

Threat Intelligence

To manage threat intelligence, in the left navigation pane, click **Manage** > **Service Settings** > **Threat Intelligence**.

The **Threat Intelligence** feature provides the most up-to-date datasets for the Secure Workload pipeline that identifies and quarantines threats by inspecting the datacenter workloads against externally known malware command and control addresses, security flaws in processes and geographical location.

The Threat Intelligence dashboard displays the updated status of threat intelligence datasets. These datasets are updated automatically.



Warning

The Threat Intelligence feature requires a connection to Cisco Secure Workload servers to automatically update. Your enterprise outbound HTTP request may require:

- Allow the following domain from the enterprise firewall outbound rules: uas.tetrationcloud.com
- Configure your Outbound HTTP Connection.

In environments without an outbound connection, upload the datasets directly. See the **Manual Uploads** section.

Table 1: Datasets

Dataset	Description
NVD CVEs	Security related software flaws, CVSS base score, vulnerable product configuration, and weakness categorization
MaxMind Geo	Identification of the location and other characteristics of source IPs
NIST RDS	NIST Reference Data Set of digital signatures of known, traceable software applications
Team Cymru	Insight on 3,000+ botnet command and control IPs
Hash Verdict	Verdict of Secure Workload on process hashes (only available with the Automatic Updates section).



Note

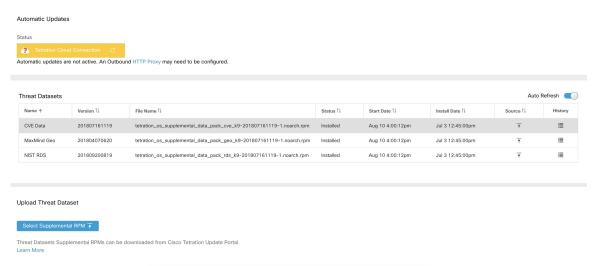
In case the MaxMind Geo dataset is manually uploaded in an earlier release, you must reupload the corresponding RPM to view the location and related information on the Flow Visibility page.

- Automatic Updates, on page 2
- Manual Uploads, on page 2

Automatic Updates

The threat dataset updates are triggered from the appliance to synchronize with the global dataset that is hosted on the Internet at uas.tetrationcloud.com, everyday between 3-4 a.m. UTC. The global dataset is refreshed weekly on Fridays or Mondays. The Threat Intelligence dashboard lists the datasets and the date on which the dataset is last updated.

Figure 1: Dashboard



Manual Uploads



Attention

Scheduling Manual Uploads—Dataset RPM files are published to Secure Workload Update Portal weekly. It is recommended to install the latest releases periodically by configuring a schedule for an administrator.

Downloading Updated Datasets

The datasets can be downloaded from Secure Workload Update Portal.

Uploading Datasets Manually

To upload dataset RPM files:

Before you begin

Log in as a Site Administrator or Customer Support.

Procedure

- Step 1 In the left navigation pane, click Manage > Service Settings > Threat Intelligence.
- Step 2 Under the Upload Threat Dataset section, click Select Supplemental RPM.
- **Step 3** Upload the RPM file downloaded from Secure Workload Update Portal.
- Step 4 Click Upload.

The RPM upload process is initiated and the status is displayed on a progress bar. After the upload, the RPM file is processed and installed in the background. The table is updated after the installation is complete.

Figure 2: Threat Datasets



Uploading Datasets Manually