Install and manage the Code42 Insider Threat app for Splunk

Who is this article for?
Find your product plan in the Code42 console on the [Account menu](https://support.code42.com/Administrator/Cloud/Code42_console_reference/01_Code42_console_overview#Account_menu).
√ Incydr Professional and Enterprise
√ Incydr Basic and Advanced
√ CrashPlan Cloud
√ CrashPlan for Small Business [https://support.code42.com/Small_Business](https://support.code42.com/Small_Business)
√ Other product plans

This article applies to **Code42 cloud environments**.

Overview

This tutorial explains how to install, manage, and uninstall the Code42 Insider Threat app for Splunk. Splunk is a solution for data analytics monitoring and visualization. The Code42 Insider Threat app for Splunk adds Code42-specific dashboards to [Splunk Enterprise](https://www.splunk.com/en_us/products/splunk-enterprise.html) or [Splunk Cloud](https://www.splunk.com/en_us/products/splunk-cloud.html) that show activity happening across your Code42 environment, which can help you identify insider risk. You can also ingest audit log and device health data from Code42.

For descriptions of dashboards in the Code42 Insider Threat app for Splunk, see [Code42 Insider Threat app for Splunk reference](https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_Insider_Threat_app_for_Splunk_reference).

Considerations

- To use the Code42 Insider Threat app for Splunk, you must have an existing [Splunk Enterprise](http://www.splunk.com/en_us/products/splunk-enterprise.html) version 7.0 or later environment or a [Splunk Cloud](https://www.splunk.com/en_us/products/splunk-cloud.html) environment.
- The devices used to run Splunk and the Code42 Insider Threat app for Splunk must have network access to the Code42 cloud.
- Code42 cannot provide technical support for Splunk. [Contact Splunk support](https://www.splunk.com/en_us/support-and-services.html) for help with Splunk.
Before you begin

Prepare a user account (https://support.code42.com/Administrator/Cloud/Configuring/Add_users_from_the_Code42_console) in your Code42 environment for configuring the Code42 Insider Threat app for Splunk. This user is used to authenticate and access data in your Code42 environment.

- **Permissions:** The Code42 Insider Threat app for Splunk returns data based on the roles assigned to this user (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Roles_resources/Manage_user_roles). To ensure that the user's rights are not too permissive, create a user with the lowest level of privilege necessary. For recommended roles, see our use case for managing a security application integrated with Code42 (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Role_assignment_use_cases#Use_case_3:_Manage_a_security_application_integrated_with_Code42). After assigning roles, you should test to confirm that the user can access the data that they need.

- **Licensing:** As a best practice, we recommend creating a user in your Code42 environment that is exclusively used to configure the Code42 Insider Threat app for Splunk.

Install the Code42 Insider Threat app for Splunk


Step 1: Install the app

Initial installation may require help from Splunk support.

1. From your Splunk home page, click the Apps button:
2. Select Browse more apps.
3. In the Browse More Apps panel, search for "Code42".
5. On the Login dialog, enter your Splunk username and password and click Login and Install.

Distributed Splunk environment

For instructions about deploying the Code42 Insider Threat app to a distributed Splunk environment, see the Splunk documentation (https://docs.splunk.com/Documentation/AddOns/released/Overview/Distributedinstall).

Step 2: Configure the app
Create an index

A Splunk index (https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Aboutindexesandindexers) acts as a data repository. Create a new index to specify where you want the Code42 data to go.

1. Go to Settings > Indexes.
2. Click New Index.
3. Configure the index. For additional details, see the Splunk documentation (https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Setupmultipleindexes).
4. (Optional) To make Code42 data appear in the main Splunk interface (as opposed to only in the Code42 Insider Threat app dashboards), select Search and Reporting in the App field.

Add an account

Add an account that you'll use to connect to your Code42 environment.

1. Navigate back to the Code42 Insider Threat Add-on app.
2. Select Configuration.
3. From the Account tab, select Add.
   The Add Account dialog appears.
4. Enter a unique Account name.
5. Enter the Authority domain you use to sign in to the Code42 console, without the protocol. For example:
   - If you sign in to the Code42 console at https://console.us.code42.com/login (https://console.us.code42.com/login) (US1), enter: console.us.code42.com
If you sign in to the Code42 console for the Ireland cloud at https://console.ie.code42.com/login (EU1), enter:

console.ie.code42.com

6. In the **Username** and **Password** fields, enter the credentials of the Code42 user that you want to use to authenticate. 
*The username and password are added as an account on the Account tab.*

---

**Code42 console URL for US2**

Code42 console URL **console.us2.crashplan.com** was formerly **www.crashplan.com/console**. For more information, see [Changes to server URLs](https://support.code42.com/Terms_and_conditions/Product_lifecycle_policy/Changes_to_server_URLs).

---

### Create inputs

Create a new [input](https://docs.splunk.com/Documentation/Splunk/latest/Data/Configureyourinputs) to configure what Code42 data appears in Splunk. You can create inputs for the following:

- File Exposure
- Alerts
- Audit Log
- Device Health

---

**File Exposure**

Create an [input](https://docs.splunk.com/Documentation/Splunk/latest/Data/Configureyourinputs) to ingest [file exposure](https://support.code42.com/Administrator/Cloud/Code42_console_reference/Forensic_Search_reference_guide) data and view it on Splunk dashboards.

1. Select **Inputs**.
2. Click **Create New Input > File Exposure**. 
   *The Add File Exposure dialog appears.*
3. Enter a unique **Name**.

4. Enter the time **Interval**, in seconds, for retrieving event data from the Code42 cloud instance. The default is the minimum of 300 seconds, or 5 minutes.

5. Select the **Index** you created earlier.

6. Select the **Code42 Account** you want to use.

7. Select a **Search Behavior** of **All Exposure Events** or **Selected Exposure Types**.
   - If you choose **All Exposure Events**, all the types below are treated as selected.
   - If you choose **Selected Exposure Types**, check one or more types below.

8. Click **Add**.

**Alerts**

Create an [input](https://docs.splunk.com/Documentation/Splunk/latest/Data/Configureyourinputs) to ingest [alerts](https://support.code42.com/Administrator/Cloud/Code42_console_reference/Review_Alerts_reference) and view them on Splunk dashboards.

1. Select **Inputs**.

2. Click **Create New Input > Alerts**.
   
   The **Add Alerts** dialog appears.
3. Enter a unique Name.

4. Enter the time Interval, in seconds, for retrieving event data from the Code42 cloud instance. The default is 300 seconds, or 5 minutes.

5. Select the Index you created earlier.

6. Select the Code42 Account you want to use.

7. Select a Search Behavior of All Alerts or Selected Alert Severities.
   - If you choose All Alerts, all the types below are treated as selected.
   - If you choose Selected Alert Severities, check one or more severity levels below.

8. Click Add.

Audit Log


1. Select Inputs.

2. Click Create New Input > Audit Log.
   The Add Audit Log dialog appears.
3. Enter a unique Name.

4. Enter the time Interval, in seconds, for retrieving event data from the Code42 cloud instance. The default is 900 seconds, or 15 minutes.

5. Select the Index you created earlier.

6. Select the Code42 Account you want to use.

7. Click Add.

Device Health


1. Select Inputs.

2. Click Create New Input > Device Health.

   The Add Device Health dialog appears.

3. Enter a unique Name.

4. Enter the time Interval, in seconds, for retrieving event data from the Code42 cloud instance. The default is 28800 seconds, or 8 hours.
5. Select the **Index** you created earlier.
6. Select the **Code42 Account** you want to use.
7. Click **Add**.

**Step 3: Test the app**

1. Sign in to Splunk.
2. From the list of apps on the Splunk home page, click Code42 Insider Threat Add-On.
   The [Incydr Overview](https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_Insider_Threat_app_for_Splunk_reference#Incydr_Overview_dashboard) appears.
3. Explore the data generated by the panels.

![Dashboard screenshot](https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_Insider_Threat_app_for_Splunk_reference#Incydr_Overview_dashboard)

**Troubleshoot the app**

**Troubleshooting considerations**

- Data may not appear in the panels immediately. Rather, data updates at scheduled intervals. The scheduled intervals are configured to avoid overloading your Code42 cloud instance with requests.
- If data for a panel is missing, confirm that the Code42 environment user account has the necessary permissions to view that data within your Code42 environment.

**Logs within Splunk Enterprise**

The Code42 Insider Threat app for Splunk updates log files that contain useful information for troubleshooting, including error messages and security warnings. For Splunk Enterprise installations, the log files are located at:

`<path-to-splunk>/var/log/splunk/TA-code42-insider-threats-add-on`
The path to your installation varies by operating system. See the Splunk Enterprise documentation for more information about [installation](http://docs.splunk.com/Documentation/Splunk/latest/SearchTutorial/InstallSplunk) and [logging](http://docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/WhatSplunklogsaboutitself).

**Support**

If you need support for the Code42 Insider Threat app for Splunk, contact our Customer Champions for [Code42 for Enterprise support](https://my.code42.com).

Our Customer Champions cannot provide technical support for Splunk. [Contact Splunk support](https://www.splunk.com/en_us/support-and-services.html) for help with Splunk.

**Splunk Answers**

[Splunk Answers](https://answers.splunk.com/index.html) is a community forum where Splunk users can post questions and get answers about Splunk usage. Go to the following URL for help with the Code42 Insider Threat app for Splunk: [https://community.splunk.com/t5/All-Apps-and-Add-ons/bd-p/apps-add-ons-all](https://community.splunk.com/t5/All-Apps-and-Add-ons/bd-p/apps-add-ons-all)

**Upgrade the app**

When a new version of the Code42 for Insider Threat app is released, perform the following steps to upgrade.

**Splunk Enterprise**

1. From your Splunk home page, click the **Apps** button:

   ![Apps button](https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Install_and_manage_the_Code42_Insider_Threat_app_on_Splunk_Enterprise.png)

2. On the **Apps** panel, browse to the row for [Code42 Insider Threat](https://splunkbase.splunk.com/app/5106/).
   
   *If there is a later version of the app available, an Update link appears on the row.*

3. Click **Update**.
4. Select the option to acknowledge the terms and conditions.
5. Click **Accept and Continue**.
6. Enter your Splunk username and password.
7. Click **Login and Continue**.
8. Click **Restart Now** to restart Splunk Enterprise and complete the upgrade.

**Splunk Cloud**

1. From your Splunk home page, click the **Apps** button:
2. On the **Apps** panel, browse to the row for the Code42 for Insider Threat app. *If there is a later version of the app available, an Update link appears on the row.*


### Uninstall the app

#### Splunk Enterprise

1. Open a terminal window (Linux or Mac) or command prompt (Windows) on your Splunk Enterprise server.

2. Run the following command to stop Splunk Enterprise:
   ```bash
   <path-to-splunk>/bin/splunk stop
   ```

3. Run the following command to remove the Code42 Insider Threat app for Splunk:
   ```bash
   <path-to-splunk>/bin/splunk remove app TA-code42-insider-threats-add-on
   ```

   *The Code42 Insider Threat app for Splunk no longer appears in the Splunk user interface.*

#### Splunk Cloud

1. From the Splunk home page, click the **Apps** button:

2. On the **Apps** panel, browse to the row for the Code42 Insider Threat app for Splunk.

3. Click the **Disable** link.

### Release history

For release information about the Code42 Insider Threat app for Splunk, see the [Release Notes in Splunkbase](https://splunkbase.splunk.com/app/5106/).

### External resources

- [The Code42 Insider Threat app on Splunktbase](https://splunkbase.splunk.com/app/5106/)
- Splunk documentation (http://docs.splunk.com/Documentation)
- Splunk Answers community (https://answers.splunk.com/app/questions/3736.html)
Related topics

- Add users from the Code42 console (https://support.code42.com/Administrator/Cloud/Configuring/Add_users_from_the_Code42_console)
- Code42 Insider Threat app for Splunk reference (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_Insider_Threat_app_for_Splunk_reference)
- Manage user roles (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Roles_resources/Manage_user_roles)