



Integrating with Cisco Threat Response

This topic contains the following sections:

- [Integrating the Appliance with Cisco Threat Response, on page 1](#)
- [Performing Threat Analysis using Casebooks, on page 3](#)
- [Improving User Experience of Cisco Web Security Appliance using Cisco Success Network, on page 6](#)

Integrating the Appliance with Cisco Threat Response

You can integrate your appliance with Cisco Threat Response, and perform the following actions in Cisco Threat Response:

- View the web tracking data from multiple appliances in your organization.
- Identify, investigate and remediate threats observed in web tracking.
- Resolve the identified threats rapidly and provide recommended actions to take against the identified threats.
- Document the threats in the portal to save the investigation, and enable collaboration of information among other devices on the portal.

To integrate your appliance with Cisco Threat Response, you need to register your appliance with Cisco Threat Response.

You can access Cisco Threat Response using the following URLs:

- <https://visibility.amp.cisco.com> (North Americas)
- <https://visibility.eu.amp.cisco.com> (Europe)
- <https://visibility.apjc.amp.cisco.com> (APJC)



Note If you have enabled and registered for CTR on your appliances, then the appliances automatically start sending the Cisco Success Network (CSN) telemetry data to Cisco. See [Improving User Experience of Cisco Web Security Appliance using Cisco Success Network](#).

Before you begin

- Access the CLI and enable the `reportingconfig > CTROBSERVABLE` command. When you enable the CTR observable indexing using this command, you can index the URLs accessed by the users. It also provides granularity to search any URLs in the appliance tracking database.
- You require a Cisco Security user account to access Cisco Threat Response. If any user in your organization already has a Cisco Security account, contact your system administrator. If you do not have a Cisco Security user account, you can create one at the Cisco Threat Response login page. Make sure that you create a user account in Cisco Threat Response with admin access rights. To create a new user account, go to the Cisco Threat Response login page using the following URL - <https://visibility.amp.cisco.com> (North Americas) or <https://visibility.eu.amp.cisco.com> (Europe) and click **Create a Cisco Security account** in the login page. If you are unable to create a new user account, contact Cisco TAC for assistance.
- Make sure that you enable Cisco Threat Response integration on the Cisco Security Services Exchange (SSE) portal. For more information, see the Cisco Threat Response documentation at <https://visibility.amp.cisco.com/help/module-wsa> (North Americas) or <https://visibility.eu.amp.cisco.com/help/module-wsa> (Europe).
- Make sure that you open HTTPS (Outbound) 443 port on the firewall for the following FQDNs to register your appliance with Cisco Threat Response:
 - `api-sse.cisco.com` (applicable for Americas users only)
 - `api.eu.sse.itd.cisco.com` (applicable for European Union (EU) users only)
 - `api.apj.sse.itd.cisco.com` (applicable for APJC users only)
 - `est.sco.cisco.com` (applicable for Americas, EU, and APJC users)
- Ensure that your DNS server can resolve the hostname configured on the management (M1) interface.

-
- Step 1** Log in to your appliance.
- Step 2** Select **Networks > Cloud Service Settings**.
- Step 3** Click **Edit Settings**.
- Step 4** Check **Enable**.
- Step 5** Submit and commit your changes.
- Step 6** Navigate back to the Cloud Service Settings page after few minutes to register your appliance with the Cisco Threat Response.
- Step 7** Choose your preferred server from the **Threat Response Server** drop-down list.
- Step 8** Obtain a registration token from Cisco Threat Response to register your appliance with the Cisco Threat Response. For more information, see the Cisco Threat Response documentation at <https://visibility.amp.cisco.com/help/module-wsa> (North Americas) or <https://visibility.eu.amp.cisco.com/help/module-wsa> (Europe).
- Step 9** Enter the registration token obtained from Cisco Threat Response and click **Register**.
- Step 10** Add your appliance as an integration module to Cisco Threat Response. For more information, see the Cisco Threat Response documentation at <https://visibility.amp.cisco.com/help/module-wsa> (North Americas) or <https://visibility.eu.amp.cisco.com/help/module-wsa> (Europe).
-

What to do next

After you add your appliance as an integration module in Cisco Threat Response, you can view the web tracking information from your appliance in Cisco Threat Response. For more information, see the Cisco Threat Response documentation at <https://visibility.amp.cisco.com/help/module-wsa> (North Americas) or <https://visibility.eu.amp.cisco.com/help/module-wsa> (Europe).



Note To deregister your appliance connection from Cisco Threat Response, click **Deregister** in the Cloud Services Settings page in your appliance.

Performing Threat Analysis using Casebooks

The casebook and pivot menu are widgets available in Cisco Threat Response.

Casebook - It is used to record, organize, and share sets of observables of interest primarily during an investigation and threat analysis. You can use a casebook to get the current verdicts or dispositions on the observables. For more information, see the Cisco Threat Response documentation at <https://visibility.amp.cisco.com/help/casebooks> for North Americas or <https://visibility.eu.amp.cisco.com/help/casebooks> for Europe regions.

Pivot Menu - It is used to perform threat response enabled tasks on observables directly from the Web Security appliance interface. These tasks can be performed through Cisco Threat Response or any of the user configured modules (for example, AMP for Endpoints, Cisco Umbrella, Cisco Talos Intelligence, and so on). For more information, see the Cisco Threat Response documentation at <https://visibility.amp.cisco.com/help/pivot-menus> for North Americas or <https://visibility.eu.amp.cisco.com/help/pivot-menus> for Europe regions.

The Web Security appliance now includes the casebook and pivot menu widgets. You can perform the following actions in your appliance using the casebook and pivot menu widgets:

- Add an observable to a casebook to investigate for threat analysis.
- Pivot an observable to a new case, an existing case, or other devices registered in Cisco Threat Response (for example, AMP for Endpoints, Cisco Umbrella, Cisco Talos Intelligence, and so on) to investigate for threat analysis.

The following is a list of observables that have the Threat Response pivot menus in the Web Security appliance user interface:

- IP addresses
- Domains
- URLs
- File Hashes (SHA-256 only)



Note

- The pivot menu widget is positioned next to the observables in the web reporting pages of your appliance.
- The casebook widget is positioned at the bottom-right corner of the web reporting pages of your appliance.

Related Topics

- [Obtaining Client ID and Client Password Credentials, on page 4](#)
- [Adding Observable to Casebook for Threat Analysis, on page 5](#)

Obtaining Client ID and Client Password Credentials

You need the client ID and client password to access the casebook and pivot menu widgets on your appliance.

Before you begin

Make sure that you meet all the prerequisites mentioned in the ‘Before you begin’ section of [Integrating the Appliance with Cisco Threat Response, on page 1](#)

Step 1 Log in to the new web interface of your appliance.

Step 2 Add a new API Client.

a) Click the **Threat Response API Clients** link.

When you click on the Threat Response API Clients link, it redirects you to the Cisco Threat Response login page.

b) Log in to Cisco Threat Response.

c) In Threat Response, click **Settings** and choose **API Clients** to go to the API Clients page.

d) Click **Add API Credentials**.

e) Enter the name of your appliance (for example, ‘Web_Security_Appliance’) as the client name.

f) Select the following scopes to provide full access to the casebook and pivot menu widgets:

- Casebook
- Enrich
- Private Intelligence
- Response
- Inspect

Note • If you want to access the casebook widget only, select the following scopes - casebook, private intelligence, and inspect.

• If you want to access the pivot menu widget only, select the following scopes - enrich and response.



g) Click **Add New Client**.

h) Copy the client ID and client password to the clipboard.

Note Make sure that you note the client ID and client password before you close the ‘Add New Client’ dialog box.

i) Click **Close**.

Note If you want to add a new API client, you do not need to delete the existing API client.

- Step 3** Click the **Casebook**  button.
- Step 4** Enter the client ID and client password obtained in Step 2 in the 'Login to use Casebook/Pivot Menu' dialog box in your appliance.
- Step 5** Select the required Cisco Threat Response server in the 'Login to use Casebook/Pivot Menu' dialog box.
- Step 6** Click **Authenticate**.
- Note** If you want to edit the client ID, client password, and Cisco Threat Response server, right-click on the Casebook  button and add the details.
-






What to do next

Add an observable to a casebook to investigate for threat analysis. See [Adding Observable to Casebook for Threat Analysis, on page 5](#)

Adding Observable to Casebook for Threat Analysis

Before you begin

Make sure that you obtain the client ID and client password to access the casebook and pivot menu widgets on your appliance. For more information, see [Obtaining Client ID and Client Password Credentials, on page 4](#).

- Step 1** Log in to the new web interface of your appliance.
- Step 2** Navigate to the Web Reporting page, click on the pivot menu  button next to the required observable (for example, schemas.microsoft.com) and click **Add to New Case** or **Add to Current Case**.
- Note**
- Use the drag and drop  button next to the observable to drag and drop the observable into an existing case.
 - Use the pivot menu  button to take threat response enabled actions on observables using Cisco Threat Response or your other configured Cisco Threat Response modules (for example, blocking a domain using Umbrella, or blocking a file hash using AMP, or investigating an IP using all modules simultaneously).
- Step 3** Click the **Casebook**  button to check whether the observable is added to a new or an existing case.
- Step 4** (Optional) Click  button to add a title, description, or notes to the casebook.
- Step 5** Click **Investigate this Case** to investigate the observable for threat analysis. For more information, see the Cisco Threat Response documentation at <https://visibility.amp.cisco.com/help/introduction> (North Americas) or <https://visibility.eu.amp.cisco.com/help/introduction> (Europe).
-

Improving User Experience of Cisco Web Security Appliance using Cisco Success Network

Overview

You can use the Cisco Success Network (CSN) feature to send your appliance and feature usage details to Cisco. These details are used by Cisco to identify the device information, list of free and licensed features and their activation statuses.

The ability to send your appliance and feature usage details to Cisco helps an organization to:

- Improve the effectiveness of the product in user networks by performing analytics on collected telemetry data and suggesting users with recommendations using a digital campaign.
- Improve user experience with Cisco Web Security Appliance.

The following table shows a sample data of appliance and feature usage details sent to Cisco:

Appliance Details

- Appliance model such as x90, x95, 100v, 300v, 600v.
- Appliance serial number and software version.
- Appliance installation date.
- Unique device identifier

Feature Details

- Name of the feature.
- List of the features that are enabled.
- Status of the feature (in compliance or not).
- Expiry date
- Feature Id

Sample Data



Note For validating the telemetry data sent to Cisco, log subscription levels of *csid_logs* and *sse_connectord_log* should be in trace mode.

You can view the details in the *sse_connectord_log.current* in trace mode.

```
Thu May XX 10:48:30 2020 Trace: {
  "version": "0.X",
  "payload": {
    "recordVersion": "X.0",
    "recordedAt": 1589453310965,
    "deviceInfo": {
      "s1VAN": "WSA",
      "installDate": 1589269184000,
```

```

    "version": "12.5.0-XXX",
    "userAccountID": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
    "model": "S600x",
    "udi": "XXXXXXXXXXXXXXXXXXXX-XXXXXXXXXXXX"
  },
  "recordType": "CST_WSA",
  "features": {
    "free": [
      {
        "enabled": "Y",
        "featureName": "Smart Software Licensing"
      },
      {
        "enabled": "N",
        "featureName": "Identity Services Engine"
      },
      {
        "enabled": "Y",
        "featureName": "Cloud Services"
      },
      {
        "enabled": "N",
        "featureName": "Proxy Auto-Configuration File Hosting"
      },
      {
        "enabled": "N",
        "featureName": "Local Reporting Service"
      },
      {
        "enabled": "Y",
        "featureName": "Centralized Reporting Service"
      }
    ],
    "licensed": [
      {
        "status": "OUT_OF_COMPLIANCE",
        "enabled": "Y",
        "featureName": "Web Security Appliance Cisco Web Usage Controls",
        "featureID":
"regid.2018-05.com.cisco.WSA-WUC,1.0_6e3a0734-ef40-4c60-bbcd-66ea1796231d",
        "expiry": 1591803862000
      },
      {
        "status": "OUT_OF_COMPLIANCE",
        "enabled": "Y",
        "featureName": "Web Security Appliance Anti-Virus Webroot",
        "featureID":
"regid.2018-05.com.cisco.WSA-AMW,1.0_794905fe-57e0-44df-8056-clfc54f968d2",
        "expiry": 1591803867000
      },
      {
        "status": "OUT_OF_COMPLIANCE",
        "enabled": "Y",
        "featureName": "Web Security Appliance L4 Traffic Monitor",
        "featureID":
"regid.2018-05.com.cisco.WSA_SB,1.0_c4b92628-15a4-4b73-94ad-9db1383054ce",
        "expiry": 1591803872000
      },
      {
        "status": "OUT_OF_COMPLIANCE",
        "enabled": "N",
        "featureName": "Web Security Appliance Cisco AnyConnect SM for
AnyConnect",
        "featureID":

```

```

"regid.2018-05.com.cisco.WSA_MUS,1.0_d3f3389a-cdc4-48e3-bc84-8b590ea2d908",
  "expiry": 1591803877000
},
{
  "status": "OUT_OF_COMPLIANCE",
  "enabled": "Y",
  "featureName": "Web Security Appliance Advanced Malware protection
Reputation",
  "featureID":
"regid.2018-05.com.cisco.WSA_AMPREPU,1.0_a51bae61-c688-475a-aa19-51f86b52671e",
  "expiry": 1591803893000
},
{
  "status": "OUT_OF_COMPLIANCE",
  "enabled": "Y",
  "featureName": "Web Security Appliance Anti-Virus Sophos",
  "featureID":
"regid.2018-05.com.cisco.WSA_AMS,1.0_fda29c84-e1e7-4bb5-a220-f872e67bc44d",
  "expiry": 1591803908000
},
{
  "status": "OUT_OF_COMPLIANCE",
  "enabled": "Y",
  "featureName": "Web Security Appliance Web Reputation Filters",
  "featureID":
"regid.2018-05.com.cisco.WSA-WREP,1.0_37bb916e-65e2-4a55-ab3e-262d290c020a",
  "expiry": 1591803857000
},
{
  "status": "OUT_OF_COMPLIANCE",
  "enabled": "Y",
  "featureName": "Web Security Appliance Advanced Malware Protection",
  "featureID":
"regid.2018-05.com.cisco.WSA-AMP,1.0_34331e7c-0be5-4898-8563-a69c0a5fefba",
  "expiry": 1591803882000
},
{
  "status": "OUT_OF_COMPLIANCE",
  "enabled": "Y",
  "featureName": "Web Security Appliance Anti-Virus McAfee",
  "featureID":
"regid.2018-05.com.cisco.WSA-AMM,1.0_b8354876-14f5-4285-8dea-ca6a2bfb74c4",
  "expiry": 1591803898000
},
{
  "status": "IN_COMPLIANCE",
  "enabled": "Y",
  "featureName": "Web Security Appliance Web Proxy and DVS Engine",
  "featureID":
"regid.2018-05.com.cisco.WSA_WP,1.0_996c8b90-5305-43de-bdb8-bf48aa9d0457",
  "expiry": 1591803903000
},
{
  "status": "OUT_OF_COMPLIANCE",
  "enabled": "N",
  "featureName": "Web Security Appliance HTTPs Decryption",
  "featureID":
"regid.2018-05.com.cisco.WSA_WD,1.0_563c38e7-7633-4cdc-a79f-3871d1284b57",
  "expiry": 1591803887000
}
}
]
},
"metadata": {

```



```
    "topic": "wsa.telemetry",  
    "contentType": "application/json"  
  }  
}
```

Related Topics

- [Enabling and Registering Cisco Success Network on the appliance, on page 9.](#)
- [Disabling Cisco Success Network, on page 9.](#)

Enabling and Registering Cisco Success Network on the appliance

Before you begin

Make sure that you register your appliance with Cisco Threat Response. See [Integrating the Appliance with Cisco Threat Response, on page 1](#)

-
- Step 1** Go to **Network > Cloud Service Settings**.
- Step 2** In the **Settings** section, click **Edit Settings** and check the **Enable** checkbox next to **Threat Response**.
- Step 3** In the **Registration** section, perform the following steps:
- Choose the appropriate threat response server from the drop-down list.
 - AMERICAS (api-sse.cisco.com)
 - EUROPE(api.eu.sse.itd.cisco.com)
 - APJC(api.apj.sse.itd.cisco.com)
 - Enter the registration token generated through the Security Service Exchange (SSE) portal.
You must access the SSE portal and generate a token for registration.
 - Click **Register**.
- Step 4** Submit and commit your changes.
- To deregister the appliance from Cisco Threat Response portal, click **Deregister**.
-

Disabling Cisco Success Network

-
- Step 1** Go to **System Administration > Cisco Success Network**.
- Step 2** Click **Edit Settings** under Cisco Network Success.
- Step 3** Uncheck the **Enable** checkbox next to **Cisco Success Network**.
- Step 4** Submit and commit your changes.
-

