



## View Threat Intelligence Dashboard

---

This chapter lists the most up-to-date data set for the Secure Workload pipeline that identifies and quarantines threats. Quarantining happens by inspecting the data center workloads against externally known malware command and control addresses, and security flaws in processes and geographical locations. The chapter also describes in detail, any identifiable communication from workloads to well-known malicious IPv4 addresses. The malicious IP addresses are updated every 24 hours. You can choose to automatically update the threat intelligence data sets or manually upload the data sets to Secure Workload.



---

**Attention** Due to recent GUI updates, some of the images or screenshots used in the user guide may not fully reflect the current design of the product. We recommend using this guide in conjunction with the latest version of the software for the most accurate visual reference.

---

- [Manage Threat Intelligence, on page 1](#)
- [Automatic Updates of Data Sets, on page 1](#)
- [Manual Upload of Data Sets, on page 2](#)

## Manage Threat Intelligence

To manage threat intelligence, from the navigation pane, choose **Manage > Service Settings > Threat Intelligence**.



---

**Note** By default, the feature to identify well-known malicious IP addresses is disabled. To enable this feature, see [Visibility of Well-Known Malicious IPv4 Addresses](#).

---

## Automatic Updates of Data Sets


Cisco Secure Workload updates threat data sets regularly between 3 to 4 a.m. UTC by synchronizing with the global data set that is available [here](#). The global data set is refreshed weekly, either on a Friday or Monday. The Threat Intelligence dashboard lists the data sets and the date on which the data set was last updated.

Figure 1: Threat Intelligence

Threat Intelligence

Automatic Updates

Status

 Secure Workload Cloud Connection

Automatic updates are active.

Threat Datasets Auto Refresh

Name ↑	Version ↑	File Name ↑	Status ↑	Start Date ↑	Install Date ↑	Source ↑	History
CVE Data	202403040000_devel	tetration_os_supplemental_data_pack_cve_k9-202403040000_devel-1.noarch.rpm	Installed	Mar 4 9:02:38am	Mar 4 9:09:44am	↓	⋮
CVE Data	202403030000_devel	tetration_os_supplemental_data_pack_cve_k9-202403030000_devel-1.noarch.rpm	Installed	Mar 3 9:03:06am	Mar 3 9:10:55am	↓	⋮
CVE Data	202403020000_devel	tetration_os_supplemental_data_pack_cve_k9-202403020000_devel-1.noarch.rpm	Installed	Mar 2 2:41:26pm	Mar 2 2:49:05pm	↓	⋮
MaxMind Geo	202403040000_devel	tetration_os_supplemental_data_pack_geo_k9-202403040000_devel-1.noarch.rpm	Installed	Mar 4 8:59:02am	Mar 4 9:00:46am	↓	⋮
MaxMind Geo	202403030000_devel	tetration_os_supplemental_data_pack_geo_k9-202403030000_devel-1.noarch.rpm	Installed	Mar 3 8:59:01am	Mar 3 9:01:14am	↓	⋮
MaxMind Geo	202403020000_devel	tetration_os_supplemental_data_pack_geo_k9-202403020000_devel-1.noarch.rpm	Installed	Mar 2 2:37:13pm	Mar 2 2:39:24pm	↓	⋮
NIST RDS	202403040000_devel	tetration_os_supplemental_data_pack_rds_k9-202403040000_devel-1.noarch.rpm	Installed	Mar 4 9:00:47am	Mar 4 9:02:38am	↓	⋮
NIST RDS	202403030000_devel	tetration_os_supplemental_data_pack_rds_k9-202403030000_devel-1.noarch.rpm	Installed	Mar 3 9:01:15am	Mar 3 9:03:05am	↓	⋮
NIST RDS	202403020000_devel	tetration_os_supplemental_data_pack_rds_k9-202403020000_devel-1.noarch.rpm	Installed	Mar 2 2:39:25pm	Mar 2 2:41:24pm	↓	⋮
Team Cymru	202403040000_devel	tetration_os_supplemental_data_pack_zeus_k9-202403040000_devel-1.noarch.rpm	Installed	Mar 4 9:09:45am	Mar 4 9:10:44am	↓	⋮

Upload Threat Dataset

Automatic updates are active. [Click here to enable manual upload.](#)

## Manual Upload of Data Sets

The **Threat Intelligence** page displays the updated status of threat intelligence data sets. These data sets are updated automatically.



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

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

In environments without an outbound connection, manually upload the data sets.



**Note** **Schedule Manual Uploads:** Data set RPM files are published to the Secure Workload **Update Portal** weekly. We recommend that you install the latest releases periodically by configuring a schedule for an administrator.

**Table 1: Data Sets**

Data set	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

Data set	Description
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 data set 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.

## Download Updated Data Sets

Download the latest threat data sets from [here](#).

## Upload Latest Data Sets

### Before you begin

Log in as a **Site Administrator** or **Customer Support Executive**.

### Procedure

- Step 1** From the navigation pane, choose **Manage > Service Settings > Threat Intelligence**.
- Step 2** Under the **Upload Threat Dataset** section, enable manual upload.
- Step 3** Click **Select Supplemental RPM** and select the RPM files that are downloaded from the 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 threat data sets are updated after the installation is complete.

**Figure 2: Threat Data Sets**

Threat Datasets							Auto Refresh <input checked="" type="checkbox"/>
Name ↕	Version ↑↓	File Name ↑↓	Status ↑↓	Start Date ↑↓	Install Date ↑↓	Source ↑↓	History
MaxMind Geo	202108060000	tetration_os_supplemental_data_pack_geo_k9-202108060000-1.noarch.rpm	Failed	Aug 10 5:22:47pm		↕	⋮
Team Cymru	202108060000	tetration_os_supplemental_data_pack_zeus_k9-202108060000-1.noarch.rpm	Failed	Aug 10 5:23:12pm		↕	⋮

