Settings

Settings

To configure your application settings, click **Settings** in the navigation menu:

- **Cisco SecureX Integration**—Enable integration with SecureX by choosing the region of your SecureX account, clicking **Authorize**, and signing in to your SecureX account.
- **Device Accounts**—Upload telemetry data in log files from one or more source proxy devices to the global threat alerts system for analysis. To access this service, the External Telemetry feature must be enabled and provisioned for your company. If you do not have the External Telemetry feature, contact your Cisco Security account team. See Proxy Device Uploads.
- **Suppressed Networks**—Hide alerts by listing which IPv4 addresses and network ranges to ignore. This is useful for filtering and suppressing unnecessary alerts such as alerts from a guest network or other, less critical pieces of your network. Enter IPv4 addresses for hosts, subnets, or IPv4 address ranges (for example: 10.100.10.1, 10.100.10.0/24, 10.100.10.1-10.100.10.254) that you want hidden from the list of incidents.
- **Global Threat Alerts API**—Use the REST API to pull information on incidents detected by global threat alerts down to your SIEM client for further analysis, incident response, and data archival.
- **Email Notifications**—Enter email addresses to be sent a summary of new and updated threats every 24 hours.
- **Release Notes**—Summarizes feature updates, changes, and fixes (shown later in this guide).

Settings