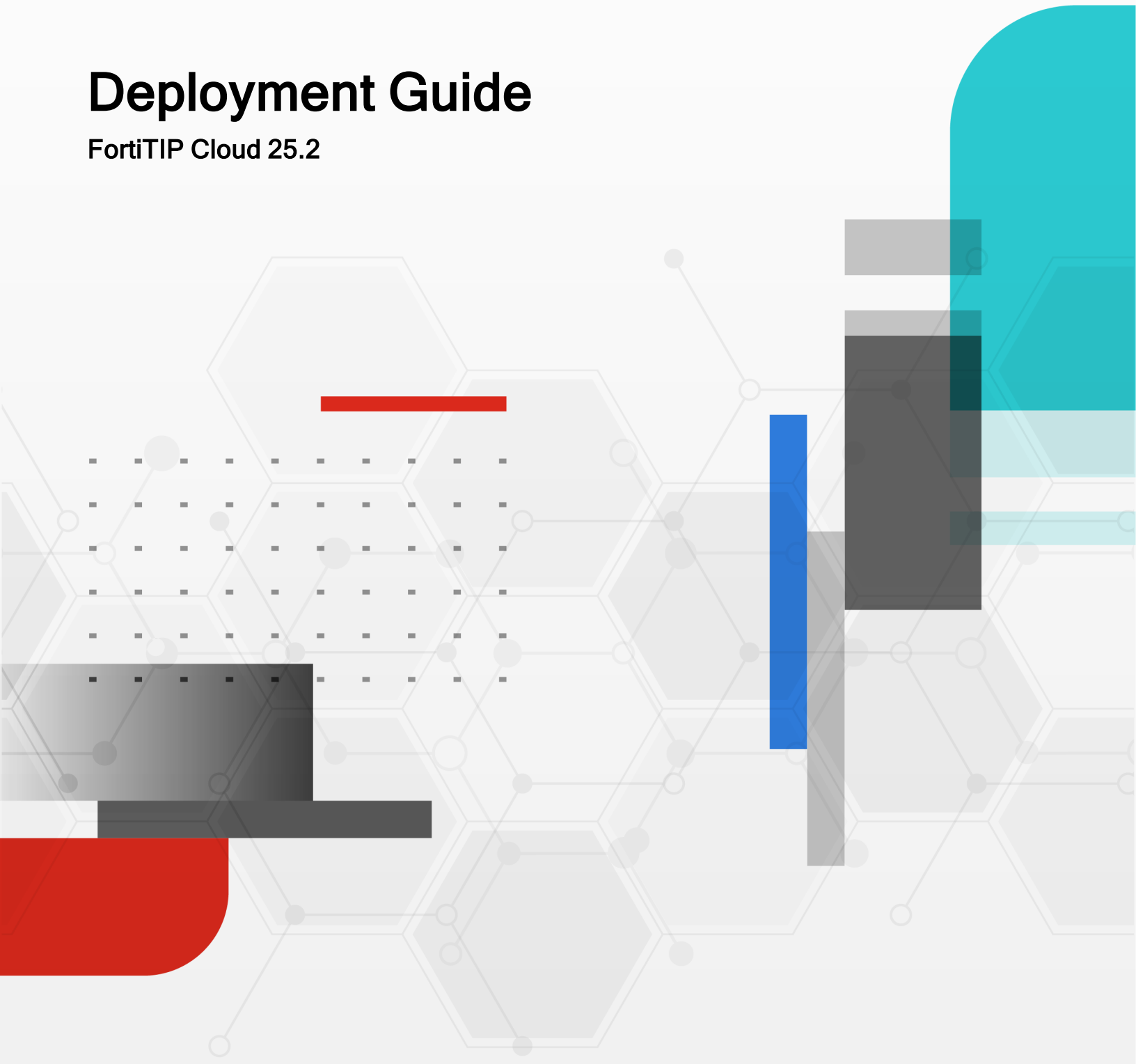
Deployment Guide

FortiTIP Cloud 25.2



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

November, 2025
FortiTIP Cloud 25.2 Deployment Guide
00-400-000000-20221031

TABLE OF CONTENTS

Change Log

Date	Change Description
8/15/2025	Initial release
11/12/2025	Added a prerequisite - upgrade the utilities connector. Refer to the Prerequisites section in the *Setting Up Outbreak Management* chapter.

Introduction

FortiTIP Cloud FortiTIP streamlines threat investigation and response by leveraging vast FortiGuard intelligence, escalated outbreak alerts, and automated workflows. This comprehensive cloud-based platform accelerates detection, response, and mitigation of advanced threats, while enhancing visibility and strengthening the security of digital ecosystems.

FortiTIP Cloud Virtual Machine Specifications

The FortiTIP Cloud VM has the following default specifications:

- 4 vCPU
- 16 GB RAM
- 250 GB available disk space: Recommended to have high-performance storage, preferably SSDs.

A FortiCloud account is required to provision FortiTIP Cloud. If you do not have one, create a FortiCloud account [here]. Access to FortiTIP Cloud requires a primary FortiCloud account, through which you can invite secondary users to access FortiTIP Cloud.

Licensing

Currently, FortiTIP Cloud is available as a part of *FortiAnalyzer Essentials*. FortiAnalyzer Essentials is available as part of Enterprise Protection bundle or à la carte. FortiTIP Cloud offers access to Outbreak Alerts for threat hunting, investigation, and incident management, as well as Threat Intel Search for malicious IPs, URLs, and hashes, providing critical insights.

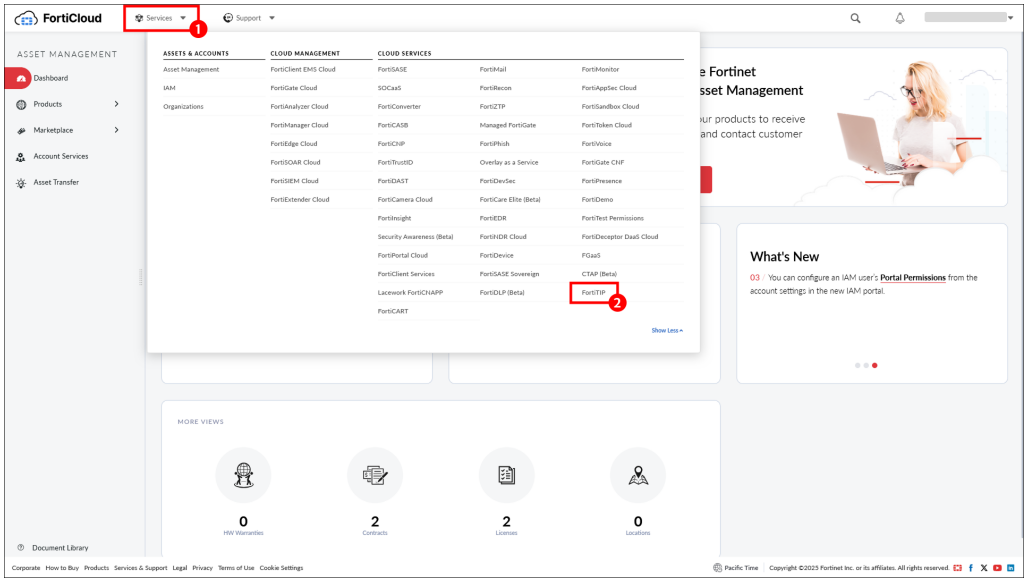
For more information, refer to FortiAnalyzer Ordering Guide.

Deploying FortiTIP Cloud

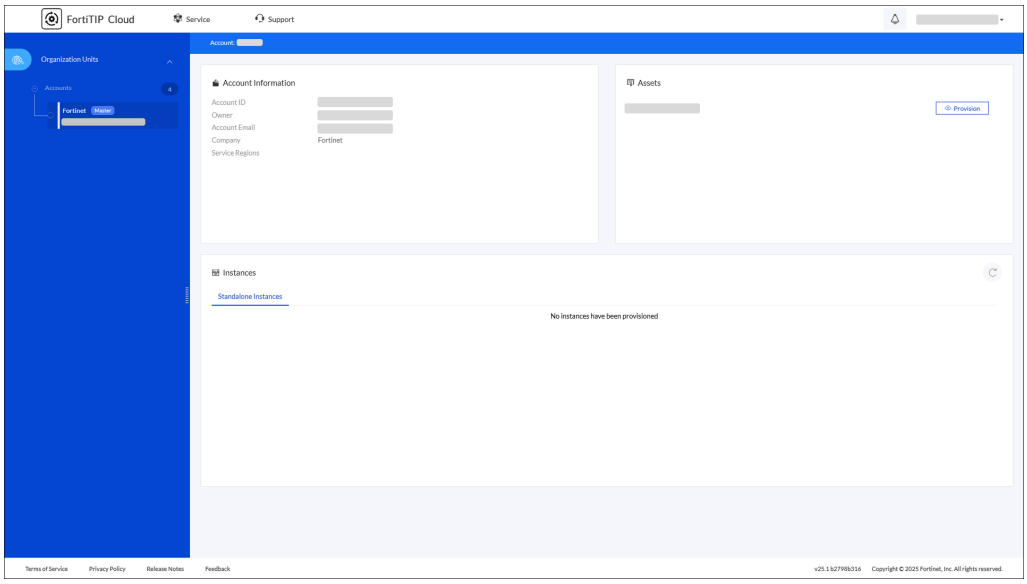
Before deploying FortiTIP Cloud ensure that you have a valid product entitlement for FortiCloud and note your account ID number from the FortiCloud portal.

If you have created a new FortiCloud account, wait 30 minutes before proceeding to the next step.

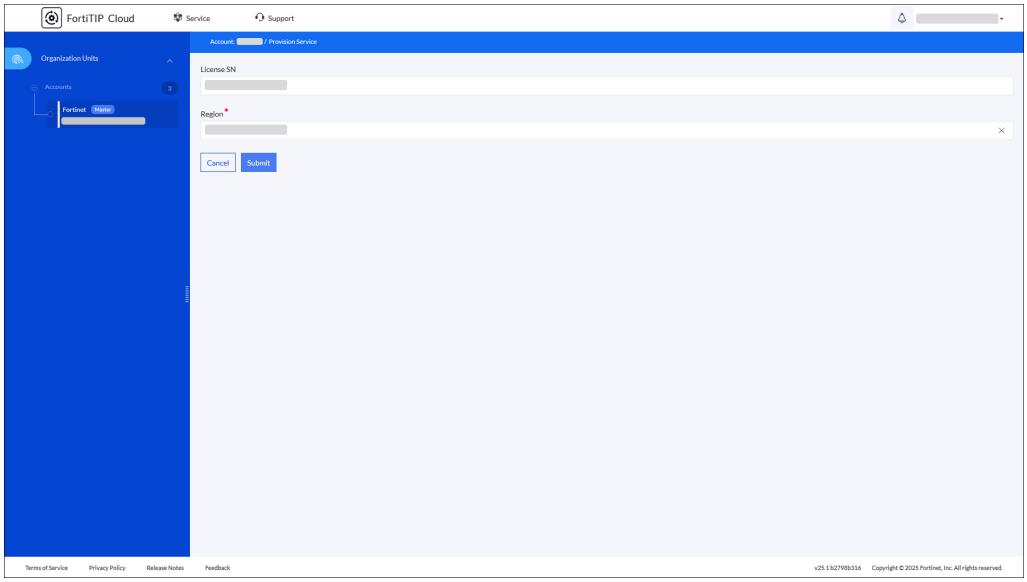
1. Click **Services** in the FortiCloud portal and select **FortiTIP Cloud** from the `Cloud Management` section to access your FortiTIP Cloud instance.



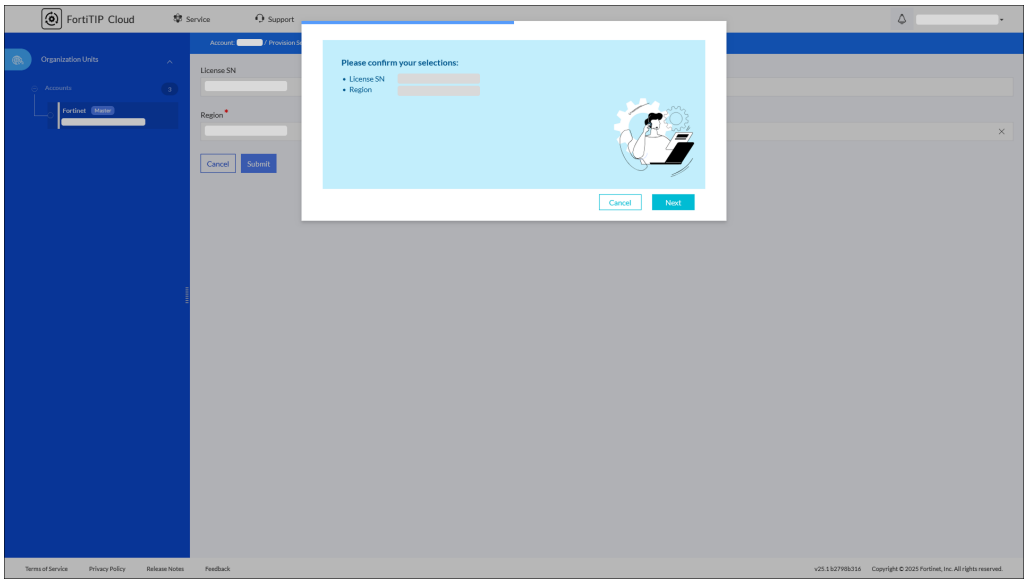
2. Select the Master FortiTIP Cloud account after logging in FortiTIP Cloud, to view the account information, including the account ID and the list of associated assets.



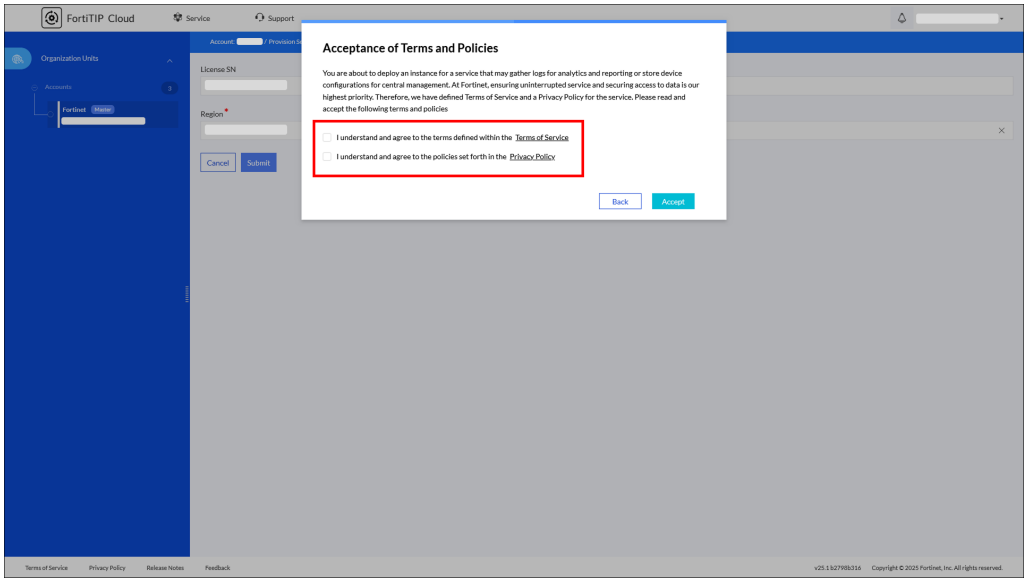
3. Click the **Provision** button, under the `Assets` section, next to the license serial number for the FortiTIP Cloud instance you wish to provision:
4. Verify the license serial number and select the **Region** where the instance has to be provisioned.



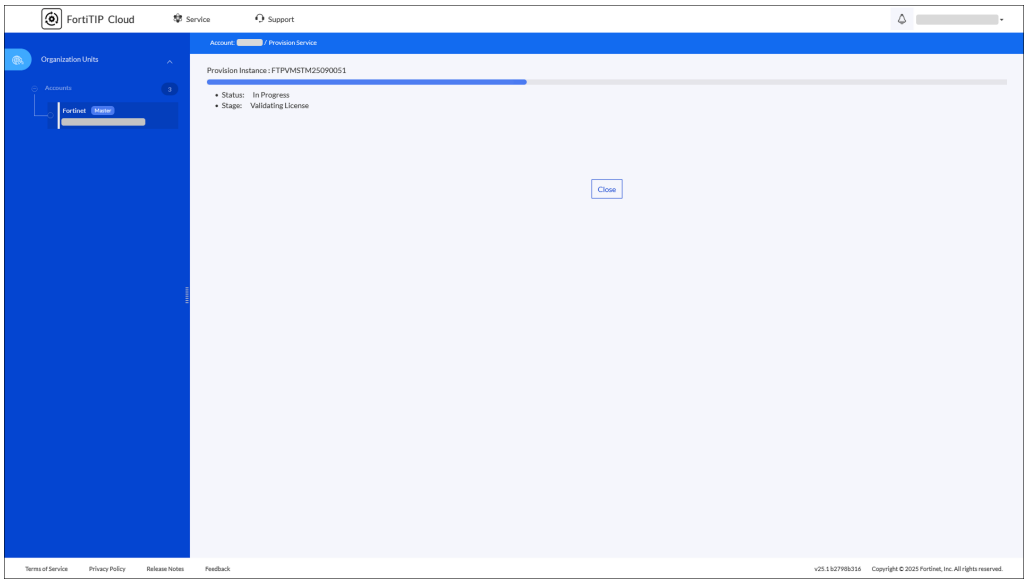
5. Click **Submit** to open a pop-up displaying your selections.



6. Click **Next** to open the **Acceptance of Terms and Policies** dialog.



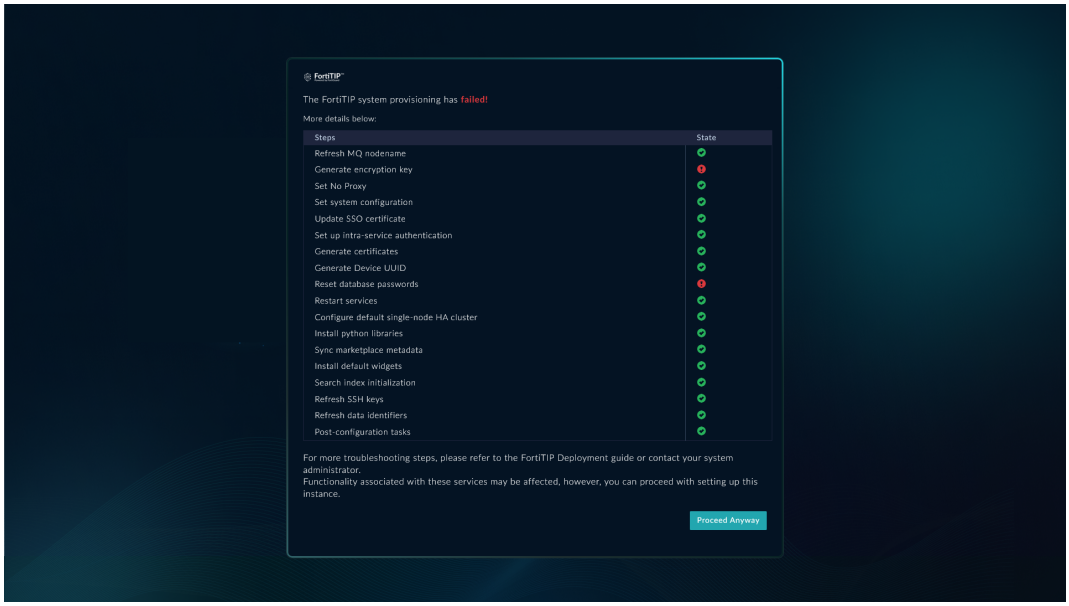
7. Select the **Terms of Service** and **Privacy Policy** checkboxes and click **Accept** to initiate the provisioning of the FortiTIP Cloud instance. The provisioning process takes a few minutes.



During provisioning, initial configuration steps for FortiTIP Cloud are performed. These steps include running the automated, non-interactive FortiTIP Cloud configuration wizard, enabling the embedded Secure Message Exchange, triggering the heartbeat between FortiCloud and FortiTIP Cloud, and installing the license.

FortiTIP Cloud VM provisioning is considered successful once FortiCloud receives the first heartbeat from FortiTIP Cloud.

If there are any provisioning issues, such as failures during the initial configuration phase using the automated non-interactive FortiTIP Cloud configuration wizard, including failures while configuring the embedded Secure Message Exchange, then a failure screen detailing the status of each configuration step is displayed, making it simpler to identify the issue. Before using FortiTIP Cloud, you must use WebSSH to resolve the issue before proceeding. If you choose to continue without fixing the issues, FortiTIP Cloud functionality may be impaired. A **Proceed Anyway** button allows you to continue, acknowledging the configuration failure:



If your instance is still not accessible after clicking **Proceed Anyway**, you can try the following steps to fix the issues:

- Restart all the services using the following command.

```
csadm services --restart
```

- Manually install *ansible* in the case of an ansible installation error using the following command:

```
sudo -u nginx /opt/cyops-workflow/.env/bin/pip install ansible==7.4.0 --extra-index-url
https://repo.fortisoar.fortinet.com/prod/connectors/deps/simple/
```

- If the failure screen keeps appearing on the FortiTIP Cloud UI, even after you have attempted to resolve all the backend issues, you can try to update the `fsr-boot.json` to update its state from *`failed`* to **`config_vm_failure_acknowledged`**.

Contact support if failures persist even after troubleshooting.

After successful provisioning, access the FortiTIP Cloud web GUI by clicking **Login** or click **WebSSH** to access the FortiTIP Cloud console.

Important Notes before using FortiTIP Cloud:

- After provisioning, it is strongly recommended to log into the WebSSH interface and immediately change the default password for the '`csadmin`' user. This improves the security of your FortiTIP Cloud instance.
- Only the primary account holder can create secondary account holders in FortiCloud. Secondary account holders can log into the same instance as 'restricted'. The primary account holder can modify the secondary user's admin profile. For more information, see the Adding a secondary account chapter.
- It is highly recommended to set up a backup user for the FortiSOAR appliance. This ensures access to the CLI in case the '`csadmin`' CLI password is forgotten or the `csadmin` user gets locked. For the steps to create a backup user, see the Creating a backup user for the FortiSOAR appliance to allow access to the CLI topic in the *Deploying FortiSOAR* chapter of the "FortiSOAR Deployment Guide."
- To restrict access to your FortiTIP Cloud instance, contact the FortiCloud team to add IP addresses to the allowlist. Only the listed IP addresses will be able to access your FortiTIP Cloud instance.

Adding an organization

You can create an organization for FortiTIP Cloud, which serves as a centralized account management service. This allows you to consolidate multiple FortiTIP Cloud accounts into Organization/Organizational Units (OUs). The organization service provides a unified interface across FortiCloud accounts, enabling you to manage assets, cloud services, invite accounts, group accounts hierarchically (using OUs), and assign access roles for user permissions. For more information, see the FortiCloud Account Services Organization Portal documentation.

To create your organization, for example, 'Fortinet FortiSOAR', follow the steps outlined in the FortiCloud Account Services Organization Portal documentation. The account used to set up the organization will act as the `root` account. Authorized users can add OUs and invite members to join the organization. OUs serve as folders that organize accounts and define the structure of the organization. You can create up to three levels of OUs.

After setting up the organization and OUs, you can invite member accounts to join the OUs using invitation tokens as described in the FortiCloud Account Services Organization Portal documentation. Additionally, you can add an administrative *IAM user* for the organization to create and manage IAM users within the OUs. For more information, see the Adding a secondary account on page 11 chapter.

Adding a secondary account

You can create a secondary account for FortiTIP Cloud to allow the Fortinet support team to troubleshoot FortiTIP Cloud deployment. Secondary accounts can be added using Identity & Access Management (IAM), FortiCare, or by setting up External IdP roles. IAM helps manage access to FortiTIP Cloud portals and assets, controlling user permissions, authentication credentials, and asset access.

Organizational Units (OUs) are only visible to IAM users, not secondary users added via FortiCare.

Adding a secondary account using IAM

1. Login to Fortinet support.
2. Navigate to **Services** > **IAM**.
3. Before you can create IAM users, you must first create permission profiles, which define the level of portal access and permissions a user has. Permission profiles allow you to explicitly enable or disable access to FortiTIP Cloud portals and grant portal-specific permissions for the enabled portals. To create permission profiles:
   a. Click the **Permission Profiles** menu item on the IAM portal:
   b. Click **Add New** to open the `New Portal Permission Profile` page:
      i. In the `Basic Info` section, provide the necessary details to create the permission profile as per your requirements. For information on creating permission profiles, see the FortiCloud Account Services Identity & Access Management documentation.
      ii. Click **Add Portal** to display the `Add These Portals To My Account` pop-up. Use this pop-up to assign portal permissions to the user. You can select the following permissions: Asset Management, FortiCare, FortiTIP Cloud, IAM, etc and click **Add**:
      iii. In the `Permissions Profile` section, select the access type you want to assign to the user for the selected permission profiles, and click **Submit**:
      This adds the permission profile that can be assigned to users:
4. To add a new IAM user:
   a. Click the **Users** menu item on the IAM portal, and then select **Add New** > **IAM User**
   b. On the `IAM User` page, fill in the user details and click **Next**.
   c. On the `User Permissions` page, assign the IAM user the appropriate permission type, scope, profile, etc., then click **Next**.
   d. Click **Confirm** to complete the user creation process.
5. On the `Successful User Registration` page, click **Generate Password** to generate a reset password link for the user to login. This password will expire in 5 days.
   Regenerating the password renders the previous password invalid.

6. Navigate to Fortinet Support.
7. Click the **IAM Login** tab.
8. Enter your account ID, username, and new (regenerated) password, then click **Log in**.
9. Once logged in, select **Services** > **FortiTIP Cloud** to access FortiTIP Cloud.

Adding a secondary account using FortiCare

1. Login to Fortinet Support.
2. Click the user profile in the top-left corner and select **My Account** to display the `Account Profile` page.
3. Click **Manage User** and then select the new user icon to add a user.
4. When creating an account for the Fortinet support team, specify an email for the secondary account and select either **Full Access** or **Limit Access**.
   - **Full Access**: Grants the same access as the primary account user.
   - **Limit Access**: Restricts access to managing only the assigned product serial number and excludes renewal notices and the ability to create additional secondary accounts.
5. In the FortiTIP Cloud section, the new account will appear as a secondary member. Click the entry to expand the view.

A secondary account can access the portal thirty days after it expires.

Modifying a secondary account

The new user must log in to FortiSOAR Cloud for the account to be displayed in the FortiSOAR instance.
When a new user logs into their account, they are automatically assigned Admin roles on FortiSOAR if they are added as Full Access users in FortiCare, and SOC Analyst roles if they are added as Limited Access users in FortiCare.

The primary user or a super user can update user accounts, including changing permissions or updating contact details. To modify a secondary account:

1. Use the primary or super user credentials and login to Fortinet Support
2. Click **My Account** > **Manage Users**, which displays the `Manage User` page containing a list of users.
3. Select the user whose account you want to modify to display the `User Details` page.
4. On the `User Details` page, click **Edit**.
5. On the `Edit User` page, modify the user account as required and click **Save**. For example, change the Permissions from 'Full Access' to 'Limit Access'.

Setting up External IdP roles

External IdP roles allow external users to log in to the FortiCloud portal using their company's credentials via a third-party ID provider. The company's ID provider verifies the identity of external IdP users. After authentication, users can access the cloud application based on their role.

Brief process to set up External IdP roles is as follows:

1. Send an enrolment request to forticloud-enroll-extidp@fortinet.com.
2. The FortiCloud team will review and approve the request.
3. Once the approved, the FortiCloud FAC and Customer Ops teams will configure and link the External IdP to the relevant FortiCloud accounts.

For more information on External IdP, see the `External IdP roles` topic in the *Identity & Access Management (IAM)* guide of the FortiCloud Account Services documentation.

Once the External IdP integration is complete, log into FortiCloud, and ensure that the defined External IDP role has access permissions in the FortiTIP Cloud's `Permissions Profile` section of the IAM portal.

Additionally, note that after logging into FortiCloud, you will be directed to the Asset Management portal, from which you can access the FortiTIP Cloud portal with the same External IdP user access.

Identifying the public IP address

You can use the FortiTIP Cloud CLI to determine the public IP address associated with FortiTIP Cloud.

To determine the public IP address:

1. Login to Fortinet Support.
2. Click **Services** > **FortiTIP Cloud**.
   If FortiTIP Cloud is not visible, click on the **Show More** link to reveal all the available services.
3. On the FortiTIP Cloud portal, click **WebSSH** to access the FortiTIP Cloud console.
4. On the SSH Login page, enter your credentials to access the FortiTIP Cloud instance,
5. Run the following command to retrieve the public IP address:

```
[csadmin@<primary-user-id-here> ~] $ curl ifconfig.me
```

You can use this public IP address to establish connections with third-party services, such as the AWS Management Portal for vCenter.

Beginning with FortiTIP Cloud

Accessing FortiTIP Cloud

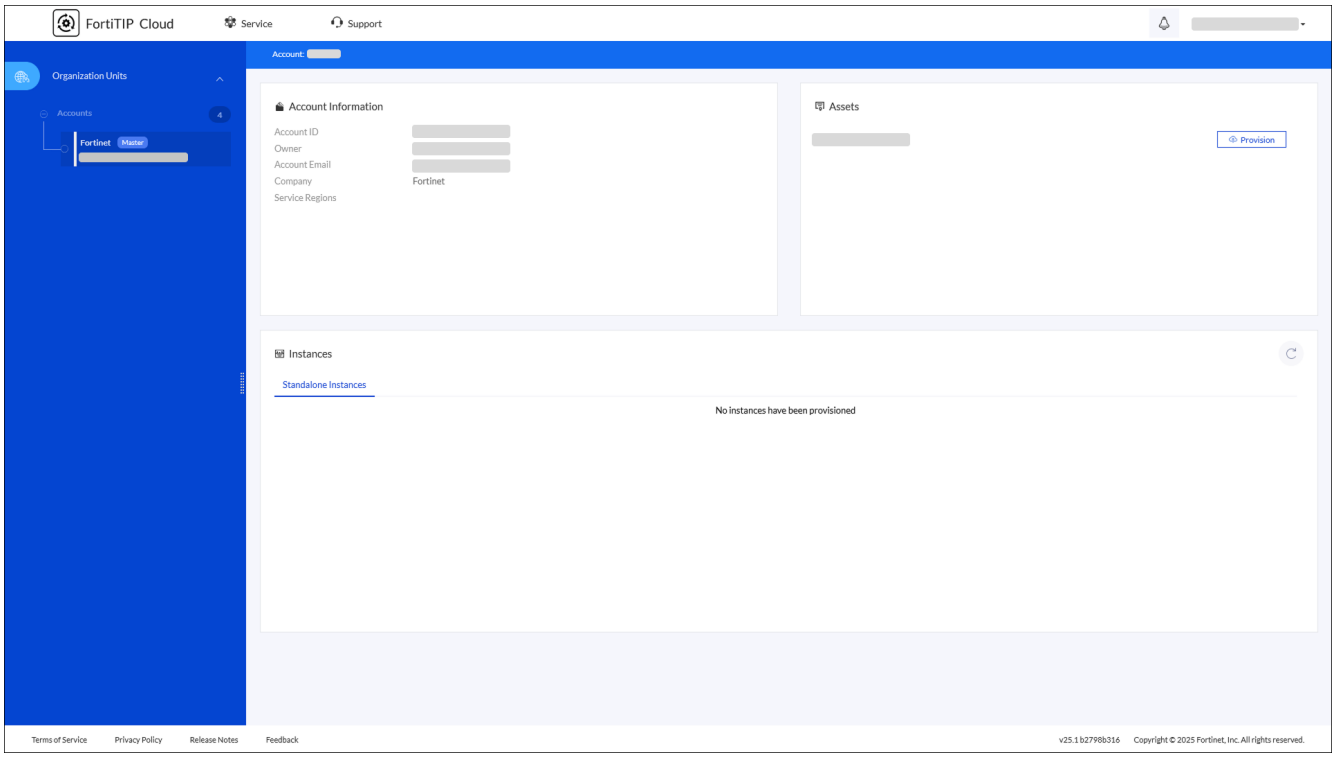
You can access FortiTIP Cloud in the following ways:

- Using fortitip.fortinet.com - This displays the FortiTIP Cloud portal's landing page.
  Click **Log in** to view the `Organization Unit (OU)` or `Accounts` page, which lists the master account and all the sub-user accounts.
  Select the account whose details you want to view.
- Using support.fortinet.com - This directly displays the `Organization Unit (OU)` or `Accounts` page if the FortiTIP Cloud instance is provisioned with a valid license.

Selecting an account on the `Organization Unit (OU)` or `Accounts` page displays a page containing details of the selected account, including assets, instances, and clusters associated with it.

The **Master** tag indicates the master account, while others are sub-user accounts.

Provisioning can only be done by the **Master** account.

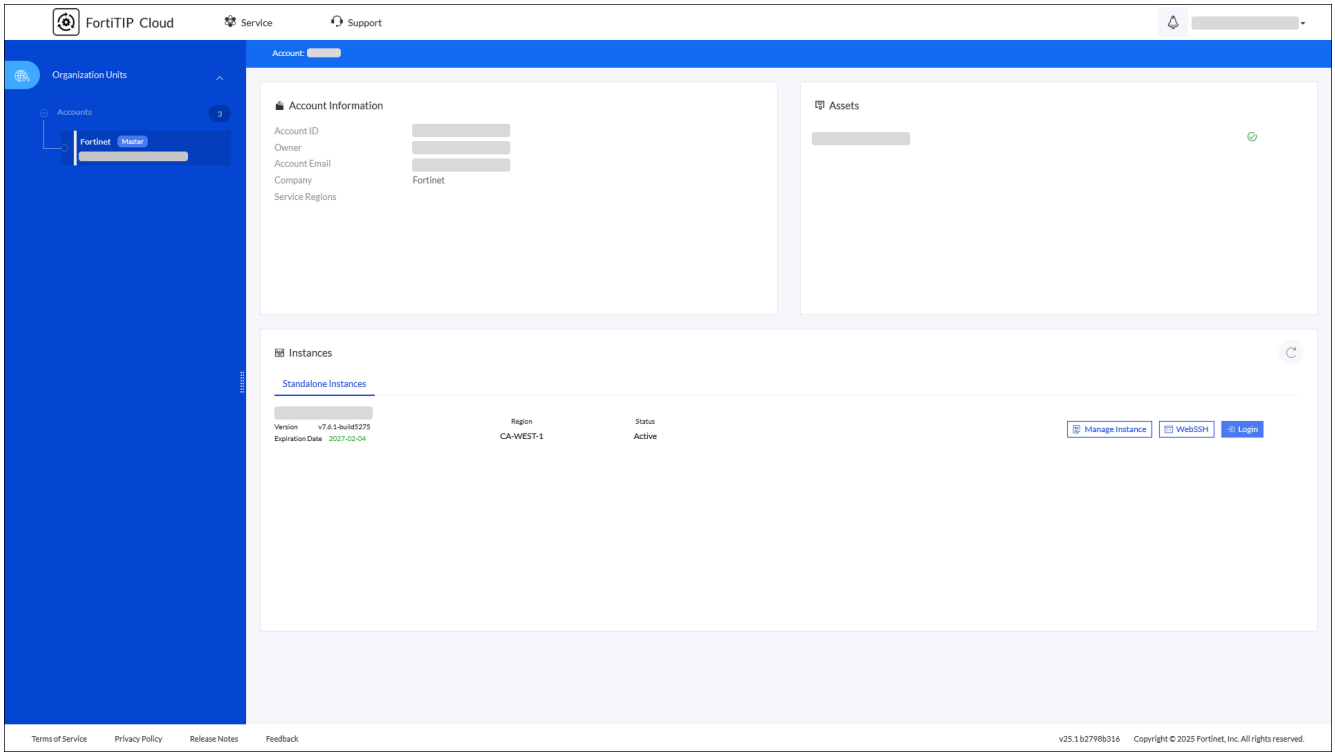


The account page displays the following details:

- **Account Information**: Displays general information about the account including its ID, owner, email address, company, and service region.
- **Assets**: Displays a list of assets (active licensed instances) associated with the account. Icons and buttons next to an asset indicate its status:
  - **Green Check** icon: Successfully provisioned instance.
  - **Blue Provision** button: Instance yet to be provisioned.
  - **Red Provision** button: Provisioning failure for the instance.
    NOTE: If provisioning fails for an instance, click the **Red Provision** button to view failure details.
  - **Expired** text in red: License for the instance has expired.
- **Instances** This section includes the following options:
  - **Instances**: Displays a list of provisioned standalone instances. Each row provides brief details of the instance including its version, expiration date, region and status. You can also use the following buttons:
    - **Login**: To access the FortiTIP Cloud UI. For more information, see the Accessing FortiTIP Cloud UI on page 16 topic.
    - **WebSSH**: To access the FortiTIP Cloud console. For more information, see the Accessing FortiTIP Cloud console on page 16 topic.
    - **Manage Instance**: To view and manage the instance . For more information, see the Instance page details on page 15 topic.

Instance page details

The `Manage Instance` page provides details such as the instance ID, license information, disk usage etc., and is used to manage the instance.



It includes the following sections:

- **Instance Information**:
  - **General**: Displays details such as the instance ID, its expiration date, FortiSOAR release on which the instance is provisioned, such as release 7.6.1-5275, its status, etc.
    You can reboot the instance by clicking the **Reboot** button.
- **License Details**: Displays details such as the type of license deployed on the instance, the start and end date for the license, etc.
- **Disk Usage**: Displays disk usage details in percentage and numbers.
- **Resource Usage**: Displays the vCPU and RAM usage.

Accessing FortiTIP Cloud console

1. To access the FortiTIP Cloud console, click **WebSSH** on the FortiCloud portal.
   If you are logging into the console for the first time, use the default SSH credentials: `csadmin/<your account_id>`.
   After logging in, you will be prompted to change the default SSH password.
   Once updated, you will be logged out and asked to log in again with the new password.
2. Upon successful login, you will be presented with the EULA acceptance pages (2 pages). Click **Accept** to proceed and start using the FortiTIP console.

You can use the FortiTIP Cloud console to perform administrative tasks using the '`csadm`' commands in the console.

Accessing FortiTIP Cloud UI

To access the FortiTIP Cloud UI:

1. Click **Login** on the FortiCloud portal.
2. If the EULA has not been accepted, you will be prompted to do so. Once accepted, you will be logged into the FortiTIP Cloud UI.
   Your assigned role (Full Access or Limited Access) will determine the actions you can perform in FortiTIP Cloud.

Secure Message Exchange

The FortiTIP Cloud instance includes an embedded Secure Message Exchange (SME), which establishes a secure channel used to relay information to external agents. The address of the embedded SME is configured as the Cloud portal address, and the Server Name Indication (SNI) is set to the instance URL. The embedded SME runs on port 5671.

If the FortiCloud account is migrated, update the SNI to the URL of the new instance.

Setting Up Outbreak Management

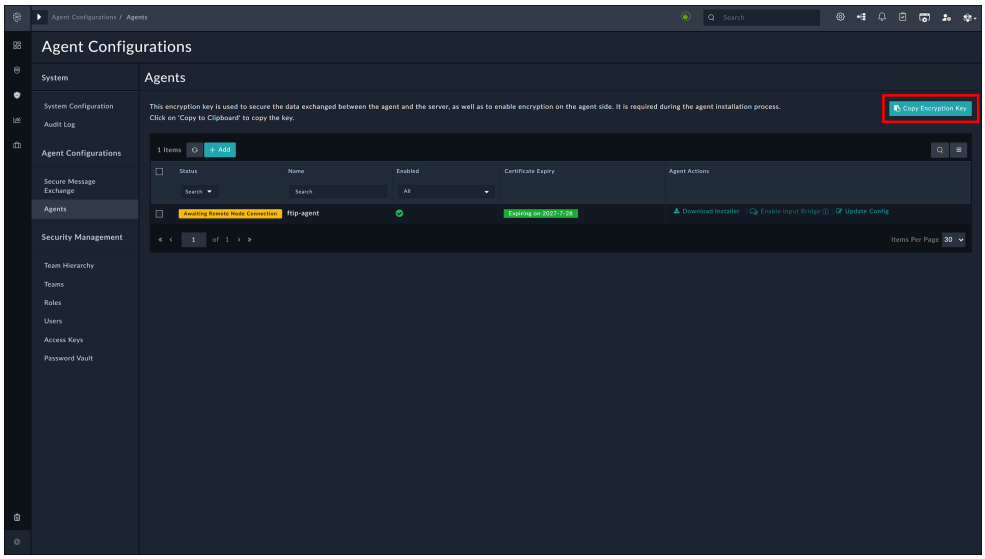
The Outbreak Response Framework configuration wizard streamlines the process of setting up FortiTIP Cloud with Outbreak Management.

Prerequisites

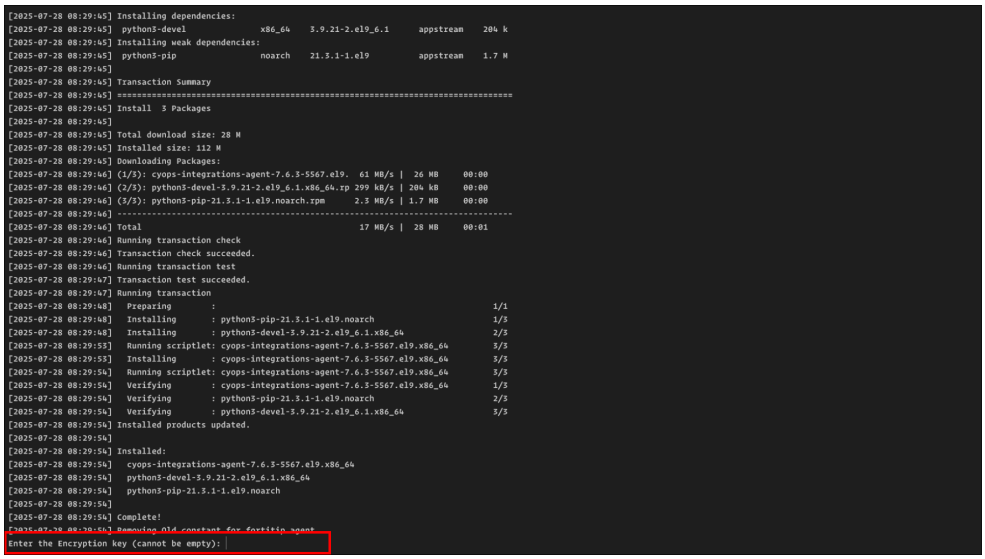
Outbreak Management on FortiTIP Cloud uses the Fortinet FortiAnalyzer connector to fetch and populate outbreak alerts. This execution of connector requires secure remote execution as Fortinet FortiAnalyzer is in a different network segment than the one where the FortiTIP Cloud is deployed. To connect to such endpoints in segmented networks, FortiTIP Cloud provides a lightweight agent.

To run FortiAnalyzer connector actions using an agent, you need the following:

1. **A virtual machine (VM) in the FortiAnalyzer network**: Refer to recommended specifications and Prerequisites for installing an agent sections in FortiSOAR product document
2. **Upgrade the Utilities Connector**: To ensure successful agent setup, upgrade the *Utilities* connector to the latest version before adding the agent. For information on upgrading a connector, refer to Working with connectors on FortiSOAR product documentation.
3. **An agent added to FortiTIP Cloud**: Refer to Adding an agent on FortiSOAR product documentation.
   - Once added, copy the encryption key by navigating to **Settings** ⚙ > **Agents**.



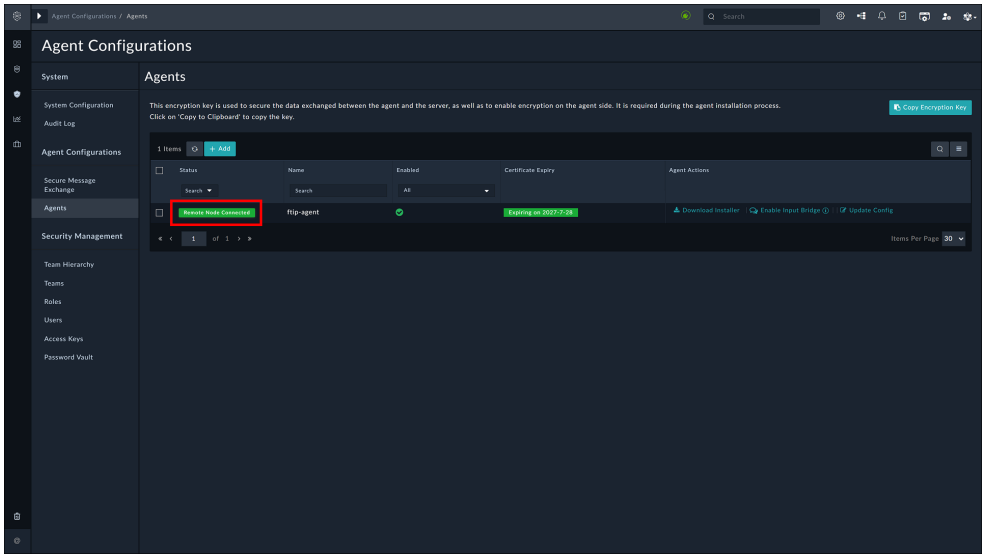
4. **An agent installed on the VM**: Refer to Installing an Agent on FortiSOAR product documentation.
   - When prompted, enter the encryption key copied while adding an agent.



   - The following message confirms a successful agent deployment:

```
Agent Deployed Successfully
```

   - On FortiTIP Cloud, navigate to **Settings** > **Agents**. The remote node status turns green upon successful agent deployment:

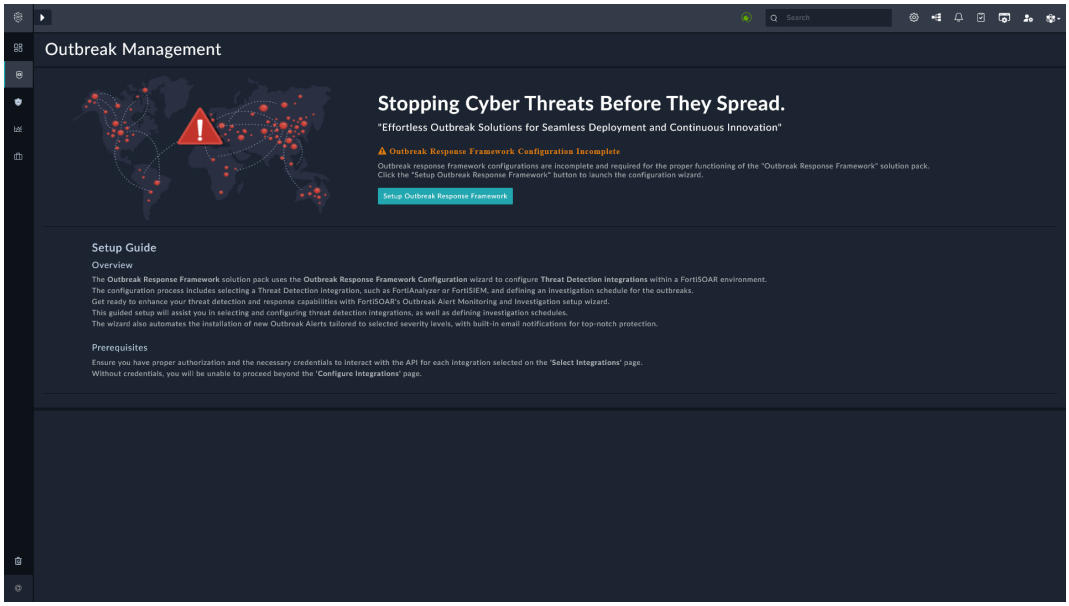


5. **Fortinet FortiAnalyzer connector installed on the Agent**: Refer to Installing a connector on an FSR agent on FortiSOAR product documentation.
6. FortiAnalyzer connector configured with the agent on FortiTIP Cloud's Outbreak Management.

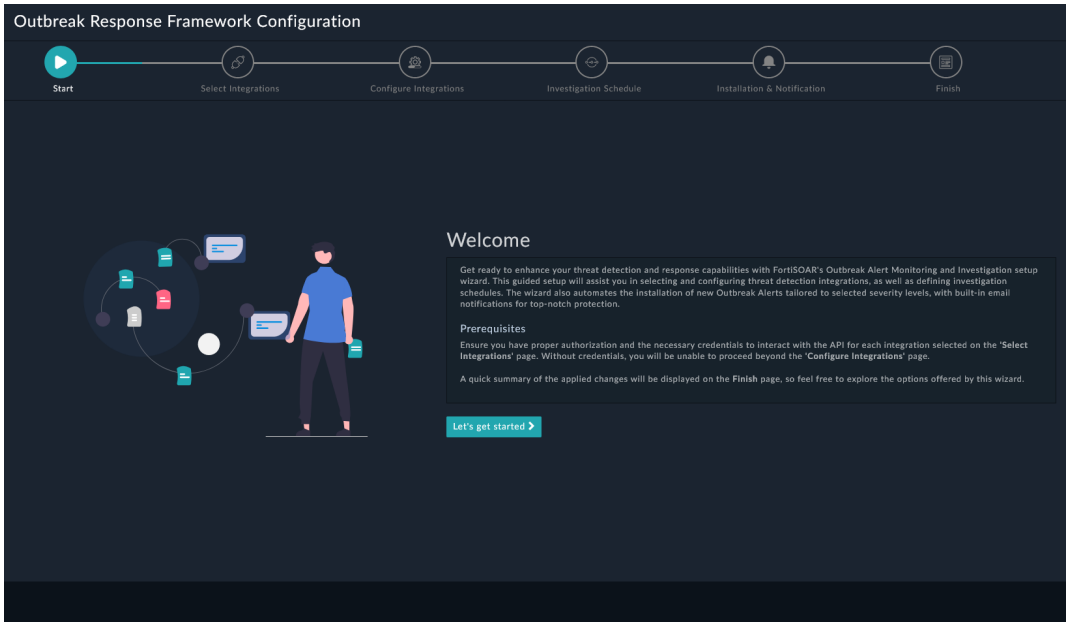
Launching the Outbreak Response Framework Configuration Wizard

You can launch the Outbreak Response Framework configuration wizard by any of the following methods:

- **From navigation menu**: Navigate to **FortiGuard Labs** > **Outbreak Alerts**, if running the wizard for the first time.
- **From Setup Guide**: Click the **Configure Outbreak Response Framework** button under **Setup Guide** > **Accelerate** > **Configure Outbreak Response Framework**.
- **From Content Hub**: Navigate to **Resources** > **Content Hub**, search **Outbreak Response Framework** and click the *Outbreak Response Framework* card.



After launching the configuration wizard, click the button **Setup Outbreak Response Framework**.

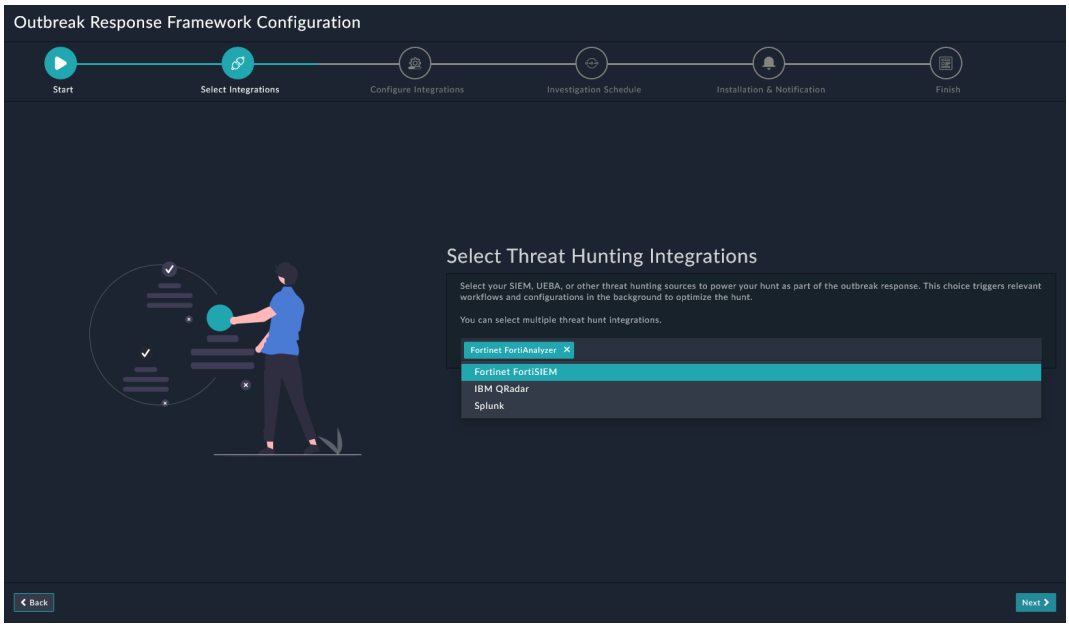


Click the button **Let's get started** on the configuration wizard.

Selecting Integrations

Select Threat Detection Integration sources to run outbreak response hunt activities and click **Next**.

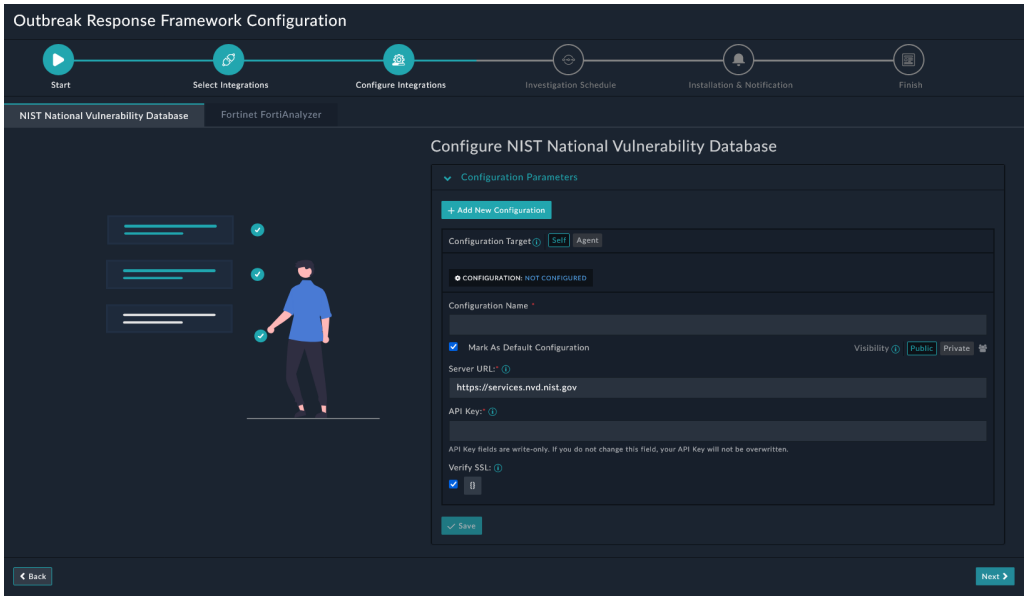
The hunt activities require searching for adversaries and their tactics, within an environment, against existing information available in the FortiTIP Cloud. The Threat Detection Integration sources help run the threat hunt activities and are an important part of the *Outbreak Response Framework*.



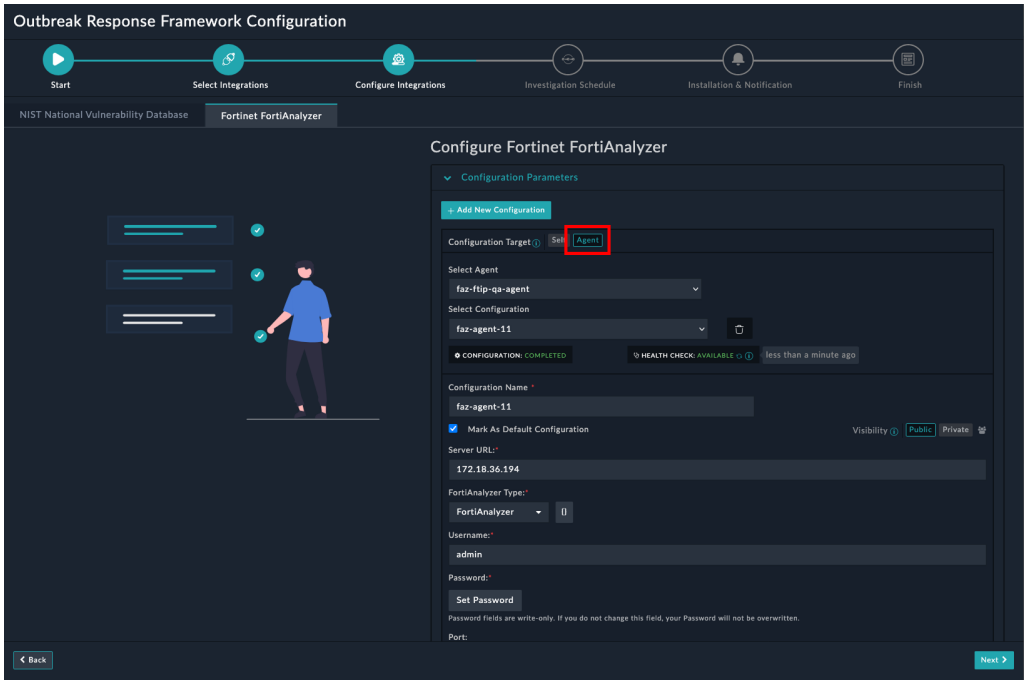
Configuring Integrations

Select each integration's tab to configure the associated connector and data ingestion parameters.

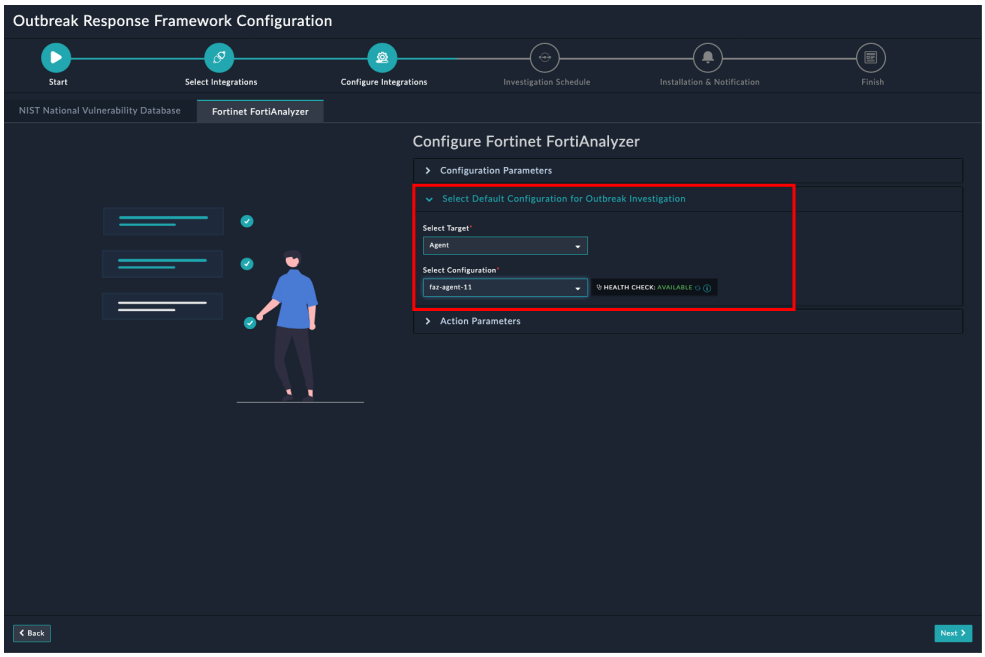
- Configure the NIST NVD connector: Refer to NIST NVD connector documentation for more information.



- Configure the Fortinet FortiAnalyzer connector on agent. If the agent is installed and configured, it appears under the **Select Configuration** drop-down.

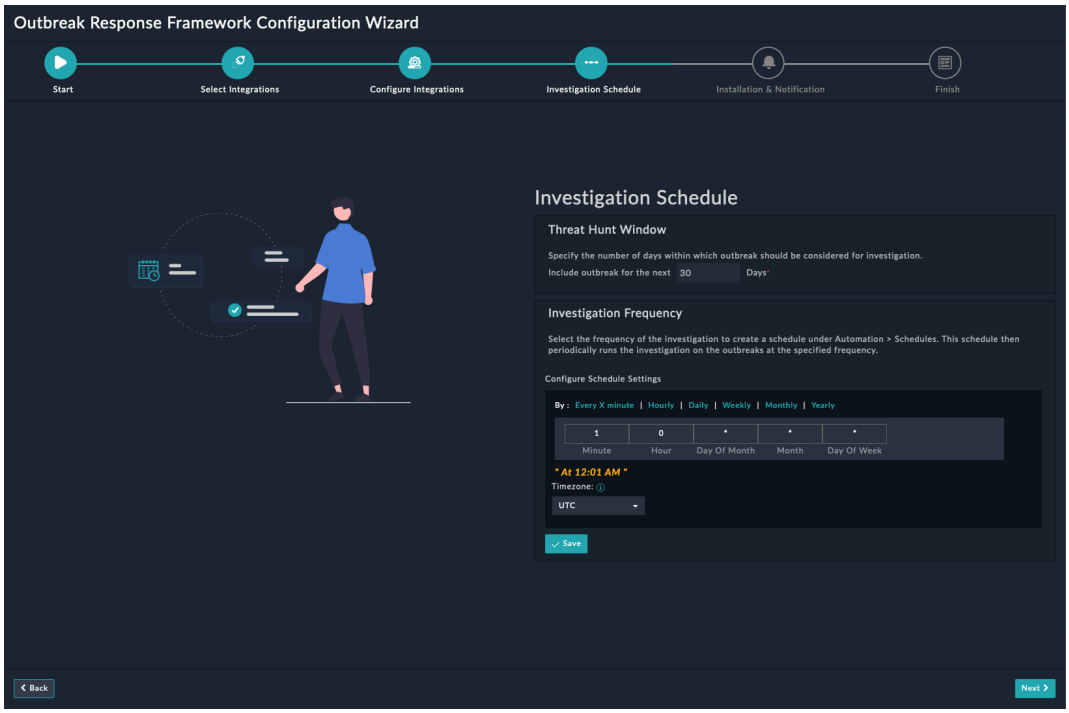


  - Select the default target and configuration to use when Outbreak Management executes the Fortinet FortiAnalyzer connector's actions.



Select the default target and configuration to use when Outbreak Management executes the Fortinet FortiAnalyzer connector's actions.

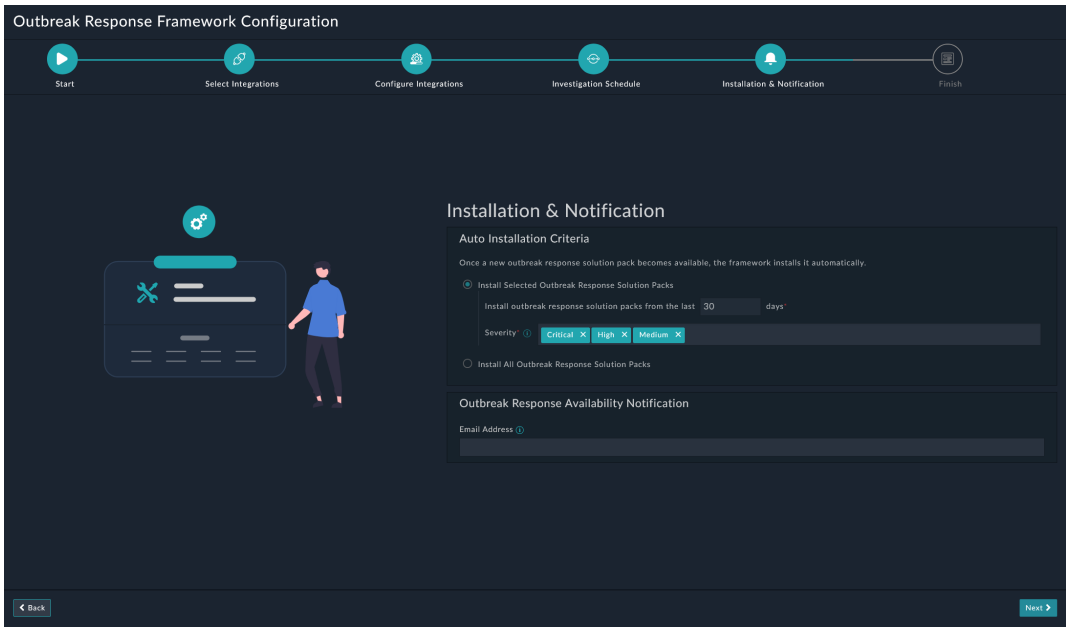
Specifying Investigation Schedule



- **Threat Hunt Window**: Specify the number of days as an interval within which outbreak should be considered for investigation.

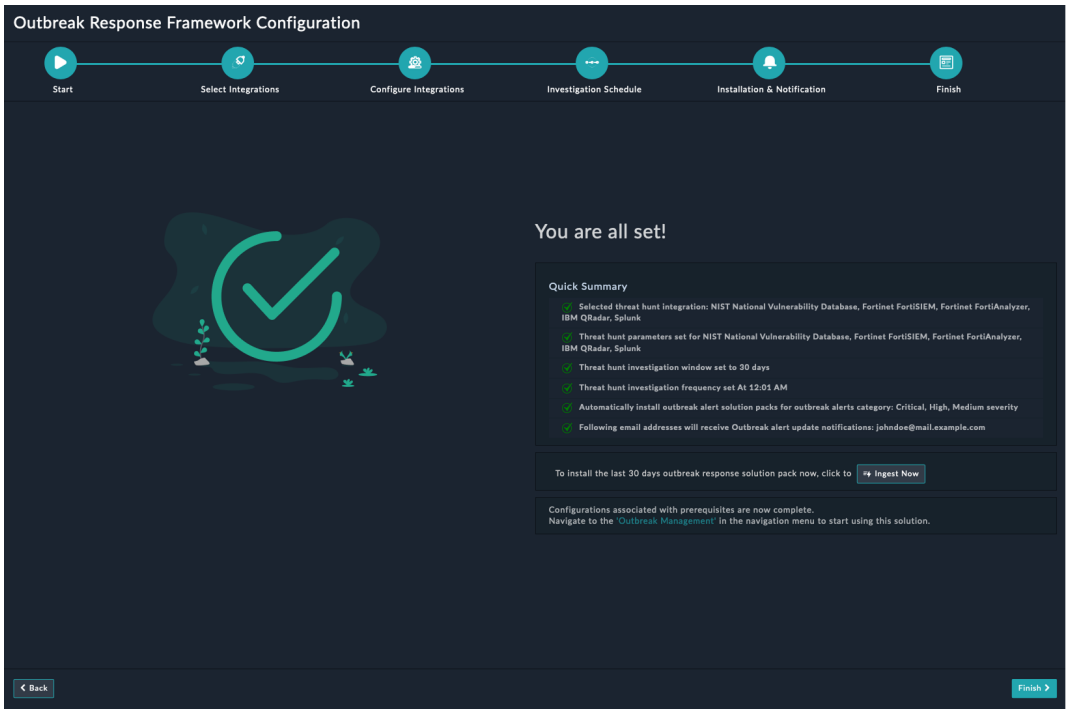
- **Investigation Frequency**: Select the frequency of the investigation to create a schedule. The created schedule can be found under Automation > Schedules. Once created, the schedule periodically runs the investigation on the reported outbreaks at the specified frequency.

Configuring Installation & Notification



- **Auto Installation Criteria**: Select one of the following options:
  - **Install Selected Outbreak Response Solution Packs**:
    Select the severity, and the last X days, of the outbreak to install the corresponding response solution pack. You can select one or more severity from the following options:
    - *Critical*
    - *High*
    - *Medium*
  - **Install All Outbreak Response Solution Packs**: Select to install all outbreak response solution packs.
- **Outbreak Alert Update Notification**: Specify email addresses authorized to receive outbreak updates. You can specify multiple email addresses separated by a comma.

Summarizing the Selected Configuration



Click the button **Ingest Now** to install the outbreak-specific response solution packs of the severity selected on the previous screen.

Click **Finish** to complete the configuration process.

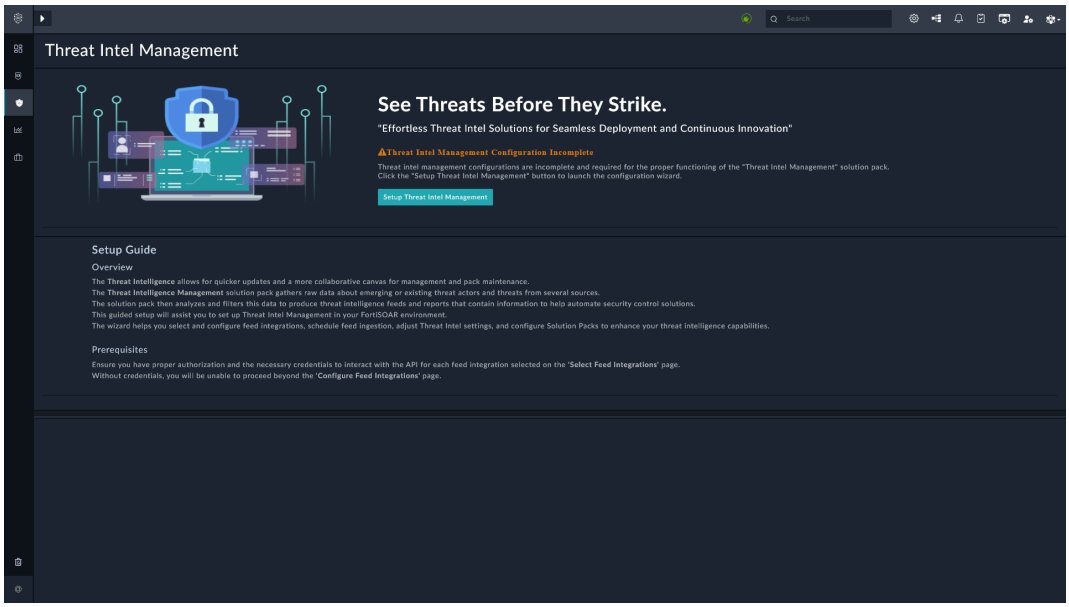
Setting Up Threat Intel Management

The Threat Intel Management configuration wizard streamlines the process of setting up FortiTIP Cloud with Threat Intel Management.

You must configure the NIST NVD connector before running the Outbreak Response Framework configuration wizard.

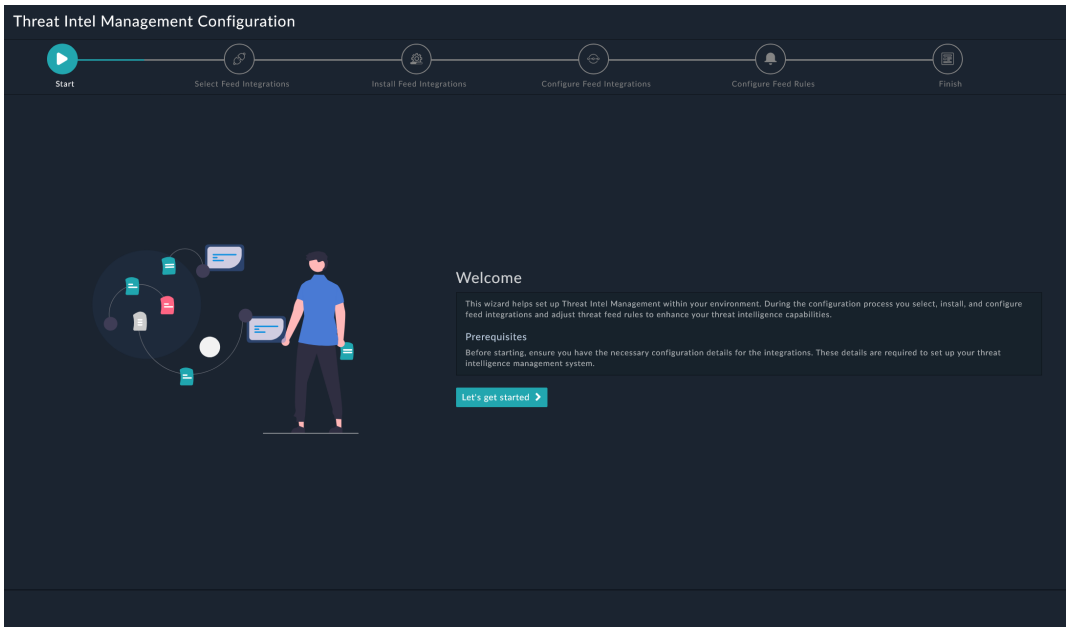
You can launch the Threat Intel Management configuration wizard by any of the following methods:

- **From navigation menu**: Navigate to **Threat Intel Management** > **Threat Intel Feeds**, if running the wizard for the first time.
- **From Setup Guide**: Click the **Configure Threat Intel Management** button under **Setup Guide** > **Accelerate** > **Configure Threat Intelligence Management**.



After launching the configuration wizard, click the button **Setup Threat Intel Management**.

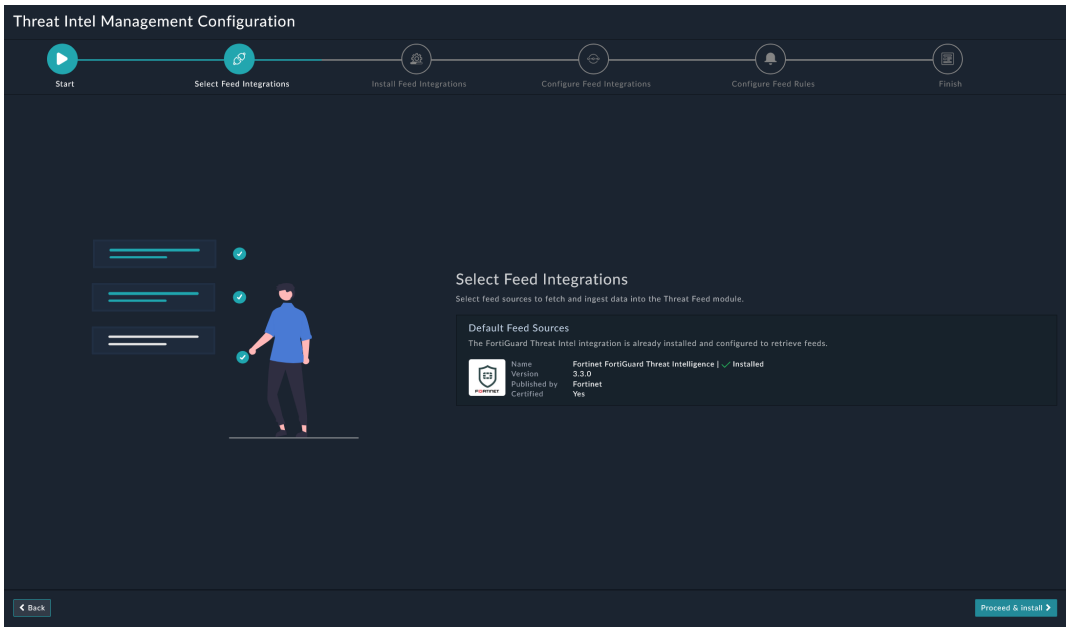
Launching Threat Intel Management Configuration Wizard



Click the button **Let's get started** on the configuration wizard.

Selecting Feed Integrations

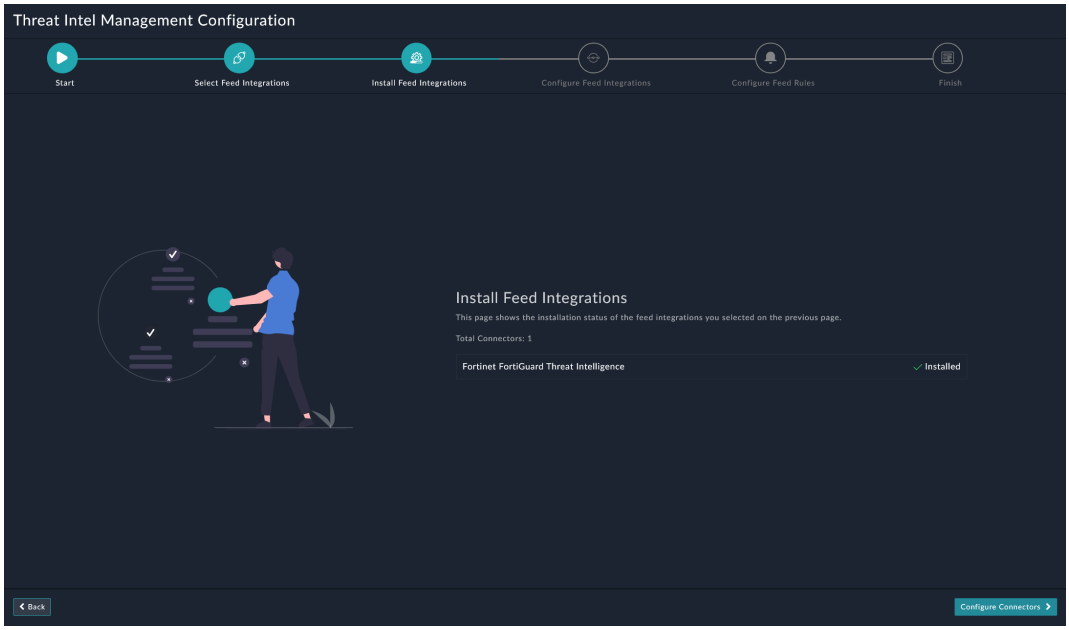
This Threat Intel Management configuration wizard page helps select integrations from where to fetch threat intel feeds.



The **Fortinet FortiGuard Threat Intelligence** connector is already installed and is listed under **Default Feed Sources**. Click the button **Proceed & Install** to proceed to the next step.

Installing Feed Sources

This Threat Intel Management configuration wizard page displays the installation status of the connectors selected for installation on the *Select Feed Integrations* screen.



Click the **Configure Connectors** button to proceed.

Configuring Feed Sources

This Threat Intel Management configuration wizard page helps configure feed integrations selected on *Select Feed Integrations* page and installed after *Install Feed Integrations* page.

Fortinet FortiGuard Threat Intelligence is already configured for use out-of-the-box.

- **Ingestion Parameters**: The ingestion parameters are retrieved from the configuration schema within the fetch playbook located in the data ingestion playbook collection. The ingestion parameters for each integration varies.

  The following parameters help adjust and save the fetch playbook configurations for use while creating the threat feeds, for **Fortinet FortiGuard Threat Intelligence**:
  - **Confidence**: Specify the confidence score to assign to the ingested feeds.
  - **Reputation**: Select the reputation to assign to the ingested feeds.
  - **TLP**: Select the TLP to assign to the ingested feeds.
  - **Expiry**: Specify the age of the feeds in days.
- **Ingestion Schedule**:
  - By default, the schedule is set to **Hourly**. To change the schedule, specify a `Cron` expression for the schedule or select some other frequency (*Daily*,).

Click the button **Configure Feed Rules** to set up and configure the threat feed rules.

The ingestion parameters and ingestion schedule become available only after the completion of configuration health check.

Configuring Feed Rules

We have introduced **Threat Feed Rules** to better leverage ingested feeds. These rules offer a structured framework for processing and analyzing threat feeds

You can configure the following feed rules to manage threat intelligence feeds from various sources like email file upload and :

- Linking Threat Feeds to Indicators
- Ingesting Unstructured Threat Feeds

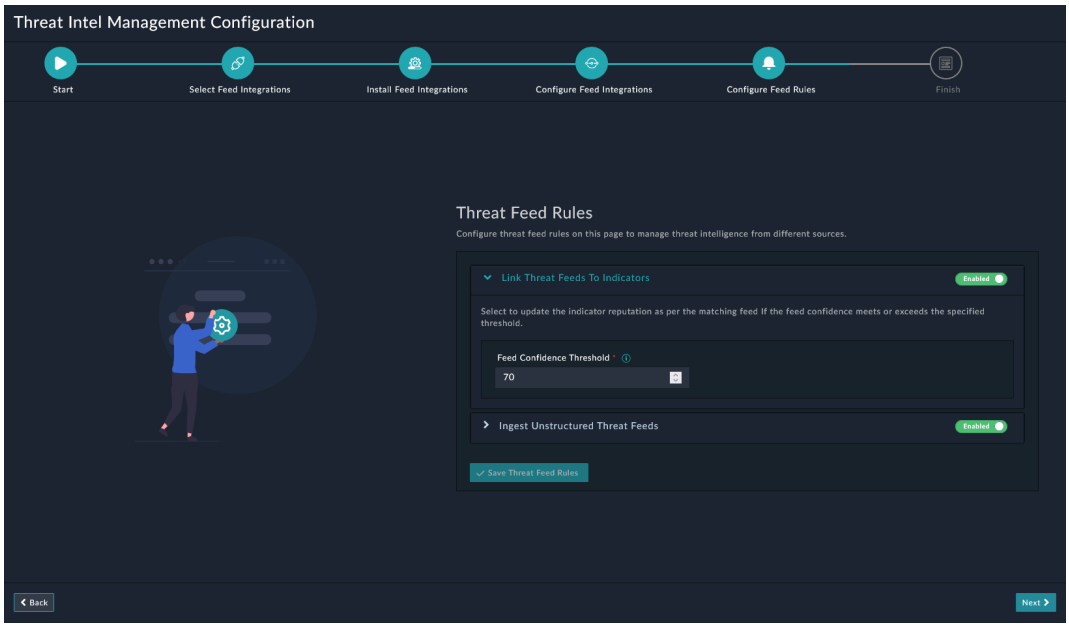
Linking Threat Feeds to Indicators

Enable this rule and specify a feed confidence threshold to automatically update indicators whose feed confidence is equal to or exceeds the specified feed confidence.

Feed Confidence Threshold: Specify a feed confidence threshold to link feeds, with confidence threshold equal to or greater than the specified value, to the indicator.

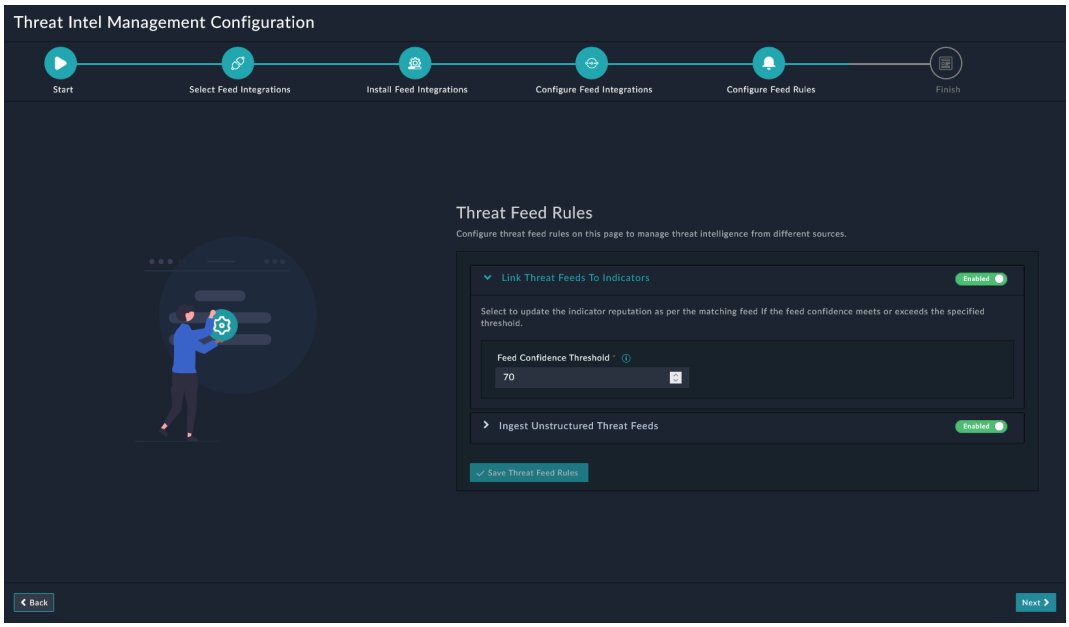
For example, if you set this value to 70, all feeds with a confidence level equal to or greater than 70 link to the indicator and update its reputation as per the feed.

The reputation is updated only for indicators created after the feeds ingestion.



Ingesting Unstructured Threat Feeds

Enable this rule to ingest unstructured threat feeds from file sources and email communications. This rule extracts critical threat feeds from unstructured data sources and automatically ingests it into the Threat Intel Feeds module.



Once enabled, you can further fine-tune the rule by defining the following parameters:

- **Ingest Threat Feeds from Files**: Select to ingest unstructured threat feeds by uploading a file. Supported file formats are `csv`, `txt`, `pdf`, `eml`, `json`, and `xlsx`. Refer to the section Importing Feeds from Files under *Usage* for more information.
- **Ingest Threat Feeds from Email Attachments**: Select to ingest unstructured threat feeds from email attachments.
  - **Email Server**: Select an email server from which to ingest emails. Currently, only *Exchange* is supported.
  - **Email Folder** : Specify the mailbox folder that contains all emails with feed attachments.

- Attachments of only unread emails are ingested, hence we recommend that you create a separate folder for emails with feed attachments with mailbox rules in place to redirect all such emails to this folder.
- The feeds are extracted only from attachments and not from the subject line or email body.

- **Ingestion Parameters**
  - **Confidence**: Specify the confidence score to assign to the ingested unstructured threat feeds.
  - **Reputation**: Select the reputation to assign to the ingested unstructured threat feeds.
  - **TLP**: Select the TLP to assign to the ingested unstructured threat feeds.
  - **Maximum Age (in days)**: Specify the age of the ingested unstructured threat feeds, in days.
  - **Source**: Specify a value to be updated as *Source* for all ingested unstructured threat feeds.
  - **Tags**: Specify comma-separated values to be assigned as tags to the ingested unstructured threat feeds.
- **Email Ingestion Schedule**: Specify the frequency at which unstructured threat feeds are ingested from emails. This schedule will then automatically run at the specified frequency to ingest unstructured threat feeds. For example, if you want to ingest emails every 5 minutes, click **Every X Minute**, and in the **minute** box enter `*/5`. This means that emails are ingested every 5 minutes.
  - **Timezone**: Select a timezone in which to export the report. Default is *UTC*.
- **Block Threat Feeds Automatically**: Select this option to block threat feeds immediately on ingestion.

Click the button **Save** to save the changes. Click **Next** to view the Configuration Summary on the **Finish** page.

For more information, refer to the Threat Feed Rules document on Threat Intel Management documentation on GitHub.

Finish

This page, apart from summarizing the configuration changes, also sets in motion the following:

- MITRE® integration's data ingestion is triggered resulting in MITRE®'s records like Techniques, Subtechniques, etc.for ingestion into FortiTIP Cloud™
- The following default data-sets are created:
  - FortiGuard Outbreak Threat Feeds
  - Phishing Threat Feeds
  - FortiGuard Threat Intel Feeds
  - Block List (Domain)
  - Block List (IP Address)
  - Block List (URL)

These data-sets can be viewed and managed from **Threat Intel Management** > **Threat Intel Feed**.

www.fortinet.com