Set to **YES** to enable HTML.
- (Optional) **Store in Outbox prior to sending?:** Set to **YES** to store outgoing messages in the outbox prior to sending.

View the Outbox from the collapsed menu on the top navigation menu.

- Use this template for:** Select a module for the template.
- (Optional) **Email body:** You can do one or both of the following:

Add Email Template Variables

Click **Add Email Template Variables**.

a. Check the box next to the variables you want to add.

b. Scroll to the bottom and click **Add**.

Enter and Format Text

Type what you want in the blank space and use the tools in the toolbar to format the email body.

m. Continue to the next step.

4. Complete the following information in the **Job Scheduling Information** section:

a. **Do you want to run job Once?:** Runs the job one time.

b. **Do you want to run this job every seconds?:** Specify how often you want the import job to run (in seconds).

c. **Do you want to schedule this job for future?:** Specify a time for the import job to run.

5. Click **Save** to save your changes.

6. Click **Run** to run the job.

You will be redirected to the **Jobs by Connection** screen. From here, you can ensure data was loaded successfully.

Jobs Details		Schedule Details		Today's Run Statistics		Published Events History	
LOOKUP IMPORT CONNECTION TYPE: FILE EDIT VIEW JOBS		SCHEDULE: ONCE LAST RUN: THU MAY 2 2019 @ 19:46:40 NEXT RUN: -		0 PUBLISHED 0 STORED 0 INDEXED		NO PUBLISHED EVENTS FOR LAST 7 DAYS	
ACTIVITY IMPORT DATASOURCE NAME: BLUECOATPROXY-PROD DEVICE TYPE: BLUECOAT PROXY INGESTER: CLOUDWINS SECURONIX.NET EDIT VIEW CONFIG PAUSE DELETE JOB		JOB TYPE: INGESTER JOB CREATE TIME: FRI APR 26 2019 @ 22:35:40 SCHEDULE: EVERY 300 SECONDS		20.1K PUBLISHED 20.1K PASSED 0 UNPUBLISHED 20.1K INDEXED 0 STORED		N/A N/A 1.3K 66 N/A N/A 8.5K Thu 25 Fri 26 Sat 27 Sun 28 Mon 29 Tue 30 Wed 1	

Third Party Intelligence

The SNYPR application can use intelligence about IP addresses and hostnames that have been classified by open source trackers. Out-of-the-box, the application comes with connectors to highly trusted third-party intelligence (TPI) sources to import IP addresses and the domain names that are malicious and black-listed. The main focus of this is to detect these hosts well in advance and avoid potential infections.

The SNYPR application uses intelligence from third-party sources to add value to the events seen from sources like DLP, web gateways or proxies, and firewall. The SNYPR application normalizes these different data feeds from the third-party sources using its built-in parsers and uses the normalized data in its Intelligence Engine.

See also: [Third-Party Intelligence screen](#).

How it Works

The SNYPR application brings in its intelligence by importing the list of malicious IP addresses and domains from these sources and looks for the presence of these addresses or domains in the activity events, adding additional value and enriching event data.

The connection details for the TPI data sources are provided out-of-the-box with the SNYPR application. Some of the datasources for the blacklisted IPs/domains are listed below:

- CIArmyIP lists
- ZeusIP and Domain lists
- SagaDC lists
- Palevo IP and Domains list
- Spyeye and Domains list

To Import Third-Party Intelligence, do the following:

Step 1: Create a Connection

Use pre-configured connections or create your own connection to import TPI from the web, files, or an API.

1. Navigate to **Menu > Add Data > Third Party Intelligence**. See also [Select TPI Source](#).
2. Click **+** to add a new connection.
3. Provide a unique name to identity the connection.
4. Click the drop-down and select one of the available options:
5. Do the following, depending on the **Collection Method** you selected in step 4:

File

- a. Complete the following information in the **Connection Properties** section:

- a. **Upload File?:** Select one of the following options:

- **YES:** Browse to upload a file on your local machine.
- **NO:** Specify the complete path to the folder in which the file to be imported is located.

- b. (Optional) **Select File to import:** This field only displays if **Upload a file?** is set to **YES**. Click **Browse** to select a file from your local machine.

- c. **File name:** Enter the file name to be imported.

The file must be located in "\$ (SECURONIX_HOME)/import/in".

- d. **TPI Type:** Select a type of third party intelligence from the drop-down.

- e. **Parser type:** Select from the drop-down.

- f. **Column Delimited:** Specify a delimiter.

- g. (Optional) **Contains Column Identifier?:** Select one of the following options:

- **YES**
- **NO**

- h. (Optional) **Column Identifier**: Specify the symbol used to enclose each column in the input file.
 - i. **Regex**: Specify a Regular Expression, such as `^\(S+\)$`.
- (Optional) **Contains Column Identifier?**:

Web

- a. Complete the following information in the **Connection Properties** section:

- a. **URL**: Enter the URL from which the data will be downloaded.

`https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist.`

- b. **File Name**: Enter the name of the file to be downloaded.
 - c. **TPI Type**: Select a type of third party intelligence from the drop-down.
 - d. **Parser Type**: Select from the drop-down.
 - e. **Column Delimiter**: Specify the delimiter between the fields in the input file.
 - f. (Optional) **Contains Column Identifier?**: Select one of the following options:
 - **YES**
 - **NO**
 - g. (Optional) **Column Identifier**: Specify the symbol used to enclose each column in the input file.

ThreatStream

ThreatStream combines threat data from feeds and other sources. SNYPR accesses ThreatStream threat intelligence feed through Anomali API in JSON format.

Before You Begin

- Ensure you have the following before importing TPI using the ThreatStream API:

- **API Username:** The unique username in email format for the Anomali API account.
- **API Key:** The 20-digit alphanumeric key for the Anomali API account.
- **API Base URL:** The base URL for your account.
- **API Resource:** The type of resource: intelligence, snapshot, or tipreport.
- **API Resource Version:** The version of the API resource: v1 or v2.
- **(Optional) API Query Conditions:** The optional query condition. Example: itype=bot_ip.

Instructions

a. Complete the following information in the **Connection Properties** section:

- API Username:** The unique user name in email format for the Anomali API account.
- API Key:** The 20-digit alphanumeric key for the Anomali API account.
- API Base URL:** The base URL for your account.
- API Resource:** The type of resource: intelligence, snapshot, or tpireport.
- API Resource Version:** The version of the API resource: v1 or v2.
- (Optional) API Query Conditions:** The optional query condition. Example: itype=bot_ip.
- TPI Type:** Click the drop-down and select the TPI type.

6. ThreatConnect

Before You Begin

Ensure you have the following before importing TPI using the **ThreatConnect** API:

- **API Access ID:** The unique access ID required to connect to ThreatConnect.
- **API Secret Key:** The secret key associated with the API access ID.
- **API URL:** The API URL for connection.
- **API Owner:** The email address of the user whose access details are used to connect with ThreatConnect.

Instructions

a. Complete the following information in the **Connection Properties** section:

- a. **API Access ID:** Enter the unique access ID required to connect to ThreatConnect.
- b. **API Secret Key:** Enter the secret key associated with the API access ID.
- c. **API URL:** Enter the API URL for connection.
- d. **API Owner**
- e. **Type of Data:** Select the type of information you want to retrieve from ThreatConnect.
- f. **Delete OldTPI Data:** Enable to remove previous data from TPI or disable to remove previous data for the lookup table.

7. Haila Taxii

Before You Begin

Ensure you have the following before importing TPI using the Haila Taxii:

- **Hostname:** The hostname of the Haila Taxii server.
- **Haila Taxii Username:** The unique username required to connect to the API.
- **Password:** The password key associated with the hostname.

Instructions

a. Complete the following information in the **Connection Properties** section:

- a. **Hostname:** Enter the hostname of the Taxii server.
- b. **Haila Taxii Username:** Enter the unique username required to connect to the API.
- c. **Password:** Enter the password key associated with the API username.
- d. **Start Time:** Enter the start time for the feeds.
- e. **Import Duration (Interval):** Enter the time duration (in seconds) for the import process. The import process starts based on the start time and runs for the duration specified in **Import Duration**.
- f. **Data feeds:** Enter the data field name.
- g. **STIX Version:** Select the STIX version such as V1.

h. **TPI Type:** Select the type of TPI you want to import. The available TPI types are:

- Malicious IP Address
- Malicious Domain
- Malicious URL
-
- Malicious Port.

i. **Delete OldTPI Data:** Enable to remove previous data from TPI or disable to remove previous data for the lookup table.

8. Recorded Future

Before You Begin

Ensure you have the following before importing TPI using the **Recorded Future** API:

- **Hostname:** The hostname of the server.
- **Recorded Future API Token:** The token required to connect to the **Recorded Future** API.

Instructions

a. Complete the following information in the **Connection Properties** section:

- a. **Hostname:** Enter the hostname of the API.
- b. **Recorded Future API Token:** Enter the token required to connect to the **Recorded Future** API
- c. **Data feeds:** Enter the data field name.
- d. **TPI Type:** Select the type of TPI you want to import. The available TPI types are:
 - Malicious IP Address
 - Malicious Domain
 - Malicious URL
 -

- Malicious Port.
 - Malicious Hash.
 - Vulnerability
- e. **Delete OldTPI Data:** Enable to remove previous data from TPI or disable to remove previous data for the lookup table.

9. IDefense

Before You Begin

Ensure you have the following before importing TPI using the **IDefense**:

Outh Token: The authorization token required to connect to **IDefense**.

Instructions

- a. Complete the following information in the **Connection Properties** section:
- a. **Outh Token:** Enter the token required to connect to **IDefense**.
 - b. **Data feeds:** Enter the data field name.
 - c. **TPI Type:** Select the type of TPI you want to import. The available TPI types are:
 - Malicious IP Address
 - Malicious Domain
 - Malicious URL
 -
 - Malware
 - File MD5
 - d. **Delete OldTPI Data:** Enable to remove previous data from TPI or disable to remove previous data for the lookup table.

AlienVault

Before You Begin

Ensure you have the following before importing TPI using the AlienVault API:

- **API Key:** The 20-digit alphanumeric key for the API account.
- Instructions

a. Complete the following information in the **Connection Properties** section:

- a. **API Key:** Enter the 20-digit alphanumeric key for the API account.
- b. **TPI Type:** Click the drop-down and select the TPI type.
- c. **Delete OldTPI Data:** Enable to remove previous data from TPI or disable to remove previous data for the lookup table.

10. Complete the following information in the **Additional Settings** section:

a. **Exclude Header:** Select one of the following options:

- **YES:** Specify the number of lines to ignore from the header.
- **NO:** Continue to the step below.

b. **Exclude Footer:** Select a criticality from the drop-down.

c. **Criticality:** Click the drop-down and select a criticality confidence for the threat data to be imported:

- **None:** 0.0
- **Low:** 0.3
- **Medium:** 0.6
- **High:** 1.0

d. (Optional) **Modification Type:** Do the following, depending on the setting you select:

YES

a. Complete the following information:

- a. **Modification Type:** Click the drop-down and select one of the following options:

- **Normalize:** Provide the criticality as a numeric value. The following configuration will normalize the criticality rating to **None** for 0, **Low** for 1-3, **Medium** for 4-6, and **High** for 7-10.

Modification Type

Normalize ▼

Set None	When criticality is =0
Set Low	When criticality is ≥1
Set Medium	When criticality is ≥4
Set High	When criticality is ≥7

- **String:** The application will set the appropriate criticality for each of the criticality string conditions provided.

b. Continue to the step below.

NO


Skip to the step below.

11. (Optional) Complete the following information in the **More Settings** section:

- a. **Source Folder:** By default, SNYPR expects the file to be in the "\$ {SECURONIX_HOME}/import/in" folder. If the input data file is located in

another location, provide the location of the folder by editing the Source Folder text box.

- b. **Success Folder:** After the import is completed, SNYPR compresses the imported data file and moves it to the Success folder (`${SECURONIX_HOME}/import/success`). Change the location of the folder by editing the Success Folder text box.
- c. **Failed Folder:** If the file fails to import, SNYPR compresses the file and moves it to the Failed folder (`${SECURONIX_HOME}/import/failed`). Change the location of the folder by editing the Failed Folder text box.

12. Click  in the top right corner to ensure the data has uploaded successfully.
13. Click **Save And Next**.

Step 2: Configure Attribute Mapping

Now that you have configured the connection, you will specify column positions from the import data that map to Securonix Fields.

Note

See [Attributes by Field Group](#) for a complete list of attributes.

To map attributes, complete the following information in the table:

1. **Field Name:** Click the drop-down and select a field name.
2. **Position:** Enter the column position.

See also [Attribute Mapping](#).

To add or remove entries, click the **+** or **-** sign in the **Actions** column.

Step 3: Run the Job

You have the flexibility to choose when to run import jobs. You can choose to run the job once or on a recurring schedule. If the job runs successfully, the status shows as completed, and you can review the Third-Party Intelligence (TPI) data that was imported.

To run the job, follow the steps below:

1. Complete the following information in the **Job Details** section:

- a. **Job Name:** By default, the text box will auto-populate with a name. If you want to change the name, delete the default and enter your own unique job name.
- b. (Optional) **Job Description:** Enter a job description.
- c. (Optional) **Enable Job Related Notifications:** Select one of the following options:

YES

Towards the bottom of the screen, you can specify notification emails to be sent to you for when a job has successfully run, failed, or for when error messages have been received:

- **On Success**
- **On Failure**
- **On Completed with Errors**

For this example, the **On Success** section is used. Click the drop-down and select one of the following options:

- **Create New Email Template**
- **Job Status**

Do the following, depending on which option you selected in the drop-down:

Create New Email Template

Complete the following information that displays in the pop **Create New Email Template** pop-up:

- a. **Sender Name:** Enter the name of the sender.
- b. **Template Name:** Enter a unique name for the template.
- c. (Optional) **Description:** Enter a description of the template.
- d. **To:** Enter the email address of the recipient.
- e. **From:** This field will auto-populate with the sender address.
- f. (Optional) **CC:** Enter email addresses of the carbon copy recipients separated by commas.

- g. (Optional) **BCC**: Enter email address of the blind carbon copy recipients separated by commas.
- h. (Optional) **Subject**: Enter a subject for the email template.
- i. (Optional) **HTML Enabled**: Set to **YES** to enable HTML.
- j. (Optional) **Store in Outbox prior to sending?**: Set to **YES** to store outgoing messages in the outbox prior to sending.

View the Outbox from the collapsed menu on the top navigation menu.

- k. **Use this template for**: Select a module for the template.
- l. (Optional) **Email body**: You can do one or both of the following:

Add Email Template Variables

Click **Add Email Template Variables**.

Check the box next to the variables you want to add. See [Email Template Variables](#).

Scroll to the bottom and click **Add**.

Enter and Format Text

Type what you want in the blank space and use the tools in the toolbar to format the email body.

Job Status - [Successful/Failed/Completed with errors]

Skip to step 2.

NO

Continue to the next step.

2. Complete the following information in the **Job Scheduling Information** section:

- a. **Do you want to run job Once?**: Runs the job one time.
- b. **Do you want to run this job every seconds?**: Specify how often you want the import job to run (in seconds).

- c. **Do you want to schedule this job for future?:** Specify a time for the import job to run.
3. Click **Save** to save your changes.
4. Click **Run** to run the job. See [Job Monitor](#) for more details.

Geolocation/Network Map Data

Unified Defense SIEM indexes the geolocation/network map data and uses it to enrich event data. By enriching each event with the geolocation/network map information, the application can use this data for threat detection, reporting, and alerting.

Geolocation/Network Map Data is enabled through an action filter when importing Activity Data. See [Managing Parsers, Normalizing, and Adding Conditional Action Filters](#).

Geolocation

Geolocation data represents the location information for IP addresses (city, state, country, etc.). This makes it easy to locate where an event has occurred and find attacks with pinpoint accuracy. Geolocation data is typically imported from MaxMind (GeoIPCityLite DB) then normalized and indexed into the ipmapping core.

Network Map

The network map is imported from a comma delimited flat file.

Network map data represents the zone of the internal IP associated with the event. For example, the LAN, DMZ, VPN, and WIFI-contiguous IP addresses on your network. The application supports CIDR (Classless Inter-Domain Routing), formatted IP addresses, and IP ranges (from-to).

Network Zone

A network zone represents a contiguous block of IP addresses that are provided with a name. Generally, the network zones are provided in a CIDR notation. For example, the block 192.168.100.0 represents the 1024 IPv4 addresses from 192.168.100.0 to 192.168.103.255. The same information may be provided in the form of IP From, IP To, and location, as this format is also supported.

When ingesting network map data in CIDR block format, the application converts the IP address block to a range of integers. For example,

- 10.30.0.0/12 - USA will be converted to:

```
>Start IP: 10.16.0.0 (168820736) End IP: 10.31.255.255  
(169869311)
```

- 10.30.150.0/24 - USA_Sanfrancisco will be converted to:

```
>Start IP: 10.30.150.0 (168820736) End IP: 10.30.150.255  
(169869311)
```

If the application receives an IP address in an event, for example 10.30.150.10 (169776650), the query will look like this:

```
>Get Country from IP_Mapping where Start_IP,169776650 and  
Last_IP>169776650
```

You will receive results for both USA and USA_Sanfrancisco, and the first result that you get will be associated with the country (USA).

Insert the network map into the Unified Defense SIEM application in this order so that the city is the first result from the query:

```
>10.30.150.0/24 - USA_Sanfrancisco 10.30.150.8/29 10.30.0.0/12 -  
USA
```

Import Geolocation

To import Geolocation from MaxMind, complete the following steps.

Step 1: Import Data from MaxMind

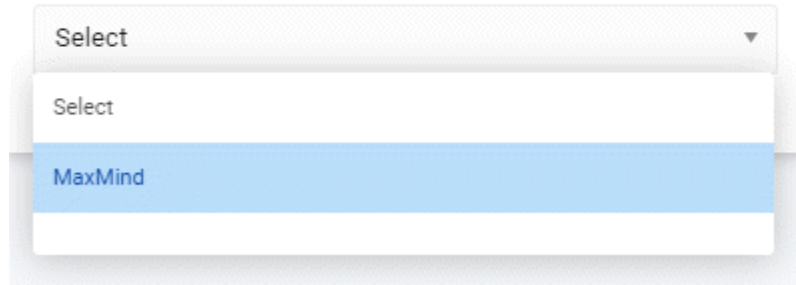
1. Navigate to **Menu > Add Data > Geolocation/Network Map**.

By default, you will be on the **Existing Connection** tab.

2. Click the **Available configurations** drop-down and select **MaxMind**.

AVAILABLE CONFIGURATIONS

Available configurations *

**Note**

If **MaxMind** is not showing as an option in the drop-down, click the **New Connection** tab to create a new connection.

3. Complete the following information in the **Available Configurations** section:

AVAILABLE CONFIGURATIONS

Available configurations *

MaxMind

 Delete Configuration

Configuration Name*

MaxMind

Select source from where to import the data

Select source type


Maxmind

Select source from where to import the data

For example -

Map's attributes like "IP From" whose format is "a.b.c.d" to position "1".

Attribute Mapping ⓘ

Position*	Name	
1	IP From(a.b.c.d) ▼	 
2	IP To (a.b.c.d) ▼	 
3	Country Code ▼	 

Connection

Maxmind

Convert IP

YES ☒

- a. **Configuration Name:** Enter **MaxMind** as the configuration name.
- b. **Select source type:** Select the source from where to import the data.
- c. **Attribute Mapping:** Specify which attribute value is at which column position.
 - **Position:** Column position (1, 2, or 3).
 - **Name:** Attribute value.
- d. **Connection:** Click the drop-down and select **MaxMind**.
- e. **Convert IP:** Select one of the following options:
 - **YES:** Converts the IP.
 - **NO:** Does not convert the IP.

4. Click **Save & Next**.

Step 2: Run the Job

You have the flexibility to choose when to run import jobs. You can choose to run them once or on a recurring schedule. If the job runs successfully, the status shows as completed, and you can review the Geolocation and Network data that was imported.

To Run the Job

1. Complete the following information in the **Job Details** section:
 - a. **Job Name:** By default, the text box will auto-populate with a name. If you want to change the name, delete the default and enter your own unique job name.
 - b. (Optional) **Job Description:** Enter a job description.

- c. (Optional) **Enable Job Related Notifications:** Select one of the following options:

YES

Towards the bottom of the screen, you can specify notification emails to be sent to you for when a job has successfully run, failed, or for when error messages have been received:

- **On Success**
- **On Failure**
- **On Completed with Errors**

For this example, the **On Success** section is used. Click the drop-down and select one of the following options:

- **Create New Email Template**
- **Job Status**

Do the following, depending on which option you selected in the drop-down:

Create New Email Template

Complete the following information that displays in the pop **Create New Email Template** pop-up:

See [Email Templates](#).

- a. **Sender Name:** Enter the name of the sender.
- b. **Template Name:** Enter a unique name for the template.
- c. (Optional) **Description:** Enter a description of the template.
- d. **To:** Enter the email address of the recipient.
- e. **From:** This field will auto-populate with the sender address.
- f. (Optional) **CC:** Enter email addresses of the carbon copy recipients separated by commas.
- g. (Optional) **BCC:** Enter email address of the blind carbon copy recipients separated by commas.
- h. (Optional) **Subject:** Enter a subject for the email template.
- i. (Optional) **HTML Enabled:** Set to **YES** to enable HTML.
- j. (Optional) **Store in Outbox prior to sending?:** Set to **YES** to store outgoing messages in the outbox prior to sending.

Note

View the Outbox from the collapsed menu on the top navigation menu.

- k. **Use this template for:** Select a module for the template.
- l. (Optional) **Email body:** You can do one or both of the following:

Add Email Template Variables

Click **Add Email Template Variables**.

Check the box next to the variables you want to add.

Scroll to the bottom and click **Add**.

Enter and Format Text

Type what you want in the blank space and use the tools in the toolbar to format the email body.

Job Status - [Successful/Failed/Completed with errors]

Skip to the next step.

NO

Skip to the next step.

2. Complete the following information in the **Job Scheduling Information** section:

- Do you want to run job Once?:** Runs the job right now.
- Do you want to run this job every seconds?:** Specify how often you want the import job to run (in seconds).
- Do you want to schedule this job for future?:** Specify a time for the import job to run.

3. Click **Save** to save your changes.

4. Click **Run** to run the job.

You will be redirected to the Jobs by Connection screen. From here, you can ensure data was loaded successfully.

Jobs Details		Schedule Details		Today's Run Statistics		Published Events History
RED LOCATION CONNECTION TYPE: WEB EDIT VIEW JOBS		SCHEDULE: ONCE LAST RUN: MON, APR 15 2019 @ 19:41:08 NEXT RUN: -		0 PUBLISHED 0 INDEXED		NO PUBLISHED EVENTS FOR LAST 7 DAYS
		CREATE TIME: WED, APR 3 2019 @ 23:53:25 START TIME: WED, APR 3 2019 @ 23:53:25 SCHEDULE: ONCE LAST RUN: WED, APR 3 2019 @ 23:53:25 NEXT RUN: NOT APPLICABLE		0 PUBLISHED 0 PARSED 0 UNPARSED 0 INDEXED 0 STORED		NO PUBLISHED EVENTS FOR LAST 7 DAYS
		SCHEDULE: ONCE LAST RUN: TUE, APR 2 2019 @ 21:49:38 NEXT RUN: -		0 UPDATED NEW		NO PUBLISHED EVENTS FOR LAST 7 DAYS

Importing a Network Map

To import a network map from a delimited file, complete the following steps:

Step 1: Import Network Map from a Delimited File

To import Network Map data from a delimited file:

1. Navigate to **Menu > Add Data > Geolocation/Network Map**.
2. Click **New Connection**.
3. Complete the following information in the **Available Configurations** section:
 - a. **Configuration Name**: Provide a name to uniquely identify this configuration.
 - b. **Select source type**: Select source from where to import the data.
4. Complete the following information in the **Additional Settings** section:
 - a. **Exclude Header**: Select one of the following options:
 - **YES**: Excludes the header lines from the input file.
 - **NO**: Includes the header lines in the input file.
 - b. **Exclude Footer**: Select one of the following options:
 - **YES**: Excludes footer lines from the input file.
 - **NO**: Includes footer lines in the input file.
 - c. (Optional) **Number of lines to Ignore**: This field only displays when fields a. or b. above are set to **YES**. Specify the number of lines to ignore in the input file.
5. Click **Save & Next**.

Step 2: Run the Job

You have the flexibility to choose when to run import jobs. You can choose to run them once or on a recurring schedule. If the job runs successfully, the status shows as completed, and you can review the Geolocation and Network data that was imported.

To Run the Job

1. Complete the following information in the **Job Details** section:

- a. **Job Name:** By default, the text box will auto-populate with a name. If you want to change the name, delete the default and enter your own unique job name.
- b. (Optional) **Job Description:** Enter a job description.
- c. (Optional) **Enable Job Related Notifications:** Select one of the following options:

YES

Towards the bottom of the screen, you can specify notification emails to be sent to you for when a job has successfully run, failed, or for when error messages have been received:

- **On Success**
- **On Failure**
- **On Completed with Errors**

For this example, the **On Success** section is used. Click the drop-down and select one of the following options:

- **Create New Email Template**
- **Job Status**

Do the following, depending on which option you selected in the drop-down:

Create New Email Template

Complete the following information that displays in the pop **Create New Email Template** pop-up:

See [Email Templates](#).

- a. **Sender Name:** Enter the name of the sender.
- b. **Template Name:** Enter a unique name for the template.
- c. (Optional) **Description:** Enter a description of the template.

- d. **To:** Enter the email address of the recipient.
- e. **From:** This field will auto-populate with the sender address.
- f. (Optional) **CC:** Enter email addresses of the carbon copy recipients separated by commas.
- g. (Optional) **BCC:** Enter email address of the blind carbon copy recipients separated by commas.
- h. (Optional) **Subject:** Enter a subject for the email template.
- i. (Optional) **HTML Enabled:** Set to **YES** to enable HTML.
- j. (Optional) **Store in Outbox prior to sending?:** Set to **YES** to store outgoing messages in the outbox prior to sending.

Note

View the Outbox from the collapsed menu on the top navigation menu.

- k. **Use this template for:** Select a module for the template.
- l. (Optional) **Email body:** You can do one or both of the following:

Add Email Template Variables

Click **Add Email Template Variables**.

Check the box next to the variables you want to add.

Scroll to the bottom and click **Add**.

Enter and Format Text

Type what you want in the blank space and use the tools in the toolbar to format the email body.

Continue to step 2 below.

Job Status - [Successful/Failed/Completed with errors]

Skip to step 2.

NO

Skip to step 2.

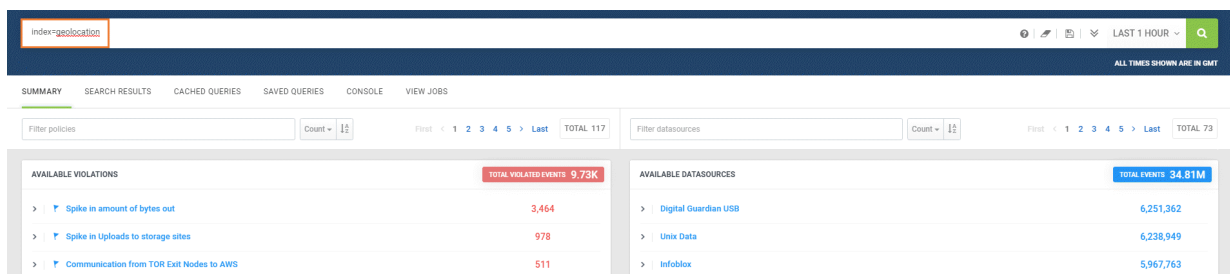
2. Complete the following information in the **Job Scheduling Information** section:
 - a. **Do you want to run job Once?:** Runs the job right now.
 - b. **Do you want to run this job every seconds?:** Specify how often you want the import job to run (in seconds).
 - c. **Do you want to schedule this job for future?:** Specify a time for the import job to run.
3. Click **Save** to save your changes.
4. Click **Run** to run the job.

You will be redirected to the **Jobs by Connection** screen. From here, you can ensure data was loaded successfully.

Search Geolocation Using Spotter

Upon successful import, Geolocation data will be available for searching in **Spotter**. To search for Geolocation in Spotter, complete the following steps:

1. Navigate to **Menu > Security Center > Spotter**.
2. Type `index=geolocationin` search bar.



The screenshot shows the Spotter search interface. The search bar at the top contains the query 'index=geolocationin'. Below the search bar, there are tabs for 'SUMMARY', 'SEARCH RESULTS', 'CACHEd QUERIES', 'SAVED QUERIES', 'CONSOLE', and 'VIEW JOBS'. The 'SEARCH RESULTS' tab is active. The results are displayed in two columns: 'AVAILABLE VIOLATIONS' and 'AVAILABLE DATASOURCES'. The 'AVAILABLE VIOLATIONS' table shows three rows of data with a total of 9,736 events. The 'AVAILABLE DATASOURCES' table shows three rows of data with a total of 34,816 events.

AVAILABLE VIOLATIONS	TOTAL VIOLATED EVENTS
> Spike in amount of bytes out	3,464
> Spike in Uploads to storage sites	978
> Communication from TOR Exit Nodes to AWS	511

AVAILABLE DATASOURCES	TOTAL EVENTS
> Digital Guardian USB	6,251,362
> Unix Data	6,238,949
> Infoblox	5,967,763

3. Click the search icon.

For more information about using Spotter, see [Spotter](#).