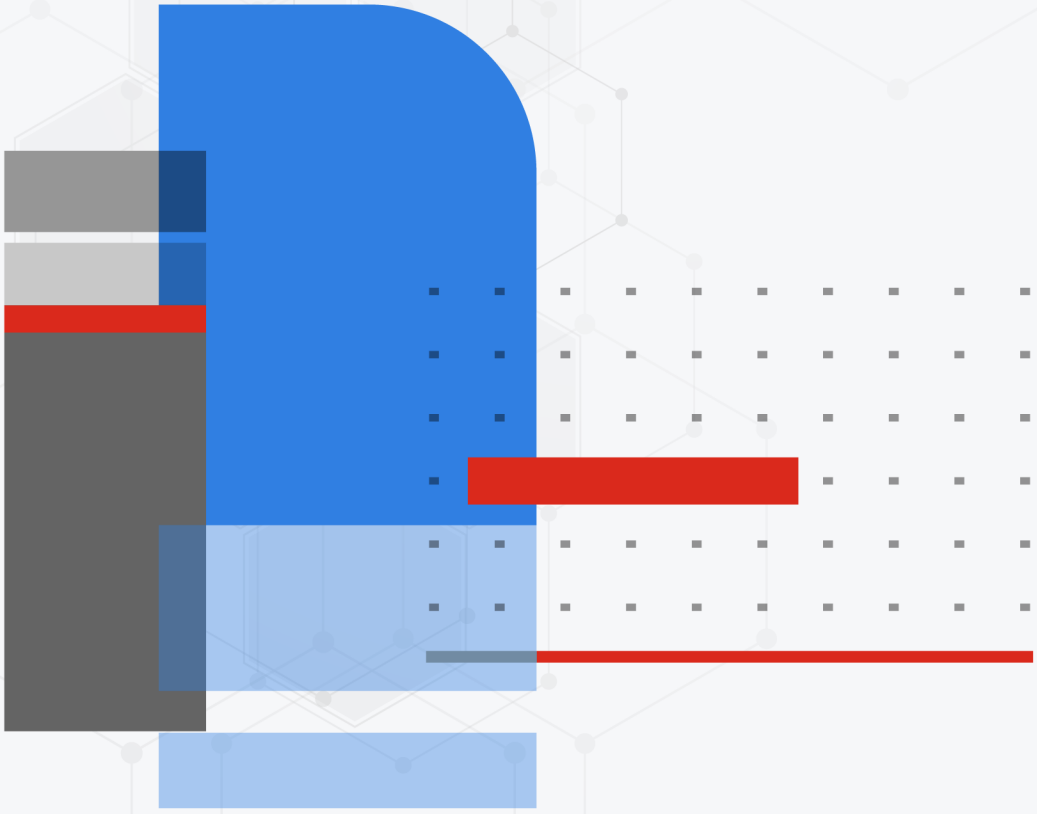
User Guide

FortiRecon 24.3.a



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

FORTINET VIDEO GUIDE
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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

October 22, 2024
FortiRecon 24.3.a User Guide
75-243-1080895-20240926

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-09-26	Initial release.
2024-09-27	Updated Creating a FortiRecon configuration in FortiFlex on page 31 topic.
2024-10-21	Updated Deploying IASM Agent topic.
2024-10-22	Updated System Requirements topic.

Introduction

FortiRecon is a Digital Risk Protection (DRP) service that operates alongside existing security solutions to provide you with both external and internal visibility into your infrastructure. This holistic view allows you to see your environment as an adversary would, enabling swift detection and mitigation of potential threats. The service maps your organization's digital footprint, both external and internal, while constantly monitoring it for abnormal activity. The service gives organizations the intelligence to mitigate credible security threats in a controlled manner as part of ongoing security efforts.

FortiRecon scans the organization's attack surface and identifies risks to assets across both external and internal domains while FortiGuard Threat Intelligence delivers early warning of risks to the organization through targeted, curated intelligence to provide an early warning of any malicious activity targeted to the organization.

The FortiRecon portal includes the following modules:

Overview	The *Overview* module provides a centralized view of your organization's digital risk posture across *Attack Surface Management (ASM)*, *Brand Protection (BP)*, and *Adversary Centric Intelligence (ACI)* modules. Discovered issues are mapped to relevant MITRE ATT&CK techniques and sub-techniques, providing a valuable framework for understanding attacker motivations and potential attack paths. See Overview.
Attack Surface Management	The External Attack Surface Management (EASM) module provides an adversary's view of the organization digital attack surface and prioritizes risks and exposures, enabling administrators to mitigate threats in a controlled manner before the threats become a problem. See EASM on page 49.
	The Internal Attack Surface Management (IASM) module provides visibility into internal network, identifying vulnerabilities within the organization's perimeter. It helps administrators discover internal assets, assess associated risks, and take mitigation steps. See IASM on page 68.
Brand Protection	The Brand Protection (BP) module continually monitors the organization's public-facing visibility for unauthorized changes, including web-based phishing attacks, typo-squatting, rogue applications, credential leaks, and brand impersonation in social media, which may impact brand value, integrity, and trust. See Brand Protection on page 100.
Adversary Centric Intelligence	The Adversary Centric Intelligence (ACI) module leverages FortiGuard Threat Analysts to provide comprehensive coverage of dark web, open source, and technical threat intelligence, including threat actor insights. This information enables administrators to proactively assess risks, respond faster to incidents, better understand their attackers, and protect assets. See Adversary Centric Intelligence on page 136.
Profile Settings	The Profile Settings module allows you to personalize your FortiRecon account and provide information on your organization. See Profile settings on page 192.

FortiRecon APIs are available on the Fortinet Developer Network (FNDN). You must first register an account on FNDN to gain access.

Requirements

A FortiCloud account is required to access the FortiRecon portal. The FortiRecon Admin for your organization also needs to create an account within FortiRecon. If either of these accounts is not created, you will not be able to log in to the FortiRecon portal. See the FortiCloud New Account Onboarding document and Getting started on page 15 for more information on registering your accounts.

If you need to create a support ticket, the FortiCloud account must be linked to your entitled license. There are two methods to link the FortiCloud account to your license:

- The account owner must create sub user accounts for all of the users in your organization. See User permissions in the FortiCloud Asset Management Administration Guide.
- Contact FortiCare support to request that your account be linked to the license in your organization. See Creating support tickets in the FortiCloud Asset Management Administration Guide.
- To access FortiRecon, Forticare or FortiCloud users must be sub users, not IAM users. IAM users are exclusively used for Organizations. See MSSP Onboarding.

Acceptable FortiRecon use cases

When using FortiRecon, there are certain acceptable use case requirements that must be followed to properly leverage FortiRecon's capabilities. FortiRecon use case requirements include the following:

- The FortiRecon solution must only be used for the licensed entity and its brands. See Requirements on page 9 and Licensing on page 10.
- Domains that are added for scanning and monitoring must be owned by the licensed entity.
- The licensed entity may not add the domains and apps of its customers, partners, or vendors to *Profile Settings* > *Seeds* or the *EASM* module for monitoring. However, up to 25 of these assets may be added for vendor monitoring in the *Adversary Centric Intelligence* module. See Vendor Risk Assessment on page 179.
- Bank identification numbers (BINs) should only be added for the licensed entity and brand. See Card Fraud on page 150.

Customer monitoring

Organizations, such as MSSPs, that want to set up monitoring for their customers can reach out to our account and sales team for suitable options.

Licensing

FortiRecon requires a license. You can choose to purchase a license for the following FortiRecon modules:

- External Attack Surface Management (EASM)
- Internal Attack Surface Management (IASM)
- Brand Protection (BP)
- Adversary Centric Intelligence (ACI)

In addition to the desired modules, the license also indicates the maximum number of assets to be monitored by FortiRecon. Following are the default capacities.

- *Takedowns*: 2
- *Executive Profiles for monitoring*: 10
- *Vendors for monitoring*: 25

Note: These are the default entitlements. Additional licenses are available for purchase, if needed.

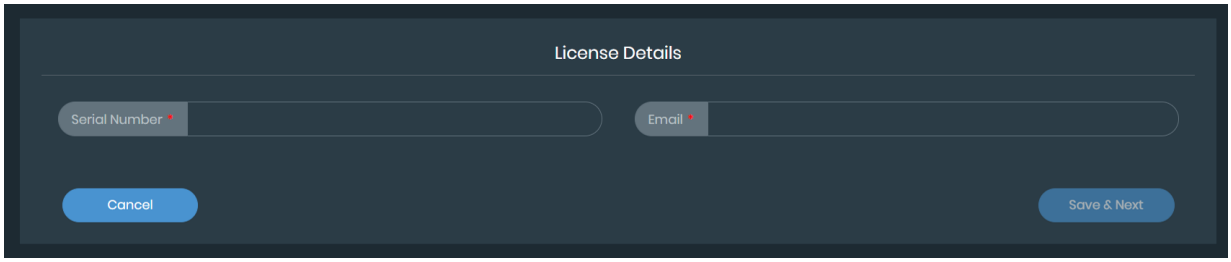
For details about the different modules and solution bundles, see the FortiRecon data sheet.

An EASM license is required to purchase an IASM license.

Upgrading Trial License

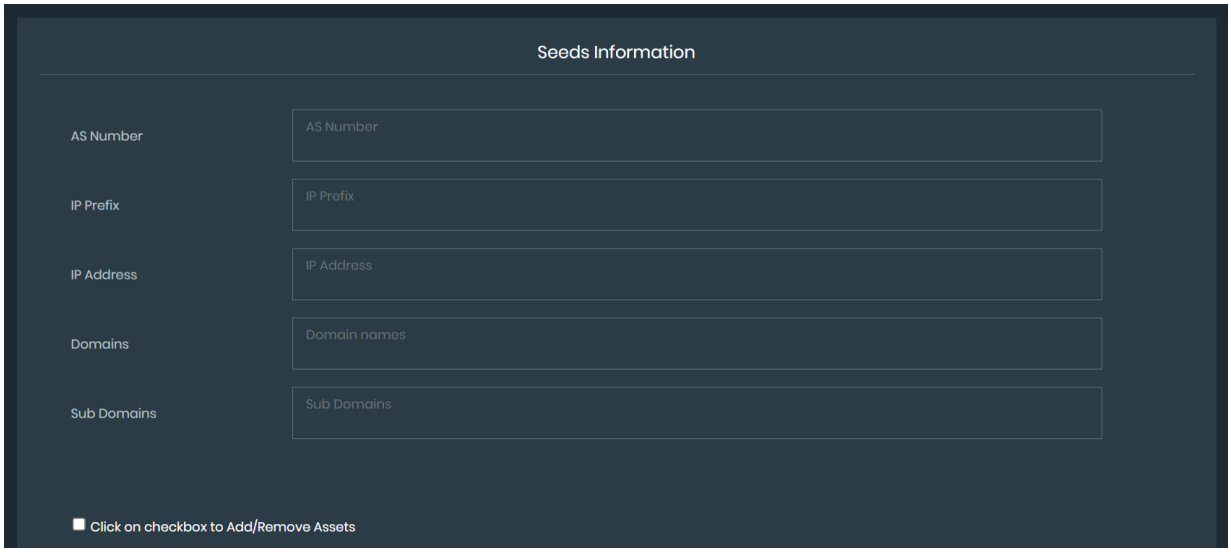
During the trial period, you have two options for upgrading:

1. **Purchasing a License**: You can purchase a license and add it to FortiRecon before the trial period expires. To add the purchased license, edit the serial and contract number fields in the *Profile Settings* page. Perfom the following steps to add a license.
   a. Go to *Profile Settings* > *Profile*.
   b. Scroll to *Subscription Details*
   c. Click edit icon next to *Contract Number*.
   d. Enter license serial number and email address used to purchase the license.



   e. Click *Save & Next*.
   f. Enter seed information. Based on the license purchased you will be able to add an additional domain or modify

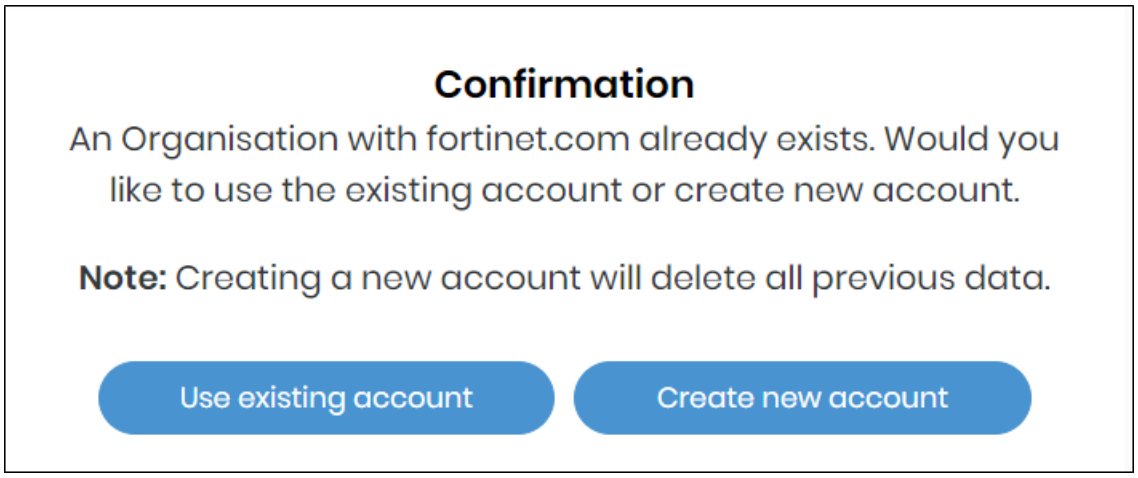
existing domain details. Select the *Add/Remove Assets* checkbox to add or remove assets.



2. **Expired Trial Period**: If the trial period has already expired, attempting to log in will display an expiration page. In this case, you can purchase a license, and perform the following steps.
   a. Log in to FortiRecon. The license expiration page is displayed. Enter the following information.
      - License Serial.
      - Contract Number.
      - Email that was used to register the contract.
   b. Click *Verify*.
   c. A One Time password (OTP) will be sent to your email and is valid for five minutes. Enter the OTP and click *Validate*. Click regenerate icon to generate a new OTP if needed.
   d. Once validated, enter the primary domain and click *Proceed*.
   e. A confirmation pop-up is displayed. Click *Use existing account* to continue with existing data, or click *Create new account* to create a new account.

      If you select *Create new account*, the FortiRecon Provisioning form is displayed. For more information on completing provisioning form, see Subscribing to FortiRecon.

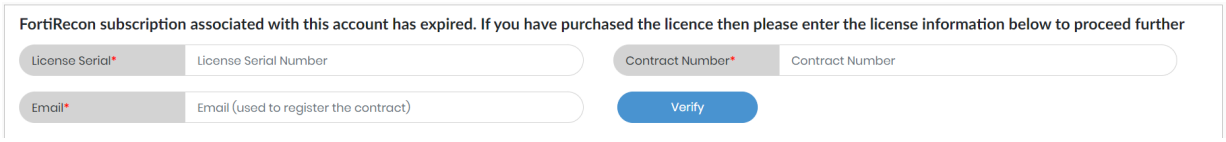
Creating a new account will delete all previous data.



Renewing Expired License

If your current license is expired, purchase a new license and perform the following steps to add it.

1. Log in to FortiRecon. The license expiration page is displayed. Enter the following information.
   - License Serial.
   - Contract Number.
   - Email that was used to register the contract.



2. Click *Verify*.
3. A One Time password (OTP) will be sent to your email and is valid for five minutes. Enter the OTP and click *Validate*. Click regenerate icon to generate a new OTP if needed.
4. Once validated, enter the primary domain and click *Proceed*.

Default alerts

FortiRecon automatically sends out default alerts if certain triggers are identified. Default alerts for each module include:

Module	Alert
External Attack Surface Management (EASM)	• New scan refresh • Leaked credentials present as part of a third party breach • Continuous monitoring refresh alert • Leaked credentials for new domain

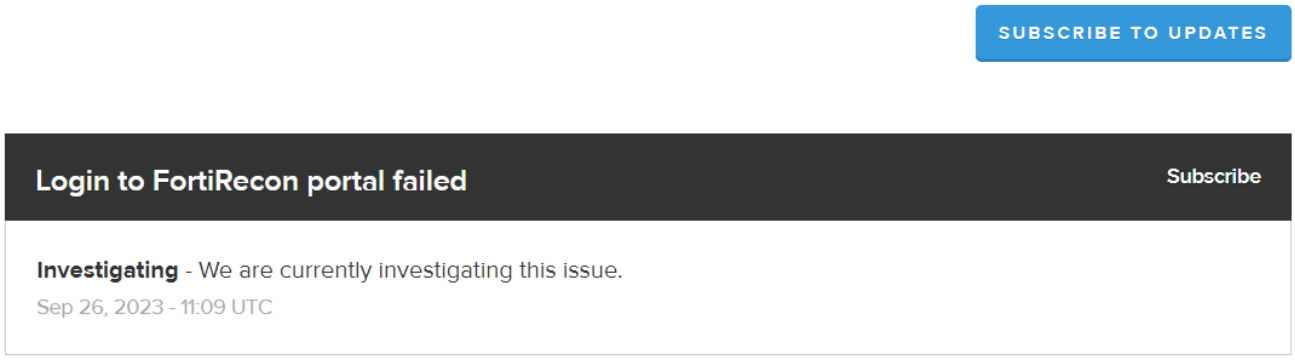
Module	Alert
Internal Attack Surface Management (IASM)	• New scan refresh
Brand Protection (BP)	• Fraudulent domains identified, such as phishing and brand impersonation • New rogue mobile application identified • Social media impersonation identified • Exposed sensitive information on code repository • Files found in open cloud storage bucket • New threats to executives in executive monitoring
Adversary Centric Intelligence (ACI)	• Any published flash alert or report • Any high relevance report • Stealer infection identified • Credit or debit cards identified on card shops • Organization or vendor listed on a ransomware naming and shaming site • Intelligence collection lookup alert, if there is a match in the default system ICL query • Daily digest

Monitoring Service Status

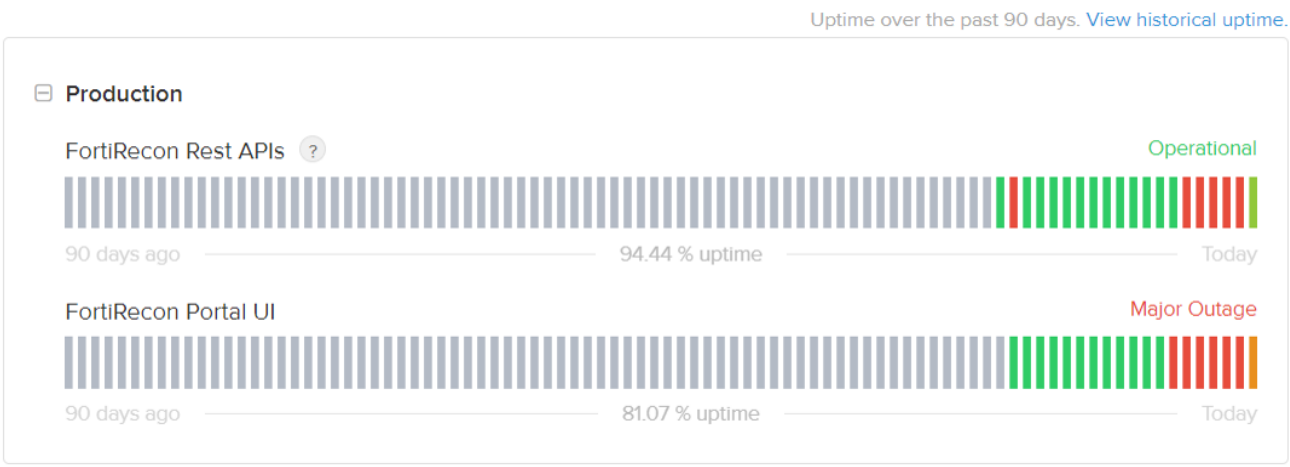
The FortiRecon Status page provides an overview of the current and historical availability of the FortiRecon service. You can receive and track notifications for incidents and downtime affecting the FortiRecon GUI and Rest APIs.

To access the FortiRecon Status page, navigate to https://status.fortirecon.forticloud.com/.

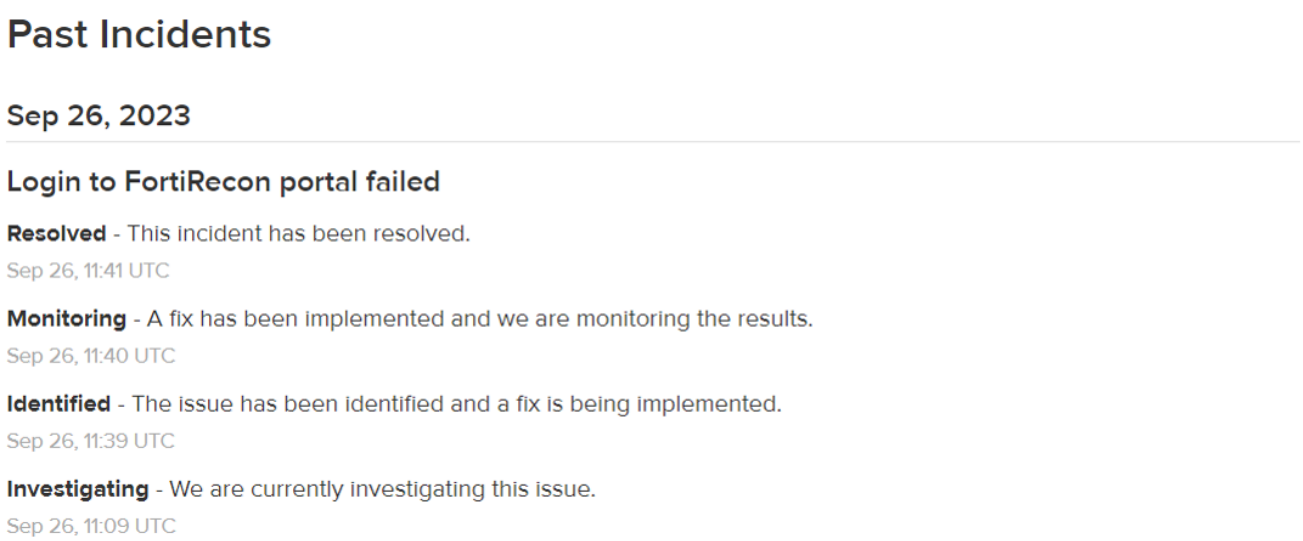
The status page displays the real-time and historical incidents affecting the FortiRecon service. The real-time events affecting the infrastructure and usage of the service are displayed on the top of the page. Click *Subscribe To Updates* to receive notifications.



The FortiRecon service uptime is displayed graphically for a period of 90 days. The downtime/outage events experienced by the service are indicated in colored bars; hover over each bar to view the details. Click *View historical uptime* to view the uptime/downtime experienced by the service in the past.



The historical incidents are listed in *Past Incidents* section.



Getting started

This section explains how to get started with FortiRecon.

When you first start with FortiRecon, you can:

- Register your FortiRecon license. See Registering the FortiRecon license on page 15.
- Subscribe to FortiRecon and start the service. See Subscribing to FortiRecon on page 16.

Registering the FortiRecon license

You must purchase and register a FortiRecon license before you can subscribe to FortiRecon. After you purchase the license, register the license using FortiCloud Account Services. For more information about registering products on FortiCloud, see the *FortiCloud Account Services > Registering products* documentation.

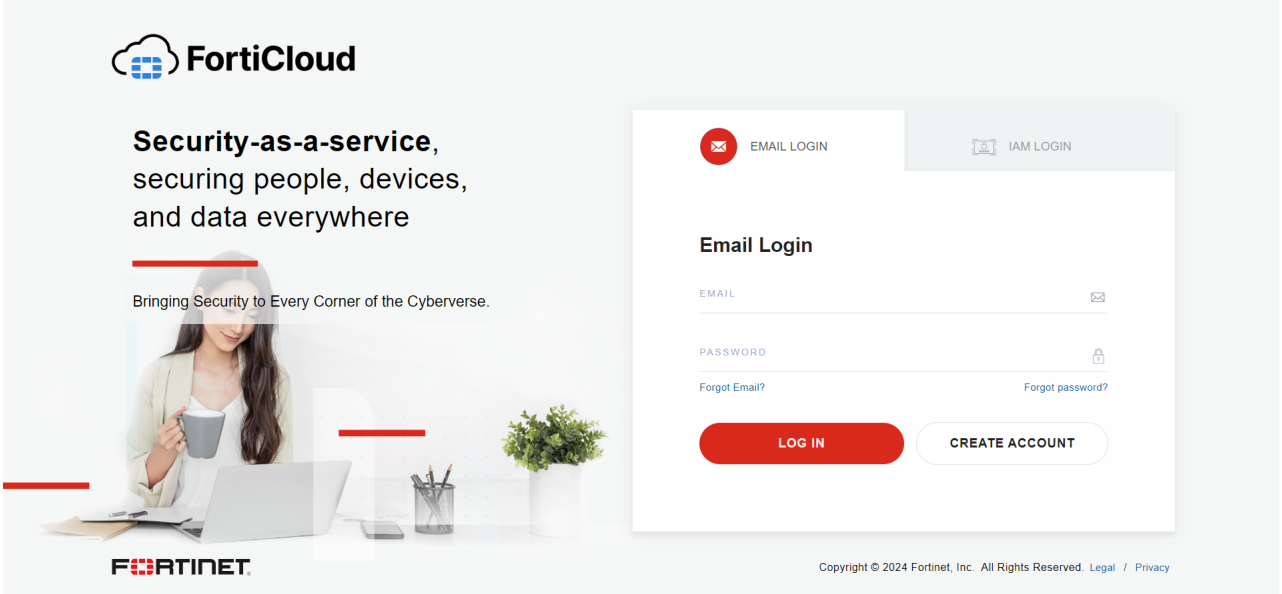
Subscribing to FortiRecon

This section describes how to subscribe to FortiRecon and start the service. Before you can subscribe to FortiRecon, you must register the license. See Registering the FortiRecon license on page 15.

To subscribe to FortiRecon:

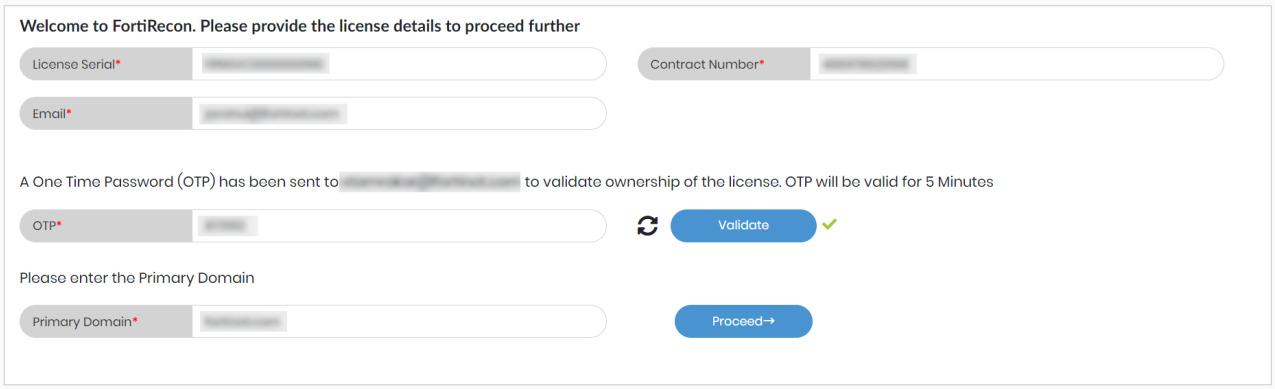
1. After the license is registered on FortiCloud, go to FortiRecon at https://fortirecon.forticloud.com.

2. Click *Login*. The FortiCloud login page is displayed.

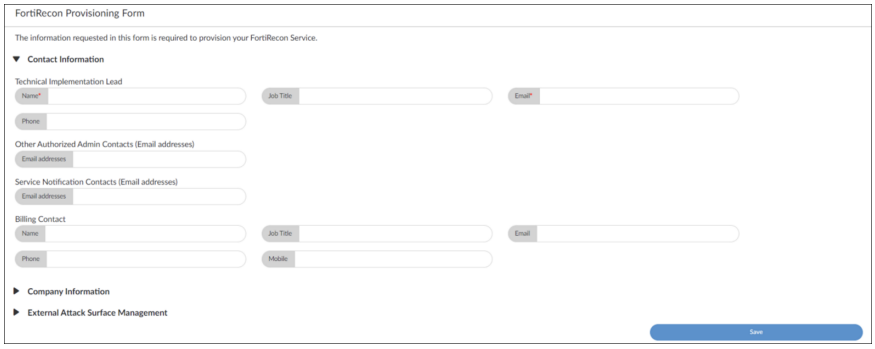


3. Enter your FortiCloud credentials.

4. After you log in to FortiRecon for the first time, the *FortiRecon Licensing* page is displayed. Enter the following information.
   - License Serial.
   - Contract Number.
   - Email that was used to register the contract.
5. Click *Verify*.
6. A One Time password (OTP) will be sent to your email and is valid for five minutes. Enter the OTP and click *Validate*. Click regenerate icon to generate a new OTP if needed.
7. Once validated, enter the primary domain and click *Proceed*.



8. The *FortiRecon Provisioning Form* is displayed.



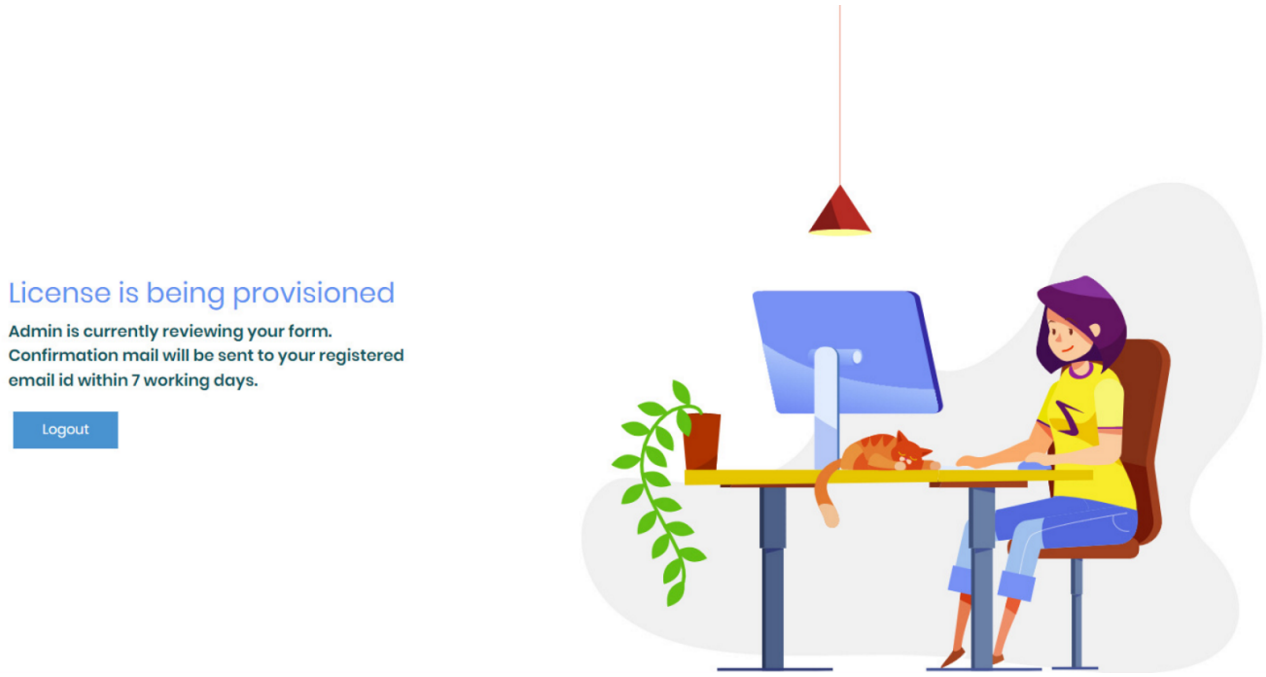
9. Enter your contact information in the *Technical Implementation Lead* fields.

Fields marked with a red asterisks are required information. Other fields are considered optional although it is suggested that you complete all of the fields provided to receive the most accurate service.

10. Enter the email addresses of members of your organization in the *Other Authorized Contacts* and *Service Notification Contacts* fields.
11. Enter the contact information of the billing contact in the *Billing Contact* fields.
12. Select the *Company Information* and *External Attack Surface Management* dropdowns. New information fields are displayed.

13. Enter your organization's information in the *Company Information* fields.
14. Enter your organization's assets IP address and domain information in the *External Attack Surface Management* fields.
15. Click *Save*. Your information will be sent to the FortiRecon team for review and provisioning.

    A confirmation page is displayed.



16. Wait for the FortiRecon team to analyze your assets and populate the FortiRecon portal for you.
17. When you receive an email from the FortiRecon team, you can access the FortiRecon portal and review the analysis. See Accessing FortiRecon portal on page 19.

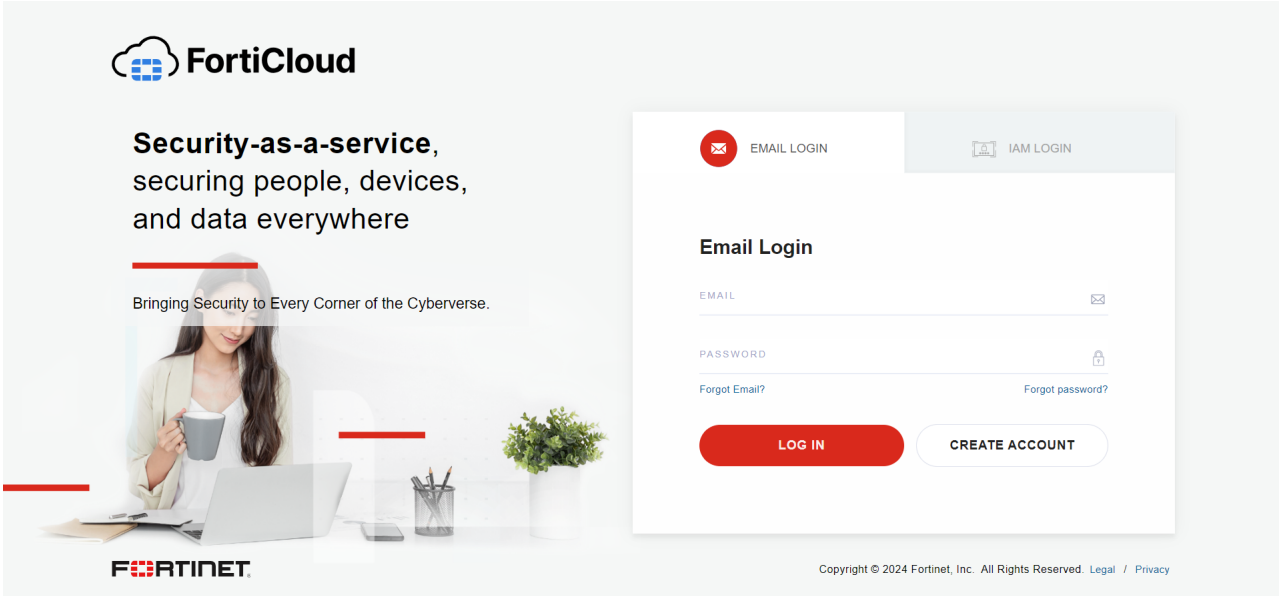
Accessing FortiRecon portal

After you have subscribed to FortiRecon and received an email from the FortiRecon team, you are ready to access the FortiRecon portal.

To access FortiRecon:

1. Go to FortiRecon at https://fortirecon.forticloud.com.

2. Click *Login*. The FortiCloud login page is displayed.

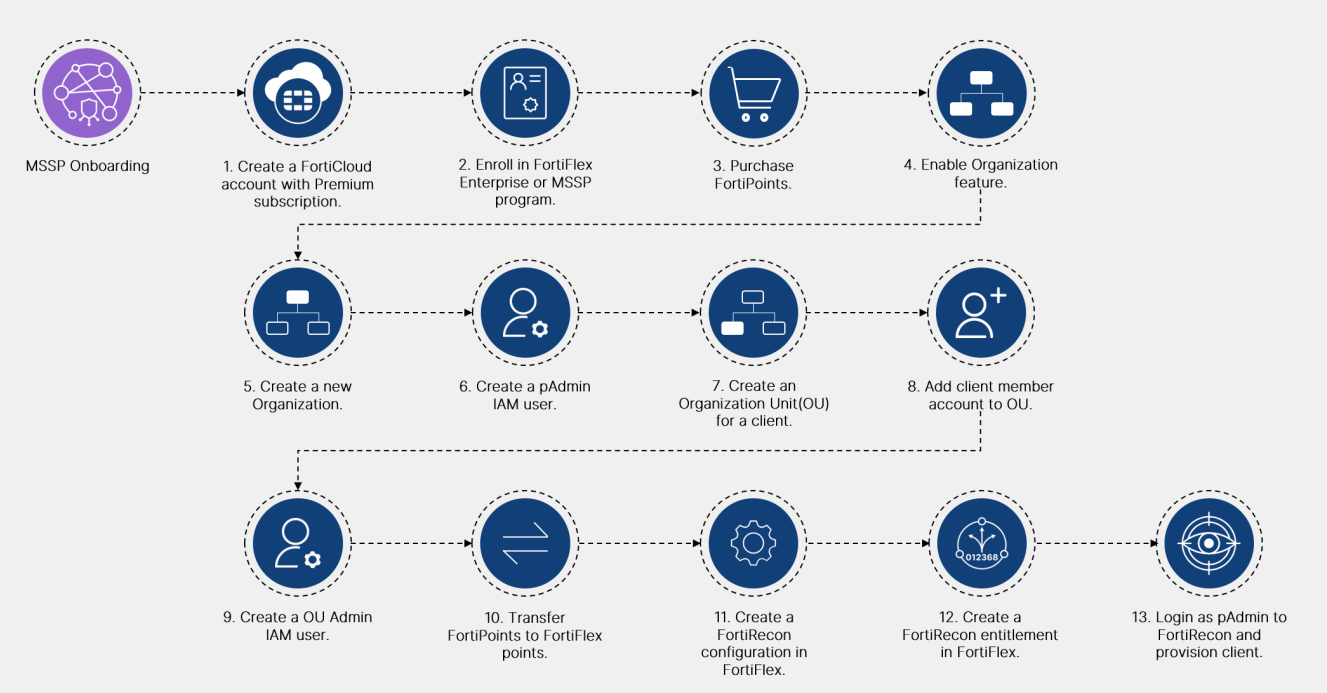


3. Enter your FortiCloud credentials.
4. Click *Login*. The *Overview* page is displayed. See Overview.

If you are part of multiple organizations, the *Organization* dashboard page is displayed. Select the organization you want and click *Login*. See Organization Dashboard.

MSSP Onboarding

FortiRecon provides a streamlined onboarding process using *FortiFlex*, making it easier for Managed Security Service Providers (MSSPs) to onboard new clients. This simplified process benefits both MSSPs and their clients by reducing the time and complexity.



Prerequisities

Before onboarding clients using FortiRecon and FortiFlex, ensure you have completed the following.

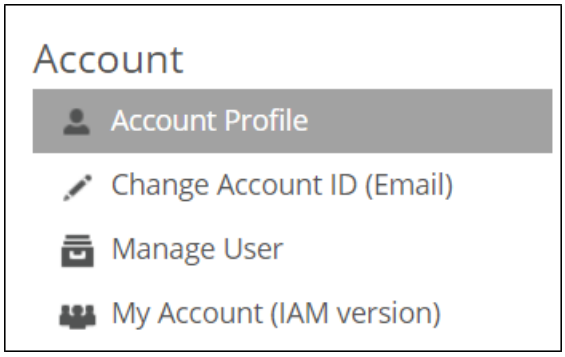
- The MSSP must create a *FortiCloud* account with *Premium* subscription. See Creating a FortiCloud account.
- Enroll in either the *FortiFlex Enterprise* or *FortiFlex MSSP* program to enable FortiFlex in *FortiCloud Marketplace*.
- Purchase sufficient *FortiPoints* to cover the resources allocated to client deployments.
- Enable the *Organizations* portal within the FortiCloud account. See Enabling Organization Portal.

- To purchase a *FortiCloud Premium license*, *FortiFlex Enterprise*, *FortiFlex MSSP*, or *FortiPoints*, contact Fortinet Support.
- Once you have purchased your licenses, register them in your FortiCloud account. See FortiCloud Services Asset Management Guide > Registering Assets.
- You can use the conversion rate and FortiFlex points calculator to estimate the total number of points that will be consumed before you purchase the FortiPoints. See Transferring FortiPoints to FortiFlex points.

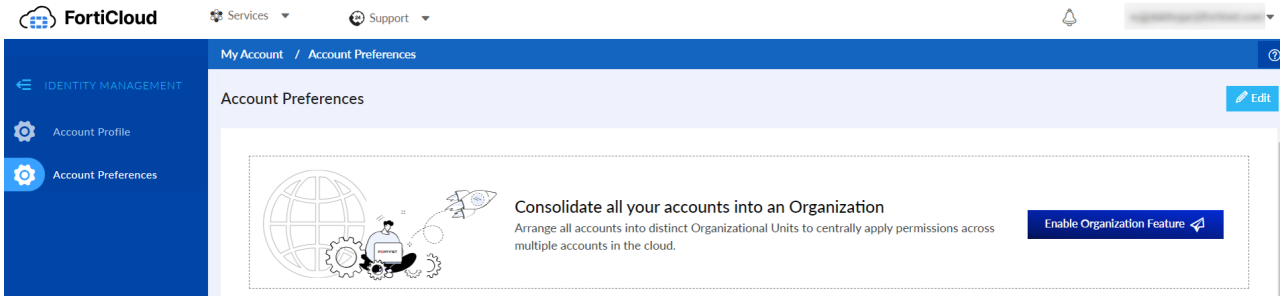
Enabling Organization Portal

To access Organization Portal in FortiCloud, perform the following steps:

1. Log in to https://support.fortinet.com/ using your FortiCloud account.
2. From the profile menu, select *My Account.*
3. In the *My Account* page, click *My Account (IAM Version)*.



4. Navigate to *Account Preferences* tab.
5. Click *Enable Organization Feature*.



Onboarding as an MSSP

To onboard as an MSSP, create a new organization within your FortiCloud account. Then, create a dedicated pAdmin account for managing your MSSP operations and client provisioning.

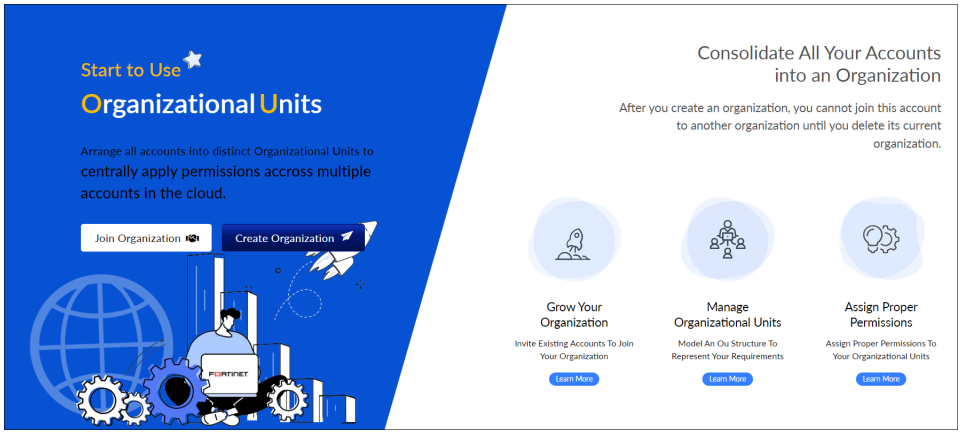
1. Create a new organization.
2. Create a pAdmin account.

Creating an Organization

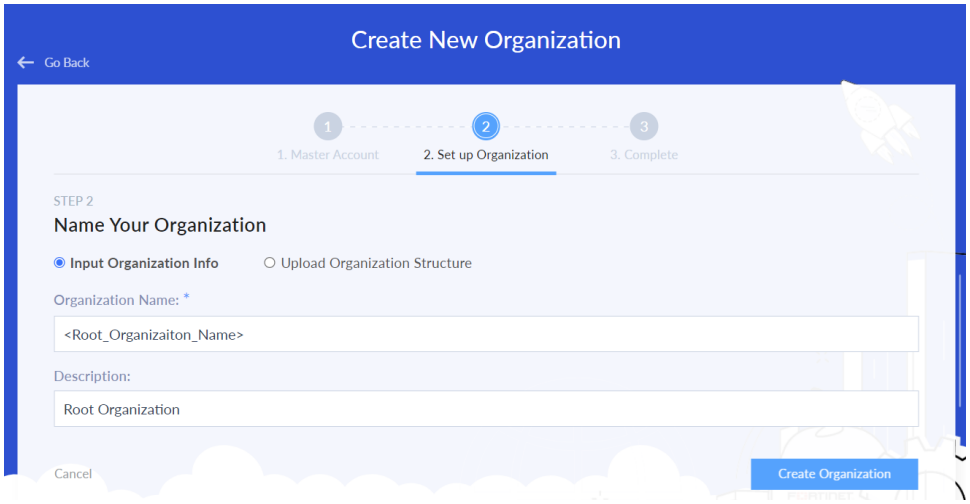
When you create an Organization your account becomes the *Root Account* for the organization.

Perform the following steps, to create an organization.

1. Ensure that you have enabled Organization Portal in your FortiCloud account. See Enabling Organization Portal.
2. In the Organization Portal, click *Create Organization*. The *Master Account* page opens.



3. Click *Next*. The *Set up Organization* page opens.



4. Provide the required information:

Input Organization Info	Select this option to create your organization with the GUI.
Upload Organization Structure	Select this option to create the organization and Organizational Units with an Excel sheet. See To create an organization with the Bulk Import template.
Organization Name	Enter a name for the organization.
Description	Enter a brief description of the organization.

5. Click *Create Organization*. The *Complete* page opens.
6. Click *Close & Go To General*. The *General* page opens.

For more information on Organizations, see FortiCloud Services > Organization Portal.

To create an organization with the Bulk Import template:

1. On the Set up Organization page, click *Upload Organization Structure*.
2. Download the Bulk Import template.
3. Use the template instructions to enter the OU information and create the organization hierarchy.
4. After you have completed the template, click *Organization Structure File Upload*, and upload the file.
5. Click *Confirm*.

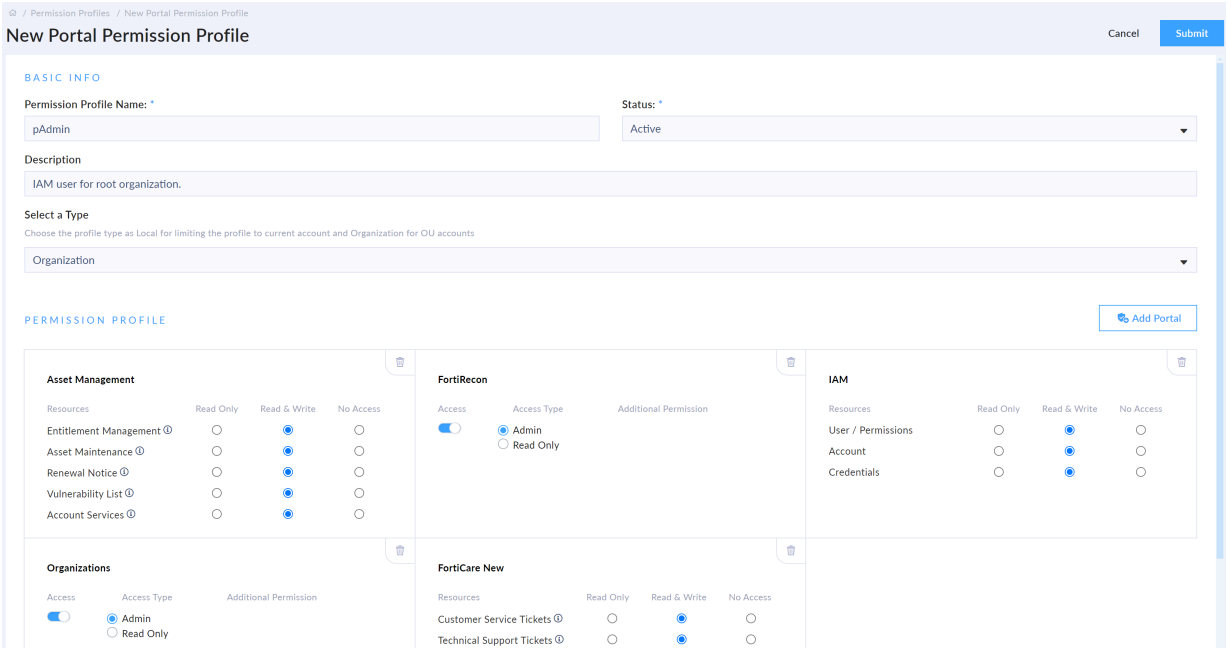
Creating a pAdmin account

The IAM account with root organization admin access is called a pAdmin account. This account is required to log in to FortiRecon and provision MSSP Clients. See User Roles.

Perform the following steps to create a pAdmin account.

1. Log in to https://support.fortinet.com/ using your FortiCloud *Root Account*.
2. Go to the *Services* > *IAM* portal.
3. Create a new permission profile for the pAdmin account.
   a. Go to *Permission Profiles* and click *Add New*.
   b. Set the type to *Organization*.
   c. Add the following portals and enable *Admin* access.
      - *FortiRecon*
      - *IAM*
      - *Organizations*
      - *FortiFlex*
      - *Asset Management*
      - *FortiCare New*

d. Click *Submit*.



For more information, see Permission profiles within Organizations in the *Identity & Access Management.*

4. Create the pAdmin user account.

a. Click *Add New* > *IAM User*. The *User Details* pane opens.

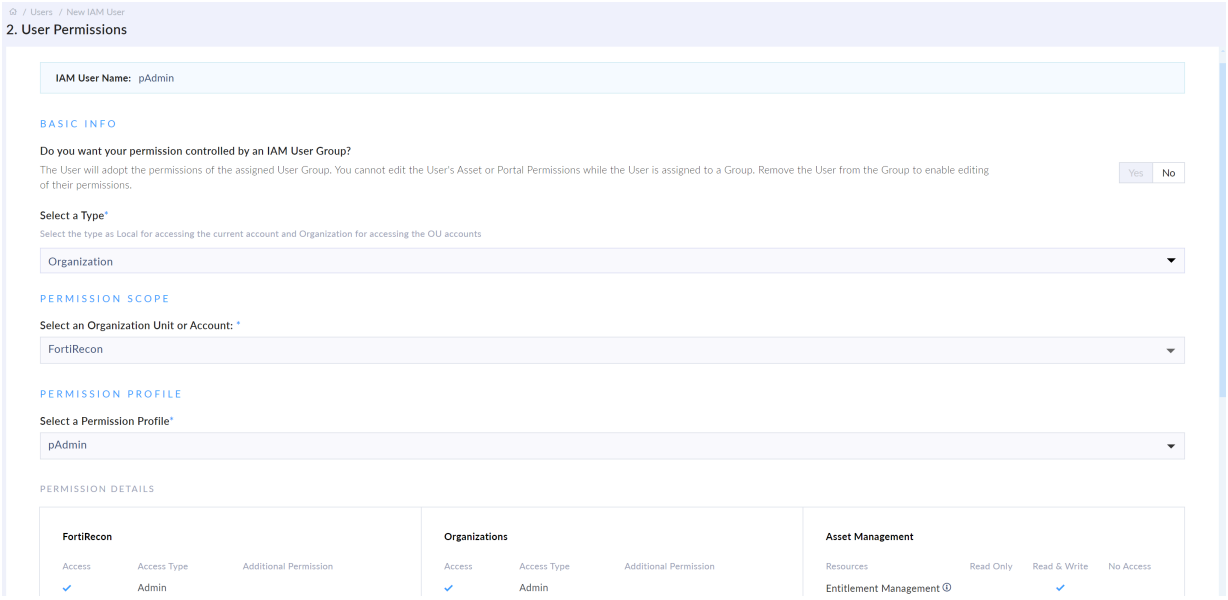
b. Enter the user's details and click *Next*.

Username	Type the username with no spaces. The username specified here will be used to log in.
Full Name	Type the user's first and last name.
Email	Type the user's email address.
Phone	Select the country code from the drop down, and type the user's phone number.
Description (Optional)	Type a description of the user.

c. Select the *Organization* user type from *Select A Type* drop down list.

d. Set the *Permission Scope* to the *Root Organization*.

e. In the Permissions Profile drop down, select the permission profile created in the previous step.



f. Click *Next*. The Confirmation page is displayed.

g. Review the user information, and click *Confirm*. The user's details are displayed.

h. Click *Generate Password* to generate a password reset link and reset the password.

For more information, see Creating users, user groups, and roles within Organizations in the *Identity & Access Management*.

Onboarding a MSSP Client

Perform the following steps to onboard a new MSSP Client to FortiRecon.

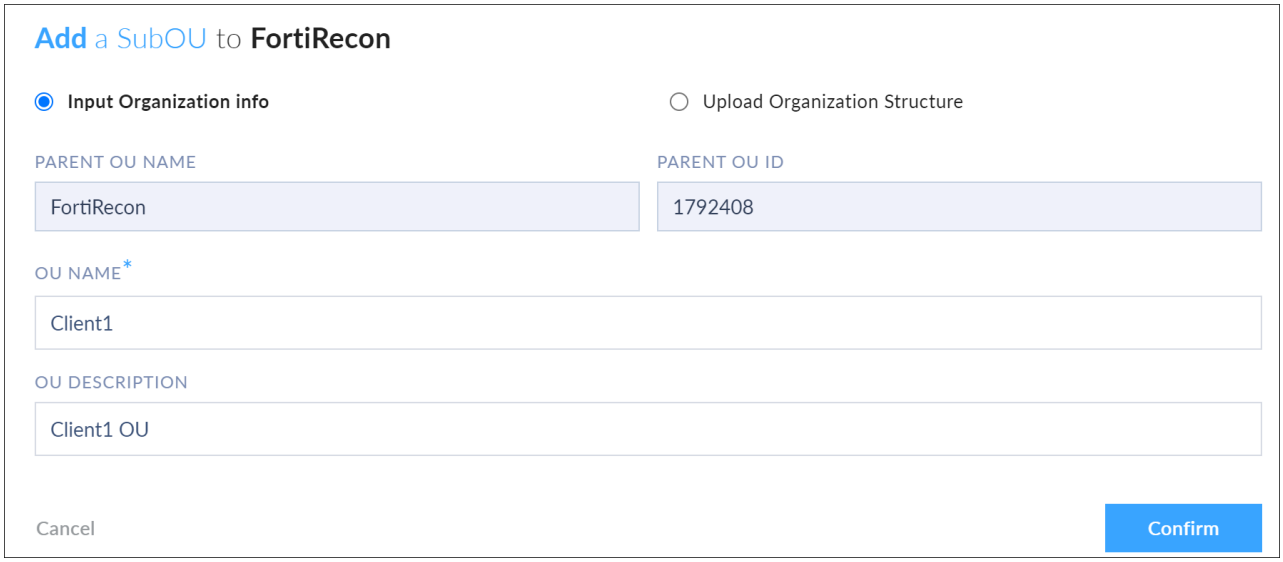
1. Create an Organization Unit(OU).
2. Create a MSSP Client Member Account.
3. Create an OU Admin account.
4. Transfer FortiPoints to FortiFlex points.
5. In FortiFlex,
   a. Create a FortiRecon configuration.
   b. Create a FortiRecon entitlement.
6. Provision FortiRecon.

Creating an Organization Unit(OU)

Organizational Units (OUs) are folders used to organize your MSSP Clients within your root organization. FortiRecon currently supports a single level of OU structure.

Perform the following steps to create an OU for a client.

1. In FortiCloud account, go to *Services* > *Organization*.
2. In the navigation menu, hover over the *Root Organization* name and click the gear icon.
3. Click *Add a SubOU*. The *Add a SubOU to <org_name>* dialog opens.
4. Enter the *OU Name* and *OU Description*, then click *Confirm*. The new OU is added to the organization.

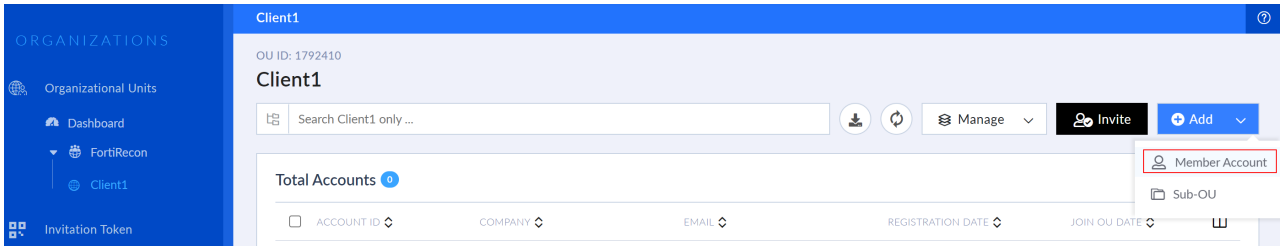


Creating a MSSP Client Member Account

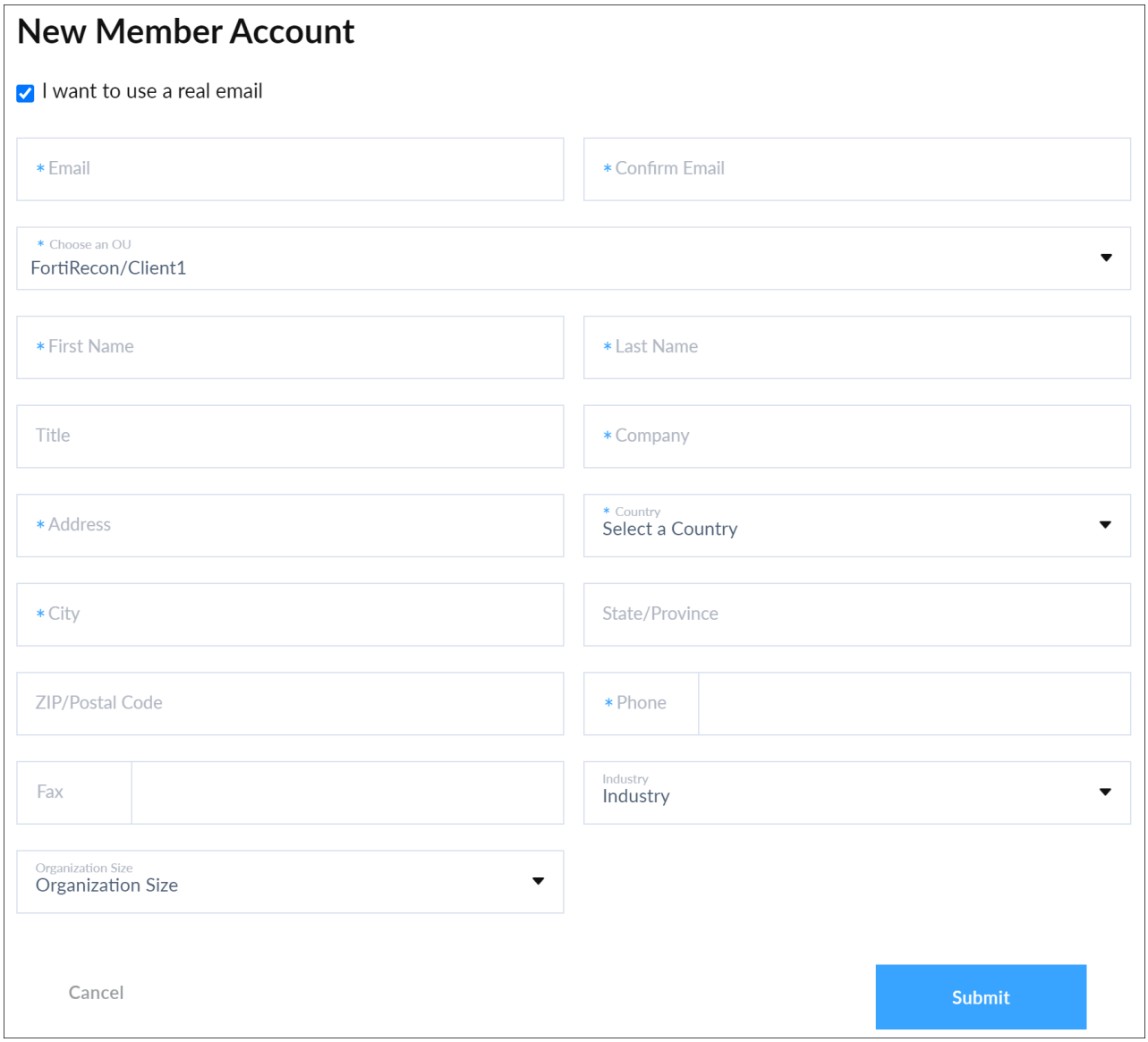
A Member Account is a FortiCloud account that joins an Organization. New Member Accounts can be created directly within the *Root account Organization* or a *SubOU*.

Perform the following steps to create a member account for a MSSP Client.

1. Select the MSSP Client Organization Unit (OU) that you want to add the Member Account to.
2. Click *Add* > *Member Account*. The *New Member Account* dialog is displayed.



3. Select *I want to use a real email* to input the email address of MSSP Client. Fields are displayed to enter the email address.
4. Select the MSSP Client OU that you want the Member Account to be linked to from the *Choose an OU* drop down menu.



5. Configure the *New Member Account* dialog fields with MSSP Client information.
6. Click *Submit*. A confirmation message is displayed.

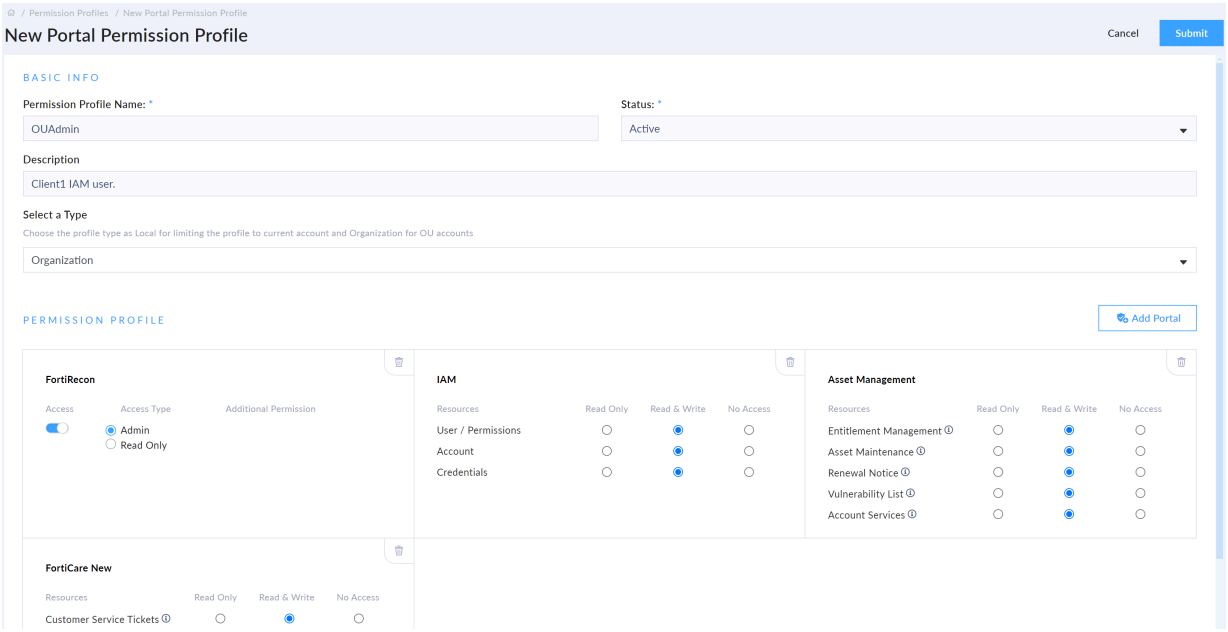
For more information on creating member account, see FortiCloud Services > Organization Portal > Creating new Member Accounts.

Creating an OUAdmin account

The IAM account with *admin* access and any *OU* except root organization as permission scope will be the OU Admin. This account is required by the MSSP Client for accessing FortiRecon. See User Roles.

Perform the following steps to create a OUAdmin account.

1. Log in to https://support.fortinet.com/ using your FortiCloud *Root Account*.
2. Go to the *Services* > *IAM* portal.
3. Create a new permission profile for the OUAdmin account.
   a. Go to *Permission Profiles* and create a new profile.
   b. Set the type to *Organization*.
   c. Add the following portals and enable *Admin* access.
      - *FortiRecon*
      - *IAM*
      - *Asset Management*
      - *FortiCare New*
   d. Click *Submit*.



For more information, see Permission profiles within Organizations in the *Identity & Access Management*.

4. Create the OUAdmin user.
   a. Click *Add New* > *IAM User*. The *User Details* pane opens.
   b. Enter the user's details and click *Next*.

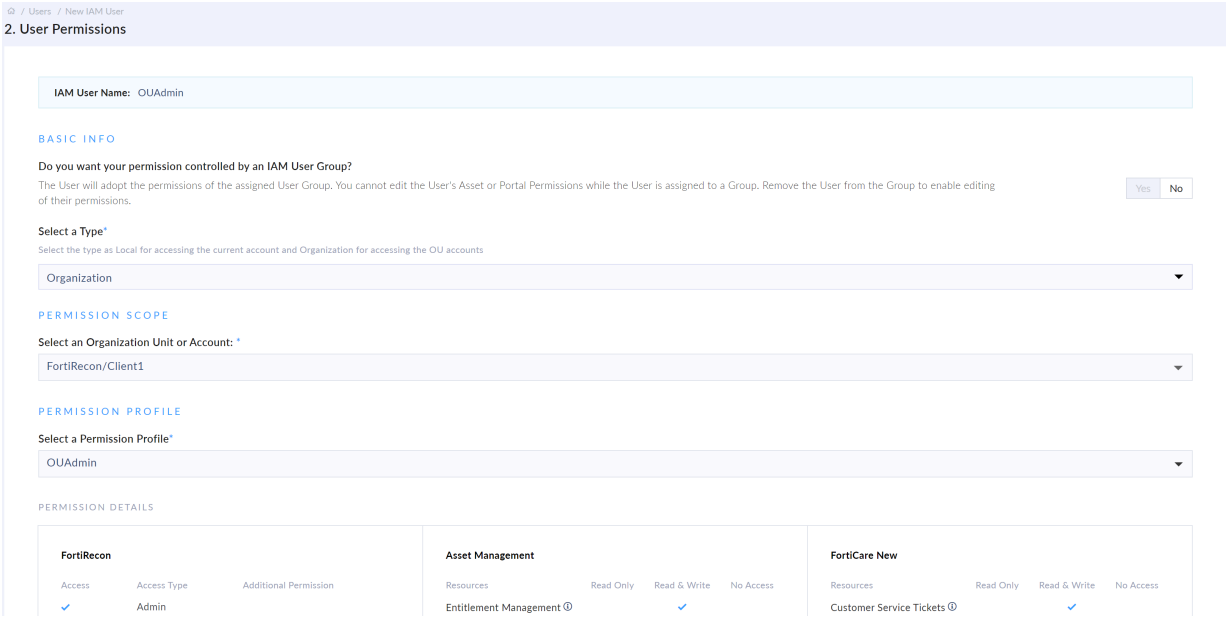
Username	Type the username with no spaces. The username specified here will be used to log in.
Full Name	Type the user's first and last name.
Email	Type the user's email address.
Phone	Select the country code from the drop down, and type the user's phone number.
Description	Type a description of the user.

(Optional)

c. Set the type to *Organization*.

d. Set the *Permission Scope* to the respective *OU* of the MSSP Client.

e. In the Permissions Profile drop down, select the permission profile created in the previous step.



f. Click *Next*. The *Confirmation* page is displayed.

g. Review the user information, and click *Confirm*. The user's details are displayed.

h. Click *Generate Password* to generate a password reset link.

For more information, see Creating users, user groups, and roles within Organizations in the Identity & Access Management.

The root account user must share the following details with the MSSP Client.

- **Account ID** - the Account ID of the root account user where IAM is added
- **Username** - the IAM username provided during user creation
- **Password reset link**

If the IAM user is logging in for the first time, email verification is required.

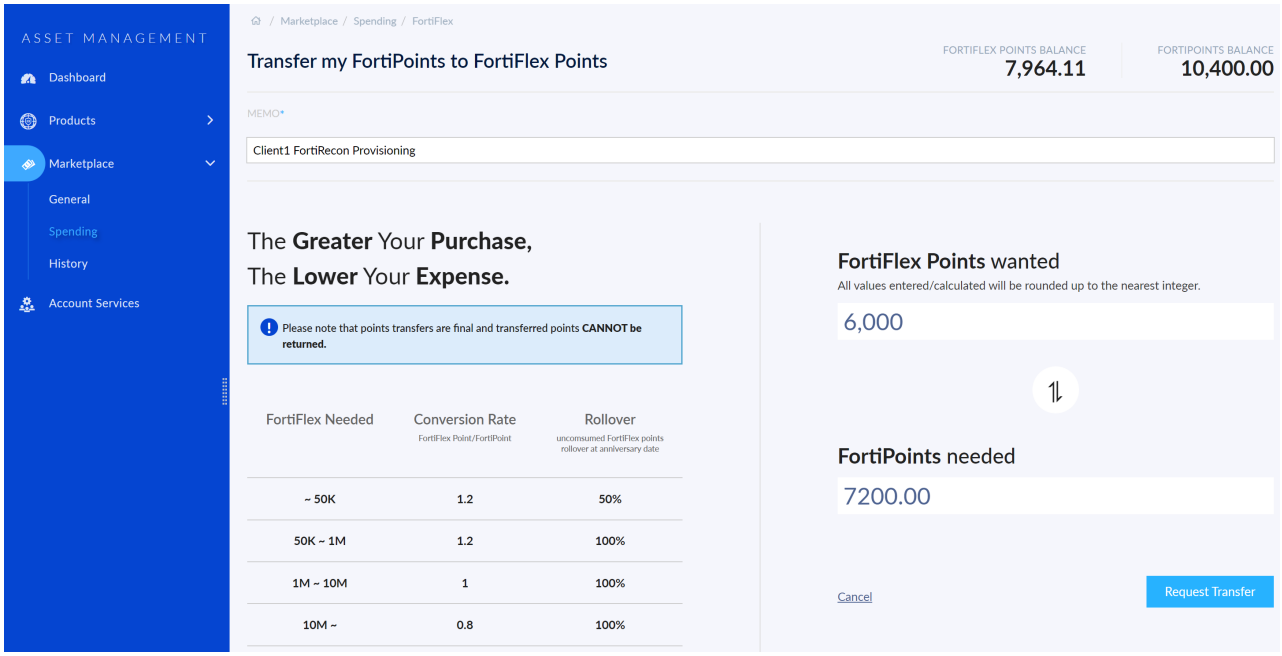
Transferring FortiPoints to FortiFlex points

FortiFlex FortiPoints can be transferred to FortiFlex points to be used in the FortiFlex portal. The conversion rate of FortiPoints to FortiFlex points, points rollover, and expiration information depend on the conversion option. Details on each option can be viewed in *FortiCloud* > *Marketplace* > *Spending* > *FortiFlex*.

You can use the FortiFlex points calculator to estimate the total number of points that will be consumed before you transfer the FortiPoints. See Points calculator in *FortiFlex Administration Guide*.

Perform the following steps to transfer FortiPoints into FortiFlex points.

1. Log in to https://support.fortinet.com/ using your FortiCloud *Root Account*.
2. Go to *Marketplace* > *Spending*.
3. Select *FortiFlex*.
4. Add a description of the transfer in the *Memo* field.
5. Enter the number of FortiFlex points you want. The *FortiPoints* needed field will update to show how many points must be transferred to receive the desired amount.
6. Click *Request Transfer*. The *Order Summary* is displayed.



- If you do not have enough FortiPoints to complete the transfer, a warning will display the number of outstanding points. Select *Register More Points* to register FortiPoints or select *Go Back* To *Edit* to reduce the number of FortiFlex points needed.
- To purchase *FortiPoints*, contact Fortinet Support. Once you have purchased your licenses, register them in your FortiCloud account. See FortiCloud Services Asset Management Guide > Registering Assets.

7. Click *Transfer Points*. The points will be transferred and the transfer record will display on the *History* page.

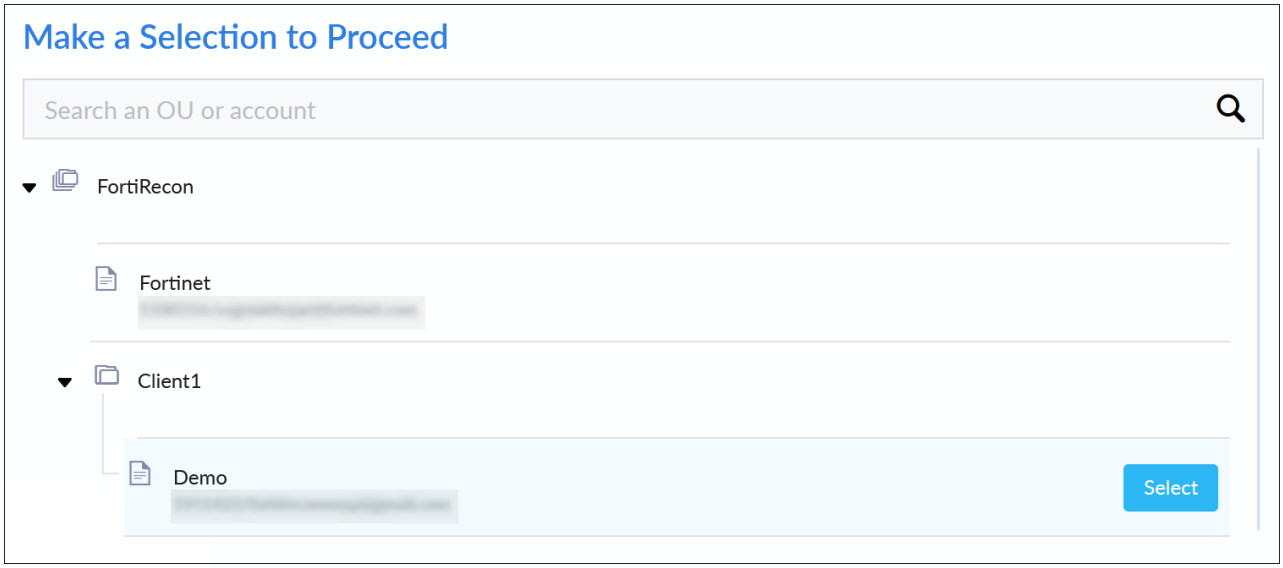
Creating a FortiRecon configuration in FortiFlex

Configurations allow you to define and customize a FortiRecon service package, including the number of assets, internal networks, executives, and vendors to be monitored.

You can use the FortiFlex points calculator to estimate the total number of points that will be consumed before you create the configuration. See Points calculator in *FortiFlex Administration Guide*.

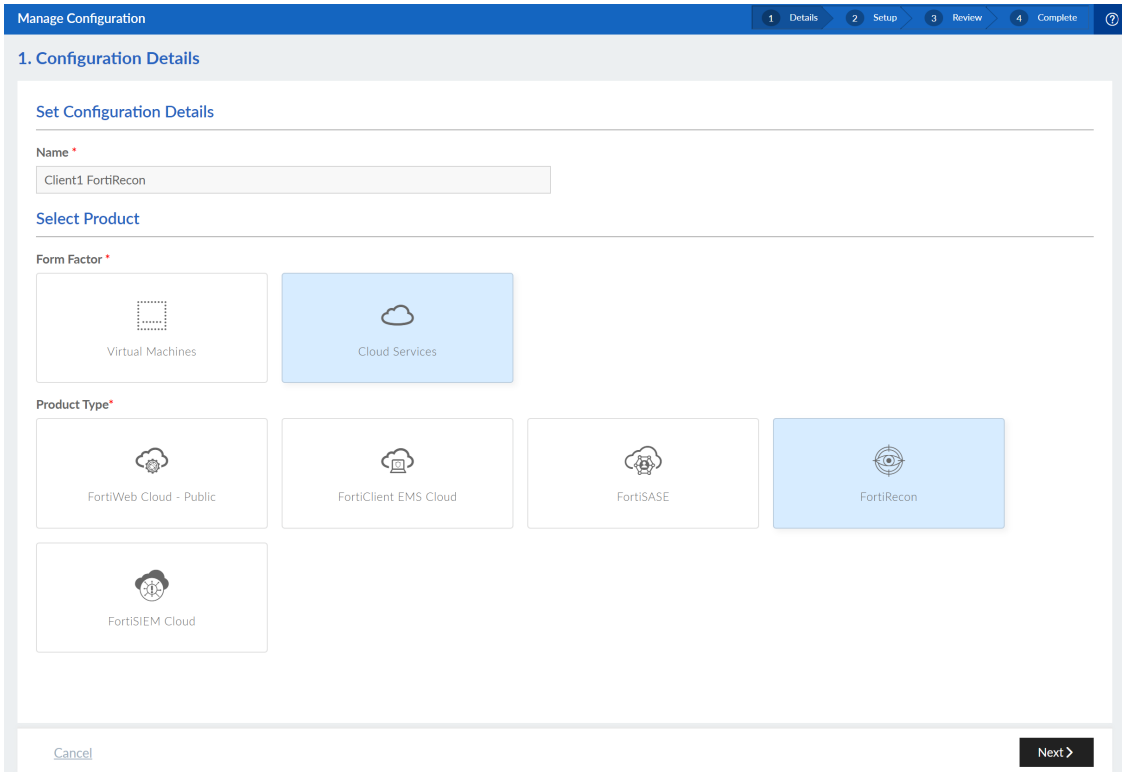
Perform the following steps to create a FortiRecon configuration in FortiFlex.

1. Log in to https://support.fortinet.com/ using your *pAdmin* account.
   a. If logging in for the first time, email verification must be completed.
2. In the *Make Selection* page, select the MSSP Client Member Account.



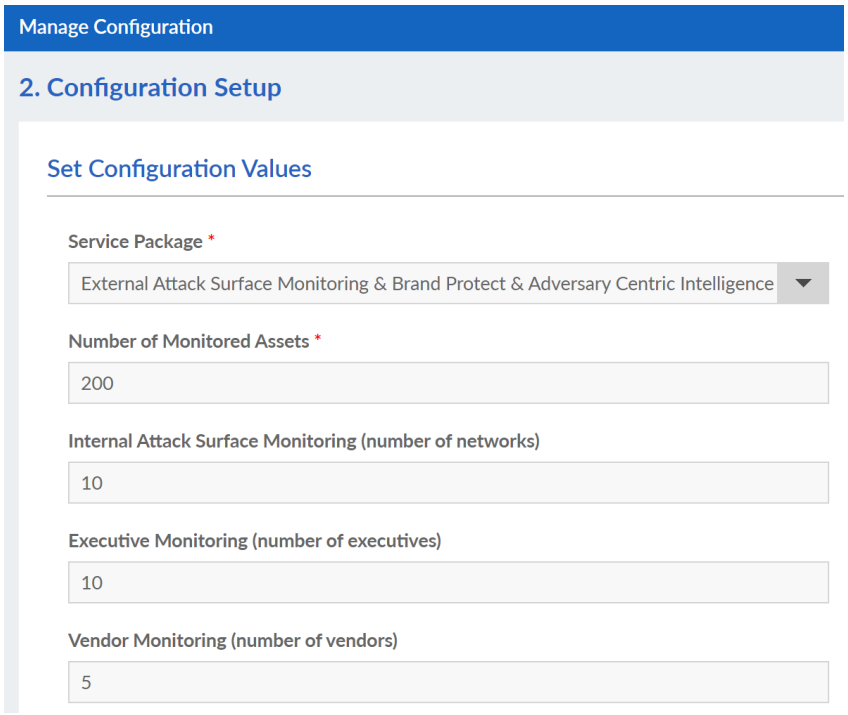
3. Go to *Services* > *FortiFlex*.
4. In FortiFlex, go to *Configurations*, and click *New Configuration*.
5. In the *Configuration Details* page, set the following configuration details and click *Next*.
   - *Name* - Enter a configuration name.
   - *Form Factor* - Select *Cloud Services*.

- *Product Type* - Select *FortiRecon*.



6. In the *Configuration Setup* page, set configuration values and click *Next*.

Service Package	Select any one from the following. *External Attack Surface Monitoring* *External Attack Surface Monitoring & Brand Protect* *External Attack Surface Monitoring & Brand Protect & Adversary Centric Intelligence*
Number of Monitored Assets	Enter a value between 200 to 1000000.
Internal Attack Surface Monitoring (number of networks)	Enter a value between 0 to 100.
Executive Monitoring (number of executives)	Enter a value between 0 to 1000. This field is only enabled when *External Attack Surface Monitoring & Brand Protect* or *External Attack Surface Monitoring & Brand Protect & Adversary Centric Intelligence* is selected as a Service Package. Otherwise, the value is set to 0.
Vendor Monitoring (number of vendors)	Enter a value between 0 to 1000. This field is only enabled when *External Attack Surface Monitoring & Brand Protect & Adversary Centric Intelligence* is selected as Service Package. Otherwise, the value is set to 0.



If the actual number of assets in the FortiRecon exceeds the licensed limit, access to modules may be restricted until the asset count is reduced to within the licensed limits.

7. Review the configuration details, and click *Submit*.
8. Click *List* to view the configuration in the *Configurations* tab.

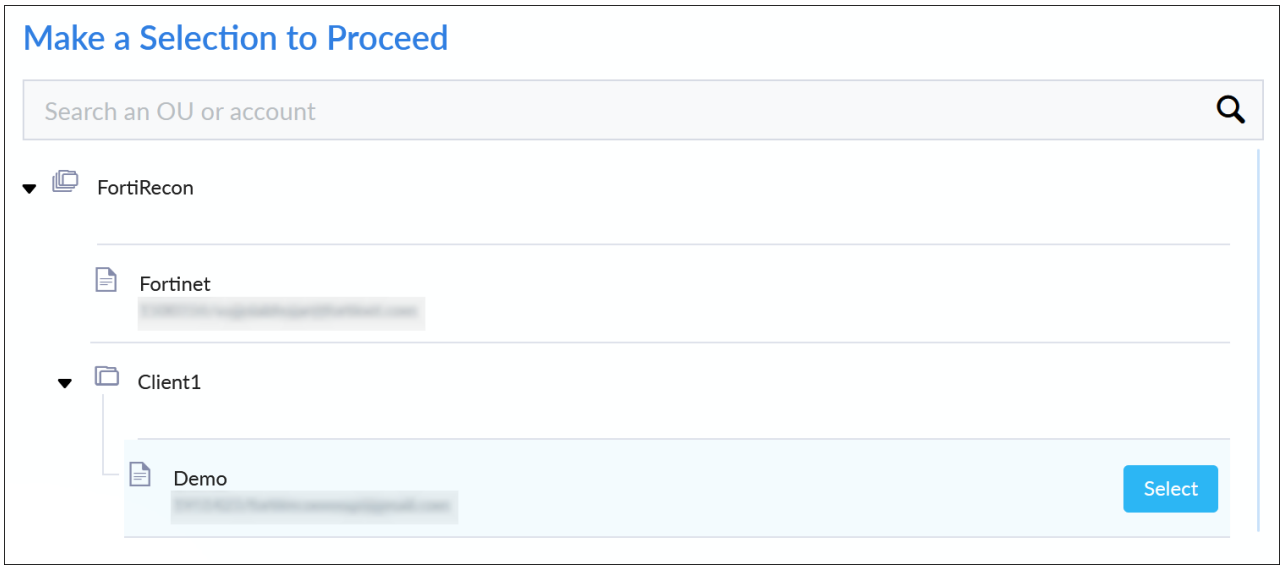
For more information, see Creating a Cloud service configuration in *FortiFlex Administration Guide*.

Creating a FortiRecon entitlement in FortiFlex

Entitlements use the configuration to create the service. FortiFlex points begin to be consumed once an entitlement is activated for the first time.

Perform the following steps to create a FortiRecon entitlement.

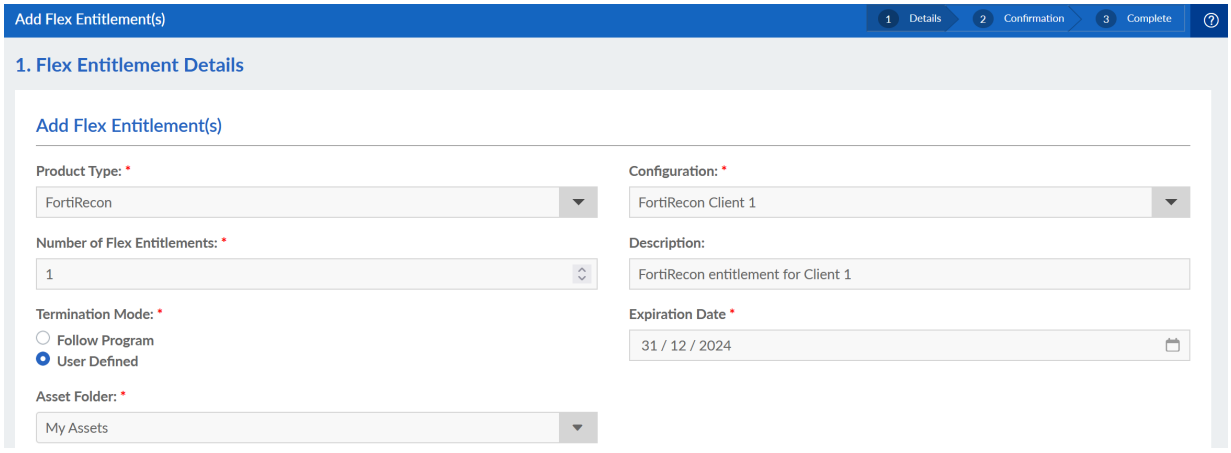
1. If not logged in, log in to https://support.fortinet.com/ using your *pAdmin* account.
2. In the Make Selection page, select the MSSP Client Member Account.



3. Go to *Services* > *FortiFlex*.
4. Go to *Flex Entitlements*, and click *New Flex Entitlement*. The *Add Flex Entitlement* page opens.
5. Configure the Cloud entitlement and click *Next*.
   - *Product Type* - FortiRecon
   - *Configuration* - Select the previously created FortiRecon configuration from the list.
   - *Number of Flex Entitlements* - Enter the number of entitlements.
   - *Description* - Enter a description.
   - *Termination Mode* - Select *Follow Program* to terminate the machine when the program expires. Select *User Defined*, and select a date in the calendar to specify the termination date.

     FortiRecon license generated through FortiFlex must have a minimum duration of 3 months.

   - *Asset Folder* - Assign the service to a folder in *My Assets*.



6. Review the *Flex Entitlement Details* and *Program Information*, and click *Submit*.

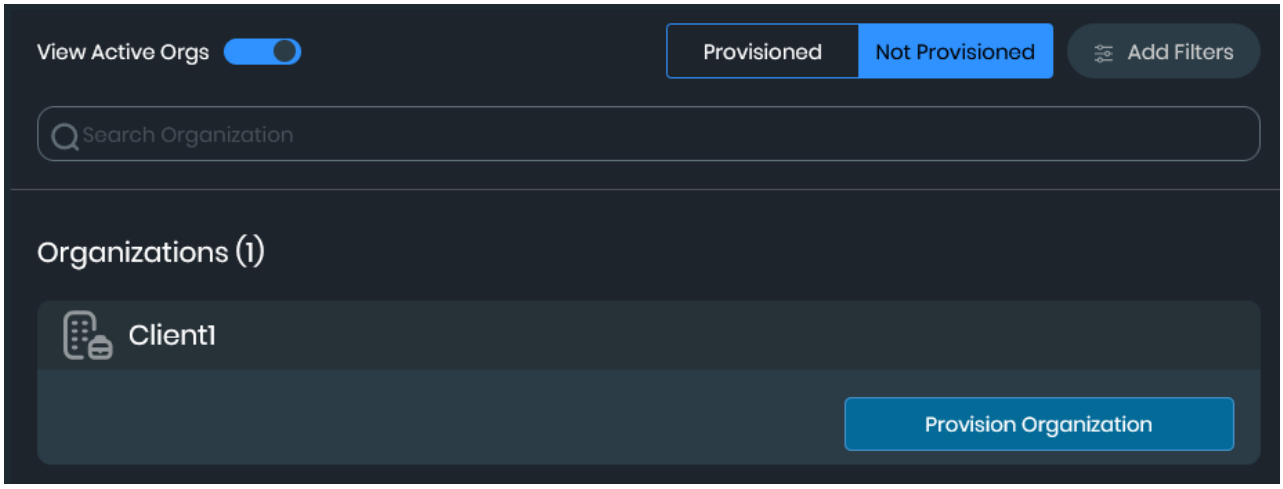
For more information on, see Creating Cloud service entitlements in *FortiFlex Administration Guide*.

Provisioning FortiRecon

Once the organization structure is created, IAM user is added, and FortlFlex entiltement created you will be able to provision FortiRecon organizations.

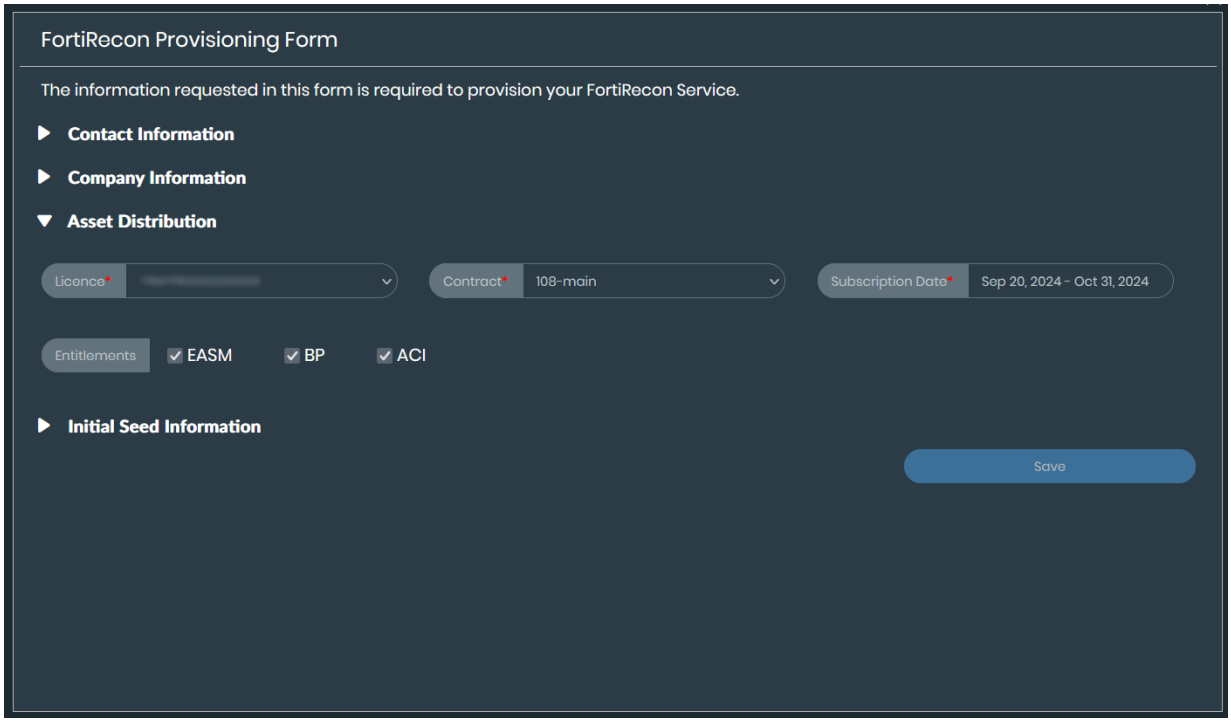
Perform the following steps to provision FortiRecon.

1. Login to FortiRecon portal using pAdmin credentials.
2. If logging in for the first time, email verification must be completed.
3. After verifying the email successfully, reload the FortiRecon portal. The FortiRecon*Organization* dashboard is displayed.
4. Enable the *View Active Orgs* toggle and select *Not Provisioned*.
5. Click *Provision Organization* for the organization that you want to provision.



6. Provide the necessary information in the FortiRecon Provisioning Form and click *Save*.
   a. In *Contact Information* section, enter the IAM username that belongs to the IAM user added to this OU, and upon entering the IAM username, other fields such as email and name will be automatically filled.
   b. In *Asset Distribution* section, the license and contract details will be retrieved from the FortiFlex entitlement. The subscription date and entitlements will be automatically filled.

c. Enter *Company Information* and *Initial Seed Information* details.



Once the Organization is provisioned , the following information is displayed. See Organization Dashboard.

- Contract activation and expiration dates.
- The entitlements available for the organization.

To log in to the FortiRecon portal for the provisioned organization, click *Login*.

When *OU User* logs in to the FortiRecon portal for the first time, *Your account is yet to be provisioned* message will be displayed.

The *pAdmin* or *OU Admin* will receive a warning for the OU User under *Profile Settings* > *Users*, where they can provide access to the user by clicking on the edit button and assigning an access template to them. Once access is granted, the *OU User* will be notified and can subsequently access the FortiRecon portal.

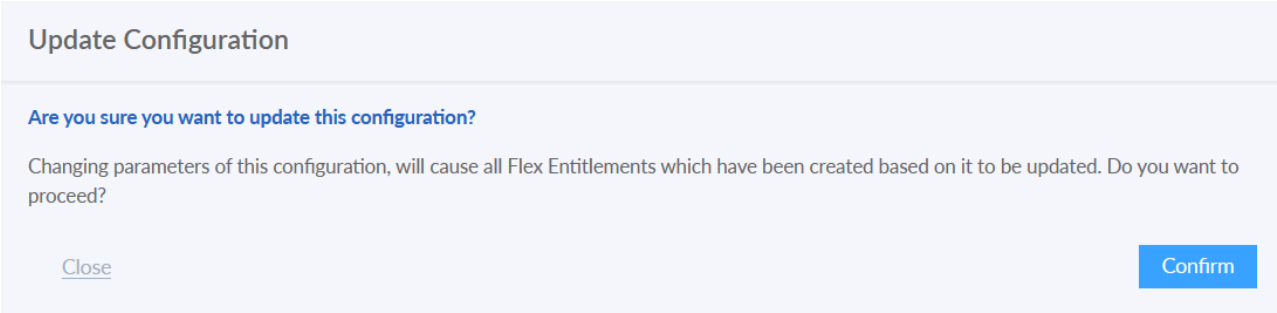
Managing Entitlements

You can modify configurations and entitlements within FortiFlex even after FortiRecon has been provisioned for your client. The process allows you to adjust resource allocation, expiration date and service details as needed.

Updating a FortiRecon Configuration

Perform the following steps to edit the configuration.

1. Log in to https://support.fortinet.com/ using your *pAdmin* account.
2. In the *Make Selection* page, select the MSSP Client Member Account.
3. Go to *Services* > *FortiFlex*.
4. In *FortiFlex*, go to *Configurations*, and click configuration name you want to modify.
5. In *Details* tab, click *Edit*.
6. Edit the configuration and click *Next*.
   a. In *Configuration Details* page, you can modify *Name*.
   b. In *Configuration Setup* page, you can modify the desired configuration values.
7. Review the configuration and click *Submit*. A confirmation dialog opens.
8. Click *Confirm* to finalize the changes.

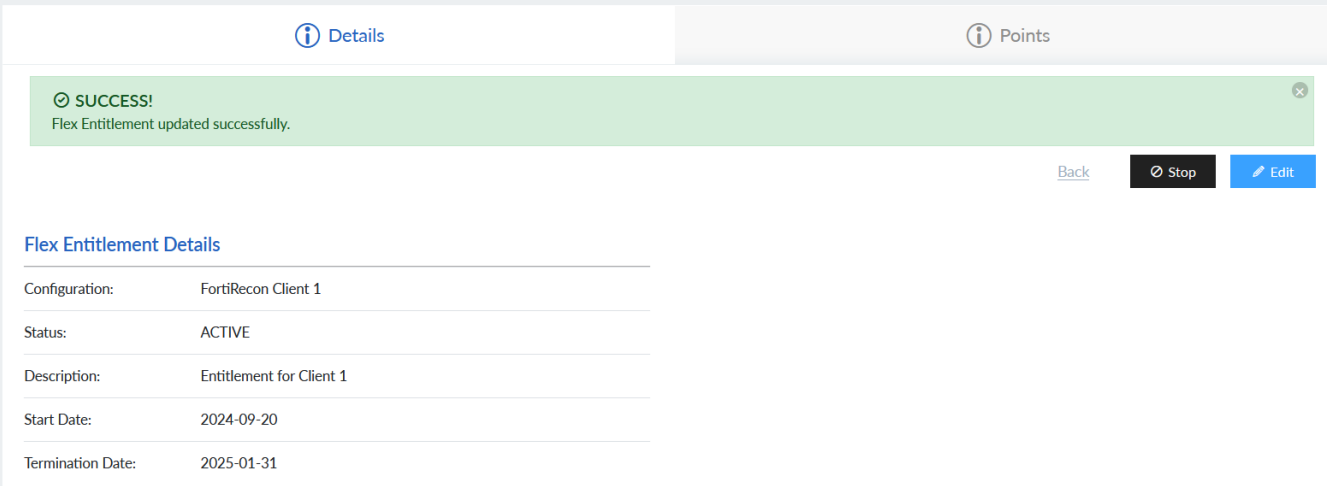


It may take up to 3 hours for any modifications to take effect in FortiRecon.

Updating a FortiRecon Entitlement

Perform the following steps to edit the entitlement.

1. Log in to https://support.fortinet.com/ using your *pAdmin* account.
2. In the *Make Selection* page, select the MSSP Client Member Account.
3. Go to *Services* > *FortiFlex*.
4. In *FortiFlex*, go to *Flex Entitlements*, and click *Serial Number* you want to modify.
5. In *Details* tab, click Edit.
6. In *Modify Flex Entitlement* page, you can modify the *Configuration* and *Expiration Date*.
7. Click *Submit*.



User Roles

Based on the access type and permission scope provided, the following roles are supported for FortiRecon:

Role	Access	Permission Scope	Description
pAdmin	Admin	Root organization	The IAM user with *admin* access and *root organization* as permission scope will be the pAdmin. pAdmins have the ability to create and edit organizations within FortiRecon.
pUser	Read-Only	Root organization	The IAM user with *read only* access and *root organization* as permission scope will be the pUsers. pUsers have a complete view of the organization/OU structure and read only access to FortiRecon portal. They cannot create or edit organizations.
OU Admin	Admin	Any OU except root	The IAM user with *admin* access and any *OU* except root organization as permission scope will be the OU Admin. OU Admins will be admins for the respective organization provisioned under their OU.
OU User	Read-Only	Any OU except root	The IAM user with *read only* access and any *OU* except root organization as permission scope will be the OU User. OU Users have read only access and can view the organization/OU structure but they will not be redirected to the FortiRecon portal unless their access is provisioned by pAdmin or OU admin.
Root Account	The account that created the organization. Only root account users will able to enable or disable other IAM users by updating user profiles in FortiCare.		

Role	Access	Permission Scope	Description
Member Account	A Member Account is a FortiCloud account that joins an Organization.		

Overview

The *Overview* page is a central hub for visualizing and analyzing your organization's digital risk posture across *Attack Surface Management (ASM), Brand Protection (BP),* and *Adversary Centric Intelligence (ACI)* modules. This holistic view allows you to gain immediate situational awareness, enabling quick prioritization and detection of critical threats across all modules.

The *MITRE ATT&CK* view displays discovered data mapped onto corresponding techniques and sub-techniques, providing a valuable framework for understanding attacker motivations and potential attack paths. Click *View* on the *Overview* page to switch to MITRE ATT&CK view.

From the Overview page, you can:

- View a summary of your organization's digital risk posture. See Viewing Digital Risk Posture.
- View discovered data mapped to MITRE ATT&CK framework. See Viewing MITRE ATT&CK Framework.
- Download the dashboard details as a PDF file. See Downloading Executive Report.

Viewing Digital Risk Posture

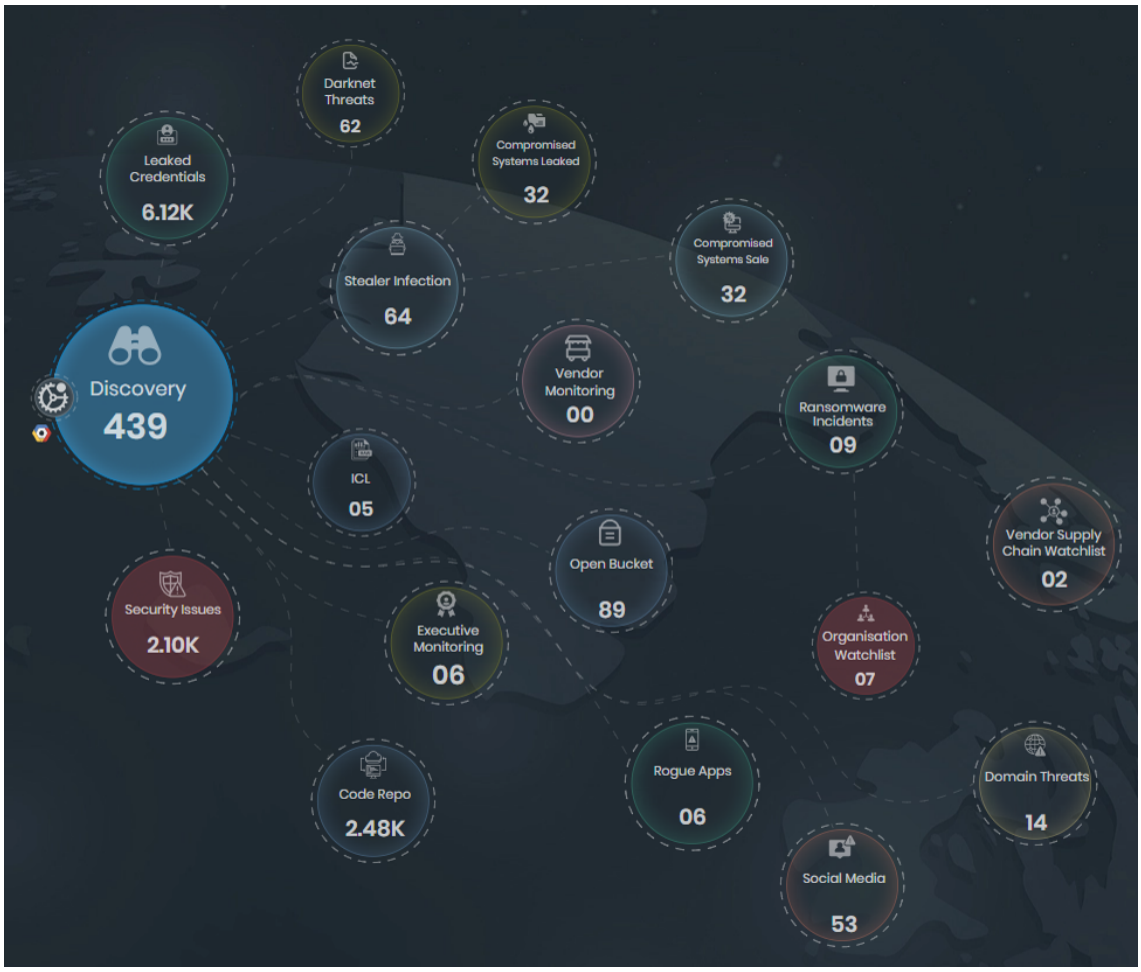
The *Overview* page displays a summary of your organization's digital risk posture including the following information.

- Digital Footprint Map
- License Details
- Trends Reporting

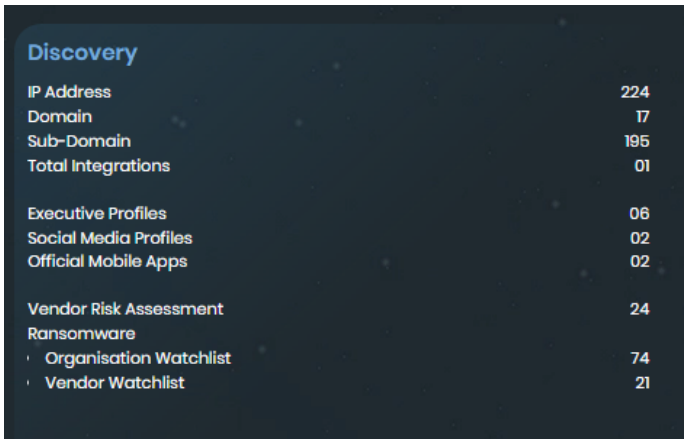
- Top Threat Actors
- Activities

Digital Footprint Map

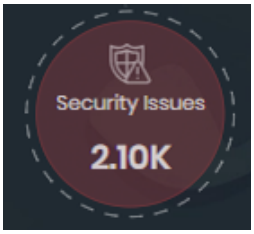
The digital footprint map is an interactive visualization tool that enables you to quickly identify and prioritize critical threats across *Attack Surface Management (ASM), Brand Protection (BP),* and *Adversary Centric Intelligence (ACI)* modules.



Clicking any bubble in the digital footprint map displays the detailed information in the information widget. Clicking any list item within the information widget opens relevant FortiRecon page in a new tab.



Bubbles highlighted in red indicates that new threats are discovered within the past 30 days and require immediate attention.

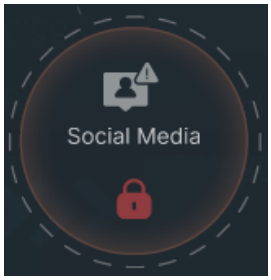


The digital footprint map includes the following information.

Bubble	Description	License Required
Discovery	Starting point of the digital footprint map. Displays the total count of discovered assets. Click the bubble to view the count for each discovered asset type. Hover over *gear* icon to view the added integrations.	FortiRecon EASM.
Security Issues	Displays the total count of potential security issues. Click the bubble to view the count for each security category.	
Leaked Credentials	Displays the total count of leaked credentials. Click the bubble to view the count for each domain.	
Domain Threats	Displays the total count of domain threats. Click the bubble to view the count for each threat type.	FortiRecon EASM and BP.
Social Media	Displays the total count of social media threats. Click the bubble to view the count for each profile type.	
Rogue Apps	Displays the total count of rogue applications. Click the bubble to view the count for each application store.	

Bubble	Description	License Required
Executive Monitoring	Displays the total count of threats for the official executive profiles added. Click the bubble to view the count for each profile added.	FortiRecon EASM, BP, and ACI.
Code Repo	Displays the total count of attributes that have been exposed in code repositories. Click the bubble to view the count for each attribute type.	
Open Bucket	Displays the total count of files exposed in open buckets. Click the bubble to view the count for each cloud service provider.	
Darknet Threats	Displays the total count of the intelligence reports available. Click the bubble to view the count for each category.	
Stealer Infection	Displays the total count of possible infected systems that are affiliated with your employees or end-users.	
CS - Leaked	Displays the total count of stolen data that has been shared over various forums where the threat actor operates. Click the bubble to view the count for employees and users.	
CS - On Sale	Displays the total count of stolen data that is currently being offered for sale on various Darknet marketplaces. Click the bubble to view the count for domain.	
Vendor Monitoring	Displays the total count of threats for the third party vendors added. Click the bubble to view the count for each vendor.	
Ransomware	Displays the total count of past and potential ransomware incidents.	
Organization Watchlist	Displays the total count of ransomware incidents for the organizations added to the watchlist. Click the bubble to view the count for each organization.	
Vendor Supply Chain Watchlist	Displays the total count of ransomware incidents for the venodrs added to the watchlist. Click the bubble to view the count for each vendor.	
Card Fraud	This bubble is only displayed for banking organizations that issue credit or debit cards.	

Access to certain bubbles is restricted based on your current license. Those marked with a lock icon require upgrading your license to view the detailed information. See Licensing.



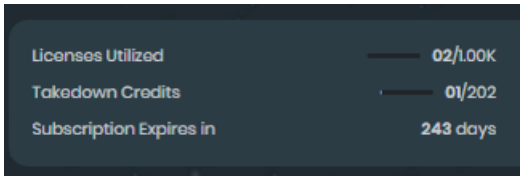
License Details

The license information widget on the right displays the following information.

License Utilized - Displays number of licenses utilized.

Takedown Credits - Displays number of takedown credits utilized.

Subscription Expires in - Displays remaining days until your FortiRecon subscription expires.



Trends Reporting

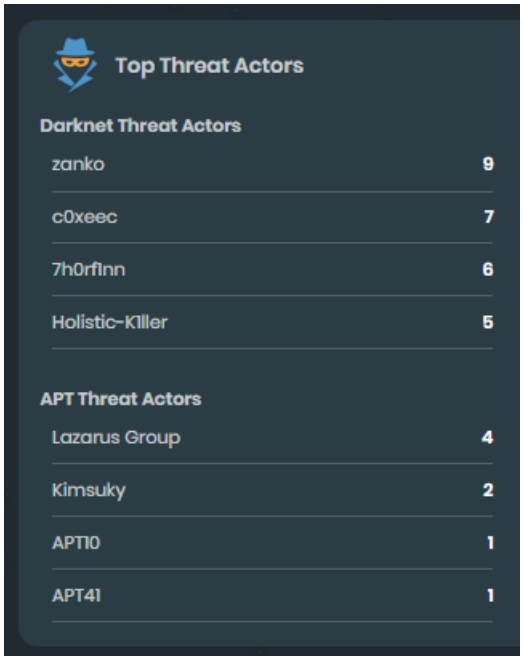
The *Trends Reporting* widget displays the latest, published intelligence reports. Automatically scrolls through the reports, or you can click the blue bars at the bottom of the widget to view specific reports.

Click any report to view the detailed information.

Top Threat Actors

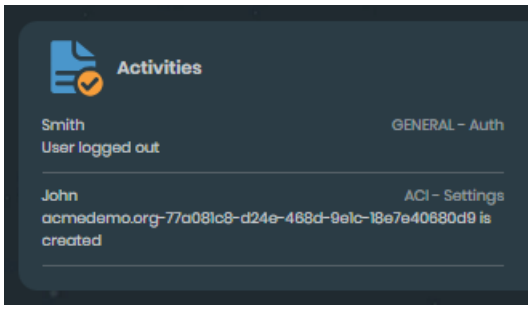
The *Top Threat Actors* widget displays the top five threat actors and Advanced Persistent Threat (APT) groups.

Click the name of a threat actor to display more details on the *Adversary Centric Intelligence* > *Reports* page.



Activities

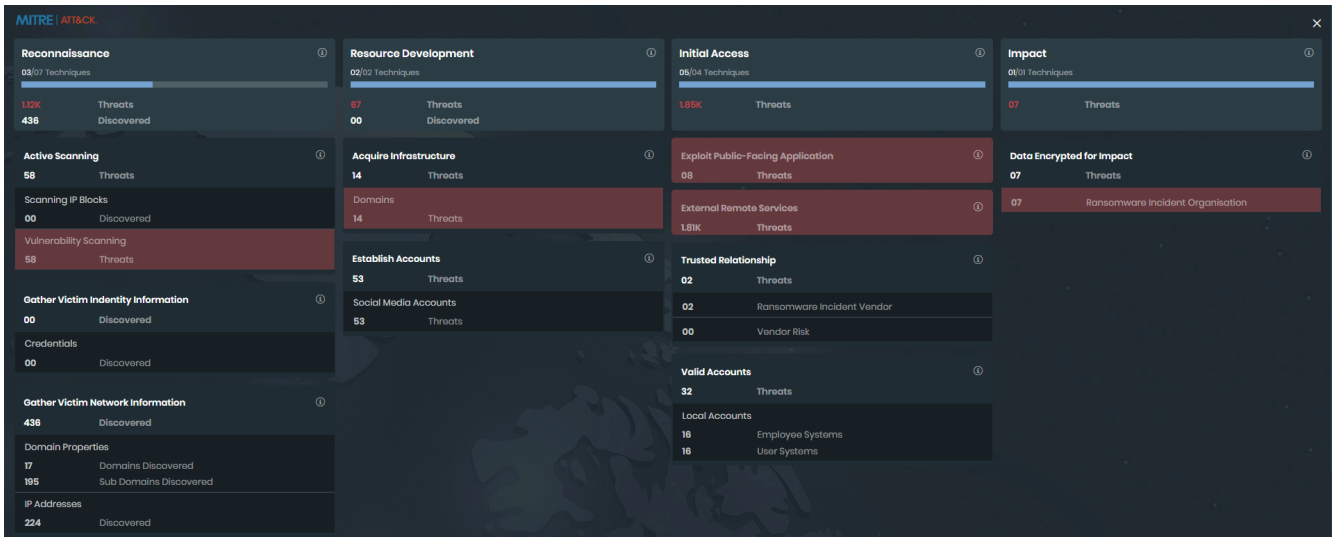
The *Activities* widget displays a log of recent activities performed within FortiRecon.



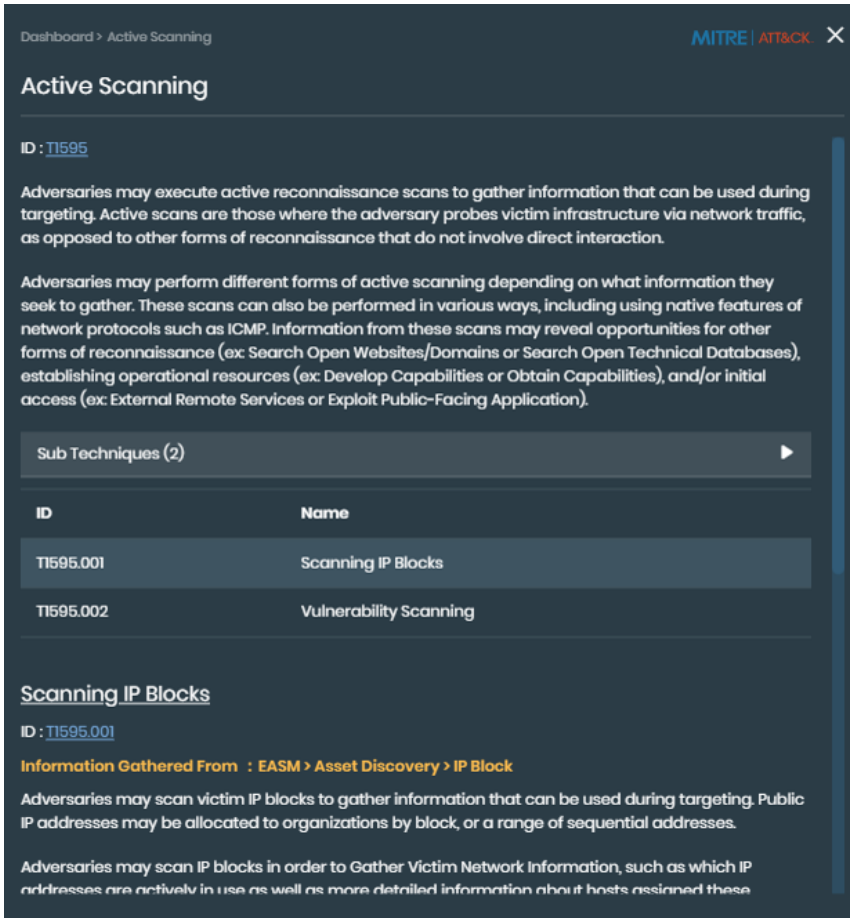
Viewing MITRE ATT&CK Framework

The *MITRE ATT&CK* view displays the discovered threats mapped to the corresponding techniques and sub-techniques of the ATT&CK framework. This allows you gain an insightful perspective into the tactics, techniques, and procedures (TTPs) employed by adversaries.

Techniques or sub-techniques highlighted in red indicates that new threats are discovered within the past 30 days and require immediate attention.



Clicking *Information* icon displays detailed information in the right pane. Clicking link next to *ID* field to opens the respective technique or sub-technique details page in *MITRE ATT&CK* website.

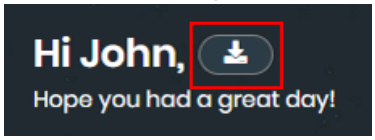


Downloading Executive Report

You can download the executive report that includes combined dashboard details as a PDF file.

To download the executive report:

1. Go to *Overview*.
2. Click *Download Report* icon.



3. Retrieve the download from *Profile Settings*. See Retrieving downloads on page 203.

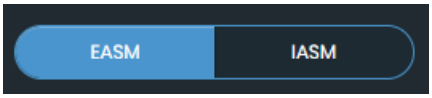
Attack Surface Management

Attack Surface Management (ASM) offers a complete view of potential risks across your external and internal digital environments. It combines discovery, vulnerability assessment, and threat intelligence to help you proactively manage and reduce your attack surface. ASM includes the following modules.

- *External Attack Surface Management (EASM)*: Provides an adversary's view of external-facing digital assets to discover potential exposures, vulnerabilities, and security gaps. See EASM.
- *Internal Attack Surface Management (IASM)*: Maps and assesses risks within your networks, discovering internal assets and identifying vulnerabilities that could be exploited by attackers. See IASM.

The ASM module displays the EASM and IASM scan results for your organization on the following pages :

The *EASM/IASM* toggle is located at the top of the *Dashboard, Asset Discovery,* and *Security Issues* pages within the ASM module. This toggle allows you to seamlessly switch between EASM and IASM data.



Dashboard	Displays widgets that summarize your discovered assets and potential security issues related to your assets. You can click some widgets to display more details on the other tabs. See EASM or IASM dashboard.
Security Issues	Displays a summary of all potential security issues and details about each issue. You can filter security issues and change the status of security issues to reflect action taken at your organization. See EASM or IASM security issues.
Asset Discovery	Displays a summary of all discovered assets and details about each asset. You can mark assets as false positives, manually add assets, and manually remove assets. See EASM or IASM asset discovery.
Asset Management	Displays tags and groups used to filter and link assets. Also, you can configure IASM. See Asset Management on page 79.
Leaked Credentials	Displays a summary of leaked credentials by year and details about each breached dataset or leaked credential incident. See Leaked Credentials on page 93.
Integrations	Displays the added integrations for *AWS, Azure, Google Cloud Platform, FortiDAST*, and *FortiGate*. See Integrations on page 96.

EASM

The External Attack Surface Management (EASM) module provides information about your digital assets, potential security issues, and leaked credentials. You can use the EASM module to identify exposed known and unknown assets,

learn about associated vulnerabilities, and prioritize the remediation of critical issues.

FortiRecon scans your digital assets and displays the results. There are two types of scans:

- **Scheduled Scan** - Full scan that consists of both *Passive* and *Active* scanners, performed weekly or monthly based on your subscription.
- **Continuous Scan** - Continuously scans all discovered assets to detect any updates such as new ports or services. The results are updated on refresh.

You can analyze EASM scan results in the FortiRecon portal.

- Dashboard
- Security Issues
- Asset Discovery

Dashboard

The *Attack Surface Management* > *Dashboard* page displays a number of widgets that summarize your discovered digital assets and potential security issues. From the *Attack Surface Management* > *Dashboard* page, you can:

- View a summary of your discovered digital assets. See Viewing discovered assets summary on page 50.
- View a summary of potential security issues related to your organization. See Viewing security issues summary on page 51.
- View a global map of your assets and the number of potential security issues affecting your organization. See Viewing a map of assets on page 52.
- Download the dashboard content to your hard drive. See Downloading the EASM dashboard details on page 53.

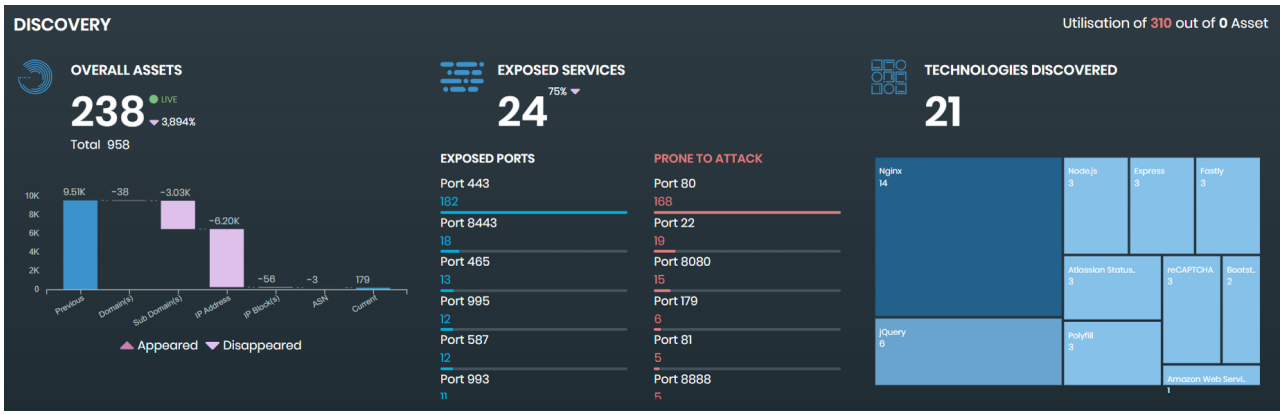
Viewing discovered assets summary

The *Attack Surface Management* > *Dashboard* page displays the following widgets that summarize your discovered digital assets in the *Discovery* section:

- Overall Assets
- Exposed Services
- Technologies Discovered

To view discovered assets summary:

1. Go to the *Attack Surface Management* > *Dashboard* page. Select *EASM* using toggle. The list of assets discovered by FortiRecon is displayed in the *Discovery* section.



2. Use the following widgets to review your discovered assets:

Overall Assets	Displays the number of following entities discovered by FortiRecon: • *Previous*: results of the previous FortiRecon scan. • *Domain*: number of domains found by the latest scan. • *Sub-domain*: number of sub-domains found by the latest scan. • *IP address*: number of IP addresses found by the latest scan. • *IP block*: number of IP blocks found by the latest scan. • *ASN* (Autonomous System Number): number of ASNs found by the latest scan. • *Org name*: number of organizations found by the latest scan. • *Current*: results of the current scan
Exposed Services	Displays all the exposed services discovered by FortiRecon, including exposed ports. FortiRecon performs port scanning by examining over 1200 well known TCP ports.
Technologies Discovered	Displays all the technologies discovered by FortiRecon.

3. Click the *Overall Assets* widget or the *Exposed Services* widget to display more details on the *Asset Discovery* page. See Asset Discovery on page 59.

Viewing security issues summary

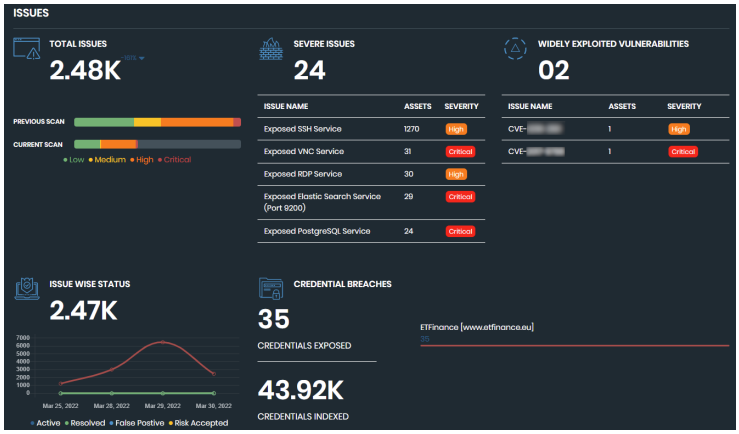
The *Attack Surface Management* > *Dashboard* page displays the following widgets that summarize potential security issues in the *Issues* section:

- Total Issues
- Severe Issues
- Widely Exploited Vulnerabilities
- Issue Wise Status
- Credential Breaches

Use the *Severe Issues* tooltip to review information on the count of unique *High* and *Critical* issues.

To view discovered assets summary:

1. Go to the *Attack Surface Management* > *Dashboard* page. Select *EASM* using toggle and scroll to the *Issues* section. The list of potential security issues is displayed.



2. Use the following widgets to review your security issues:

Total Issues	Displays the total number of issues discovered by the latest scan compared to the results of the previous scan.
Severe Issues	Displays the number of severe issues, and then lists the name, affected assets, and severity rating of the issues.
Widely Exploited Vulnerabilities	Displays the number of widely exploited vulnerabilities discovered, and then lists the name, affected assets, and severity rating of the issues.
Issue Wise Status	Displays a graph visualizing the number of issues in each status over time.
Credential Breaches	Displays the number of exposed credentials and the number of indexed credentials.

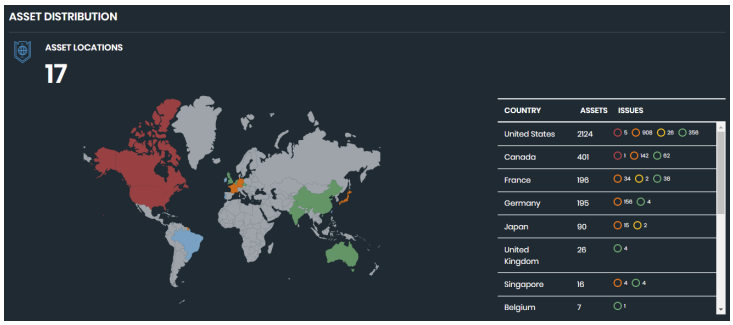
3. Click an issue or vulnerability to display more details on the *Security Issues* page. See Security Issues on page 53.

Viewing a map of assets

The *Attack Surface Management* > *Dashboard* page displays a global map of your digital assets in the *Asset Distribution* section. The color of the country aligns with the highest severity level of potential issues. If the country is blue, no issues are recorded.

To view a map of assets:

1. Go to the *Attack Surface Management* > *Dashboard* page. Select *EASM* using toggle and scroll to the *Asset Distribution* section. A global map of your discovered assets is displayed.



2. Use the table to view the number of assets and potential security issues in each country.

Column	Description
Country	Lists countries where your digital assets were discovered.
Assets	Displays the number of assets discovered in each country.
Issues	Displays the number of potential security issues and indicates the severity rating of the issues by color: • Red indicates critical. • Orange indicates high. • Yellow indicates medium. • Green indicates low. The colors on the map align with the severity level of the issues.

3. Click a country or issue in the table to display more details on the *Security Issues* page. See Security Issues on page 53.

Downloading the EASM dashboard details

The Attack Surface Management dashboard details can be downloaded to your hard drive. The process downloads a zip file that contains the following items:

- List of discovered assets in Microsoft Excel format
- List of issues in Microsoft Excel format
- An attack surface summary dashboard in PDF

To download the EASM dashboard:

1. Go to *Attack Surface Management* > *Dashboard*.
2. Choose *EASM* using toggle.
3. Click *Download*.
4. Retrieve the download from *Profile Settings*. See Retrieving downloads on page 203.

Security Issues

The *Attack Surface Management* > *Security Issues* page provides a summary of all potential security issues and details about each issue. From the *Security Issues* page, you can:

- View a summary about and details of all potential security issues related to your assets. See Viewing security issues on page 54.
- Apply filters to the list of security issues to hone in on specific issues. See Filtering security issues on page 55.
- Change the status of security issues to reflect changes made at your organization to address the issues. See Changing the status of security issues on page 57.
- Add a comment to explain status changes made to security issues. See Adding a comment to a security issue on page 58.
- Export security issues to an Excel file. See Exporting security issues.

Viewing security issues

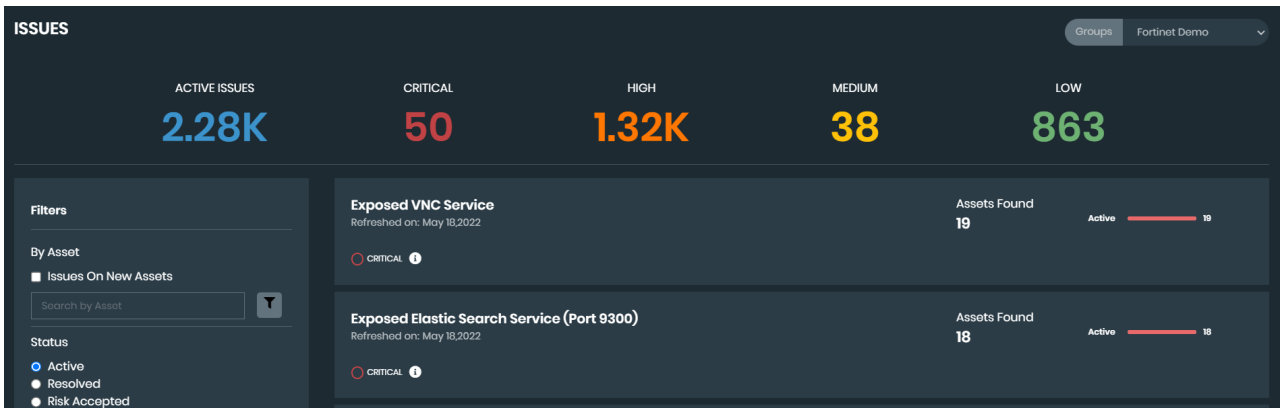
The *Attack Surface Management* > *Security Issues* page displays the number of active security issues and how many of the active security issues are rated critical, high, medium, and low. Color indicates the severity of a security issue:

Critical	Security issues rated *Critical* are red.
High	Security issues rated *High* are orange.
Medium	Security issues rated *Medium* are yellow.
Low	Security issues rated *Low* are green.

You can use search and filters to change the list of reports that are displayed, and then click each report to display its details.

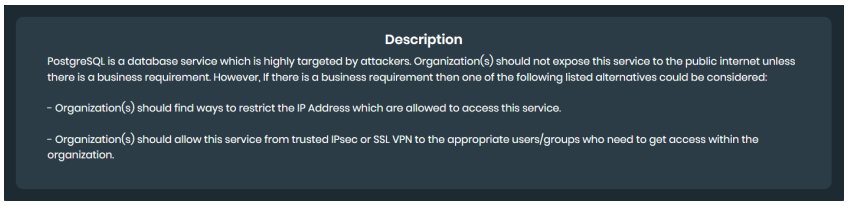
To view security issues:

1. Go to *Attack Surface Management* > *Security Issues*. Choose *EASM* using toggle, the respective security issues are displayed.
   The *Issues* bar across the top displays the number of active security issues and the number of active security issues that are rated critical, high, medium, and low security risk.
   For each report, the number of affected assets is also displayed.

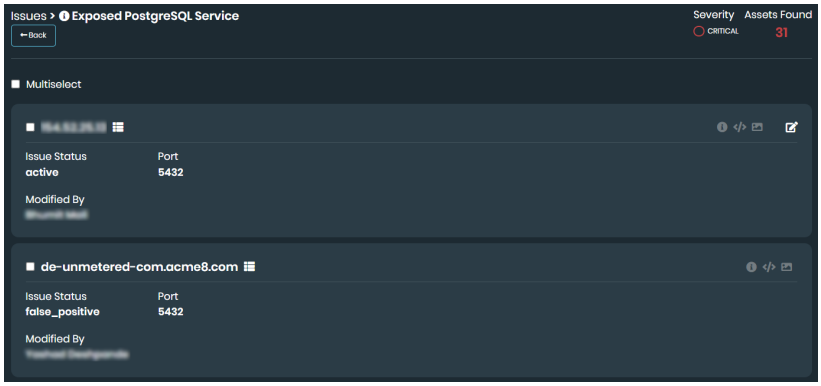


2. In the *Issues* section, click the number under *Critical*, *High*, *Medium*, or *Low*. The corresponding filter is selected and only those reports are displayed.

3. For each report, click the *i* icon to display a description of the issue and suggested remediation steps.



4. Click the title of a report to display details about affected assets.



5. If available, view the path used to discover the issue:
   a. Click the *Discovery Path* icon. The discovery path is displayed.

   b. Click the *X* in the top-right corner to close the window.
6. When available, click the following icons:

Additional Information	Displays additional information about the security issue.
Raw Data	Displays raw data about the security issue.
Edit	Click to change the status of a security issue to reflect action taken by your organization to address the issue. See Changing the status of security issues on page 57.

7. Click the *Back* button.

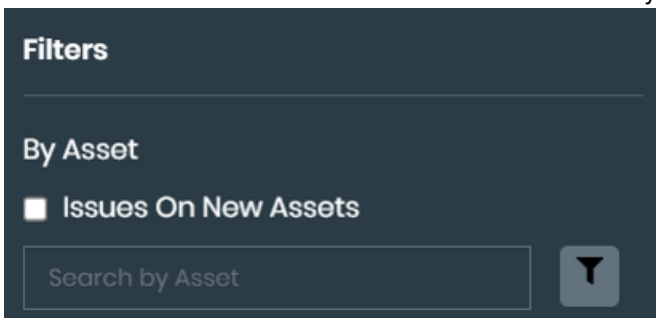
Filtering security issues

By default, the *Attack Surface Management* > *Asset Discovery* page displays all potential security issues, starting with critical security issues. You can use filters to display specific types of issues.

You can search for specific security issues using the *Search by Asset* field. Enter IP address information, such as 192.168.10.10 or 192.168.12.0/24.

To filter security issues:

1. Go to *Attack Surface Management* > *Security Issues*. Choose *EASM* using toggle, the respective security issues are displayed.
2. Select the *Issues On New Assets* checkbox to filter security issues on newly discovered assets.



3. Add advanced search features:
   a. Click the filter icon. The advanced search fields are displayed.
   b. Select the *Search Type*.
   c. Click *Search*.
4. Select one or more filters, and click *Search*:

Filter	Options
Status	Select one of the following statuses: • Active • Resolved • Risk accepted • False positive
Severity	Select one or more of the following severity statuses: • Critical • High • Medium • Low
Category	Select one or more of the categories. The list of categories changes based on the displayed security issues.
Country	Select one or more countries.

   The list of filtered security issues is displayed.
5. (Optional) In the *Filters* list, toggle on *False Positive*. The list displays only issues marked with a status of *False Positive*.
6. In the *Filters* list, click *Clear* to remove all filters.

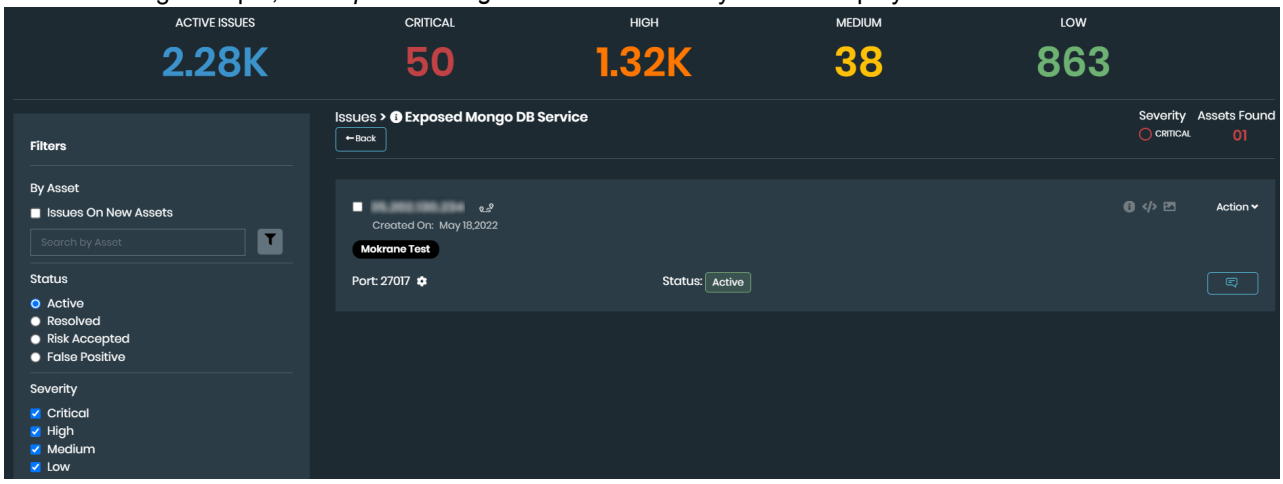
Changing the status of security issues

As you review and address security issues reported by FortiRecon, you can change the status of each issue to reflect your understanding and actions:

Mark as Active	Available only after you change the status of a security issue from active to another status. Select to move an issue back to the active status.
Mark as Resolved	Select to indicate actions taken at your organization have resolved the security issue.
Risk Accepted	Select to indicate actions taken at your organization have not fully resolved the security issue, but the current level of risk is acceptable.
False Positive	Select to indicate that the security issue is not an issue for your organization. The issue is considered a *False Positive* issue.

To change the status of security issues:

1. Go to *Attack Surface Management* > *Security Issues*. Select *EASM* using toggle. The discovered assets are displayed.
2. If necessary, select one or more filters, and click *Search*.
   The list of filtered security issues is displayed.
3. Click an issue title to display its details.
   In the following example, the *Exposed Mongo DB Service* security issue is displayed:



4. Click *Edit* in the top-right corner to change the status by selecting one of the following options:
   - Mark as Resolved
   - Risk Accepted
   - False Positive
5. Click *Back* to display the list of issues again.

Adding a comment to a security issue

When editing a security issue on *Attack Surface Management* > *Security Issues*, the client can leave a comment to describe the changes and why they were made.

Selecting the comment button will open all comments for that issue. This allows you to review all changes and discussions related to the issue.

To add a comment to a security issue:

1. Go to *Attack Surface Management* > *Security Issues*.
2. Select a type of security issue.
3. Locate the issue you would like to make a change to.
4. Click the comment button. A list of previous comments and a text box is displayed.
5. Enter a comment related to the status change.
6. Click *Add*.

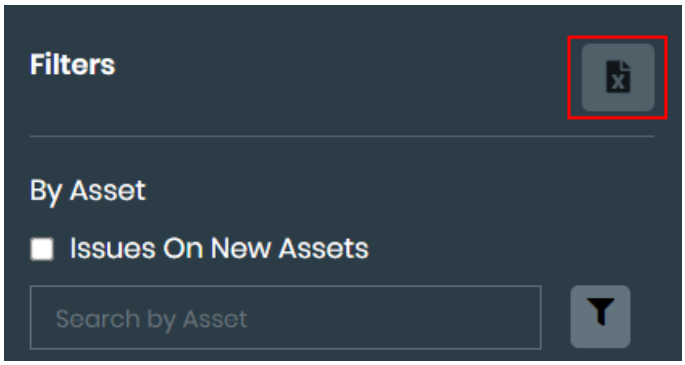
Exporting security issues

You can export a list of security issues into an Excel file. The spreadsheet will include the information on:

- Issue Category
- Issue Name
- Severity
- Asset
- Port
- Issue Status
- Tags
- Groups
- Last Refreshed On
- Additional Details
- Recommendations

To export the security issues:

1. Go to *Attack Surface Management* > *Security Issues*. Select *EASM* using toggle.
2. Optionally, apply filters to export specific security issues. See Filtering security issues.
3. Click *Download* icon. The file is downloaded to your computer.



Asset Discovery

The *Attack Surface Management* > *Asset Discovery* page provides a summary of all discovered assets and details about each asset. From the *Asset Discovery* page, you can:

- View a summary about and details of your assets. See Viewing asset details on page 59.
- Mark discovered assets as false positives to remove them from the next scheduled FortiRecon scan. See Marking assets as false positives on page 61.
- Manually add assets to FortiRecon to include them in the next scheduled scan. See Adding assets manually on page 62.
- Manually remove assets from the next scheduled FortiRecon scan. See Removing assets manually on page 63.
- Assign tags to assets for focused filtering. See Assigning tags on page 63.

> Tags are created in *Attack Surface Management* > *Asset Management*. Assets can also be assigned to tags in bulk in the *Asset Management* page. See Asset Management on page 79.

- Perform a FortiDAST vulnerability scan on assets. See Performing a FortiDAST scan on page 65.
- View DNS health report for your domains. See DNS Health Report on page 66.
- Export a list of assets to an Excel file. See Exporting assets.

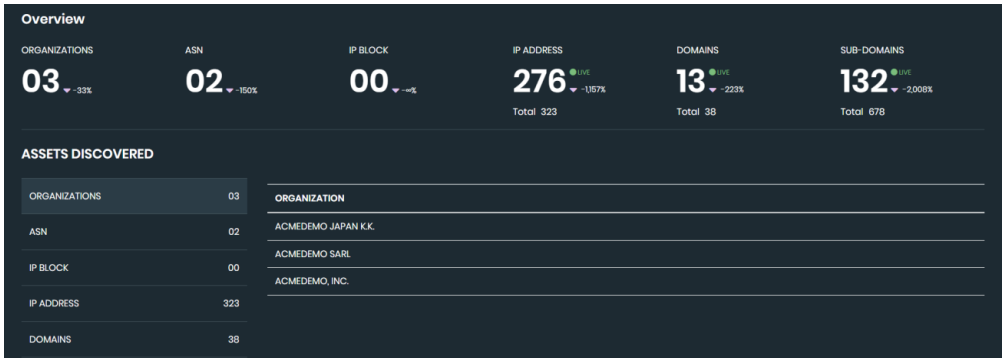
Viewing asset details

The *Attack Surface Management* > *Asset Discovery* page displays the number of assets in an *Overview* section and in an *Assets Discovered* list.

You can display details about an asset by clicking a number in the *Overview* section or a category in the *Assets Discovered* list. When you are reviewing asset details, you can mark assets as *False Positive* as needed to remove them from future FortiRecon scans.

To view asset details:

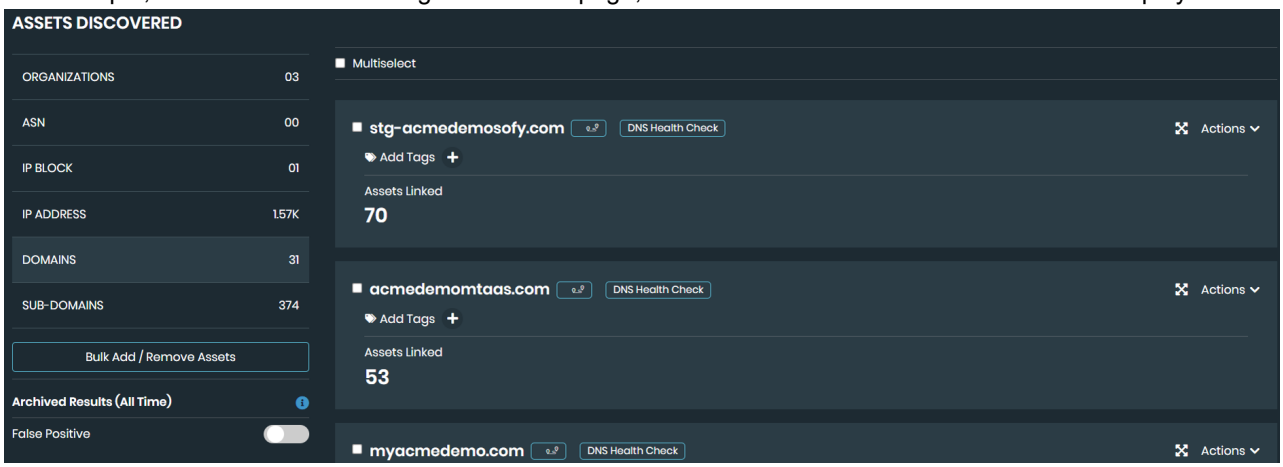
1. Go to *Attack Surface Management* > *Asset Discovery*.
2. Choose *EASM* using toggle. The number of discovered assets display in an *Overview* section across the top and in an *Assets Discovered* list on the left side of the page.



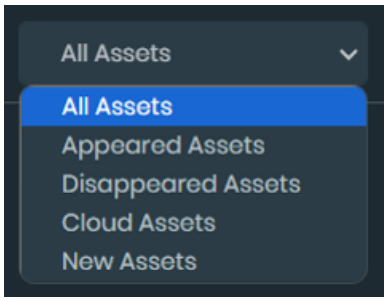
The following information is available:

Organizations	The number of organizations that have been detected as belonging to you.
ASN	The number of autonomous system numbers (ASNs) that are linked to the detected organizations.
IP blocks	The number of IP blocks associated with the ASNs.
IP address	The number of IP addresses that are linked to the IP blocks.
Domains	The number of domains linked to your organization.
Sub-domains	The number of sub-domains linked to your organization.

3. In the *Overview* bar, click a number, or in the *Assets Discovered* list, click an asset category. Details about the selected item are displayed on the right side of the page.
For example, click *Domains*. On the right side of the page, the names of the discovered domains are displayed.



4. Filter the assets from the dropdown menu:



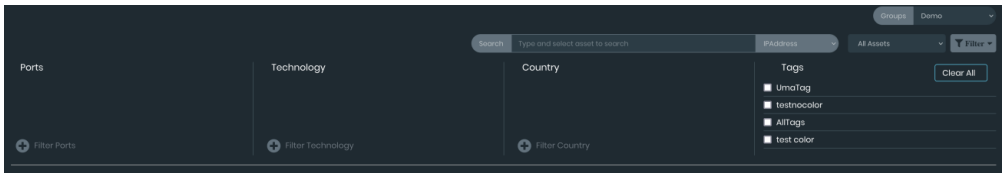
a. Select *Appeared Assets* to show assets that appeared in the latest scan.
b. Select *Disappeared Assets* to show assets that disappeared in the latest scan.
c. Select *Cloud Assets* to show cloud-based assets.

Cloud assets can only be filtered if the AWS cloud environment has been integrated. See Integrations on page 96.

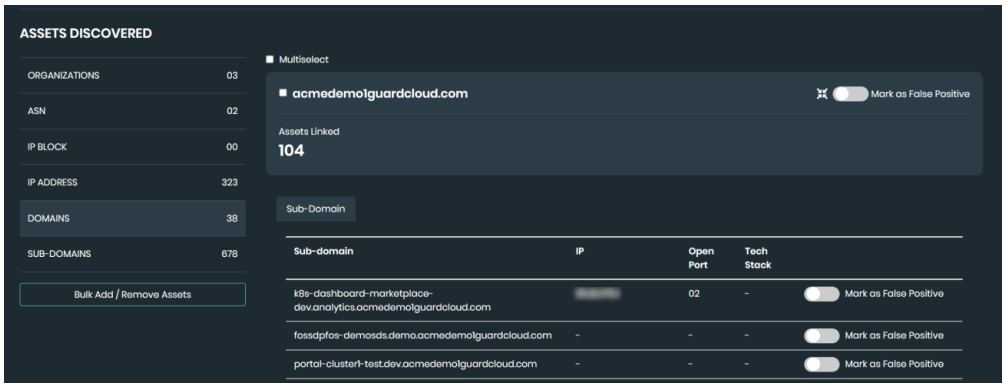
---

d. Select *New Assets* to show new assets or assets that have updates.

5. Select *Filter* to define ports, technology, country, tag, and group filters.



6. Click the *Expand* icon. Details about the domain are displayed.



7. If an asset should be removed from the next scheduled FortiRecon scan, mark the asset as *False Positive*. See also Marking assets as false positives on page 61.

Marking assets as false positives

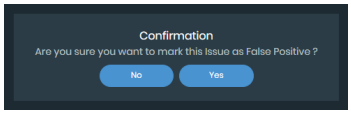
You can manually mark any of the following discovered assets as false positives to remove them from the next scheduled FortiRecon scan:

- ASN
- IP blocks
- IP addresses

- Domains
- Sub-domains

To mark false positives:

1. Go to *Attack Surface Management* > *Asset Discovery*. Select *EASM* using toggle. The discovered assets are displayed.
2. Click one of the following assets to display its details:
   - ASN
   - IP Blocks
   - IP Address
   - Domains
   - Sub-domains
3. Select an asset, and toggle on *Mark as False Positive*.



You can also select the *Multiselect* checkbox to select all or some assets, and then mark them as false positives.

A confirmation dialog is displayed.

4. Click *Yes*.

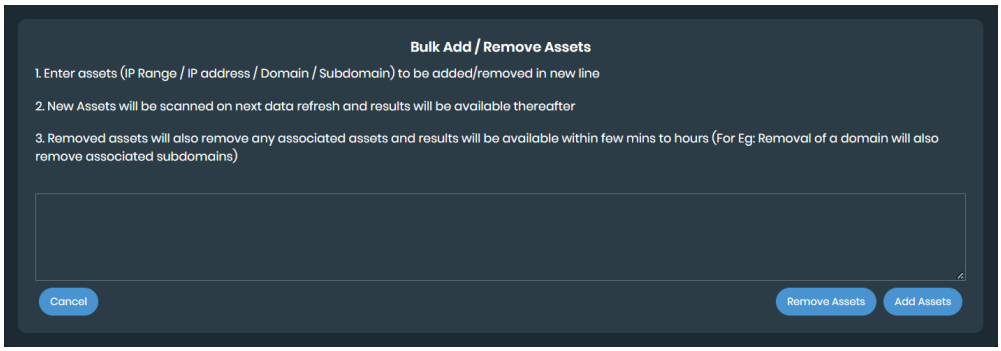
Adding assets manually

FortiRecon discovers assets for you. You can also manually add assets to FortiRecon scans.

When you manually add assets to FortiRecon, results for the assets are visible after the next scheduled FortiRecon scan.

To add assets:

1. Go to *Attack Surface Management* > *Asset Discovery* > *EASM*. The discovered assets are displayed.
2. Click *Bulk Add / Remove Assets*. The *Bulk Add / Remove Assets* dialog is displayed.



3. Enter the assets, and click *Add Assets*.

The scan results for the newly added assets will be available within 24 hours in FortiRecon portal.

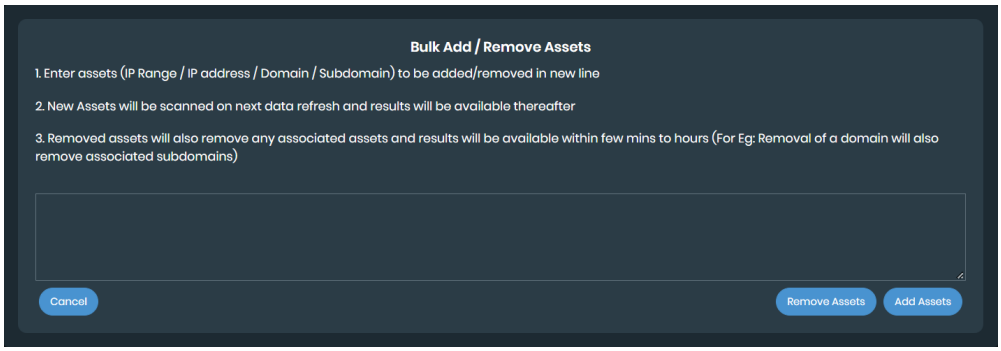
Removing assets manually

FortiRecon discovers assets for you. You can also manually remove assets from FortiRecon scans.

When you manually remove assets from FortiRecon, any associated assets are also removed. The changes are visible within minutes or hours, depending on the change.

To remove assets:

1. Go to *Attack Surface Management* > *Asset Discovery* > *EASM*. The discovered assets are displayed.
2. Click *Bulk Add / Remove Assets*. The *Bulk Add / Remove Assets* dialog is displayed.



3. Enter the assets, and click *Remove Assets*.

Assigning tags

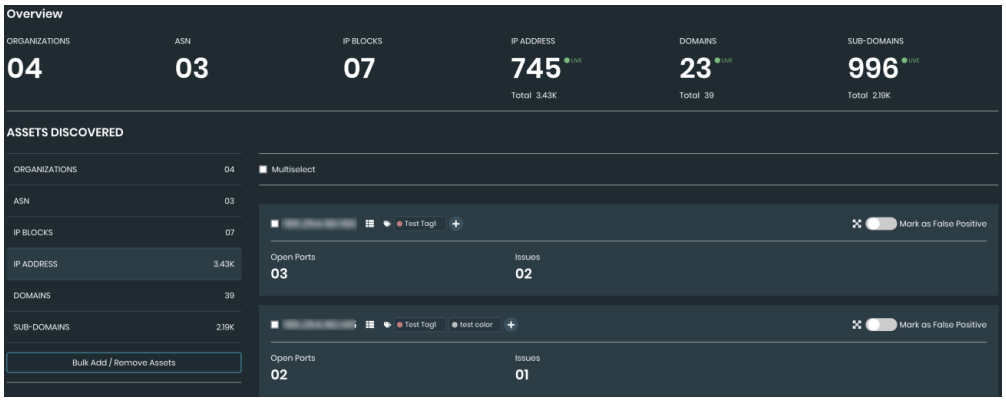
Tags can be assigned to assets for focused filtering in the *EASM* > *Asset Discovery* page. For more information on tags, see Asset Management on page 79.

To assign a tag to an asset:

1. Go to *Attack Surface Management* > *Asset Discovery*.
2. Find the asset you want to tag and click the + icon. The *Add Tags* dialog is displayed.

To create a new tag, click *Create* in the *Add Tags* dialog or go to *Attack Surface Management* > *Asset Management* page. See Creating a tag on page 79.

3. Select the tags you would like to assign.
4. Click *Add*.

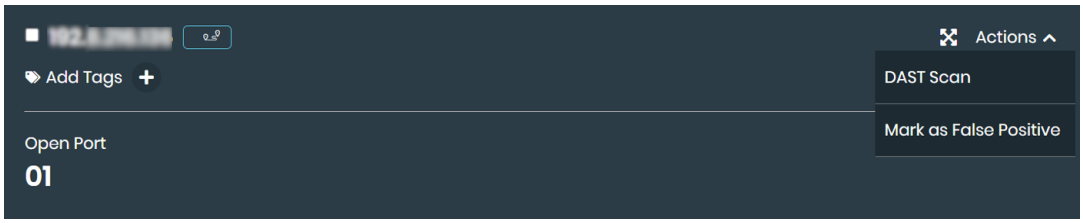


Performing a FortiDAST scan

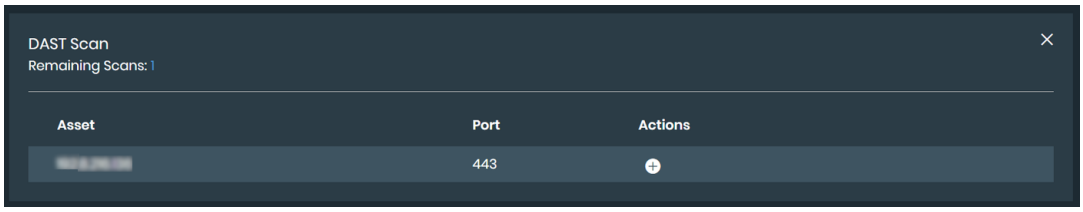
You can use FortiDAST to perform a vulnerability scan on your assets. By leveraging a FortiDAST integration with FortiRecon, you can identify vulnerabilities and security gaps within your assets. See the FortiDAST User Guide for more information on how the integration and scanning works.

To scan an asset with FortiDAST:

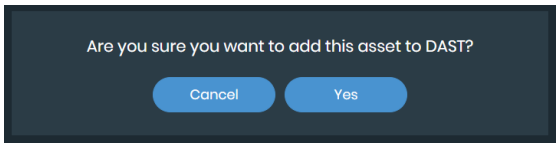
1. Add a FortiDAST integration to FortiRecon. See Adding integrations on page 96.
2. Go to *Attack Surface Management* > *Asset Discovery*.
3. Navigate to the asset you want to scan.
4. Select *Actions* > *DAST Scan*.



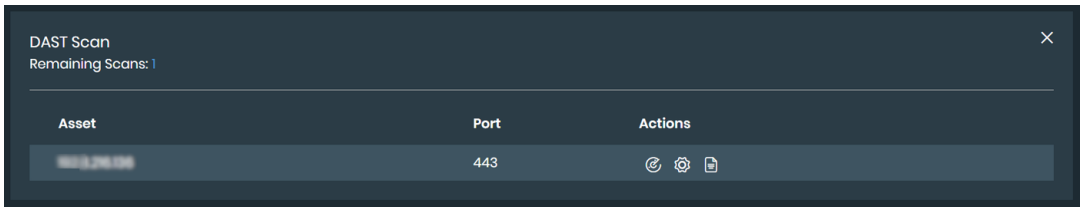
The *DAST Scan* dialog opens with number of *Remaining Scans* displayed.



5. Click *Add* beside the asset you want to add to DAST. A confirmation message is displayed.



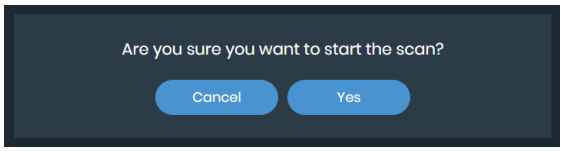
6. Click *Yes*. The *Scan*, *Config Scan*, and *View Result* buttons become available for the asset.



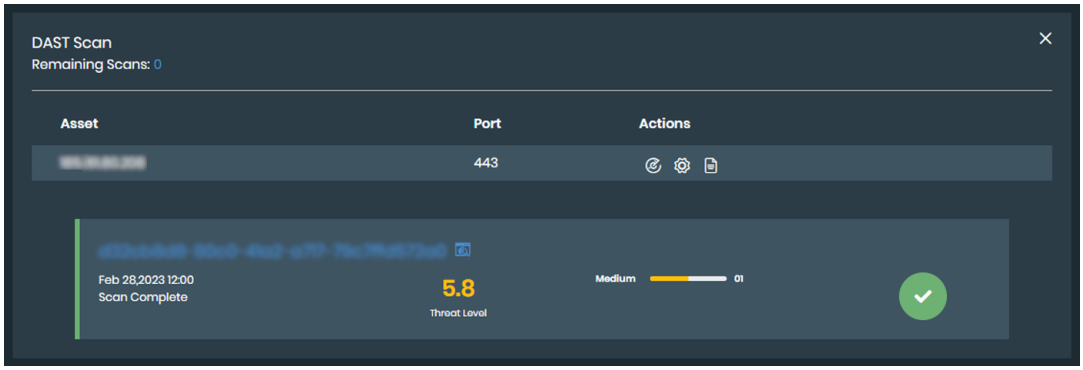
7. Click *Config Scan*. You will be redirected to FortiDAST.

Only master or sub users will be redirected to FortiDAST to complete the configuration. Other users will be prompted with a dialog on how to proceed.

8. Configure the scanner. See the FortiDAST User Guide for more information.
9. Click *Scan*. A confirmation message is displayed.



10. Click *Yes*.
11. Once the scan has started, click *View Result* to view the status of the scan.



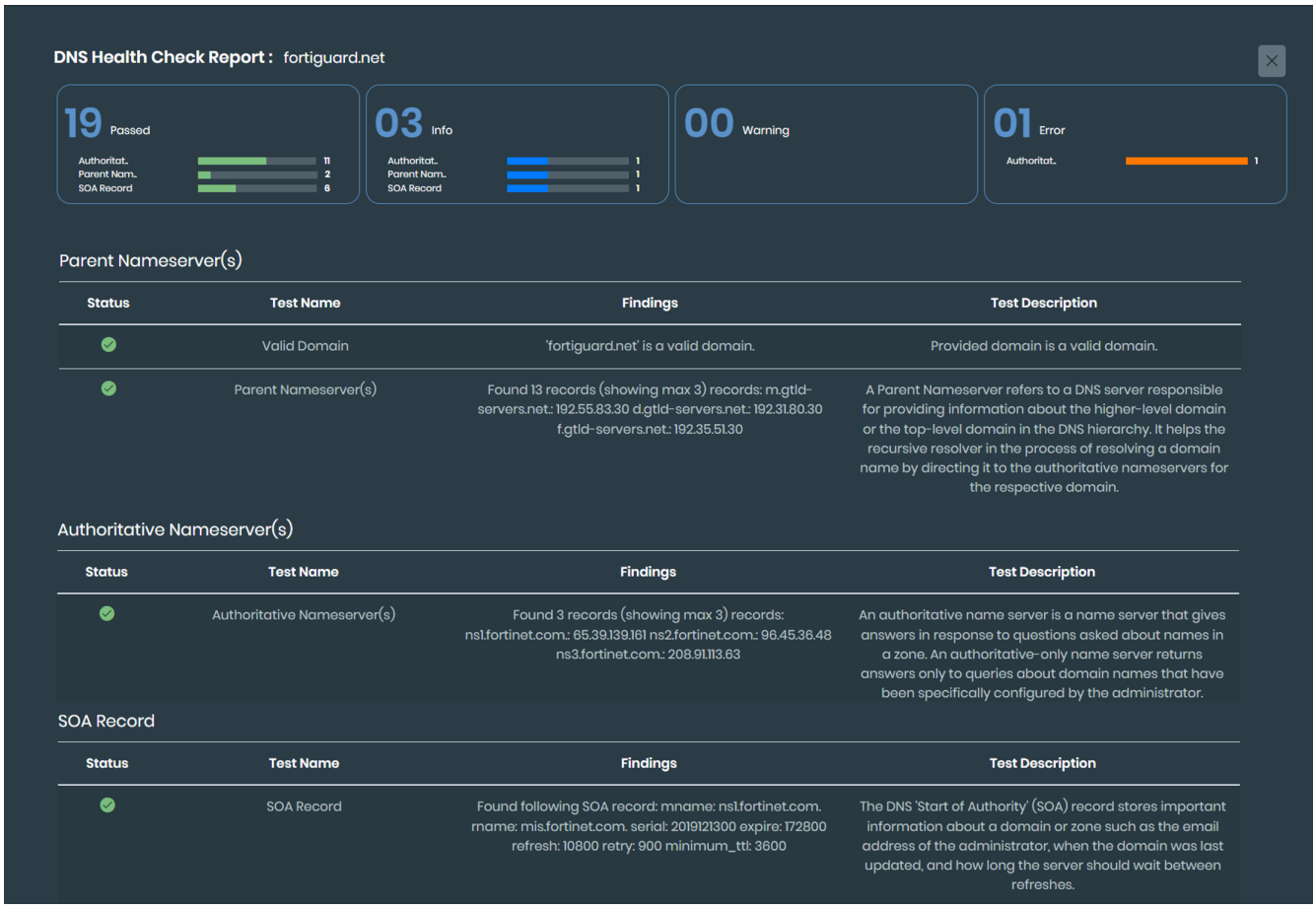
You can scan the same asset again by selecting *ReScan*.

DNS Health Report

FortiRecon's DNS Health Report feature is a powerful tool that provides a comprehensive analysis of your domain's DNS health. This feature offers detailed information on passed, info, warning, and error counts, allowing you to quickly identify and address any potential issues. The report includes sections dedicated to the *Parent Nameserver(s)*, *Authoritative Nameserver(s)*, and *SOA Records*, offering valuable insights into the overall health and adherence to DNS standards of your domain.

To view DNS health report:

1. Go to *Attack Surface Management* > *Asset Discovery* > *EASM* >*Domain*.
2. Navigate to the domain you want to view the report for.
3. Select *DNS Health Check*.



Exporting assets

You can export a list of assets into an Excel file. The spreadsheet will include the information on:

- Asset
- Open Ports
- Linked Assets
- Total Issues
- Country
- Tags
- Groups
- Discovery
- Last Refreshed On

To export discovered assets:

1. Go to *Attack Surface Management > Asset Discovery > EASM*.
2. Optionally, apply the required filters to export specific types of assets. See Viewing asset details.
3. Click *Download* icon. The file is downloaded to your computer.

IASM

Internal Attack Surface Management (IASM) provides comprehensive internal asset discovery, vulnerability assessment, and web application analysis for attack surface management.

IASM allows you to scan multiple subnets and deploy the *IASM Agent* across multiple sites to ensure complete visibility into your internal attack surface. *IASM Agent* is a Docker container deployed within your network, responsible for executing scans and relaying discovered data to the FortiRecon.

To get started with IASM, follow these steps:

1. Configure IASM settings in *Asset Management* > *IASM Configuration* and download the configuration file (.yml). See IASM Configuration.
2. Use the configuration file to deploy the IASM Agent on a device within your internal network. See IASM Agent.
3. Access and analyze IASM scan results in the FortiRecon portal.
   - Dashboard
   - Security Issues
   - Asset Discovery

IASM Agent

The IASM Agent is deployed within your internal network to enhance your internal security posture. It performs the following tasks.

- *Asset discovery*: Scans your network to map and identify all connected devices.
- *Port scan*: Determines open ports on discovered assets, revealing potential points of access.
- *Service enumeration*: Identifies services and their versions running on open ports, providing insights for targeted vulnerability assessments.
- *Web application enumeration*: Sends tailored probes to identify the specific technologies (programming languages, frameworks) behind each discovered web application.
- *Vulnerability detection*: Performs non-intrusive scans to identify security misconfigurations and known vulnerabilities in discovered web applications. This includes checks for missing HTTP headers, misconfigured Cross-Origin Resource Sharing (CORS) policies, and SSL/TLS certificate issues.
- *WordPress CMS security*: Scans vulnerabilities commonly found in WordPress CMS.

FortiRecon currently scans TCP ports only.

The IASM agent transmits collected data to FortiRecon for centralized analysis and reporting. FortiRecon analyzes the data to identify vulnerabilities in discovered services and technologies. It then cross-references these vulnerabilities with the FortiRecon threat intelligence database to determine if they correspond to known, actively exploited attacks.

System Requirements

Following are the hardware and software requirements to deploy IASM Agent.

Hardware

Ensure your system meets the following hardware requirements for optimal IASM Agent performance.

Use Case	CPU Cores	RAM (GB)	Disk Space (GB)
Less Than 10 Subnets	4	8	75
More Than 10 Subnets	8	16	100

Software

The IASM Agent is only compatible with *Ubuntu 22.04*.

Prerequisites

Ensure that the following prerequisites are met for proper functioning of IASM Agent.

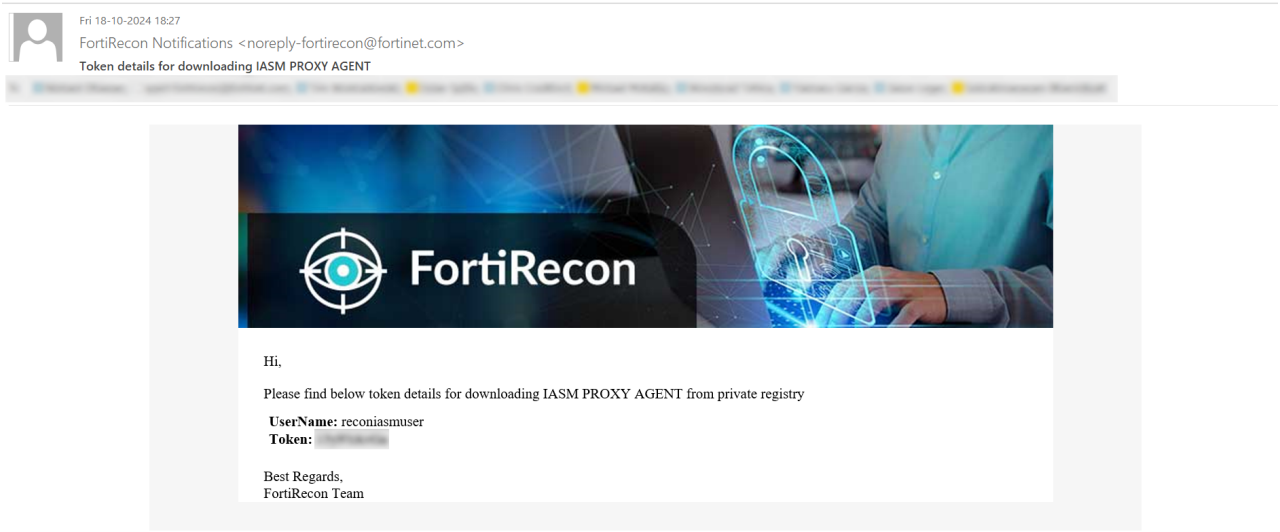
- The IASM Agent must be deployed on a virtual machine or physical server within your internal corporate network. This ensures the agent has proper network access to reach and scan the specified subnets.
- Ensure the machine hosting the IASM Agent has full network access to all subnets you intend to scan.
- Verify that the IASM system/VM has outbound internet access to *https://fortirecon.forticloud.com/iasm* on port *443*. This connection is necessary for the agent to communicate with the FortiRecon.

Deploying IASM Agent

Perform the following steps to deploy IASM Agent.

Ensure that System Requirements and Prerequisites are met before deploying IASM Agent.

1. Install *Ubuntu 22.04* on a physical server or virtual machine.
2. Install the latest version of Docker engine and the Docker compose.
   ```
   sudo apt install docker.io
   sudo apt install docker-compose
   ```
3. Configure IASM settings in *Asset Management* > *IASM Configuration* and download the configuration file (*iasmproxy.yml*). See IASM Configuration.
4. Copy the configuration file to the Linux machine.
5. Using a terminal or command prompt on the machine with Docker installed, navigate to the directory containing the downloaded *iasmproxy.yml* file.
6. Log in to the Docker registry using the following command.
   ```
   sudo docker login demo.fortirecon.forticloud.com
   ```
   You will then need to enter the credentials that were shared with you through the email notification.



7. Execute the following command.

```
sudo docker-compose -f <iasmproxy.yml> up -d
```

The *Attack Surface Management* > *Asset Management* > *IASM Configuration* page displays the IASM Agent status. A green icon indicates the agent is communicating with FortiRecon, while a red icon initially appears, indicating the agent is not yet communicating. There will be a delay 30 seconds before the status of the agent changes from red to green.

Dashboard

The *Attack Surface Management* > *Dashboard* page displays a number of widgets that summarize your discovered digital assets and potential security issues. From the *Attack Surface Management* > *Dashboard* page, you can:

- View a summary of your discovered digital assets. See Viewing discovered assets summary.
- View a summary of potential security issues related to your organization. See Viewing security issues summary.
- View a global map of your assets and the number of potential security issues affecting your organization. See Viewing a map of assets.
- Download the dashboard content to your hard drive. See Downloading the IASM dashboard details.

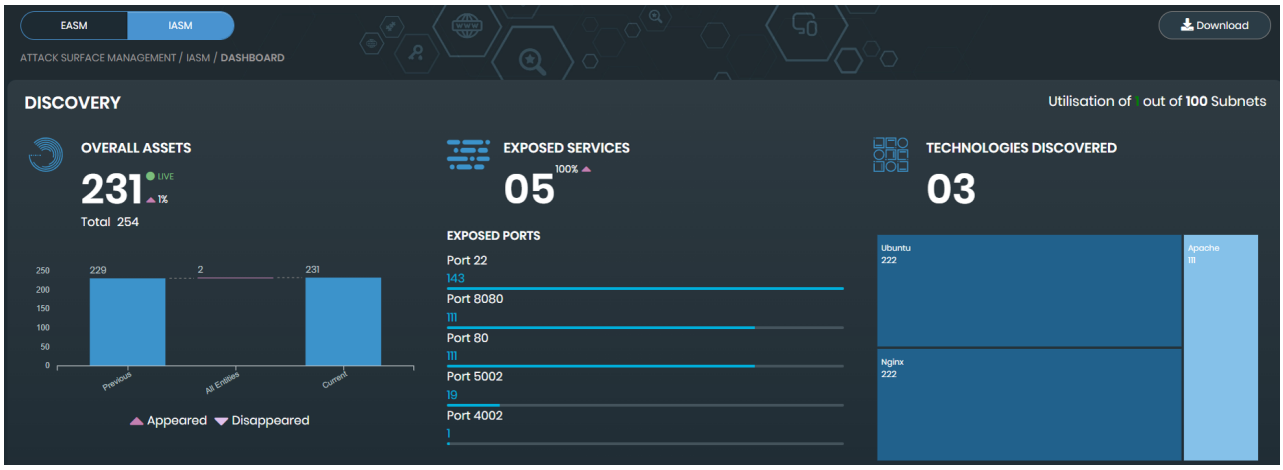
Viewing discovered assets summary

The *Attack Surface Management* > *Dashboard* page displays the following widgets that summarize your discovered digital assets in the *Discovery* section:

- Overall Assets
- Exposed Services
- Technologies Discovered

To view discovered assets summary:

1. Go to the *Attack Surface Management* > *Dashboard* page. Select *IASM* using the toggle. The list of assets discovered by FortiRecon IASM module is displayed in the *Discovery* section.



2. Use the following widgets to review your discovered assets:

Overall Assets	Displays the number of following entities discovered by FortiRecon: • *Previous*: results of the previous FortiRecon scan. • *All Entities*: number of organizations found by the latest scan. • *Current*: results of the current scan
Exposed Services	Displays all the exposed services discovered by FortiRecon, including exposed ports. FortiRecon currently scans TCP ports only.
Technologies Discovered	Displays all the technologies discovered by FortiRecon.

3. Click the *Overall Assets* widget or the *Exposed Services* widget to display more details on the *Asset Discovery* page. See Asset Discovery.

Viewing security issues summary

The *Attack Surface Management* > *Dashboard* page displays the following widgets that summarize potential security issues in the *Issues* section:

- Issue Wise Status
- Total Issues
- Severe Issues
- Widely Exploited Vulnerabilities

To view discovered assets summary:

1. Go to the *Attack Surface Management* > *Dashboard* page. Select IASM using toggle and scroll to the *Issues* section. The list of potential security issues is displayed.

2. Use the following widgets to review your security issues:

Issue Wise Status	Displays a graph visualizing the number of issues in each status over time.
Total Issues	Displays the total number of issues discovered by the latest scan compared to the results of the previous scan.
Severe Issues	Displays the number of severe issues, and then lists the name, affected assets, and severity rating of the issues.
Widely Exploited Vulnerabilities	Displays the number of widely exploited vulnerabilities discovered, and then lists the name, affected assets, and severity rating of the issues.

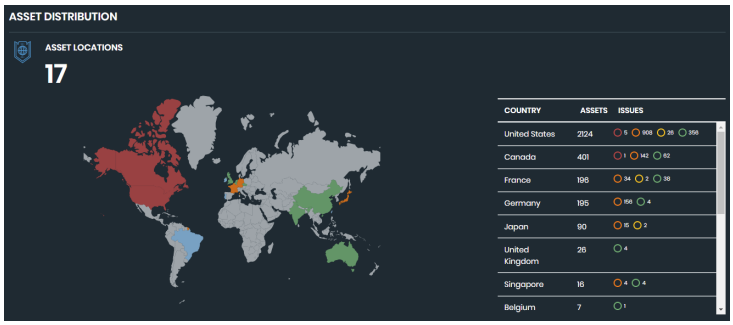
3. Click an issue or vulnerability to display more details on the *Security Issues* page. See Security Issues.

Viewing a map of assets

The *Attack Surface Management* > *Dashboard* page displays a global map of your digital assets in the *Asset Distribution* section. The color of the country aligns with the highest severity level of potential issues. If the country is blue, no issues are recorded.

To view a map of assets:

1. Go to the *Attack Surface Management* > *Dashboard* page. Select *IASM* using toggle and scroll to the *Asset Distribution* section. A global map of your discovered assets is displayed.



2. Use the table to view the number of assets and potential security issues in each country.

Column	Description
Country	Lists countries where your digital assets were discovered.
Assets	Displays the number of assets discovered in each country.
Issues	Displays the number of potential security issues and indicates the severity rating of the issues by color: • Red indicates critical. • Orange indicates high. • Yellow indicates medium. • Green indicates low. The colors on the map align with the severity level of the issues.

3. Click a country or issue in the table to display more details on the *Security Issues* page. See Security Issues.

Downloading the IASM dashboard details

The Attack Surface Management dashboard details can be downloaded to your hard drive. The process downloads a zip file that contains the following items:

- List of discovered assets in Microsoft Excel format
- List of issues in Microsoft Excel format
- An attack surface summary dashboard in PDF

To download the EASM dashboard:

1. Go to *Attack Surface Management* > *Dashboard.*
2. Choose *IASM* using toggle.
3. Click *Download*.
4. Retrieve the download from *Profile Settings*. See Retrieving downloads on page 203.

Security Issues

The *Attack Surface Management* > *Security Issues* page provides a summary of all potential security issues and details about each issue. From the *Security Issues* page, you can:

- View a summary about and details of all potential security issues related to your assets. See Viewing security issues.

- Apply filters to the list of security issues to hone in on specific issues. See Filtering security issues.
- Change the status of security issues to reflect changes made at your organization to address the issues. See Changing the status of security issues.
- Add a comment to explain status changes made to security issues. See Adding a comment to a security issue.
- Export security issues to an Excel file. See Exporting security issues.

Viewing security issues

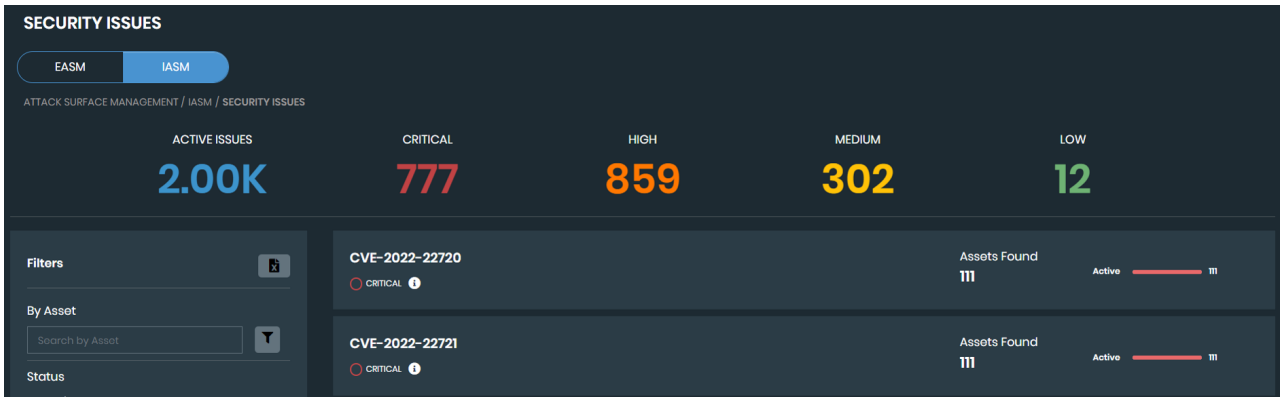
The *Attack Surface Management* > *Security Issues* page displays the number of active security issues and how many of the active security issues are rated critical, high, medium, and low. Color indicates the severity of a security issue:

Critical	Security issues rated *Critical* are red.
High	Security issues rated *High* are orange.
Medium	Security issues rated *Medium* are yellow.
Low	Security issues rated *Low* are green.

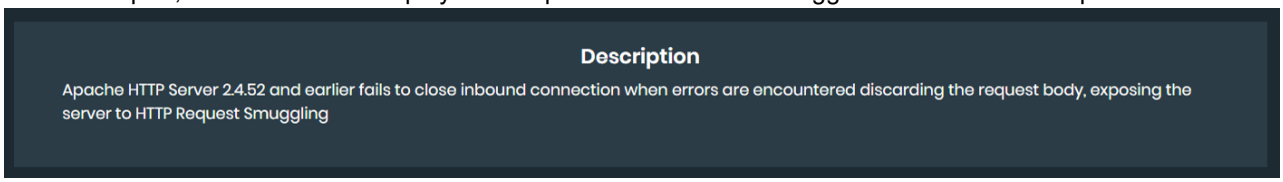
You can use search and filters to change the list of reports that are displayed, and then click each report to display its details.

To view security issues:

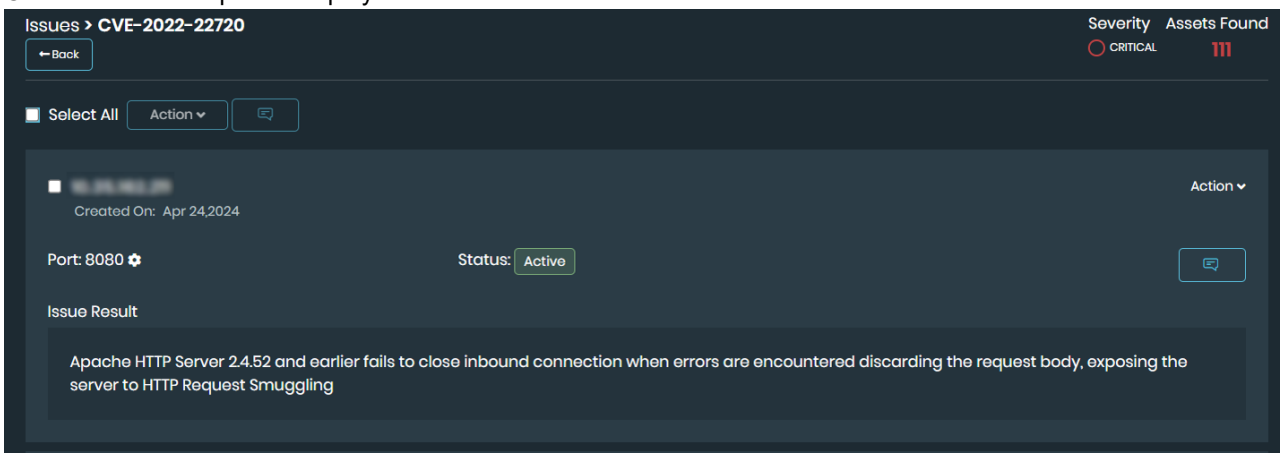
1. Go to *Attack Surface Management* > *Security Issues*. Choose *IASM* using toggle, the respective security issues are displayed.
   The *Issues* bar across the top displays the number of active security issues and the number of active security issues that are rated critical, high, medium, and low security risk.
   For each report, the number of affected assets is also displayed.



2. In the *Issues* section, click the number under *Critical*, *High*, *Medium*, or *Low*. The corresponding filter is selected and only those reports are displayed.
3. For each report, click the *i* icon to display a description of the issue and suggested remediation steps.



4. Click the title of a report to display details about affected assets.



5. Click gear icon next to Port to view *Service Discovery* information.
6. Click the *Back* button.

Filtering security issues

By default, the *Attack Surface Management* > *Asset Discovery* page displays all potential security issues, starting with critical security issues. You can use filters to display specific types of issues.

To filter security issues:

1. Go to *Attack Surface Management* > *Security Issues*. Choose *IASM* using toggle, the respective security issues are displayed.
2. Filter by Asset. You can search for specific security issues using the *By Asset* field. Enter IP address information, such as 192.168.10.10 or 192.168.12.0/24.
3. Add advanced search features:
   a. Click the filter icon. The advanced search fields are displayed.
   b. Select the *Search Type*.
   c. Click *Search*.
4. Select one or more filters, and click *Search*:

Filter	Options
Status	Select one of the following statuses: • Active • Resolved • Risk accepted • False positive
Severity	Select one or more of the following severity statuses: • Critical • High • Medium • Low

Filter	Options
Category	Select one or more of the categories. The list of categories changes based on the displayed security issues.
Country	Select one or more countries.

The list of filtered security issues is displayed.

5. (Optional) In the *Filters* list, toggle on *False Positive*. The list displays only issues marked with a status of *False Positive*.
6. In the *Filters* list, click *Clear* to remove all filters.

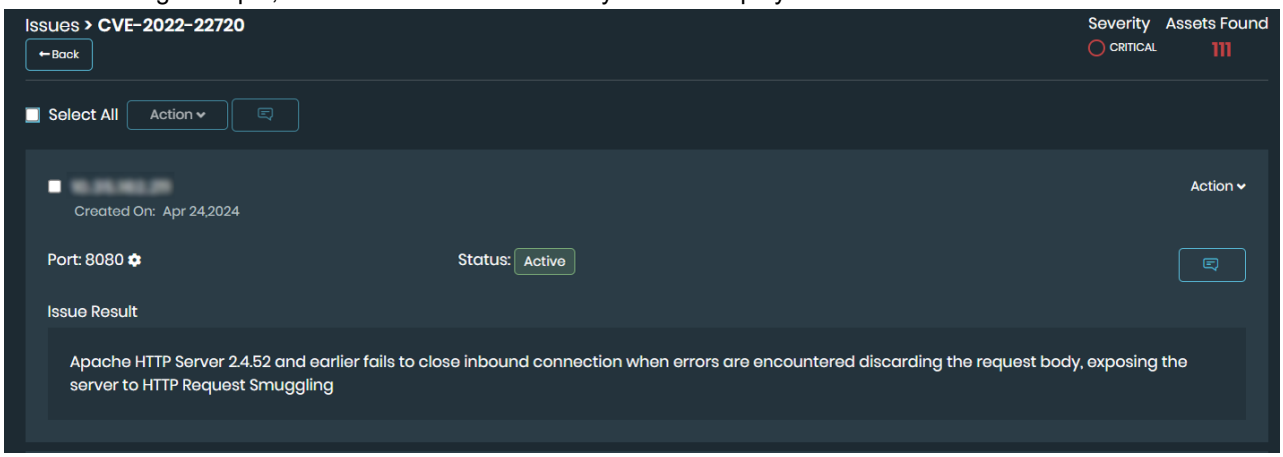
Changing the status of security issues

As you review and address security issues reported by FortiRecon, you can change the status of each issue to reflect your understanding and actions:

Mark as Active	Available only after you change the status of a security issue from active to another status. Select to move an issue back to the active status.
Mark as Resolved	Select to indicate actions taken at your organization have resolved the security issue.
Risk Accepted	Select to indicate actions taken at your organization have not fully resolved the security issue, but the current level of risk is acceptable.
False Positive	Select to indicate that the security issue is not an issue for your organization. The issue is considered a *False Positive* issue.

To change the status of security issues:

1. Go to *Attack Surface Management* > *Security Issues*. The discovered assets are displayed.
2. If necessary, select one or more filters, and click *Search*.
   The list of filtered security issues is displayed.
3. Click an issue title to display its details.
   In the following example, the *CVE-2022-22720* security issue is displayed:



4. Click *Edit* in the top-right corner to change the status by selecting one of the following options:
   - Mark as Resolved
   - Risk Accepted
   - False Positive
5. Click *Back* to display the list of issues again.

Adding a comment to a security issue

When editing a security issue on *Attack Surface Management* > *Security Issues*, you can leave a comment to describe the changes and why they were made.

Selecting the comment button will open all comments for that issue. This allows you to review all changes and discussions related to the issue.

To add a comment to a security issue:

1. Go to *Attack Surface Management* > *Security Issues*.
2. Select a type of security issue.
3. Locate the issue you would like to make a change to.
4. Click the comment button. A list of previous comments and a text box is displayed.
5. Enter a comment related to the status change.
6. Click *Add*.

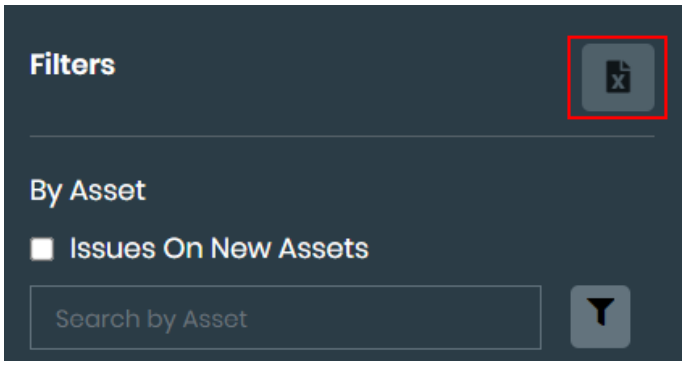
Exporting security issues

You can export a list of security issues into an Excel file. The spreadsheet will include the information on:

- Issue Category
- Issue Name
- Severity
- Asset
- Port
- Issue Status
- Tags
- Groups
- Last Refreshed On
- Additional Details
- Recommendations

To export the security issues:

1. Go to *Attack Surface Management* > *Security Issues*. Select *IASM* using the toggle.
2. Optionally, apply filters to export specific security issues. See Filtering security issues.
3. Click *Download* icon. The file is downloaded to your computer.



Asset Discovery

The *Attack Surface Management* > *Asset Discovery* page provides a summary of all discovered assets and details about each asset. From the *Asset Discovery* page, you can:

- View a summary about and details of your assets. See Viewing asset details.

Viewing asset details

The *Attack Surface Management* > *Asset Discovery* page displays the number of assets in an *Overview* section and in an *Assets Discovered* list.

You can view details about an asset by clicking a number in the *Overview* section or a category in the *Assets Discovered* list.

To view asset details:

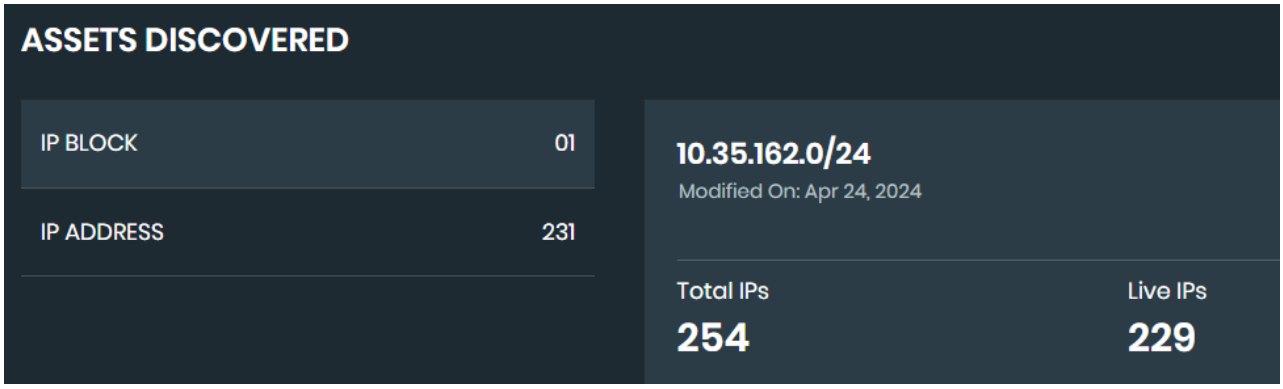
1. Go to *Attack Surface Management* > *Asset Discovery*.
2. Choose *IASM* using toggle. The number of discovered assets display in an *Overview* section across the top and in an *Assets Discovered* list on the left side of the page.

3. The following information is available:

Total Assets	The number of total assets discovered.
IP blocks	The number of IP blocks discovered.
IP address	The number of IP addresses that are linked to the IP blocks.

4. In the *Overview* bar, click a number, or in the *Assets Discovered* list, click an asset category. Details about the selected item are displayed on the right side of the page.

For example, click *IP Block*. On the right side of the page, the IP blocks discovered are displayed.



Asset Management

The *Attack Surface Management* > *Asset Management* page allows you to create and manage asset tags and groups, and configure your IASM settings. From the *Asset Management* page, you can:

- Create and manage tags and rules. See Tag Managment.
- Create and manage groups. See Group Management
- Limit access to specific assets and security issues using groups and tags. See Limiting access to assets and issues on page 89.
- Configure IASM settings. See IASM Configuration.

Tags and groups are integrated throughout the *Attack Surface Management* pages. You can filter by tags in the *Asset Discovery* and *Security Issues* pages; see Viewing asset details on page 59. Groups can be filtered in all *Attack Surface Management* pages.

Tag Managment

The *Tag Managment* page allows you to create, modify, and manage tags and rules.

- Create a new asset tag. See Creating a tag on page 79.
- Assign individual and bulk assets to an asset tag. See Adding assets to a tag on page 80.
- Manage, edit, and delete asset tags. See Managing tags on page 82.
- Create a new tagging rule. See Creating a tagging rule.
- View, clone, edit and delete rules. See Managing rules.

Creating a tag

Asset tags can be used to mark specific assets for focused filtering in the *Security Issues* and *Asset Discovery* pages. When creating a tag, a tag color is selected so that assets can be differentiated by tag. Tags must be configured in the *Tag Management* > *Tags* tab before assets can be assigned.

Some tags are automatically generated and cannot be edited or deleted.

To create a tag:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Tag Management* tab.
3. Click *+Add* and select *Create Tags*. The *Create Tag* dialog is displayed.
4. Enter a *Tag Name*.
5. Enter a *Tag Description*.
6. Select the *Theme Color* icon to assign the tag color.
7. Click *Submit*. The new tag is added to the *Tag Management* > *Tags* tab.

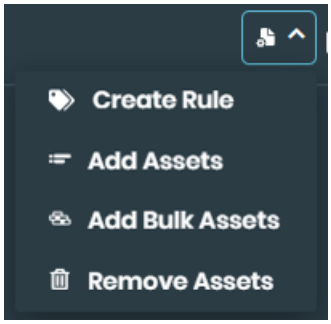
Adding assets to a tag

You can add individual or bulk assets to a tag from the *Tag Management* > *Tags* tab. You can also add assets to tags by creating tagging rules.

- Assets must be included in *Attack Surface Management* > *Asset Discovery* before they can be tagged. See Adding assets manually on page 62.
- Tags can also be assigned to assets in *Attack Surface Management* > *Asset Discovery*. See Assigning tags on page 63.

To create a tagging rule

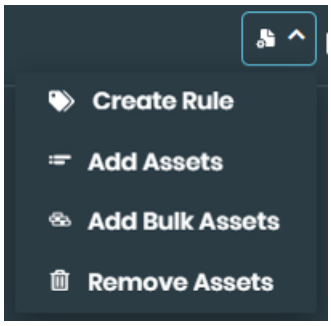
1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Tag Management* > *Tags* tab.
3. For a single tag, locate the tag you want to create tagging rule and click *Settings* icon. A dropdown menu is displayed. Click *Create Rule*.



   For multiple tags, select the tags you want to create tagging rule for and click *+Add* > *Create Rules*.
4. Enter the required information and click *Save*. See Creating a tagging rule.

To add assets to a tag:

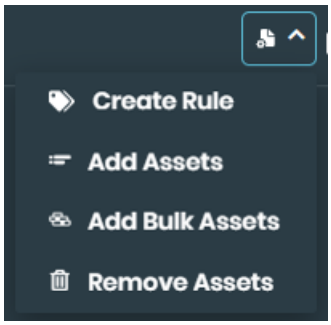
1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Tag Management* > *Tags* tab.
3. Locate the tag you want to add assets to and click *Settings* icon. A dropdown menu is displayed.



4. Select *Add Assets*.
5. Select the assets to add from the *Validated Assets list*.
6. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
7. Click the right arrow. The selected assets will be moved into the tag field.
8. Click *Save*.

To add bulk assets to a tag:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Tag Management* > *Tags* tab.
3. Locate the tag you want to add assets to and click *Settings* icon. A dropdown menu is displayed.



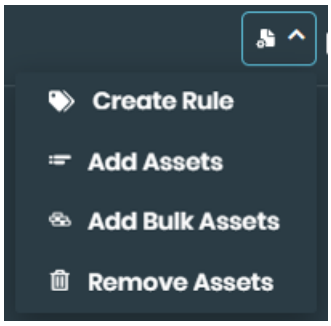
4. Select *Add Bulk Assets*.
5. Enter the asset information in the left field.
6. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
7. Click *Validate*. Once validated, assets are displayed in the right field. Any assets that failed validation are listed.
8. Click *Save*.

Managing tags

Asset tags can be managed from the *Tag Management* > *Tags* tab. You can remove assets from a tag, edit a tag, or delete a tag.

To remove an asset from a tag:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Tag Management* > *Tags* tab.
3. Locate the tag you want to remove assets from and click *Settings* icon. A dropdown menu is displayed.



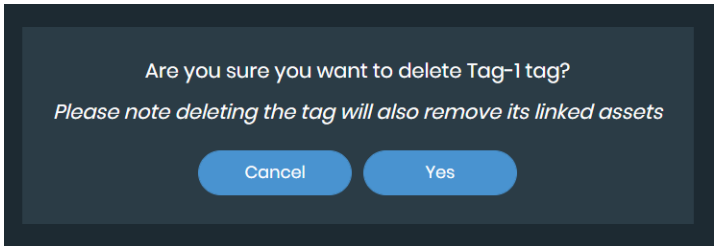
4. Select *Remove Assets*.
5. Select the assets you want to remove or click *Select All*.
6. Click *Remove Selected*.

To edit a tag:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Tag Management* > *Tags* tab.
3. Locate the tag you want to edit and click the *Edit* icon.
4. Edit the fields.
5. Click *Submit*.

To delete a tag:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Tag Management* > *Tags* tab.
3. Locate the tag you want to delete and click the *Delete* icon. A confirmation message is displayed.



4. Click *Yes*.

Creating a tagging rule

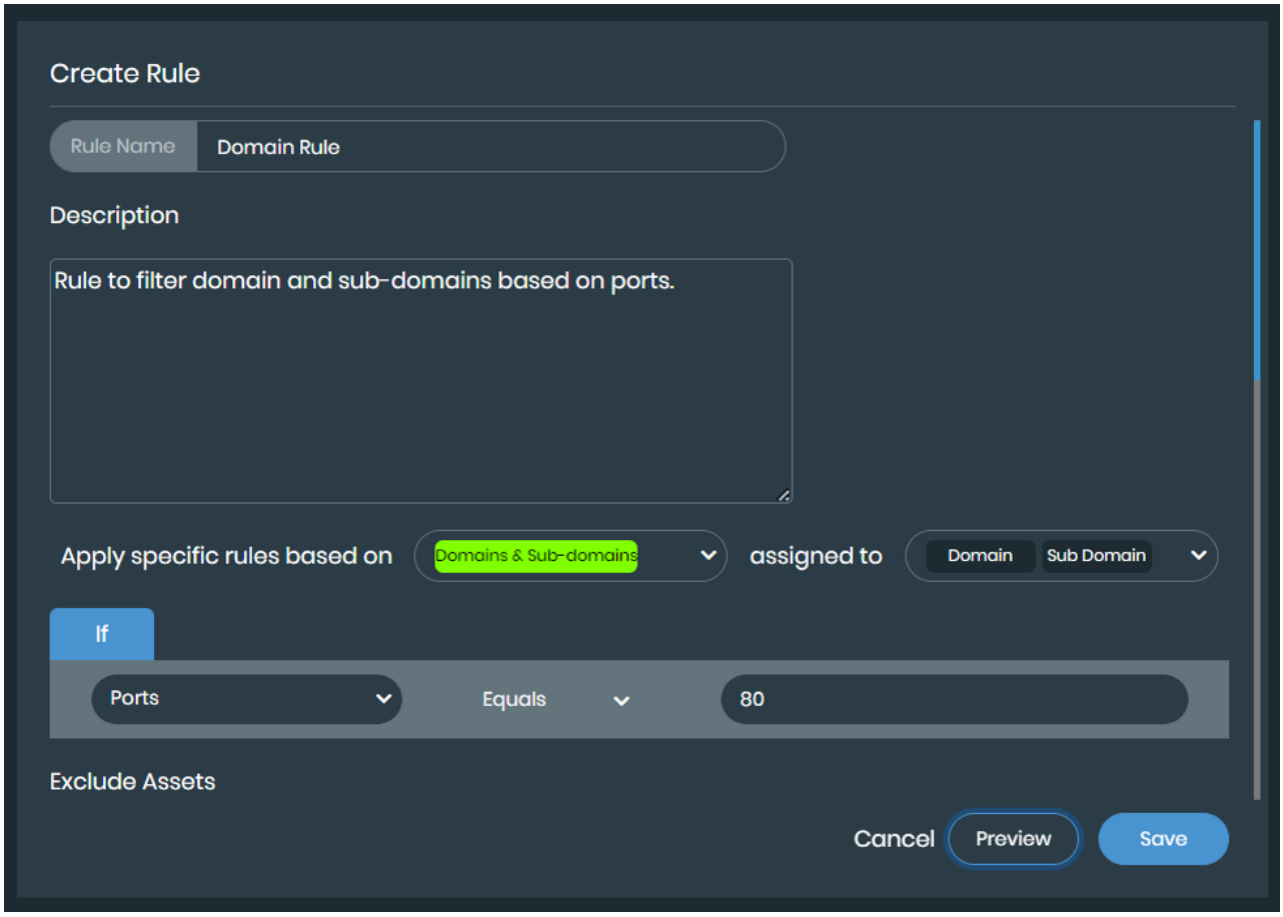
Rule-based tagging allows you to automatically assign tags to assets that meet user-defined conditions. This helps categorize and organize assets enhancing searchability and filtering.

Ensure tags exist before creating tagging rules. See Creating a tag.

To create a tagging rule:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Tag Management* tab.
3. Click *+Add* and select *Create Rules*. The *Create Rule* dialog is displayed.
4. Enter a *Rule Name*.
5. (Optional) Enter a *Description*.
6. Select *Tags* and *Asset type*.
7. Define your rule using supported conditions.
8. (Optional) Specify the assets to exclude from the rule.
9. Click *Preview* to see a sample of assets the rule would affect displayed in the *Assets Tagged* section.

10. Click *Save*. The new rule is added to the *Tag Management* > *Rules* tab.



- For domains, the tag will be applied to the domain, its associated sub-domains, and its IP addresses.
- For IP prefixes, the tag will be applied to all IP addresses within the specified prefix.
- For ASNs, the tag will be applied to the ASN's associated IP prefixes and their corresponding IP addresses.

Supported asset types and conditions

The following table details the supported asset types and conditions for rule-based tagging.

Asset Type	Conditions
Domain	• Port (Equals) • Asset Name (Starts with, Ends with, Wildcard) • Technologies (Equals) • Services (Equals) • Parent Asset (Equals)
Sub-domain	• Port (Equals)

Asset Type	Conditions
	• Asset Name (Starts with, Ends with, Wildcard) • Technologies (Equals) • Services (Equals) • Parent Asset (Equals)
IP Address	• Port (Equals) • Asset Name (Starts with, Ends with, Wildcard) • Services (Equals) • Parent Asset (Equals) • Countries (Equals) • IP Range (between) • Part of Prefix (Equals)
IP Prefix	• Asset Name (Starts with, Ends with, Wildcard) • Parent Asset (Equals)
ASN	• Asset Name (Starts with, Ends with, Wildcard) • Parent Asset (Equals)

Managing rules

Tagging rules can be managed from the *Tag Management* > *Rules* tab. You can view, clone, edit, or delete a rule.

To view a rule:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Tag Management* > *Rules* tab.
3. Locate the rule you want to view. Click *View* icon in Actions column.

To clone a rule:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Tag Management* > *Rules* tab.
3. Locate the rule you want to clone and click the *Clone* icon.
4. Enter a name and description.
5. Click *Submit*.

To edit a rule:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Tag Management* > *Rules* tab.

3. Locate the rule you want to edit and click the *Edit* icon.
4. Enter
5. Click *Submit*.

To delete a rule:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Tag Management* > *Rules* tab.
3. Locate the rule you want to delete and click the *Delete* icon. A confirmation message is displayed.
4. Click *Yes*.

Group Management

The *Group Managment* page allows you to create, modify, and manage groups.

- Create a new asset group. See Creating a group on page 86.
- Assign individual and bulk assets to an asset group. See Adding assets to a group on page 87.
- Manage, edit, and delete asset groups. See Managing groups on page 87.
- Filter *Attack Surface Management* pages by group. See Filtering by group on page 88.

Creating a group

Asset groups can be used to consolidate related assets. Groups can be viewed in the *Dashboard*, *Asset Discovery*, and *Security Issues* pages. An asset group must be created in the *Group Management* tab before assets can be assigned.

Assets can also be grouped based on subsidiary hierarchy. This allows for separate reporting and delegation of remediation responsibilities.

To create a group:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Group Management* tab.
3. Click *Create*. The *Create Group* dialog is displayed.
4. Enter a *Group Name*.
5. Enter a *Group Description*.
6. Click *Submit*. The new group is added to the *Group Management* tab.

Once a group has been created, you can assign assets to the group. See Adding assets to a group on page 87.

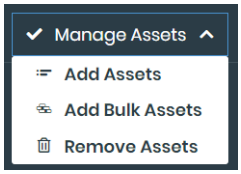
Adding assets to a group

You can add individual or bulk assets to a group from the *Group Management* tab.

Assets must be included in *Asset Discovery* before they can be tagged. See Adding assets manually on page 62.

To add assets to a group:

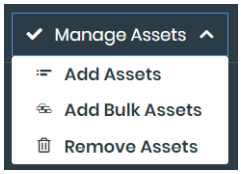
1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Group Management* tab.
3. Locate the group you want to add assets to and click *Manage Assets*. A dropdown menu is displayed.



4. Select *Add Assets*.
5. Select the assets to add from the *Validated Assets list*.
6. Click the right arrow. The selected assets will be moved into the tag field.
7. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
8. Click *Save*.

To add bulk assets to a group:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Group Management* tab.
3. Locate the group you want to add assets to and click *Manage Assets*. A dropdown menu is displayed.



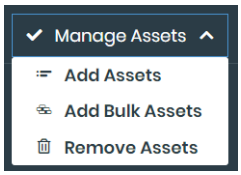
4. Select *Add Bulk Assets*.
5. Enter the asset information in the left field.
6. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
7. Click *Validate*. Once validated, assets are displayed in the right field. Any assets that failed validation are listed.
8. Click *Save*.

Managing groups

Asset tags can be managed from the *Group Management* tab. You can remove assets from a group, edit a group, or delete a group.

To remove an asset from a group:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Group Management* tab.
3. Locate the group you want to remove assets from and click *Manage Assets*. A dropdown menu is displayed.



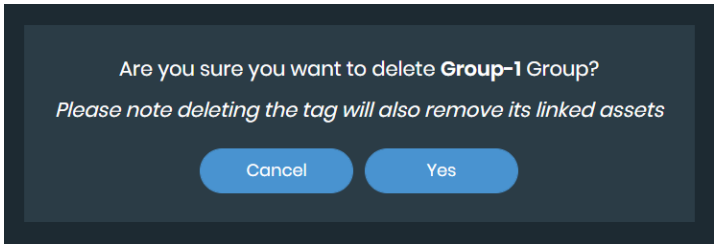
4. Select *Remove Assets*.
5. Select the assets you want to remove or click *Select All*.
6. Click *Remove Selected*.

To edit a group:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Group Management* tab.
3. Locate the group you want to edit and click the *Edit* icon.
4. Edit the fields.
5. Select *Assign Group To All Users* to make the assets visible to all users. See Limiting access to assets and issues on page 89.
6. Click *Submit*.

To delete a group:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Group Management* tab.
3. Locate the group you want to delete and click the *Delete* icon. A confirmation message is displayed.



4. Click *Yes*.

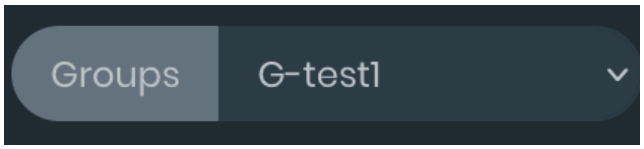
Filtering by group

Once a group has been created, you can filter by group in the *Attack Surface Management* > *Security Issues* and *Attack Surface Management* > *Asset Discovery* pages using the *Groups* dropdown menu. The Groups filter will be set to all assets of the organization by default.

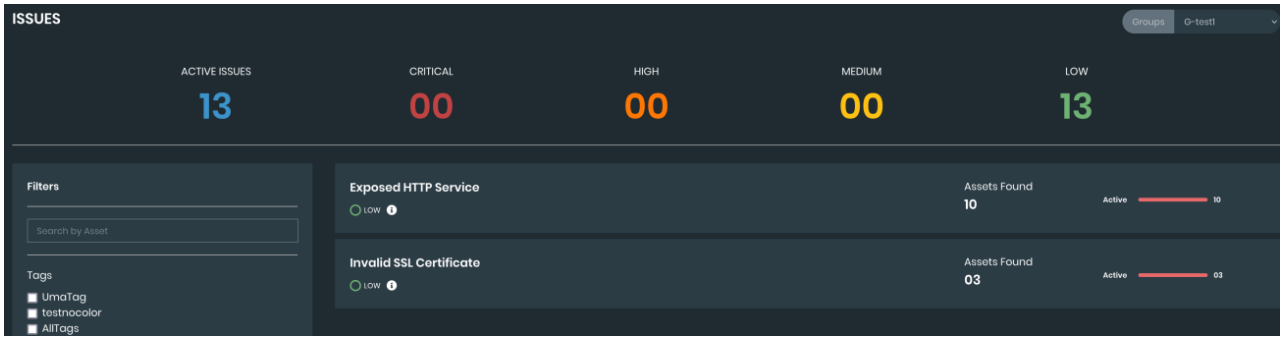
The following example demonstrates filtering by group in the *Attack Surface Management* > *Security Issues* page.

To filter by group:

1. Go to *Attack Surface Management* > *Security Issues*.
2. Click the *Groups* dropdown menu.



3. Select the group you want to filter by. The page will displayed information related to the selected group.



Limiting access to assets and issues

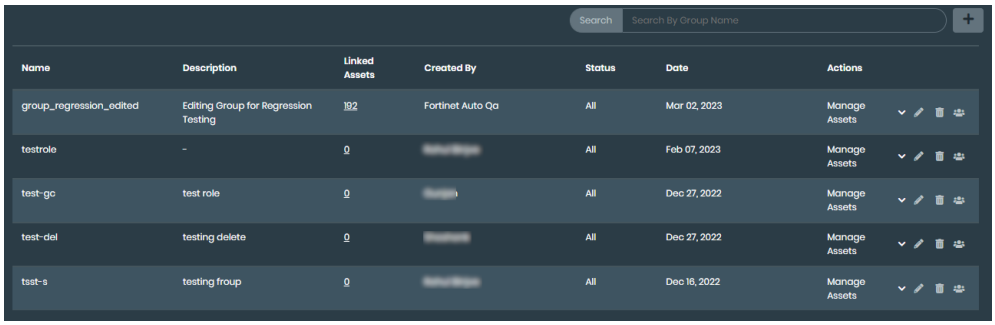
User access to specific assets and security issues can be limited through the use of groups and tags. User asset and security issue visibility is limited to the groups they are assigned to and any tags associated with these group assets.

The following table presents examples of visible and hidden assets based on the groups that a user is assigned to:

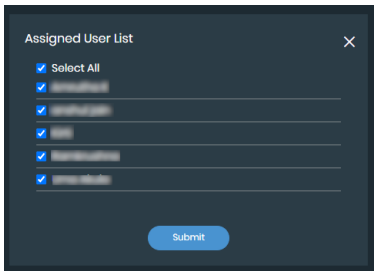
User assigned to	Visible assets	Hidden assets
A single group with no tags assigned	• All assets that have been added to the group	• Assets that have not been added to the group
A single group with tags assigned to the assets	• Assets that have been added to the group that also have the tags assigned	• Assets that have not been added to the group • Any assets included in the assigned group that do not have the tags assigned
Multiple groups with no tags assigned	• All assets that have been added to any of the assigned groups	• Assets that have not been added to any of the groups
Multiple groups with tags assigned to the assets	• Assets that have been added to any of the assigned groups that also have the tags assigned	• Assets that have not been added to any of the groups • Any assets included in the assigned groups that do not have the tags assigned

To assign users to a group:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select the *Group Management* tab.



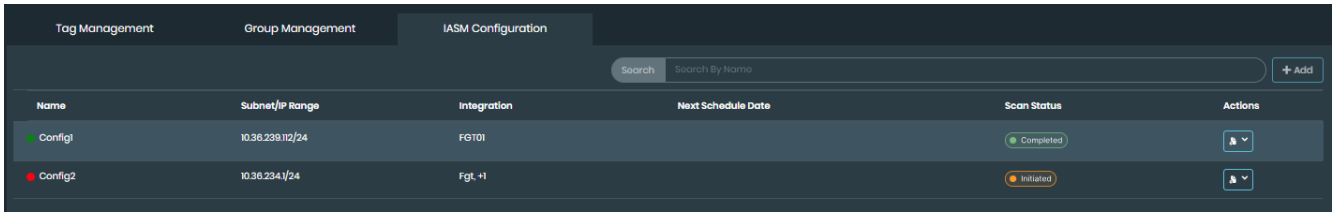
3. Select *Assign User*. The *Assigned User List* dialog is displayed.



4. Select the users you want to assign:
   - Select specific users to assign to the group.
   - Select *Select All* to make the group assets and security issues visible to all users.
5. Click *Submit*.

IASM Configuration

The *Asset Management* > *IASM Configuration* page allows you to configure and manage your IASM scan settings. You can create new scan configurations, monitor the status of IASM Agent, and download the necessary configuration files for agent deployment.



The following information is displayed for existing IASM configurations.

- *IASM Agent Status*: A green indicator signifies a connected IASM agent; red indicates a disconnected agent.
- *Name*: The identifying name assigned to the configuration.
- *Subnet/IP Range*: The subnet(s) specified in the scan configuration.

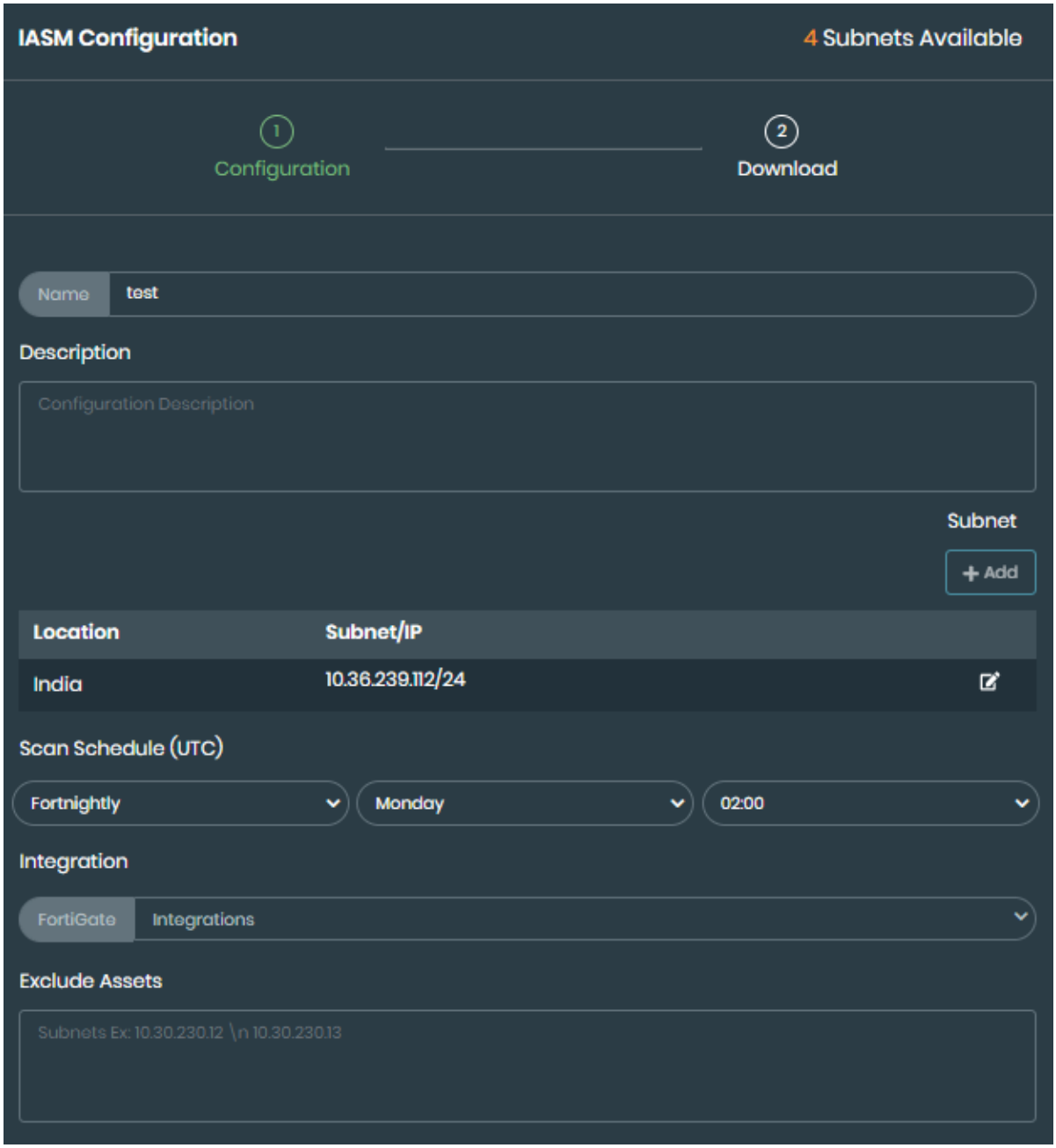
You can configure up to 100 subnets per IASM agent.

- *Next Scheduled Date*: The date and time (in UTC) of the next scheduled scan.
- *Scan Status*: Shows the current status of the scan (Initiated, Scanning, Failed, Completed).
- *Actions*: Options to edit the configuration or download the associated .yml file.

To add a new configuration:

1. Navigate *Attack Surface Management* > *Asset Management* > *IASM Configuration*.
2. Click *+Add*.
3. Provide a name and description.
4. Click *+Add* under the subnets section and enter the following information.
   a. *Location*: Select the country from the dropdown.
   b. *Subnets*: Enter the subnet in CIDR notation or specify an IP range.
   c. Click *Save*.
5. Schedule your scans to run weekly or fortnightly, select the desired days of the week, and specify the start time in UTC.
6. (Optional) Select FortiGate integration. You can integrate FortiGate with IASM to discover the attack surface of the devices managed by FortiGate.
7. (Optional) In *Exclude Assets* section, enter IP addresses of any assets to be excluded from the scan.
8. Review the details and click *Next*.
9. Click *Download* to download the configuration file (.yml) or *Copy* to copy the file. The downloaded .yml file is required to deploy the IASM agent within your internal network. See IASM Agent.

10. Click *Save*.



To edit an existing configuration:

1. Navigate *Attack Surface Management* > *Asset Management* > *IASM Configuration*.
2. Click *Actions* icon next to the configuration you want to modify and click *Edit*.
3. Update the details and click *Update*.

Leaked Credentials

The FortiRecon team continually monitors for credential leaks and provides alerts to you through the FortiRecon portal. If any leaked or breached credentials that involve email addresses of the organizations or the users of their systems are detected, the FortiRecon portal automatically displays the information.

As part of consolidated collection, the leaked credentials are gathered from multiple sources:

- Publicly leaked or breached databases
- Privately shared databases
- Paste sites
- Malware infections

Leaked credentials are the primary source of *Password Re-Use Attacks*. It is important for any organization to quickly neutralize leaked credentials.

On the *Attack Surface Management* > *Leaked Credentials* page, you can:

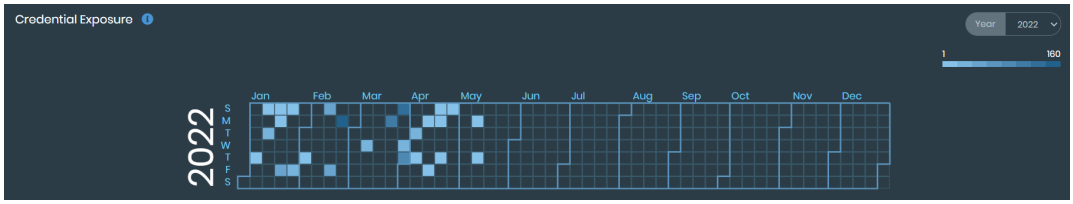
- View leaked credentials by year. See Viewing leaked credentials by year on page 93.
- View breached datasets. See Viewing breached datasets on page 94.
- View leaked credential details. See Viewing leaked credential details on page 93.
- Export a list of leaked accounts. See Exporting leaked accounts on page 95.

Viewing leaked credentials by year

The *Attack Surface Management* > *Leaked Credentials* page provides a calendar year of all breaches. You can change the year to view previous year data.

To view leaked credentials by year:

1. Go to *Attack Surface Management* > *Leaked Credentials*. The *Credential Exposure* year is displayed. Colored blocks indicate a breach. Light colored blocks indicate few affected credentials, and dark colored blocks indicate many affected credentials.



2. Hover over the block to display details about the breach.
3. From the *Year* menu, select a different year. The calendar changes to the selected year.
4. Click a color block to display details on the *Leaked Credentials* page. See Viewing leaked credential details on page 93.

Viewing leaked credential details

On the *Attack Surface Management* > *Leaked Credentials* page, click the *Leaked Credentials* tab to view the results.

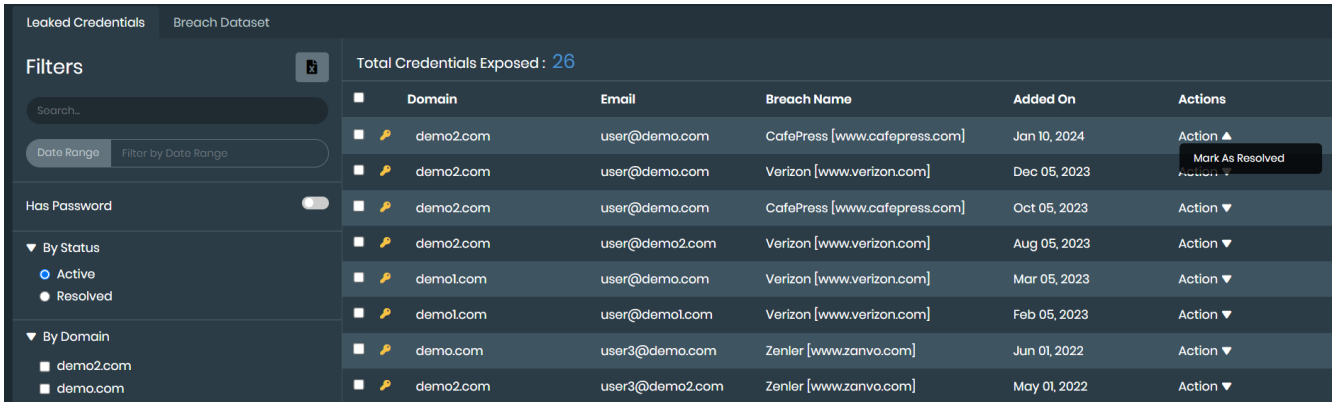
You can filter the list of leaked credentials by date and domain, and you can search for keywords.

To view leaked credential details:

1. Go to *Attack Surface Management* > *Leaked Credentials*, and click *Leaked Credentials*.
2. Apply the filters that you want.
3. Click a domain name to display more details.
4. Change the status of a report by selecting *Mark as Resolved* or *Mark as Active* in the *Actions* dropdown.

To filter leaked credentials details:

1. Go to *Attack Surface Management* > *Leaked Credentials*.
2. On *Leaked Credentials* tab, filter reports by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range. Only reports from the date range are displayed.
   d. Click the *Filter Report by Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
   b. The threats are filtered to display only threats with the keyword.
   c. Click the *X* beside the keyword to remove the filter.
4. Toggle *Has Password* option to filter reports that contain passwords.
5. Filter by status in the *By Status* section:
   - Select *Active* or *Resolved* to filter threats by their assigned status.
6. Filter by domain in the *By Domains* section.



Viewing breached datasets

On the *Attack Surface Management*> *Leaked Credentials* page, you can click the *Breach Dataset* tab to view results displayed on the following tabs:

- The *Relevant* tab displays breach information that contains email addresses related to your organization's domains.
- The *Other* tab displays all breach information indexed in FortiRecon's database, including breach information related to third-parties that does not contain email addresses related to your organization's domains.

You can filter the list of breached datasets by date, and you can search for keywords.

To view breached datasets:

1. Go to *Attack Surface Management* > *Leaked Credentials*. Select *Breached Dataset* tab. The following columns of information are available:

Breach Name	Displays the name of the breach.
Breach Date	Displays the date that the breach occurred.
Added On	Displays the date that the information was made available to other malicious actors.
Compromised Accounts	Displays the number of known compromised accounts.

2. Apply the filters that you want.
3. Click a breach to display more information about it.

To filter breached datasets:

1. Go to *Attack Surface Management* > *Leaked Credentials*, and click *Breached Dataset*.
2. Filter reports by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range. Only reports from the date range are displayed.
   d. Click the *Filter Report by Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
   b. The threats are filtered to display only threats with the keyword.
   c. Click the *X* beside the keyword to remove the filter.
4. Toggle *Has Password* option to filter reports that contain passwords.
5. Filter the reports by relevance in *By Relevance* section.

Exporting leaked accounts

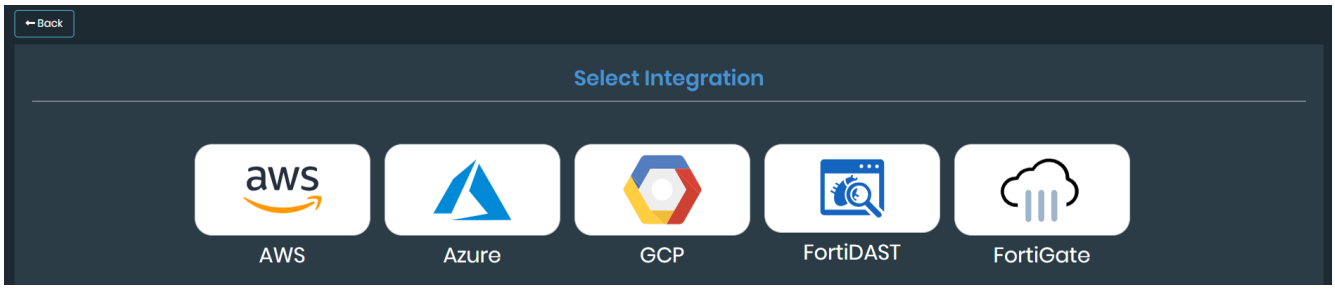
You can export a list of leaked accounts to Microsoft Excel format.

To export leaked accounts:

1. Go to *Attack Surface Management* > *Leaked Credentials*.
2. Select *Leaked Credentials* or *Breach Dataset* tab.
3. Click *Download* icon in the filters section. The file is downloaded to your computer.

Integrations

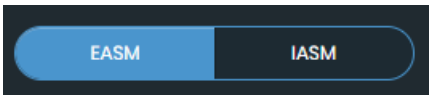
You can enable read only access to your environments and discover their cloud assets. Once assets are discovered, they are added to the *Attack Surface Management* > *Asset Discovery* and *Security Issues* pages. Click the *i* on the *Integrations* page for more information.



On the *Attack Surface Management> Integrations* page, you can:

- Add new integrations for AWS, Azure, Google Cloud Platform, FortiDAST, and FortiGate. See Adding integrations on page 96.
- Edit and delete existing integrations. See Editing integrations on page 99.

The *EASM/IASM* toggle is located at the top of the *Integrations* page. This toggle allows you to filter between EASM and IASM integrations.



Adding integrations

The *Attack Surface Management* > *Integrations* page displays all existing integrations. You can manually add new integrations as needed.

- AWS
- Azure
- Google Cloud Platform
- FortiDAST
- FortiGate

IASM only supports FortiGate integration.

To add a new AWS integration:

1. Go to *Attack Surface Management* > *Integrations*.
2. Click the + icon.
3. Select *AWS*. The *Add AWS* page is displayed.

For more information on creating an AWS IAM policy and role, click *Need Help?*.

4. Select *EASM*.
5. Enter the account ID number in the *Account ID* field.
6. Enter a descriptive name in the *Integration Name* field.
7. Click *Save*.

To add a new Azure integration:

1. Go to *Attack Surface Management* > *Integrations*.
2. Click the + icon.
3. Select *Azure*. The *Add Azure* page is displayed.
4. Select *EASM*.
5. Enter the relevant values in the *Subscription ID*, *Client ID*, *Tenant ID*, and *Client Secret* fields.

These four values are necessary to create read-only access for your Azure cloud account. For information on generating these values, click *Need Help?*.

6. Enter a descriptive name in the *Integration Name* field.
7. Click *Save*.

To add a new Google Cloud Platform integration:

1. Go to *Attack Surface Management* > *Integrations*.
2. Click the + icon.
3. Select *GCP*. The *Add GCP* page is displayed.
4. Select *EASM*.
5. Enter a descriptive name in the *Integration Name* field.

6. Enter the *JSON* information from the GCP configuration file.

For information on generating the GCP key file and downloading JSON, click *Need Help?*.

7. Click *Validate*.

To add a new FortiDAST integration:

1. Go to *Attack Surface Management* > *Integrations*.
2. Click the + icon.
3. Select *FortiDAST*. The *Add FortiDAST* page is displayed.
4. Select *EASM*.
5. Enter the master email address in the *Email* field.
6. Enter the *API Key* from FortiDAST.
7. Click *Save* to verify the key.

Once the FortiDAST integration is verified, you can scan assets in the *EASM* > *Asset Discovery* page. See Performing a FortiDAST scan.

FortiGate Integration

Integrating FortiGate with FortiRecon enhances the asset discovery capabilities of FortiRecon EASM. It does this by adding FortiGate Interface IPs and all IPs behind NAT to the *Attack Surface Management* > *Asset Discovery* page. Once the integration is verified, all assets discovered via FortiGate will have additional metadata, including:

- Name of Virtual IP on FortiGate
- Mapped Internal IP
- MAC address of Internal IP
- Mapped External Port
- Mapped Internal Port
- Operating System

You can use this metadata to take action faster on security vulnerabilities and threats.

To add a new FortiGate integration:

1. Go to *Attack Surface Management* > *Integrations*.
2. Click the + icon.
3. Select *EASM* or *IASM* using toggle.
4. Select *FortiGate*. The *Add FortiGate* page is displayed.
5. Enter a name for the integration.
6. Enter FortiGate IP address in the *Host* field.
7. Enter the *Port* number.
8. Enter the FortiGate access *Token*.

For information on creating token, click *Need Help?*

9. Select *Use HTTPs* checkbox if required.
10. Click *Save*.

Editing integrations

You can edit and delete existing integrations from the *EASM* > *Integrations* page.

To edit an integration:

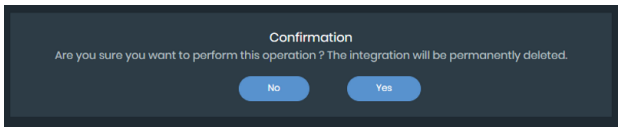
1. Go to *EASM* > *Integrations*.
2. Click *Edit*. The integration details are displayed.
3. Edit the fields you want to change.

You cannot edit the *External ID* field for an AWS integration. You cannot edit the *Account ID*, *Subscription ID*, or *Tenant ID* for an Azure integration.

4. Click *Save*.

To delete an integration:

1. Go to *EASM* > *Integrations*.
2. Click *Delete*. The *Confirmation* message is displayed.



3. Select *Yes*.

Brand Protection

The Brand Protection (BP) module uses proprietary algorithms to detect common techniques used by cyber threat actors, such as web-based phishing attacks, typo-squatting, defacements, rogue apps, credential leaks, and brand impersonation in social media. You can use the Brand Protection module to detect activity early and take action, such as web site or application takedown, to protect your brand value, trust, integrity, and reputation.

The *Brand Protection* module contains the following pages:

Dashboard	Displays a summary of typo-squatting domains, flash alerts and reports, rogue apps, phishing campaigns, and takedown requests. See Dashboard on page 101.
Domain Threats	Displays a list of typo-squatted domains and phishing URLs. You can initiate domain takedown or the suspension of monitoring. See Domain Threats on page 103.
Social Media Threats	Displays all discovered profiles that may be impersonating your organization's social media pages. You can filter profiles, initiate profile takedown, and export a Microsoft Excel file containing profile details. See Social Media Threats on page 108.
Rogue Mobile Apps	Displays all discovered apps that may be impersonating your organization's assets. You can filter apps, assign status, initiate app takedown, and export a Microsoft Excel file with app details. See Rogue Mobile Apps on page 117.
Executive Monitoring	Displays threats targeted at high-profile individuals of your organization. You can filter threats and add executive profiles for monitoring. See Executive Monitoring.
Code Repo Exposure	Displays a list of attributes exposed in code repositories. See Code Repo Exposure on page 125.
Open Bucket Exposure	Displays a list of files exposed in open buckets. See Open Bucket Exposure on page 128.
Take Down	Displays a list of takedown request tickets and their current status. See Take Down on page 130.

Brand Protection also includes *Logo Monitoring* feature which provides an additional method for identifying your brand on known phishing or malicious pages. This feature enhances the accuracy of identifying cases involving brand impersonation.

FortiRecon logo monitoring feature performs the following tasks:

- Analyzes all active typo-squatted domains to determine whether they host pages containing your organization's logo or logos that are resembling. When such domains are identified, a *Logo Detection* tag is assigned to the domain.
- Examines all domains and pages that are processed, which are obtained through phishing feeds to identify any instances where your organization might be impacted.
- Inspects all pages that are identified through the detection of the FortiRecon watermark.

Dashboard

The *Brand Protection* > *Dashboard* page provides information on threats to your organization's public facing assets, such as brand abuse, domain threats, and information exposure. From the *Brand Protection* > *Dashboard* page, you can:

- View a summary of domain threats to your organization. See Viewing the domain threat summary on page 101.
- View a summary of brand abuse, such as rogue apps or social media threats. See Viewing the brand abuse summary on page 101.
- View a summary of information exposure, including code and file exposure. See Viewing the information exposure summary on page 102.
- View trends and important alerts of threats to your brand. See Viewing the alert summary on page 102.
- View total credits used and available for domain takedown. See Viewing the takedown credit summary on page 103.

Viewing the domain threat summary

The *Dashboard* displays a summary of domain threats in the *Summary* widget.

To view the domain threat summary:

1. Go to *Brand Protection* > *Dashboard*.
2. Scroll to the *Summary* widget. *Total Threats* and the distribution of threat type is displayed.

3. Hover over the threat type distribution bar to see the number of threats for each type.

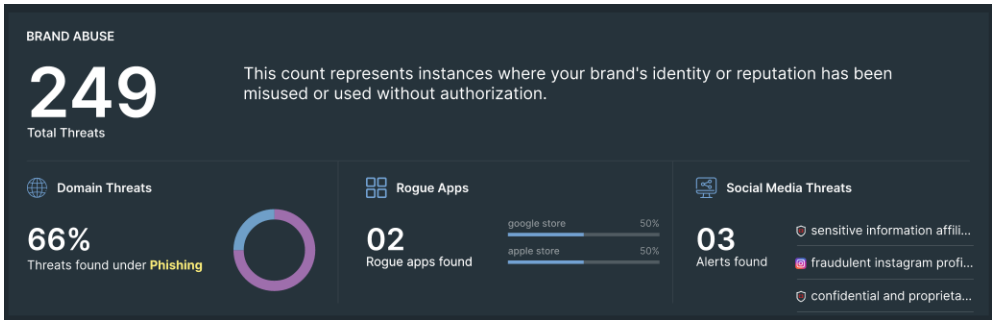
Viewing the brand abuse summary

The *Dashboard* displays information on domain phishing, rogue apps, and social media threats in the *Brand Abuse* widget.

To view the brand abuse summary:

1. Go to *Brand Protection* > *Dashboard*.
2. Scroll to the *Brand Abuse* widget. High level information on *Total Threats*, *Domain Threats*, *Rogue Apps*, and *Social*

Media Threats are displayed.



Viewing the information exposure summary

The *Dashboard* displays information on discovered, exposed information, such as code and file exposure in the *Information Exposure* widget.

To view the information exposure summary:

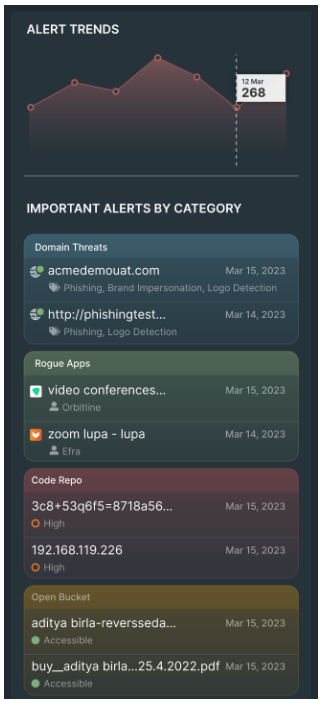
1. Go to *Brand Protection* > *Dashboard*.
2. Scroll to the *Information Exposure* widget. High level information about code and file exposure is displayed.

Viewing the alert summary

The *Dashboard* displays high level information on alerts in the *Alert Trends* widget.

To view the alert summary:

1. Go to *Brand Protection* > *Dashboard*.
2. Scroll to the *Alert Trends* widget. Trends are displayed in a graph and important alert highlights are organized by category.



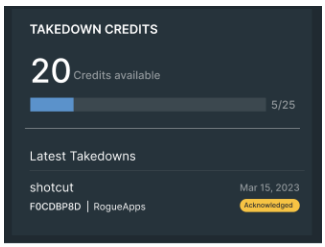
3. Hover over the graph for more information on daily alerts.

Viewing the takedown credit summary

The *Dashboard* displays information on available and used takedown credits and the most recent domain takedowns in the *Takedown Credits* widget.

To view the takedown credit summary:

1. Go to *Brand Protection* > *Dashboard*.
2. Scroll to the *Takedown Credits* widget. The number of used, total, and available credits is displayed.



Domain Threats

The *Domain Threats* page displays a list of domains impersonating your organization's domain, such as typo-squatted domains and phishing URLs.

From the *Brand Protection* > *Domain Threats* page, you can:

- Review discovered domain threats and high level threat information. See Reviewing domain threats on page 104.
- Take action against impersonating domains, such as requesting domain takedown. See Managing domain threats on page 105.
- Filter the list of domains. See Filtering domains on page 105.
- Create a digital watermark. See Digital watermark on page 106.
- Add a new domain or URL for monitoring or takedown. See Adding a new domain or URL.

Following are the techniques used to detect domains and URLs that either are impersonating your organization's brand or potentially may do so in the future.

- *Typo-squatting* - This is a technique where several combinations of keywords are generated that are lookalikes of your organization's own domain names. These are matched against newly observed domains, and any matching domains are kept under monitoring.
- *Digital Watermarking* -This technique involves generating an obfuscated JavaScript code that can be embedded into your organization's websites. This allows for rapid detection of phishing campaigns that copy web pages from official websites.
- *Phishing Feeds Integration* -This method involves matching reported and known phishing URLs against your organization's brand.
- *Brand impersonation* - This is a technique where it is determined if the detected domain or URL is hosting content that is maliciously impersonating your organization's brand. Although, it may not be explicitly hosting a phishing page.
- *Logo Detection* - This technique supplements the *Brand Impersonation* technique by identifying whether the captured domain or URL is hosting a web page that displays your organization's logo.
- *MX Record Detection* - MX records are used to specify which mail server is responsible for handling email for a particular domain. This technique is used to identify domains that, even if they are not hosting any malicious web content, may still be configured to send phishing emails.

Threat actors often use homoglyphs to create look-alike domain names. This means they replace a letter in the domain name with a similar-looking number or letter from other languages with characters that resemble English characters.

For example:

- fortìnet.com
- fortınet.com
- f0rtinet.com

In first two domain names, the ascii 'i' has been replaced with similar looking unicode letters from non-ascii scripts. In the third one, the 'o' has been replaced with ascii representation of 'zero'.

FortiRecon's typosquatting algorithm anticipates these possibilities. It generates both Unicode and Punycode combinations for your organization's original domains and hunts for any newly registered domains that match any of these combinations.

Reviewing domain threats

You can review information about domain threats in the *Brand Protection* > *Domain Threats* page. Information displayed about domain threats includes:

- Domain name and URL
- Registration date
- Threat type tags
- Threat status
- Original domain

To review exposed attributes:

1. Go to *Brand Protection* > *Domain Threats*.
2. Review the high level threat information:
   - Review the distribution of threat types and the total number of discovered threats in the *Summary*.
   - Review the distribution of threat statuses in *Domain Status*.
   - Review the number of takedown credits available in *Takedown Credits*.
3. Select a threat to review detailed threat information.

Managing domain threats

You can interact with discovered domain threats, such as marking the files as resolved or request domain takedown.

To manage a threat:

1. Go to *Brand Protection* > *Domain Threats*
2. Find the threat you want to manage.
3. Change the status:
   - Select *Action* > *Mark as Resolved* to indicate that the domain threat has been resolved.
   - Select *Action* > *Take Down* to initiate the domain takedown process.
   - Select *Action* > *Mark as Safelist* to add the domain to a safelist. FortiRecon will stop monitoring the safelisted domain.
   - Select *Action* > *Mark as False Positive* to mark the domain threat as a false alarm.
4. Click *Comment* to add a comment to the threat history.

Filtering domains

You can filter threats by date, status, threat type tags, or original domain.

To filter domain threats:

1. Go to *Brand Protection* > *Domain Threats*
2. Filter threats by a date range:
   a. Click *Filter By Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. Select a month, year, and day to specify the end date of the range.
   Only threats from the date range are displayed.
   d. Click the *Filter By Date Range* box, and click *X* to remove the date range filter.

3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
      The threats are filtered to display only threats with the keyword.
   b. Click the *X* beside the keyword to remove the filter.
4. Filter by action in the *By Action* section:
   - Select *Active*, *Resolved*, *Safelist*, or *Takedown* to filter threats by the actions performed.
5. Filter by status in the *By Status* section:
   - Select *Online*, *Offline*, or *Non Functional* to filter threats by their assigned status.
6. Select the threat type in the *By Tags* section.
7. Click *Search*. The files with the matching filters are displayed.

Digital watermark

FortiRecon uses digital watermarks on official login and sensitive pages to track cloning and re-hosting of the web pages as phishing sites on another IP address. A small script that helps the FortiRecon research team track the cloning or re-hosting of the site is provided for you to embed into your website. This process also helps you identify whether any of your customers have been victims of phishing on any cloned pages, and then take remedial actions.

Adding watermarks

You can create a digital watermark to be embedded into your website on the *Domain Threats* page. You can download the digital watermark in two formats:

- CDN Link: The JavaScript code is hosted on Fortinet's server, and you must embed the link into the index or login page of your web application using the `<script>` tag.
- JavaScript file: The code is hosted on your own server, and you must embed the file using the `<script>` tag, or paste the code into the index or login page of your web application.

To create a digital watermark:

1. Go to *Brand Protection* > *Phishing* and select *Digital Watermark*. A list of current watermarks are displayed.
2. Click *Add Watermark*. The *Code Preview* pane is displayed.

3. Enter a name for the watermark in the *Digital Watermark Name* text box.
4. Under *Select Domains*, select the domains you want to include. The *Generate* button is displayed.

5. Review the code in *Code Preview* and click *Generate*. The list of watermarks is displayed after the new watermark is generated.
6. Download the watermark:
   a. Click *Copy CDN Link* to copy the CDN Link to your computer's clipboard.
   b. Click *Download Digital Watermark* to download the JavaScript file to your computer.

   The digital watermark can be added to your website.

A maximum of 10 domains can be added to a digital watermark when choosing domains in *Select Domains*.

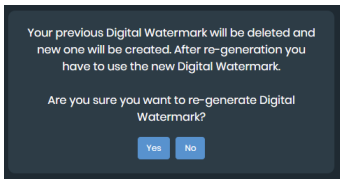
Editing watermarks

You can edit digital watermarks through the *Brand Protection* > *Phishing* page.

To edit a digital watermark:

1. Go to *Brand Protection* > *Domain Threats* and select *Digital Watermark*. A list of current watermarks is displayed.
2. Find the watermark you want to edit and select *View & Regenerate*. The *Code Preview* is displayed.

3. Make changes to *Digital Watermark Name* and *Select Domains* as needed.
   Review the changed code in *Code Preview* and select *Regenerate*. A confirmation message is displayed.



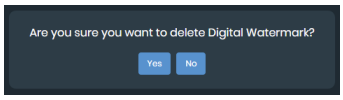
4. Click *Yes*.

Deleting watermarks

You can delete digital watermarks through the *Brand Protection* > *Phishing* page.

To delete a digital watermark:

1. Go to *Brand Protection* > *Domain Threats* and select *Digital Watermark*. A list of current watermarks is displayed.
2. Find the watermark you want to remove and click *Delete*. A confirmation message is displayed.



3. Click *Yes*.

Adding a new domain or URL

You can add a new domain or URL for monitoring or takedown.

To add a new domain:

1. Go to *Brand Protection* > *Domain Threats*.
2. Click *Add Domains*.
3. Click *Add* icon.
4. Select the *Original Domain* from the dropdown.
5. Enter the *Domain* information.
6. Click *Save*.

To add a new URL:

1. Go to *Brand Protection* > *Domain Threats*.
2. Click *Add Domains*.
3. Click *Add* icon.
4. Select *URL* tab.
5. Select the *Original Domain* from the dropdown.
6. Enter the *URL* information.
7. Click *Save*.

After you add a new domain or URL, the status field in the *Add Domains* page will indicate one of the following:

- **In Review**: The FortiRecon team is currently assessing the newly added asset.
- **Accepted**: The asset has been validated and approved.
- **Rejected**: The asset was deemed invalid. A comment will explain the reason for rejection.

Social Media Threats

The *Social Media Threats* page displays a list of profiles impersonating your organization's social media profiles. This feature is supported for **Twitter**, **LinkedIn**, **Facebook** and **Instagram** social media platforms.

From the *Brand Protection* > *Social Media Threats* page, you can:

- View the list of profiles that are social media threats. See Reviewing social media threats on page 109.
- Take action against impersonating profiles, such as requesting profile takedown. See Managing social media threats on page 110.
- Filter the list of profiles. See Filtering social media threats on page 110.
- Add official social media profiles. See Adding official profiles on page 110.
- Add a new social media profile for monitoring. See Adding a new social media profile.
- Export information on discovered profiles. See Exporting impersonating profiles.
- View archived alerts. See Alerts on page 112.

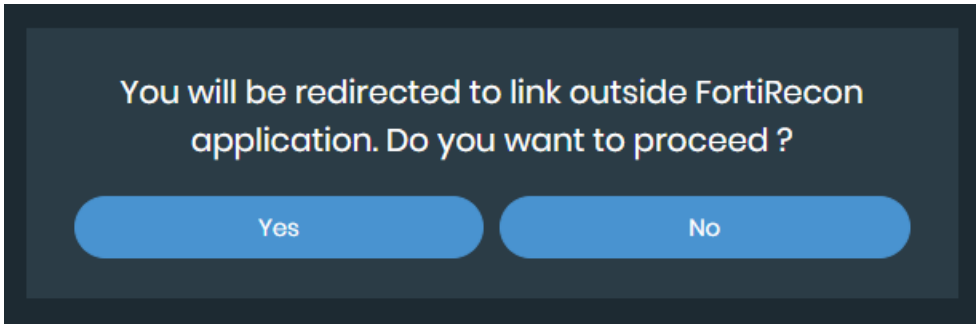
Reviewing social media threats

You can review information about social media threats in the *Brand Protection* > *Social Media Threats* page. Information displayed about social media threats includes:

- Profile name
- Handle name
- Location
- Friends count
- Followers count
- Posts count

To review social media threats:

1. Go to *Brand Protection* > *Social Media Threats*.
2. Review the high level threat information:
   - Review the distribution of profile types and the total number of discovered profiles in the *Alert Summary*.
   - Review the distribution of threat profiles based on the social media platforms in *Threats by Social Media*.
   - Review the number of takedown credits available in *Takedown Credits*.
3. Click  icon next to a discovered threat profile to open the profile in a new tab. A warning message is displayed.



4. Click *Yes*.

Managing social media threats

You can interact with discovered social media threats, such as marking the profile as false positive or request profile takedown.

To manage a threat:

1. Go to *Brand Protection* > *Social MediaThreats*
2. Find the threat you want to manage.
3. Change the status:
   - Select *Action* > *Mark as False Positive* to indicate that the social media threat has been falsely identified.
   - Select *Action* > *Take Down* to initiate the profile takedown process.
4. Click *Comment* to add a comment to the threat history.

Filtering social media threats

You can filter threats by date, status, threat type tags, or original domain.

To filter domain threats:

1. Go to *Brand Protection* > *Social Media Threats*
2. Filter threats by a date range:
   a. Click *Filter By Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. Select a month, year, and day to specify the end date of the range.
   Only threats from the date range are displayed.
   d. Click the *Filter By Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
   The threats are filtered to display only threats with the keyword.
   b. Click the *X* beside the keyword to remove the filter.
4. Filter by status in the *By Alert Status* section:
   - Select *Active*, *False Positive*, or *Active Takedown* to filter threats by their assigned status.
5. Select the social media platform in the *By Social Media* section.
6. Click *Search*. The profiles with the matching filters are displayed.

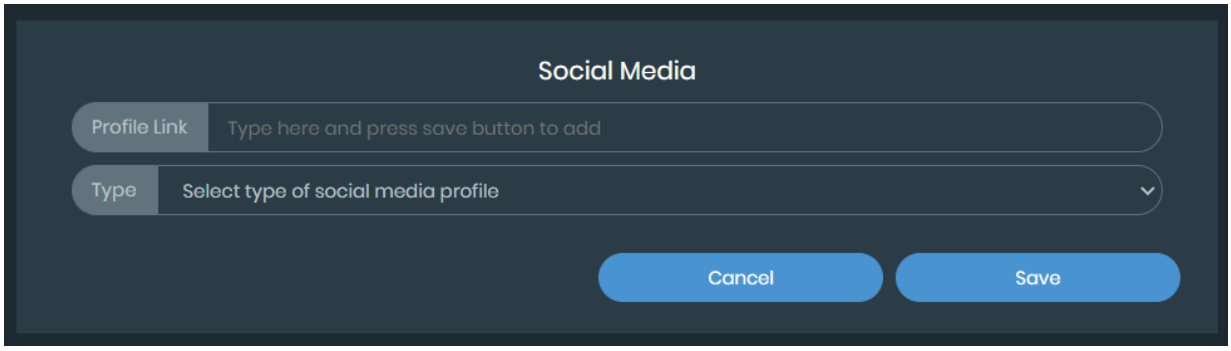
Adding official profiles

You can add official social media profile of your organization from *Brand Protection* > *Social Media Threats* page to differentiate between legitimate and impersonating profiles.

To add official profiles:

1. Go to *Brand Protection* > *Social Media Threats*
2. Click *Official Profiles* on the top right corner.

3. Click add icon.
4. Provide the required information:
   a. Enter the profile URL.
   b. Select the social media platform.

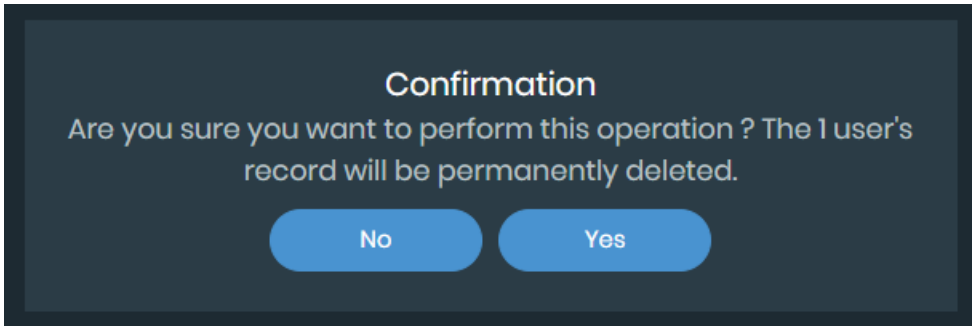


5. You can also add official social media profiles in bulk by uploading excel (XLS) file containing profile information including profile URL and type.
   a. Click Upload XLS icon.
   b. Browse and select the file. Click *Open*.

   Note: Ensure that the format in which the profiles data is stored matches with the required format. To view the required format click Download Sample XLS icon.

To delete an official profile:

1. Go to *Brand Protection* > *Social Media Threats*
2. Click *Official Profiles* on the top right corner.
3. Select the required profile.
4. Click Delete icon.
5. A confirmation message is displayed. Click *Yes*.



Adding a new social media profile

You can add social media profiles for monitoring.

To add a new social media profile:

1. Go to *Brand Protection* > *Social Media Threats*.
2. Click *Add Profiles*.
3. Click *Add* icon.
4. Select the *Type* of social media from the dropdown.
5. Enter the *Profile Link*.
6. Click *Save*.

After you add a new social media profile, the status field in the *Add Profiles* page will indicate one of the following:

- **In Review**: The FortiRecon team is currently assessing the newly added profile.
- **Accepted**: The profile has been validated and approved.
- **Rejected**: The profile was deemed invalid. A comment will explain the reason for rejection.

Alerts

FortiRecon lists flash reports prior to version 23.2.0 on the *Brand Protection* > *Social Media Threats* > *Show Archived* page.

From the *Archived Alerts* page, you can:

- View flash reports. See Viewing flash reports on page 112.
- Filter through all flash reports available. See Filtering reports on page 113.
- Download flash reports as threat intelligence reports in PDF or as an observable Microsoft Excel file. See Downloading reports on page 113.
- Email and share links to flash reports with others. SeeSharing reports on page 115
- Rate flash reports for relevance. See Rating reports on page 116.
- Review reports and send queries to FortiRecon. See Reviewing reports on page 116.

Viewing flash reports

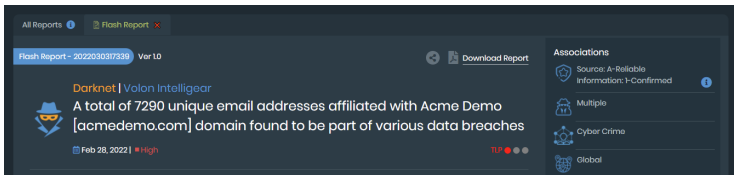
The *Brand Protection* > *Social Media Threats* > *Show Archived* page displays all the flash reports archived to you. By default all reports are displayed, starting with the latest report. Reports include in depth information, such as:

- Threat summary
- Threat detail
- Assessment

A *Takedown* button is included in the report details of reports related to brand abuse. Select the button to begin the takedown process.

To view flash reports:

1. Go to *Brand Protection* > *Social Media Threats* > *Show Archived*. The *All Reports* tab displays all flash reports.
2. Click a report title to open the report details.



Filtering reports

You can adjust the reports that display on the *Alerts* page.

To filter reports:

1. Go to *Brand Protection* > *Alerts*.
2. Filter reports by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range. Only reports from the date range are displayed.
   d. Click the *Filter Report by Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
   The reports are filtered to display only reports with the keyword.
   b. Click the *X* beside the keyword to remove the filter.

   The reports that match the set filters display.

Downloading reports

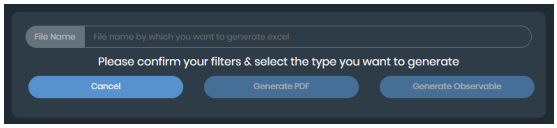
You can download reports from the *Alerts* tab as brand protection alerts in PDF or as an observable Microsoft Excel file. Brand protection alerts provide information from a flash report whereas observables outline any Indicators of Compromise (IOCs) highlighted in the flash report.

Downloaded reports can be set to include:

- All reports available
- Several, specific reports
- Single reports

To download all reports available:

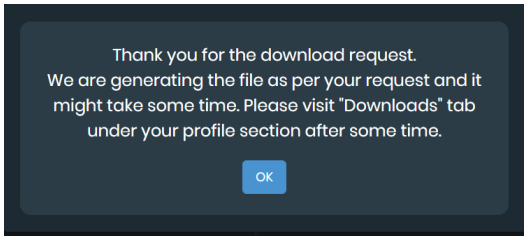
1. Go to *Brand Protection* > *Social Media Threats* > *Show Archived*, and select *Downloads*. A confirmation dialog is displayed.



2. Enter a name for the downloaded file in the *File Name* text box.

3. Select the format of the downloaded file:
   - Select *Generate PDF* to download a brand protection alert in PDF.
   - Select *Generate Observable* to download details in Microsoft Excel format.

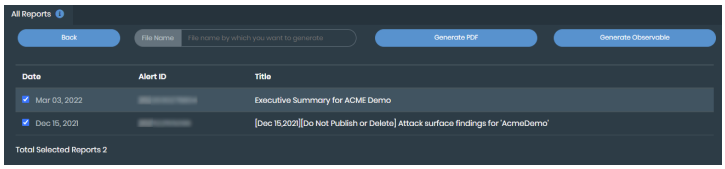
   The following message is displayed:



4. Click *OK*.
5. Retrieve the report. See Retrieving downloads on page 203.

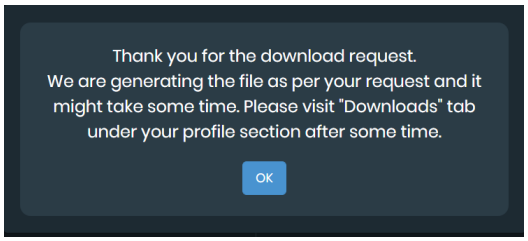
To download specific reports:

1. Go to *Brand Protection* > *Social Media Threats* > *Show Archived*.
2. Click the filter icon and set the desired report filters. See Filtering reports on page 113
3. Select *Download Specific Reports*, and select the reports to include in the report.
4. Select *Downloads*. A list of the selected reports is displayed with download options.



5. Enter a name for the downloaded file in the *File Name* text box.
6. Select the format of the downloaded file:
   - Select *Generate PDF* to download a brand protection alert in PDF.
   - Select *Generate Observable* to download details in Microsoft Excel format.

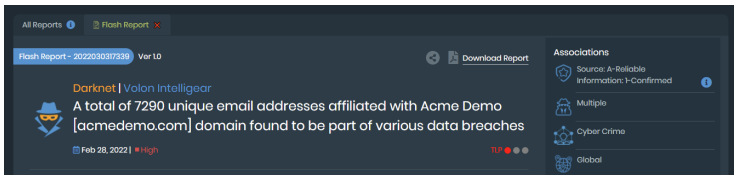
   The following message is displayed:



7. Click *OK*.
8. Retrieve the report. See Retrieving downloads on page 203.

To download a single report:

1. Go to *Brand Protection* > *Social Media Threats* > *Show Archived* and click the desired report. The report details open in a new tab.



2. Click *Download Report*.
   The report downloads to your computer in PDF.

Sharing reports

You can share a link so that other users can access details of the report without needing to download a file. You can email the link or copy the link to share in a format of your choice.

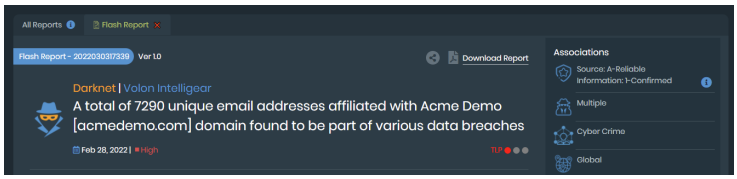
Only recipients who have a FortiRecon account can access reports through a shared link.

The Traffic Light Protocol (TLP) level dictates who you can share a report with:

- *TLP Red*: The report cannot be shared outside of your organization and should be restricted only to personnel who need to know.
- *TLP Amber*: The report can only be shared with members of your organization and clients who need to know the information to protect themselves.
- *TLP Green*: The report can be shared with peers and partner organizations but cannot be shared on publicly accessible channels.
- *TLP White*: The report can be shared without restriction.

To share a link to a report:

1. Go to *Brand Protection* > *Social Media Threats* > *Show Archived* and select the report you want to share. The report details are displayed in a new tab.



2. Hover your mouse over *Share Link*. *Copy Link* and *Email* display.

3. Select how you would like to share the link:
   a. Click *Copy Link* to share the link in a format of your choice.
      The link is copied to your computer clipboard, and you can paste it into a message as needed.
   b. Click *Email* to email the link.
      Your personal email opens with a draft that includes the report link.

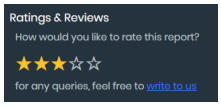
You cannot share Executive Summaries.

Rating reports

You can rate reports in a five star scale. The collection of ratings helps the FortiRecon team provide more relevant reports.

The rating scale is based on five stars. The rating can range from one to five by moving left to right along the stars, with the leftmost star representing one.

To rate a report:

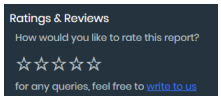
1. Go to *Brand Protection* > *Social Media Threats* > *Show Archived* and select the report you want to rate.
   The report details are displayed in a new tab.
2. Hover your mouse over the stars in *Ratings & Reviews*.
   The stars turn yellow as you move the mouse across them.
   

3. Click the star that corresponds to your rating out of five.
   Your rating is saved, and you can change it at any time by selecting a different star.

Reviewing reports

You can send reviews and queries to the FortiRecon team. Any questions or reviews on reports can be sent using the *write to us* feature.

To review a report:

1. Go to *Brand Protection* > *Social Media Threats* > *Show Archived* and select the report you want to review.
   The report details are displayed in a new tab.
2. In *Ratings & Reviews*, select *write to us*.
   

   Your personal email opens with a draft that is ready to be sent to the FortiRecon team.

Rogue Mobile Apps

On the *Brand Protection* > *Rogue Mobile Apps* page, the FortiRecon research team continuously monitors a number of application stores to identify newly created applications that appear similar to your organization's official application.

From the *Brand Protection* > *Rogue Mobile Apps* page, you can:

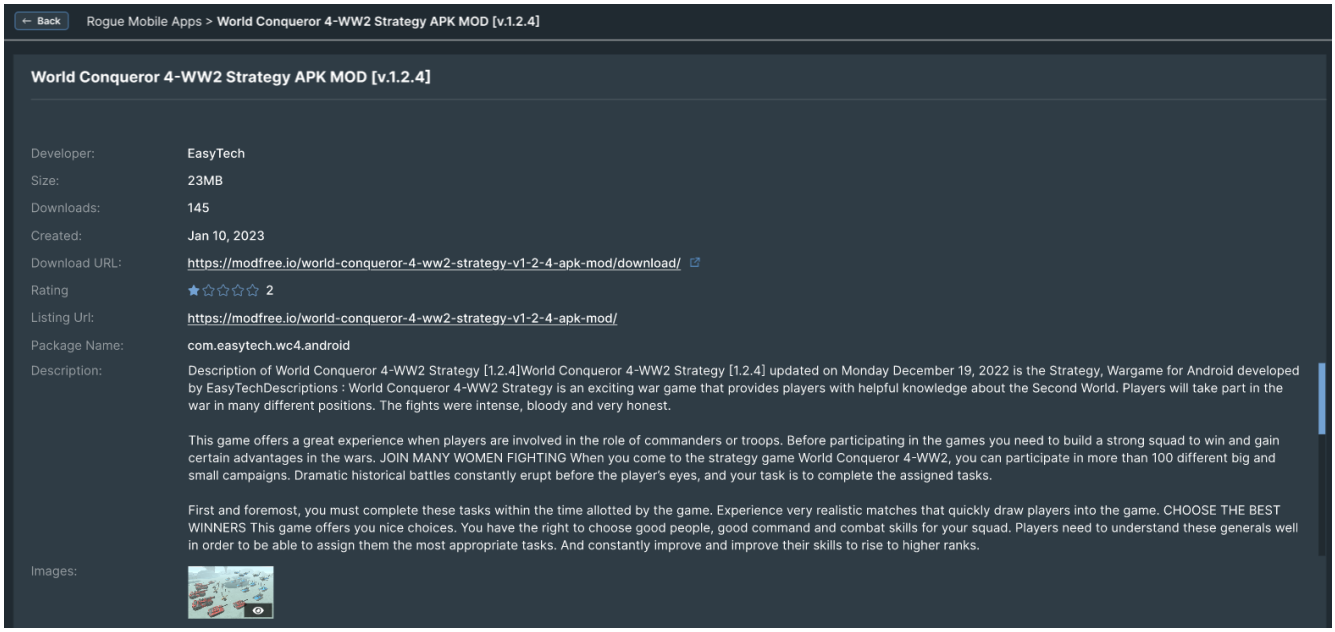
- View information on monitored applications. See Reviewing rogue applications on page 117.
- Filter for specific mobile applications. See Filtering rogue applications on page 118.
- Add official applications. See Adding official applications on page 118.
- Assign an app status. See Assigning application status on page 119.
- Initiate takedown of a rogue application. See Taking down rogue apps on page 120.
- Export information on applications. See Exporting rogue applications on page 120.

Reviewing rogue applications

You can view more information on monitored applications on the *Rogue Mobile Apps* page.

To review rogue applications:

1. Go to *Brand Protection* > *Rogue Mobile Apps*.
2. Review the high level threat information:
   - Review the distribution of application types and the total number of discovered rogue applications in the *Rogue App Summary*.
   - Review the distribution of applications based on the app stores in *By App Stores*.
   - Review the number of takedown credits available in *Takedown Credits*.
3. Filter for the application you want to review. See Filtering rogue applications on page 118.
4. Select the application you want to review. The app information is displayed in a new tab.



Filtering rogue applications

You can filter the apps that appear on the *Rogue Mobile Apps* page by *App Status*, *App Stores* and *Start & End Date*.

To filter apps:

1. Go to *Brand Protection* > *Rogue Mobile Apps*.
2. Filter reports by a date range:
   a. Click *Filter By Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range.
   Only apps from the date range are displayed.
   d. Click the *Filter By Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
   The apps are filtered to display only apps with the keyword.
   b. Click the *X* beside the keyword to remove the filter.
4. Select the *App Status*, either *Unofficial* or *Rogue*.
5. Select the *App Stores*.
6. Click *Search*. The applications with the matching filters are displayed.

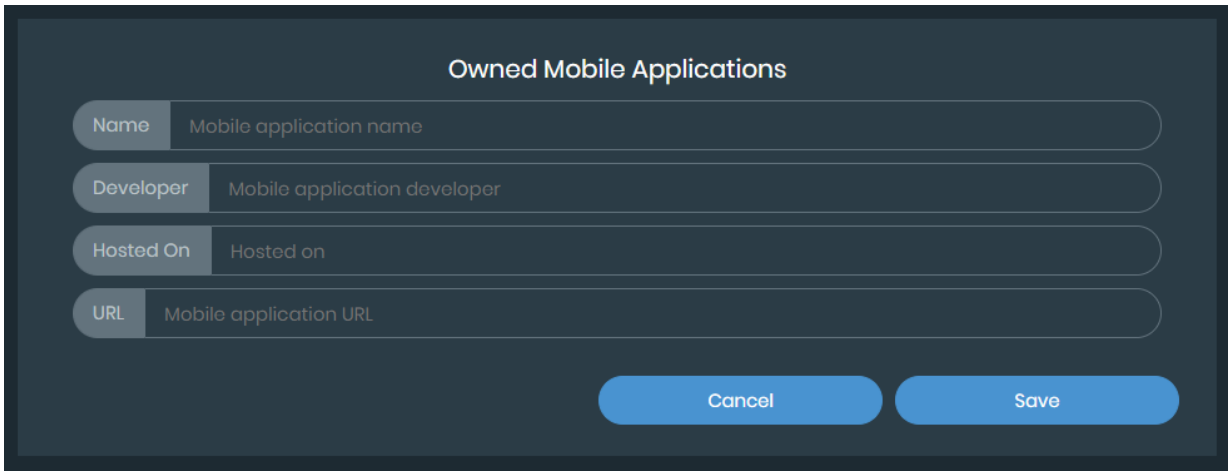
Adding official applications

You can add officia lapplications of your organization from *Brand Protection* > *Rogue Mobile Apps* page to differentiate between legitimate and rogue applications.

To add official applications:

1. Go to *Brand Protection* > *Rogue Mobile Apps*
2. Click *Official Apps* on the top right corner.
3. Click add icon.
4. Enter the following information in the confirmation pop-up:
   a. Application name.
   b. Developer
   c. Hosted on

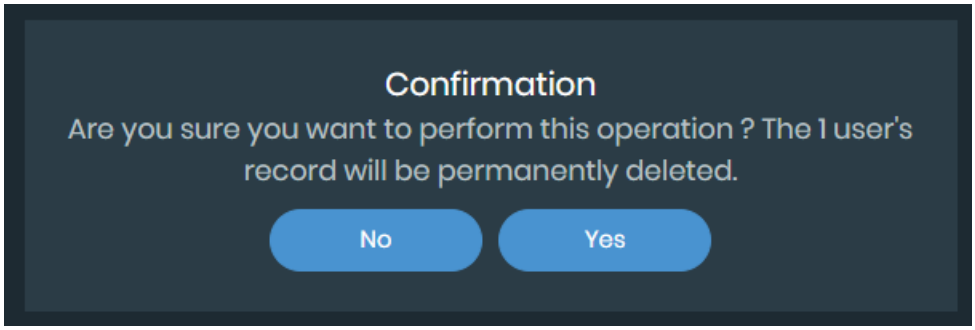
d. URL



5. You can also add official applications in bulk by uploading excel (XLS) file containing application information including application name, mobile app developer, hosted on and app URL.
   a. Click Upload XLS icon.
   b. Browse and select the file. Click *Open*.
   Note: Ensure that the format in which the profiles data is stored matches with the required format. To view the required format click Download Sample XLS icon.

To delete an official application:

1. Go to *Brand Protection* > *Rogue Mobile Apps*
2. Click *Official Profiles* on the top right corner.
3. Select the required application.
4. Click Delete icon.
5. A confirmation message is displayed. Click *Yes*.



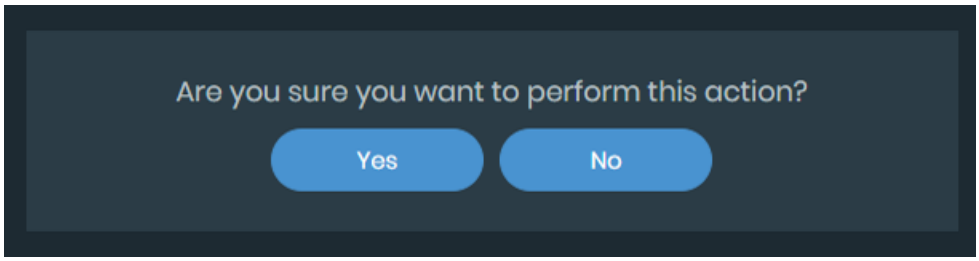
Assigning application status

You can use the following status designations to define app status on the *Rogue Mobile Apps* page:

- *Unofficial*: The app is not published by officially recognized users.
- *Rogue*: The app is unofficial and potentially malicious. If an application is marked as *Rogue*, the *Takedown* function becomes available.

To assign a new application status:

1. Go to *Brand Protection* > *Rogue Mobile Apps* and find the app.
2. Click Actions and select the new application status. A confirmation message is displayed.



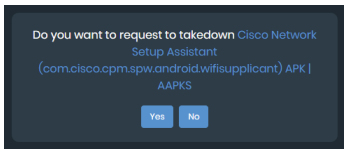
3. Click *Yes*.

Taking down rogue apps

If an app is determined to be malicious and rogue, you can initiate the takedown process in the *Rogue Mobile Apps* page.

To initiate takedown of a malicious application:

1. Go to *Brand Protection* > *Rogue Mobile Apps* and find the app.
2. If the application is assigned to *Unofficial*, change the application status to *Rogue*. See Assigning application status on page 119.
3. Click *Takedown*. A confirmation message is displayed.



4. Click *Yes*. A tracking *Ticket* appears.
5. Go to *Brand Protection* > *Take Down* to review the status of the application takedown.

Exporting rogue applications

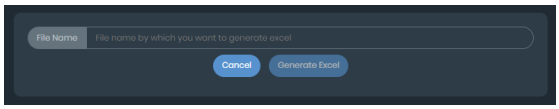
You can export details on potentially rogue mobile applications in the *Rogue Mobile Apps* page. Information included in exported file includes:

- App name and size
- Description
- Developer name and URL
- Download count and URL
- Date the app was discovered

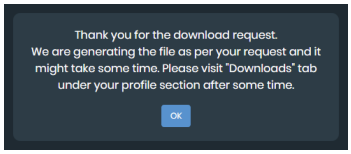
- Listing URL
- Package name
- Source name
- Status

To export rogue application details:

1. Go to *Brand Protection* > *Rogue Mobile Apps*.
2. Set the desired filters. See Filtering rogue applications on page 118
3. Click *Download* icon next to the Filters title. A confirmation dialog is displayed.



4. Enter a name for the export file in the *File Name* text box.
5. Select *Generate Excel*. A confirmation message is displayed.



6. Click the menu in the top-right corner and select *Profile Settings*.
7. Go to the *Downloads* tab. The list of available downloads are displayed.
8. Click the download. A file with the name you set is downloaded to your computer in Microsoft Excel format.

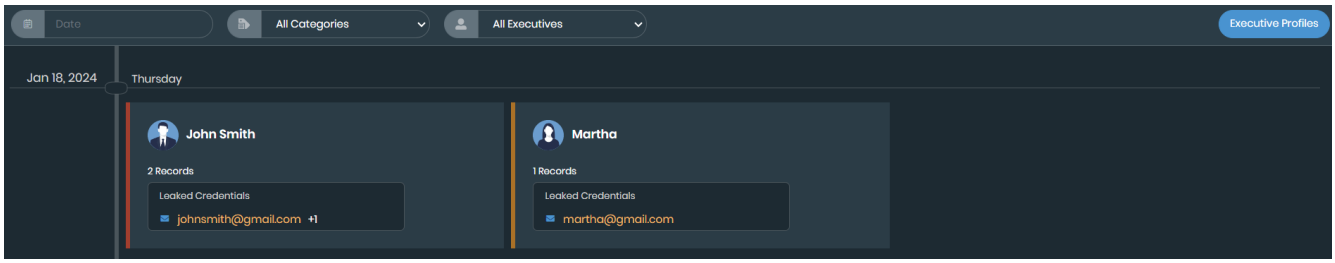
Executive Monitoring

The *Brand Protection* > *Executive Monitoring* page provides enhanced visibility and proactive threat detection, enabling you to monitor high-profile individuals for any malicious activity, providing real-time alerts and actionable insights to mitigate potential security risks.

From the *Brand Protection* > *Executive Monitoring* page, you can:

- View the timeline of threats for the official executive profiles added. See Reviewing executive profile threats on page 122.
- Filter the list of executive profile threats. See Filtering executive profile threats on page 122.
- Add official executive profiles. See Adding executive profiles on page 123.

By default, a maximum of 10 executive profiles can be added for monitoring. To monitor additional profiles, you can purchase a separate license.



Reviewing executive profile threats

You can review information about executive profile threats in the *Brand Protection* > *Executive Monitoring* page. Information includes comprehensive overview of identified threats categorized into various types, including leaked credentials, Telegram mentions, Dox site mentions, Darknet mentions, social media threats, stealer infections, and leaked documents.

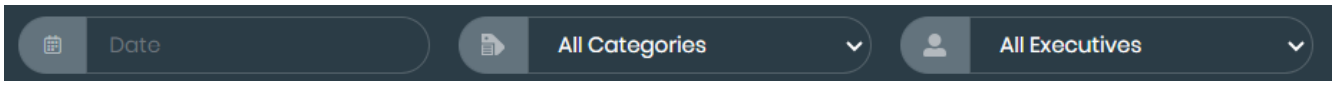
Threat Category	Description
Leaked Credentials	Instances where the executive's credentials have been exposed or compromised.
Telegram Mentions	References or discussions related to the executive on the Telegram messaging platform.
Dox Site Mentions	Mentions or references of the executive on websites known for sharing personal or private information.
Darknet Mentions	References or discussions related to the executive on the darknet.
Social Media Threats	Threats posed to the executive's security or reputation on social media platforms (*LinkedIn, Facebook, Instagram* and *Twitter*).
Stealer Infections	Indications of malware or malicious software infecting the executive's devices with the intent of stealing sensitive information.
Leaked Documents	Instances where documents or files associated with the executive have been leaked or made publicly accessible without authorization

To review executive profile threats:

1. Go to *Brand Protection* > *Executive Monitoring*.
2. Select the desired report.
3. Review the identified threats.

Filtering executive profile threats

You can filter threats by date, threat category, or executive profile.



To filter domain threats:

1. Go to *Brand Protection* > *Executive Monitoring*
2. Filter threats by a date range:
   a. Click *Date* . Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. Select a month, year, and day to specify the end date of the range.
   Only threats from the date range are displayed.
   d. Click the *Date* box, and click *X* to remove the date range filter.
3. Filter by threat category:
   - Click *All Categories* and select the desired category from the dropdown, to filter threats by their categories.
4. Filter by executive profiles:
   - Click *All Executives* and select the desired profile from the dropdown, to filter threats by profile.

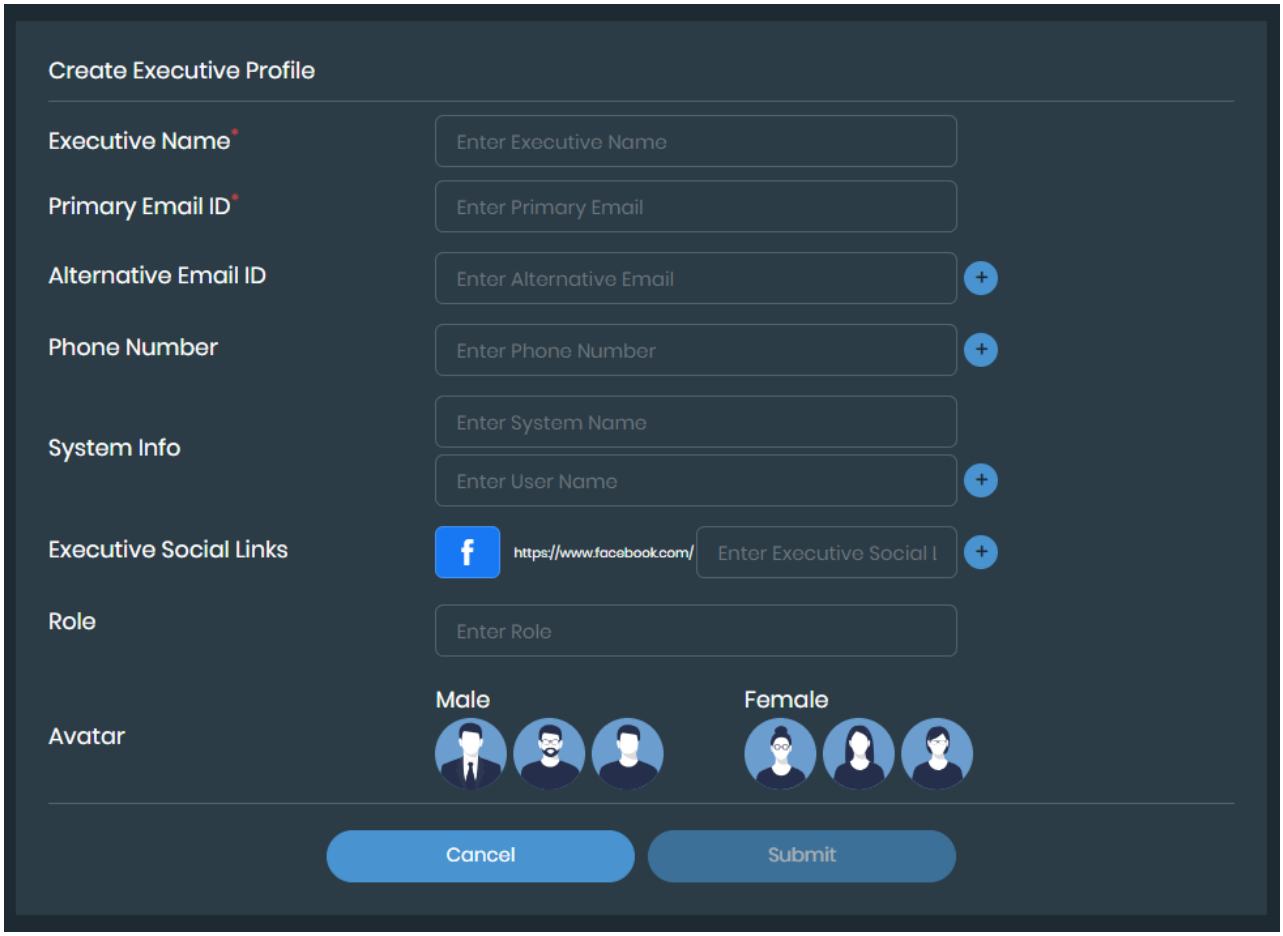
Adding executive profiles

You can add official executive profiles of your organization from *Brand Protection* > *Executive Monitoring* page.

To add official profiles:

1. Go to *Brand Protection* > *Executive Monitoring*.
2. Click *Executive Profiles* on the top right corner.
3. Click *+Add Profiles.*
4. Provide the required information, including:
   a. *Executive Name* - Enter the name of the high-profile individual.
   b. *Primary Email ID* - Enter the main email address associated with the executive.
   c. *Alternative Email ID* - Enter an additional email address.
   d. *Phone Number* - Enter the contact number.
   e. *System Name* - Enter the system and user name.
   f. *Executive Social Links* - Enter the social media profile links. Select the social media platform by clicking the social media icon and selecting desired platform. Click + icon to add more than one social media profile link.
   g. *Role* - Enter the role of the executive.
   h. *Avatar* - Choose the avatar from the available options.

5. Click *Submit*.

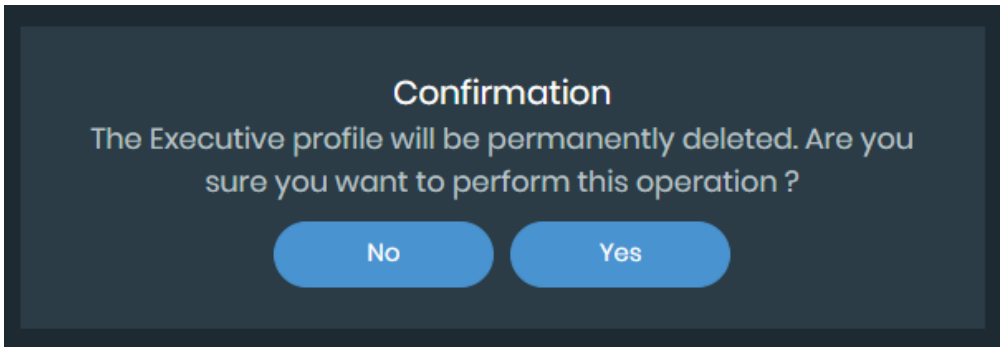


To edit a executive profile:

1. Go to *Brand Protection* > *Executive Monitoring*.
2. Click *Executive Profiles* on the top right corner.
3. Click Edit icon on the desired executive profile.
4. Make the necessary changes and click *Submit*.

To delete a executive profile:

1. Go to *Brand Protection* > *Executive Monitoring*.
2. Click *Executive Profiles* on the top right corner.
3. Click Delete icon on the desired executive profile.
4. A confirmation message is displayed. Click *Yes*.



Code Repo Exposure

The *Code Repo Exposure* page displays a list of attributes that have been exposed in code repositories.

From the *Brand Protection* > *Code Repo Exposure* page, you can:

- Add or delete custom keywords. See Managing keywords.
- Review attribute information. See Reviewing attributes on page 127.
- Take action against the discovered attributes. See Managing attributes on page 127.
- Filter attributes. See Filtering attributes on page 128.

Managing keywords

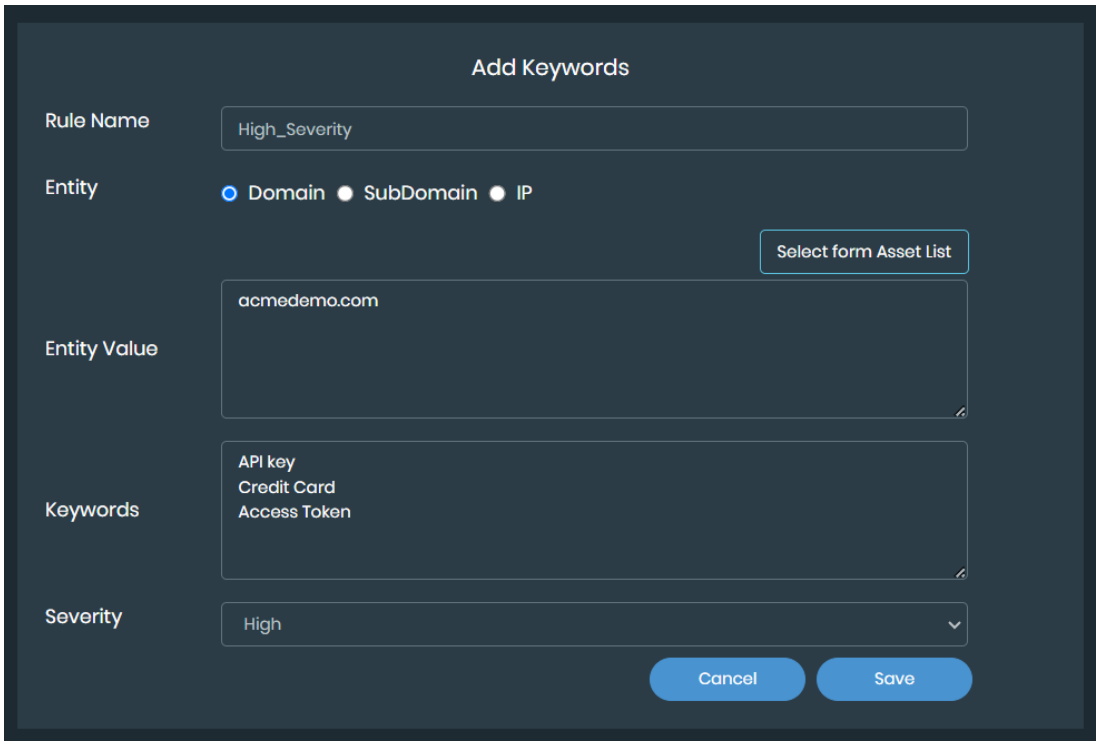
You can add a custom rule to match keywords against the discovered domains, sub domains and IPs.

To add a keyword rule:

1. Go to *Brand Protection* > *Code Repo Exposure*.
2. Click *Keyword Watchlist*.
3. Click **+** icon.
4. In the *Add Keywords* pop-up, enter the following information and click *Add*.
   a. *Rule Name*: Enter a name for the rule.
   b. *Entity*: Select the type of entity.
   c. *Entity Value*: Based on the entity type selected, you can either enter entity values or select the required entities from the *Select from Asset List*. The *Select from Asset List* contains a list of assets discovered by the EASM module. You can add multiple entities separated by a comma or by adding each entity in a new line.
   d. *Keywords*: Enter the required keywords. You can add multiple keywords separated by a comma or by adding each keyword in a new line.

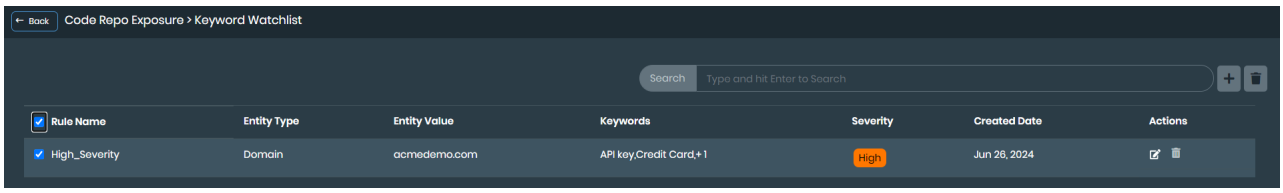
e. *Severity*: Select the severity level from the dropdown.

You can only add multiple keywords with a single entity, or vice versa. You cannot add both multiple keywords and multiple entities together.



To delete a keyword rule:

1. Go to *Brand Protection* > *Code Repo Exposure*.
2. Click *Keyword Watchlist*.
3. Optionally, search for the specific keyword using the search bar.
4. Click *Delete* icon next to the desired keyword rule.
5. To bulk delete all the rules, select the checkbox in the header. Once all the keywords are selected, click *Delete* icon next to search bar.



To edit a keyword rule:

1. Go to *Brand Protection* > *Code Repo Exposure*.
2. Click *Keyword Watchlist*.
3. Optionally, search for the specific keyword using the search bar.

4. Click *Edit* icon next to the desired keyword rule.
5. Update the details and click *Update*. You can update *Rule Name* and *Severity* fields only.

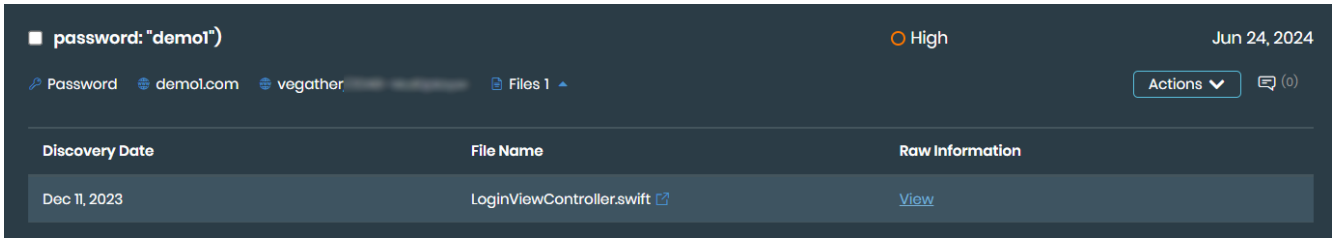
Reviewing attributes

You can review information about exposed code attributes in the *Brand Protection* > *Code Repo Exposure* page. Information displayed about discovered exposed code includes:

- Attributes and values
- Matched domains identified with the exposure
- Files discovered with raw information about the exposure
- Discovery date
- Risk status

To review exposed attributes:

1. Go to *Brand Protection* > *Code Repo Exposure*.
2. Review the high level attribute information:
   - Review the risk level and total number of the alerts in the *Alert Summary*.
   - Review the attribute types in *Top 5 Attributes*.
3. Select an alert to view the attribute type, domain, repository name and files discovered.
4. Click *Files* to view the list of files discovered. Click *Link* icon next to the file name to view the file. Click *View* to view the raw information.



Managing attributes

You can interact with discovered exposed code, such as marking the attribute as resolved or ignored, or adding a comment to the attribute history. Archived attributes can be viewed by selecting *Show Archived*.

To manage an attribute:

1. Go to *Brand Protection* > *Code Repo Exposure*.
2. Find the attribute you want to adjust.
3. Change the status:
   - Select *Action* > *Mark as Resolved* to indicate that the exposed code risk has been resolved.
   - Select *Action* > *Mark as False Positive* if the discovered code is not a risk.
   - Select *Action* > *Mark as Ignored* to indicate that the identified exposure can be ignored.
4. Click *Comment* to add a comment to the attribute history.

To manage multiple attributes at once:

1. Go to *Brand Protection* > *Code Repo Exposure*.
2. Select the attributes you want to adjust. The *Action* dropdown menu is displayed.
3. Adjust the status or comment history of all of the attributes:
   - Select *Action* > *Mark as Resolved* to indicate that the exposed code risk has been resolved for all of the selected attributes.
   - Select *Action* > *Mark as False Positive* if the discovered code is not a risk.
   - Select *Action* > *Mark as Ignored* to indicate that the identified exposures can be ignored.

Filtering attributes

You can filter attributes by date, status, risk level, or attribute.

To filter attributes:

1. Go to *Brand Protection* > *Code Repo Exposure*
2. Filter attributes by a date range:
   a. Click *Filter By Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. Select a month, year, and day to specify the end date of the range.
   Only attributes from the date range are displayed.
   d. Click the *Filter By Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
   The attributes are filtered to display only attributes with the keyword.
   b. Click the *X* beside the keyword to remove the filter.
4. Filter by status in the *By Alert Status* section:
   - Select *Active*, *Resolved*, or *Ignored* to filter attributes by their assigned status.
5. Filter by risk level in the *By Risk Level* section:
   - Select *High*, *Medium*, or *Low* to filter by risk level.
6. Select the domain from the *By Matched Domain* section.
7. Select the keyword rule from the *By Rule* section.
8. Select the attribute type in the *By Attributes* section to filter by type.
9. Click *Search*. The attributes with the matching filters are displayed.

Open Bucket Exposure

The *Open Bucket Exposure* page displays a list of files exposed in open buckets.

From the *Brand Protection* > *Open Bucket Exposure* page, you can:

- Review files exposed on open buckets. See Reviewing files on page 129.
- Take action against discovered files. See Managing files on page 129.

- Filter files. See Filtering files on page 130.

Reviewing files

You can review information about exposed files in the *Brand Protection* > *Open Bucket Exposure* page. Information displayed about discovered exposed files includes:

- File name
- File type
- Bucket source
- Bucket name
- Discovery date
- File accessibility

To review exposed attributes:

1. Go to *Brand Protection* > *Open Bucket Exposure*.
2. Review the high level file information:
   - Review the distribution of bucket sources and the total number of discovered files in the *Alert Summary*.
   - Review the distribution of file types in *Top 5 File Types*.
3. Select a file to review detailed file information.

Managing files

You can interact with discovered exposed files, such as marking the files as resolved or ignored, or adding a comment to the attribute history. Archived files can be viewed by selecting *Show Archived*.

To manage a file:

1. Go to *Brand Protection* > *Open Bucket Exposure*
2. Find the file you want to adjust.
3. Change the status:
   - Select *Action* > *Mark as Resolved* to indicate that the exposed risk has been resolved.
   - Select *Action* > *Mark as Ignored* to indicate that the identified exposure can be ignored.
4. Click *Comment* to add a comment to the file history.

To manage multiple files at once:

1. Go to *Brand Protection* > *Open Bucket Exposure*
2. Select the files you want to adjust. The *Action* dropdown menu is displayed.
3. Adjust the status or comment history of all of the file:
   - Select *Action* > *Mark as Resolved* to indicate that the exposure risk has been resolved for all of the selected files.
   - Select *Action* > *Mark as Ignored* to indicate that the identified exposures can be ignored.
   - Click *Action* > *Comment* to add a global comment to the file history of the selected files.

Filtering files

You can filter files by date, status, risk level, or attribute.

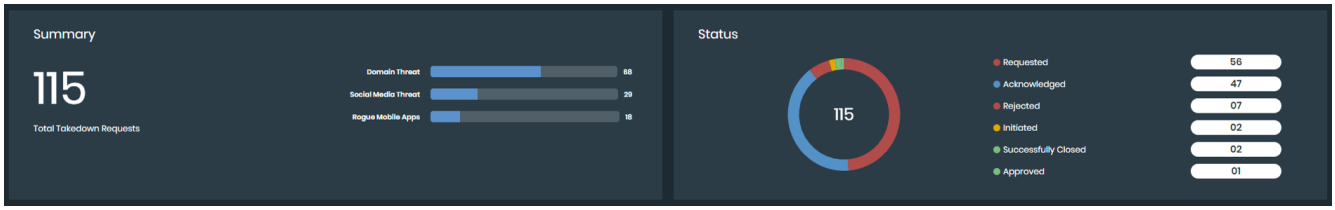
To filter files:

1. Go to *Brand Protection* > *Open Bucket Exposure*
2. Filter files by a date range:
   a. Click *Filter By Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. Select a month, year, and day to specify the end date of the range.
   Only files from the date range are displayed.
   d. Click the *Filter By Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
   The files are filtered to display only files with the keyword.
   b. Click the *X* beside the keyword to remove the filter.
4. Filter by status in the *By Alert Status* section:
   - Select *Active*, *Resolved*, or *Ignored* to filter files by their assigned status.
5. Filter by accessibility in the *By File Status* section.
6. Select the open bucket source from the *By Bucket* section.
7. Select the file type in the *By Type* section.
8. Click *Search*. The files with the matching filters are displayed.

Take Down

The FortiRecon team uses a proprietary Digital Millennium Copyright Act (DMCA) process to execute the takedown. During the takedown process, notices are sent to the offending parties, hosting providers, and registrars with provisions of local and international laws to demand that the account be taken down on account of impersonation, phishing, and so on.

You can review the current status of takedown requests in the *Brand Protection* > *Take Down* page. The *Summary* widget displays the total count of takedown requests, along with a count for each category. The *Status* widget displays the count of takedown requests for each status.



From the *Brand Protection* > *Take Down* page, you can:

- Create and manage Authority Letters. See Authority Letters.
- Filter for specific takedown requests by date, category, status, and ticket number. See Filtering takedown requests on page 134.

Authority Letters

An Authority Letter is a legal document that grants FortiRecon the authorization to initiate takedown requests on your behalf. This letter is a mandatory component of the takedown process, demonstrating your ownership of intellectual property and your right to request the removal of infringing content.

- Creating Authoring Letters
- Uploading the Signed Authority Letter
- Viewing Authority Letter Status

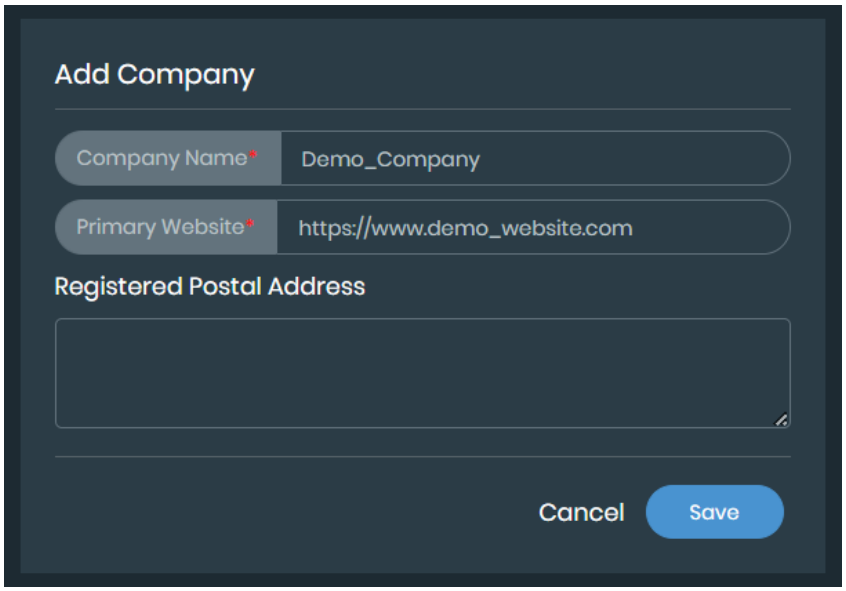
Creating Authoring Letters

Perform the following steps to create a new Authority Letter. Click *Save as Draft* anytime during authority letter creation to save the draft and continue later.

1. Navigate to *Brand Protection* > *Take Down*.
2. Click *Authority Letters*.
3. In the *Authority Letters* page, click *+ Add*.
4. In the *Client Profile* page enter the following information and click *Next*.
   - *Document Name*: Name for the document.
   - *Organization Name*: Your organization's name.
   - *Start & End Date*: Start and end dates for the Authority Letter's validity. The subscription dates are pre-filled by default.
   - *Authorized User Name*: Name of the person authorized to initiate take down requests.

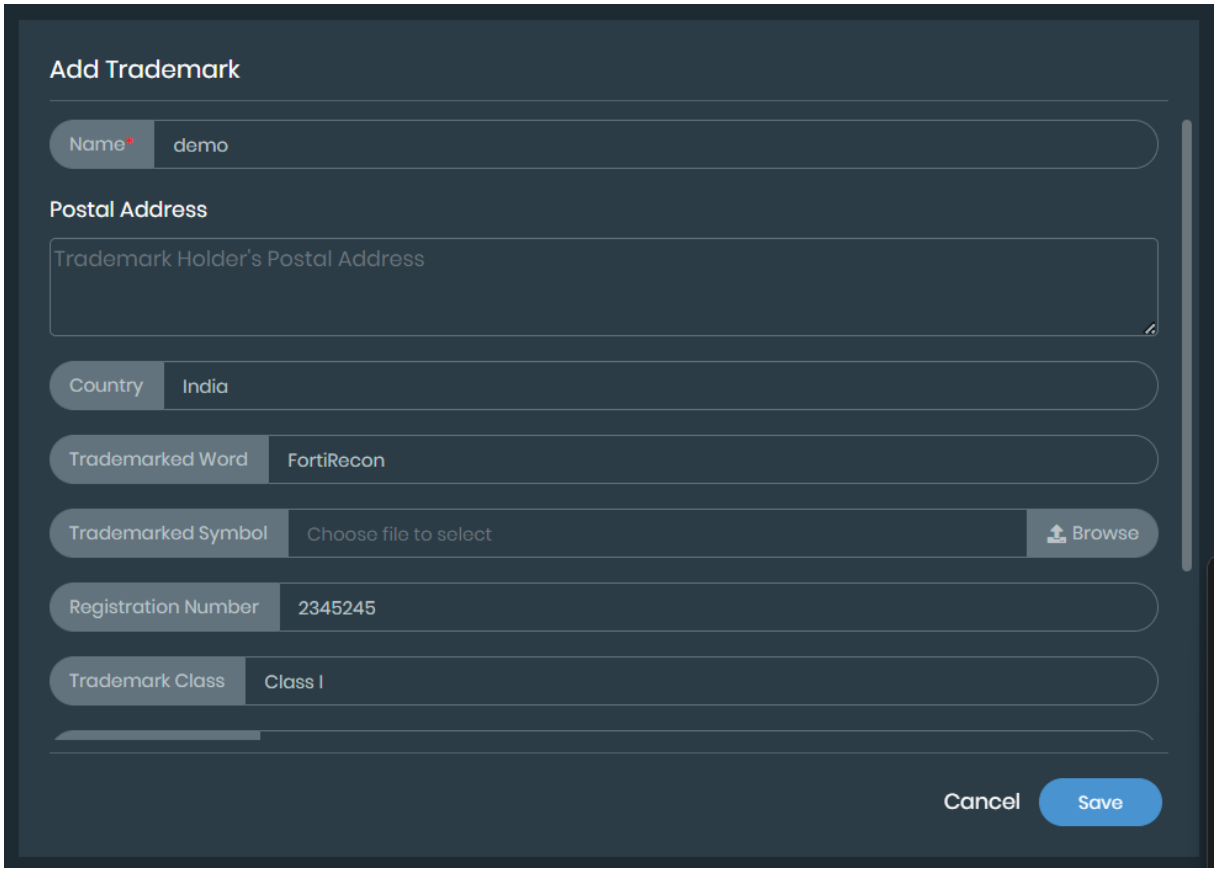
- *Designation*: Designation of the person authorized to initiate take down requests.

5. In the *Company Details Overview* page, click + *Add Company* to add a new company and enter the following details.
.
   - Company Name
   - Primary Website
   - (Optional) Registered Postal Address



6. Click *Save*. The added company is listed. Click *Edit* under Actions to edit the company details or *Delete* to delete the added company.
7. Click *Next*.

8. In the *Trademark Portfolio Management* page, click *+ Add Trademark* to add trademark details and enter the following information for each trademark.
   - Trademark holder's name.
   - Postal Address
   - Country
   - Trademarked Word
   - Trademarked Symbol
   - Registration Number
   - Trademark Class
   - Registration Office



9. Select *Yes* if you have direct link to trademark search page and enter the trademark URL. Else, select *No* and upload the proof of trademark.

10. Click *Save*. The added trademark is listed. Click *Edit* under Actions to edit the trademark details or *Delete* to delete the added trademark.
11. Click *Save*.

Uploading the Signed Authority Letter

Once a new Authority Letter is created, you will receive an email containing *Authority Letter Template* in Word format and detailed instructions for completing and signing the Authority Letter. You can also download the *Authority Letter Template* from *Authority Letters* page in *Brand Protection* > *Take Down*.

To upload the signed Authority Letter, perform the following steps.

1. Follow the instructions in the email to sign the Authority Letter.
2. In FortiRecon portal, navigate to *Brand Protection* > *Take Down*.
3. Click *Authority Letters*.
4. Locate the relevant Authority Letter and click *Upload Signed Authority Letter*.

5. Browse and upload the signed Authority Letter.

The uploaded Authority Letter will undergo an internal validation process. Any required changes or additional information will be communicated through comments in the FortiRecon portal and email alerts.

Viewing Authority Letter Status

The following status is displayed for Authority Letters.

- *Draft* : The Authority Letter is saved as draft. Click *Actions* > *Edit* to continue Authority Letter creation.
- *In Progress*: The Authority Letter has been created successfully. You can still make edits or delete it if needed.
- *In Review*: The signed Authority Letter has been uploaded and is being checked for validity.
- *Rejected*: There are issues with the Authority Letter. Check the comments for details. You can edit and re-upload the letter, or delete it.
- *Expired*: The Authority Letter's validity period has ended.

Filtering takedown requests

You can filter the takedown requests or search for specific *Ticket* numbers on the *Take Down* page.

To filter requests by category and status:

1. Go to *Brand Protection* > *Take Down*.
2. Filter requests by a date range:
   a. Click *Filter By Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range.
   Only requests from the date range are displayed.
   d. Click the *Filter By Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a *Ticket* number, and press *Enter*.
   The requests are filtered to display only requests with the keyword.
   b. Click the *X* beside the keyword to remove the filter.

4. Filter by status in the *By Status* section:
   - Select *Requested*, *Acknowledged*, *Rejected*, *Approved*, *Initiated*, or *Successfully Closed* to filter takedown requests by their assigned status.
5. Filet by category in the By Category section:
   - Select *Domain Threat*, *Social Media Threat*, or *Rogue Mobile Apps* to filter takedown request by threat category.

   The take down requests that match the set filters are displayed.

Adversary Centric Intelligence

The Adversary Centric Intelligence (ACI) module leverages FortiGuard Threat Analysts to provide comprehensive coverage of dark web, open source, and technical threat intelligence, including threat actor insights. This information enables administrators to proactively assess risks, respond faster to incidents, better understand their attackers, and protect assets

The *Adversary Centric Intelligence* module contains the following pages:

Dashboard	Displays a summary of your organization's risk exposure to overall global threats. See Dashboard on page 136.
Reports	Displays the threat intelligence analyst reports and FortiAI Insights available to you. See Reports on page 140.
Card Fraud	Displays information about credit or debit cards that are for sale on darknet marketplaces. See Card Fraud on page 150.
Stealer Infections	Displays information about possible infected systems that are affiliated with your employees or end-users and are for sale on darknet market places. See Stealer Infections on page 152.
OSINT - Cyber Threats	Displays OSINT-based intelligence reports about threat events. See OSINT Cyber Threats on page 157.
Vulnerability Intelligence	Displays information on monitored CVEs. See Vulnerability Intelligence on page 162.
Ransomware Intelligence	Displays information on total and potential ransomware incidents. See Ransomware Intelligence on page 169.
Vendor Risk Assessment	Displays information on a vendor watchlist and the vendor's security hygiene. See Vendor Risk Assessment on page 179.
Intelligence Collection Lookup	Displays threat intelligence from various sources to let you search for a specific posts or messages using a simple search query. See Intelligence Collection Lookup.
Investigation	Displays tabs to let you search for and investigate the reputation of an IPv4 address, domain, file hash, or CVE. See Investigation on page 190.

Dashboard

The *Adversary Centric Intelligence* > *Dashboard* page provides a summary of your organization's risk exposure to global threats. From the *Adversary Centric Intelligence* > *Dashboard* page, you can:

- Change the date range for the dashboard content. See Changing the dashboard date range on page 137.
- View your organization's risk exposure. See Viewing risk exposure summary on page 137.
- View global threat reports. See Viewing global threat report summary on page 139.

Changing the dashboard date range

By default, the *Adversary Centric Intelligence* > *Dashboard* page displays information for the last 90 days. You can change the date range.

To change the dashboard date range:

1. Go to the *Adversary Centric Intelligence* > *Dashboard* page.
   The banner identifies the date range for the displayed information. In the following example, the date range is *From Feb 11, 2022 to May 12, 2022*.

2. From the calendar dropdown list, select a different date range.

Viewing risk exposure summary

The *Adversary Centric Intelligence* > *Dashboard* page displays the following widgets in the *Risk Exposure* section that summarize the risk exposure of your organization to global threats:

- Credential Exposure
- Stealer Infection
- Associated Threats
- Global Event Exposure
- Card Fraud

To view risk exposure summary:

1. Go to the *Adversary Centric Intelligence* > *Dashboard* page, and scroll to the *Risk Exposure* section. A summary of your organization's risk exposure is displayed.

2. Use the following widgets to review your exposure to risk:

Credential Exposure	Displays the number of email addresses related to your organization's domains that are part of third-party credential breaches. The number of exposed credentials and the number of indexed credentials are displayed.
Stealer Infection	Displays data from potentially infected systems that are affiliated with your employees or end-users and are leaked or for sale on credential stealer marketplaces on the darknet. The total number of compromised systems along with number of leaked and on sale compromised systems are displayed. Hover your mouse over on the *Employees/Users* chart to view the number of affected employees and users on a specific date. Hover your mouse over on the *Compromised Systems/Stealers* chart to view the number of compromised systems and stealers on a specific date.
Associated Threats	Displays information about threats reported against your industry and geographical area. The number of reported threats that are specific to your industry and the number of reported threats in your geographic area are displayed. Click the widget to display more details on the *Adversary Centric Intelligence* > *Reports* page.
High Relevance Reports	Displays the reports that are flagged as highly relevant to your organization. Reports must meet certain criteria to be considered relevant. The newest reports are displayed at the top. Click a report to display more details on the *Adversary Centric Intelligence* > *Reports* page.
Global Event Exposure	Displays the latest, published intelligence reports related to notable cyber events from around the globe. Automatically scrolls through the reports, or click the blue bars at the bottom of the widget to view specific reports.
Card Fraud This widget is only displayed for banking organizations that issue credit or debit cards.	Displays statistics related to credit or debit cards that are listed for sale on darknet marketplaces.

	The number of cards for sale is displayed as well as how many of the cards are credit cards and how many are debit cards. Click the *Cards for Sale* number to display more details on the *Adversary Centric Intelligence* > *Card Fraud* page. Hover your mouse over the bars in the chart to view the number of card frauds on a specific date. The top card bin numbers are also displayed.

Viewing global threat report summary

The *Adversary Centric Intelligence* > *Dashboard* page displays the following widgets in the *Global Threats* section that summarize latest intelligence reports related to ongoing, notable, global cyber events:

- Relevance
- Categories
- Motivational Tags
- Latest Intelligence
- Actively Exploited CVEs
- Top Actors
- Notable Category Reporting

To view global threat report summary:

1. Go to the *Adversary Centric Intelligence* > *Dashboard* page, and scroll to the *Global Threats* section. The number of global threat reports is displayed as well as several widgets.

2. Use the following widgets to review the global threat intelligence reports:

Relevance	Displays the number of reports that are relevant to your organization and are rated high, medium, or low risk. Reports must meet certain criteria to be considered high, medium, or low risk. Click the widget to display more details on the *Adversary Centric Intelligence* > *Reports* page.
Categories	Displays the number of reports for each category, such as Darknet, TechINT, OSINT, and HUMINT.

	Click a category to display more details on the *Adversary Centric Intelligence* > *Reports* page.
Motivational Tags	Displays the available motivational tag filters for reports. Click a tag to display the *Adversary Centric Intelligence* > *Reports* page filtered on the tag.
Latest Intelligence	Displays the latest, published intelligence reports organized into the following categories: • Flash Alert • Flash Report • Threat Alert • Threat Report Automatically scrolls through the reports, or you can click the blue bars at the bottom of the widget to view specific reports.
Actively Exploited CVEs	Displays the number of currently and previously exploited CVEs and identifies a list of newly exploited CVEs. Click the widget to display more details on the *Adversary Centric Intelligence* > *Investigation* page.
Top Actors	Displays the number of actors being tracked as well as the number of reports on the actors. Displays a summary of top actors. Click the name of a top actor to display more details on the *Adversary Centric Intelligence* > *Reports* page.
Notable Category Reporting	Click a report to display more details on the *Adversary Centric Intelligence* > *Reports* page.

Reports

The *Adversary Centric Intelligence* > *Reports* section provides comprehensive threat intelligence reports. This section includes the following component.

- Analyst Reports
- FortiAI Insights

Analyst Reports

The *Adversary Centric Intelligence* > *Reports* > *Analyst Reports* page displays curated reports by our expert threat analysts, offering in-depth insights into emerging threats and trends. From the *Adversary Centric Intelligence* > *Reports* > *Analyst Reports* page, you can:

- View the details of each report. See Viewing analyst reports on page 141.
- Apply filters to the list of reports to hone in on specific reports. See Filtering analyst reports on page 142.
- Download a PDF of reports. See Downloading analyst reports and observables on page 144.
- Share reports. See Sharing analyst reports on page 145.
- Export observables to Microsoft Excel format. See Exporting observables on page 146.

Viewing analyst reports

The *Adversary Centric Intelligence* > *Reports* > *Analyst Reports* page displays all the reports available to you on the *All Reports* tab. By default all reports are displayed, starting with the latest report.

You can filter the list of reports, and search the list of reports using a keyword. See Filtering analyst reports on page 142.

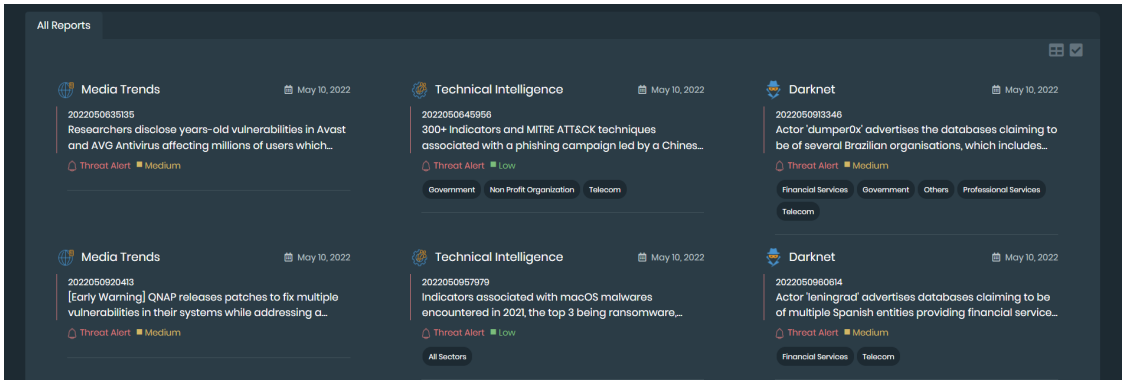
When you open a report, its details are displayed on a separate tab, and you can download a PDF of the report, share the report with another person, and access related reports. When the report contains associated observables, you can download them in Microsoft Excel format.

From an open report, you can also click associated tags to filter the list of reports on the *All Reports* tab, and then access additional related reports.

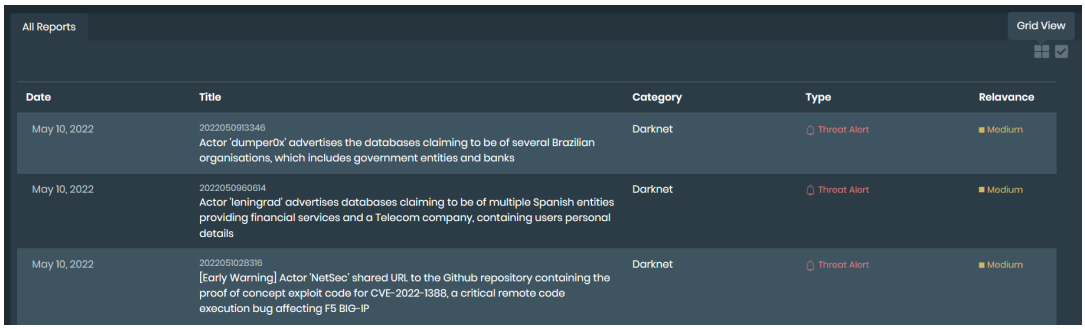
See also Rating reports on page 116.

To view analyst reports:

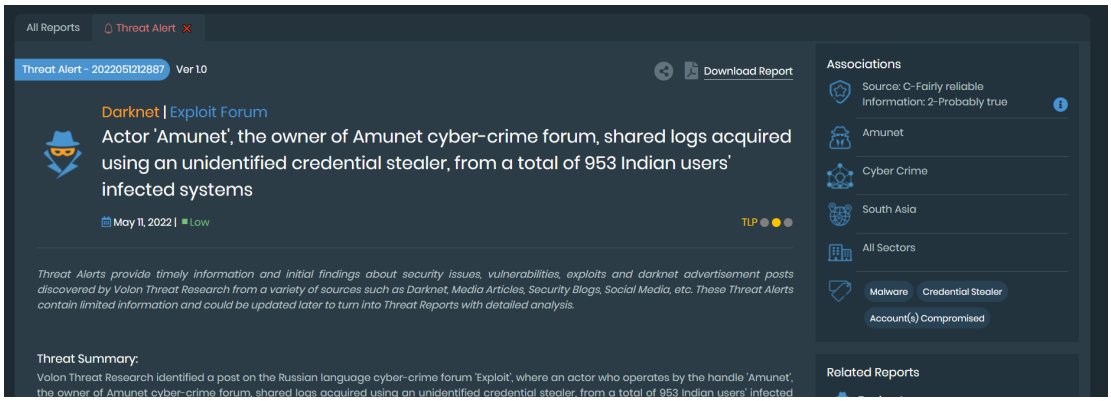
1. Go to *Adversary Centric Intelligence* > *Reports* > *Analyst Reports*. All reports are displayed in the *All Reports* tab.



2. On the *All Reports* tab, toggle between *Grid View* and *Table View*.
In the following example, *Table View* is selected, and you can click the *Grid View* button to change to *Grid View*.



3. Click a report title to display the report details in a new tab.



From the report details page, you can:

- Hover over various icons and words to view tooltips of information.
- Click some words to display more information. For example, click *TLP* (traffic light protocol) to display definitions of the different TLPs and rules around sharing the information.
- Click the *Share Link* button to share a link to the report with another person who has a FortiRecon account.
- Click the *Download Report* link to download a PDF of the report to your computer.
- View and search associated observables as well as click *Export Observables* to download the list of observables in Microsoft Excel format.

From *Associations* area on the right, you can:

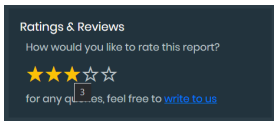
- View what is associated with the report, such as the reliability rating, adversary, motivation, tags, and so on.
- Click the *i* icon to view information about reliability ratings.
- Click a tag to return to the *All Reports* tab to view the list of reports filtered on the selected tag.

From *Related Reports* area on the right, you can:

- View a list of reports related to the open report.
- Click a related report to open it in a new tab.
- Click a tag to return to the *All Reports* tab to view the list of reports filtered on the selected tag.

From *Ratings & Reviews* area on the bottom-right, you can:

- Click the *Write to us* link to open an email message and send a query.
- Rate the report by clicking the stars at the bottom-right of the page.

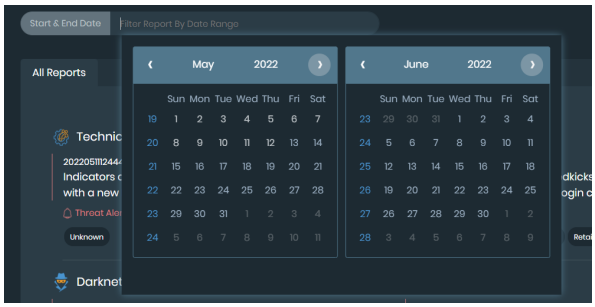


Filtering analyst reports

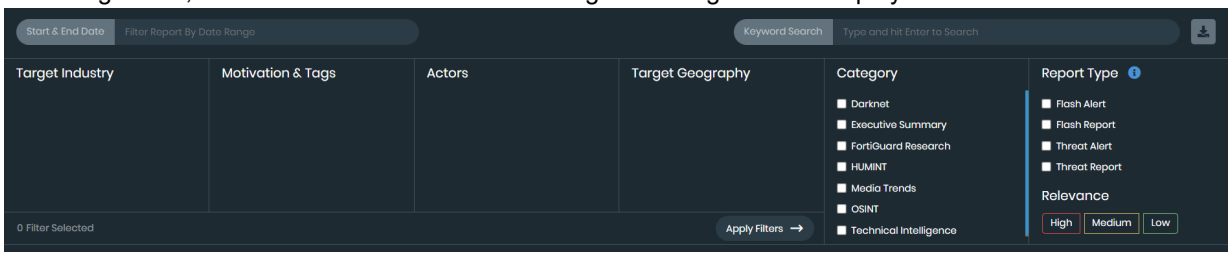
Reports can by filtered by date range, keywords, categories of filters, and relevance to your organization.

To filter reports:

1. Go to *Adversary Centric Intelligence* > *Reports* > *Analyst Reports*.
2. Filter reports by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.

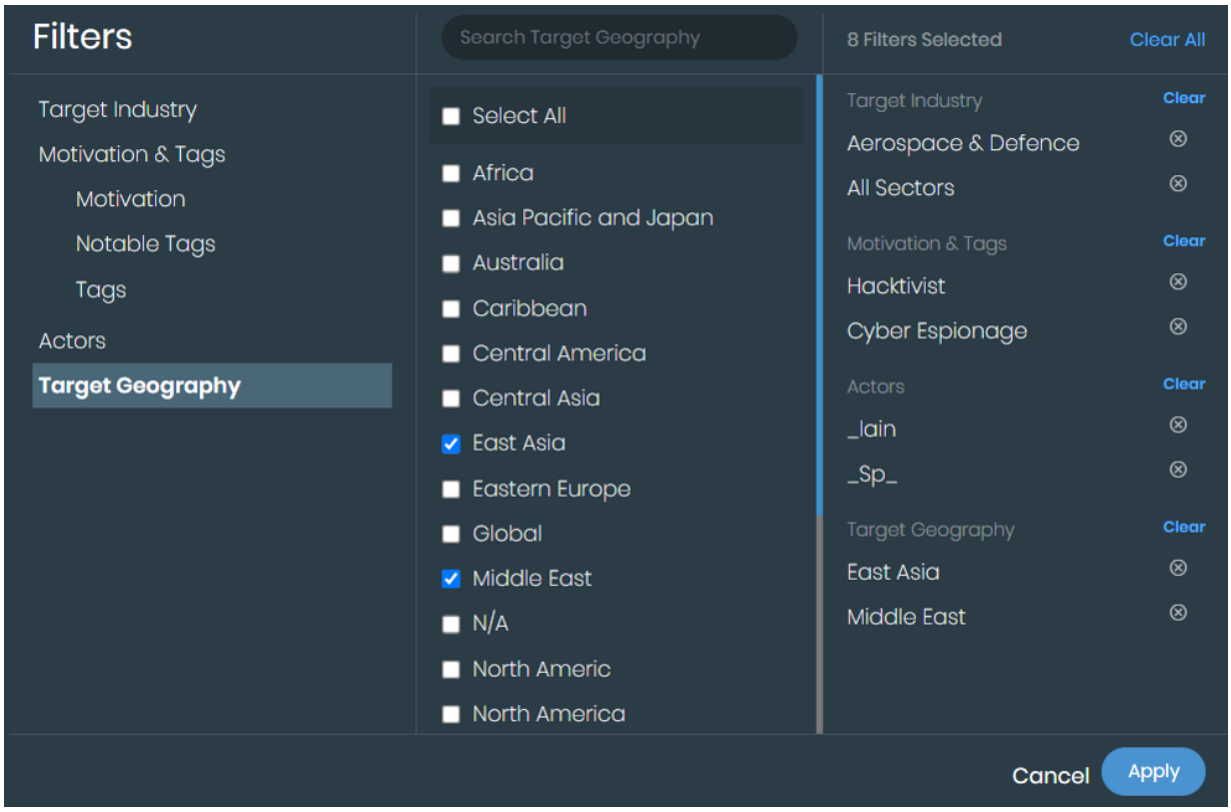


   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range.
   Only reports from the date range are displayed.
   d. Click the *Filter Report by Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
   The reports are filtered to display only reports with the keyword.
   b. Click the *X* beside the keyword to remove the filter.
4. Filter reports by categories:
   a. On the right side, click the *Filters* button. The following filter categories are displayed:



   - *Target Industry*
   - *Motivation & Tags*
   - *Actors*
   - *Target Geography*
   - *Category*
   - *Report Type*

   b. Click *Apply Filters*, and select one or more filters for *Target Industry*, *Motivation & Tags*, *Actors*, and *Target Geography* categories. Click *Apply*.



To clear all the selected filters click *Clear All*. To clear the selected filters for a specific category, click *Clear* next to the category name in the *Filters Selected* pane.

c. Under *Category* and *Report Types*, select checkboxes to enable the filters, and clear checkboxes to disable filters.

d. Under *Report Type* > *Relevance*, click *High*, *Medium*, and/or *Low* to enable the filters, and clear the filters to disable them.

Downloading analyst reports and observables

You can download a PDF of the reports displayed on the *Adversary Centric Intelligence* > *Reports* page to your hard drive. A maximum of 300 reports can be downloaded at one time.

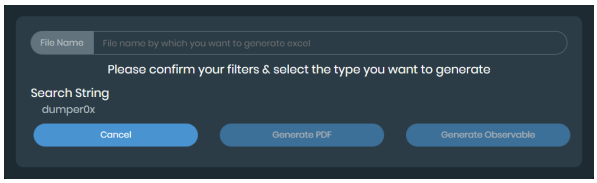
When the report includes Indicators of Compromise (IOCs), you can click the *Generate Observable* button to download the IOCs in Microsoft Excel format.

When you open a report, you can download a PDF of the open report.

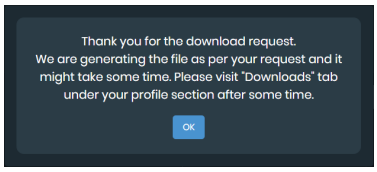
To download reports:

1. Go to *Adversary Centric Intelligence* > *Reports* > *Analyst Reports*.
2. Filter the reports. See Filtering analyst reports on page 142.
   The filtered list of reports is displayed.
3. (Optional) Select which of the filtered reports to download:
   a. Click the *Download Specific Reports* button. Checkboxes are displayed beside each report title.
   b. Select the checkbox beside each report you want to download.

4. Click the *Downloads* button. A confirmation dialog is displayed.



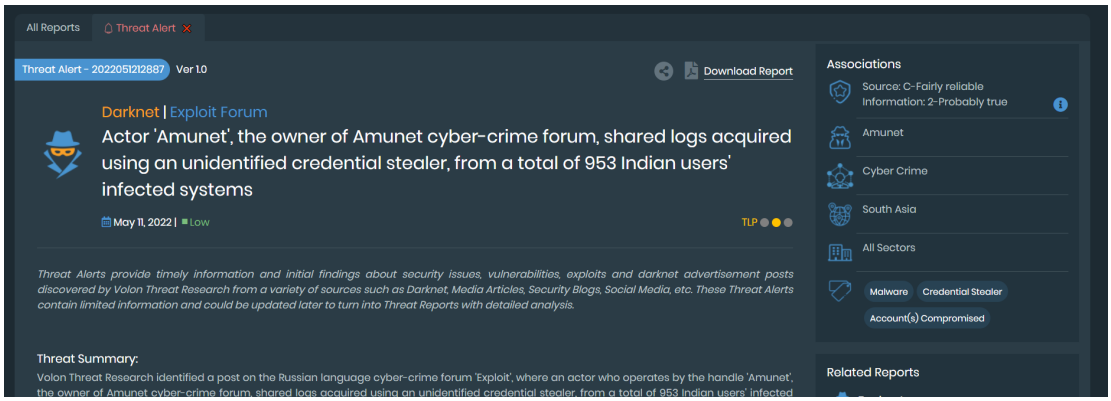
5. In the *File Name* box, type a name.
6. (Optional) If the report contains IOC information, you can click *Generate Observable* to download IOC information in Microsoft Excel format.
7. Click *Generate PDF*.
   A dialog is displayed.



8. Click *OK*.
9. Retrieve the download. See Retrieving downloads on page 203.

To download a PDF from an open report:

1. Go to *Adversary Centric Intelligence* > *Reports*.
2. Click a report to display its details.



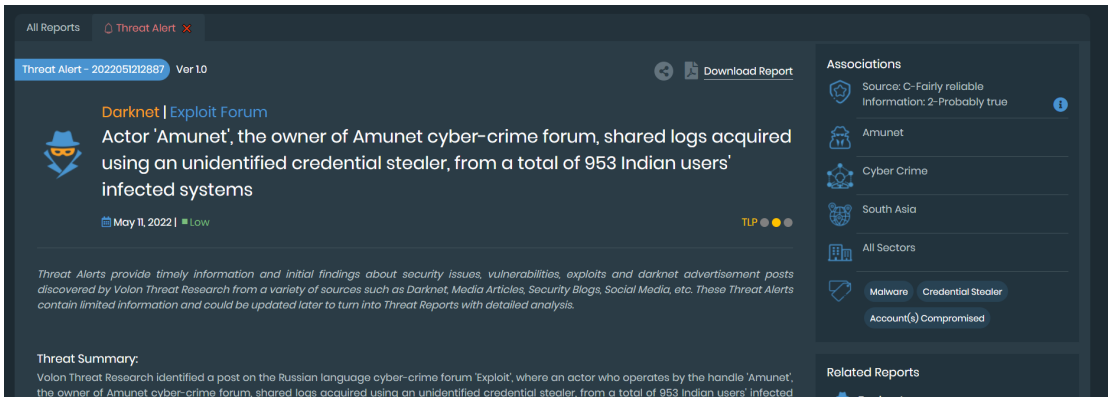
3. Click the *Download Report* button.
   A PDF of the report is downloaded to your computer.

Sharing analyst reports

You can share reports by using a link or an email.

To share a report:

1. Go to *Adversary Centric Intelligence* > *Reports* > *Analyst Reports*.
2. Click a report to display its details.



3. Click the *Share Link* button.
   The *Email* and *Copy Link* buttons are displayed.

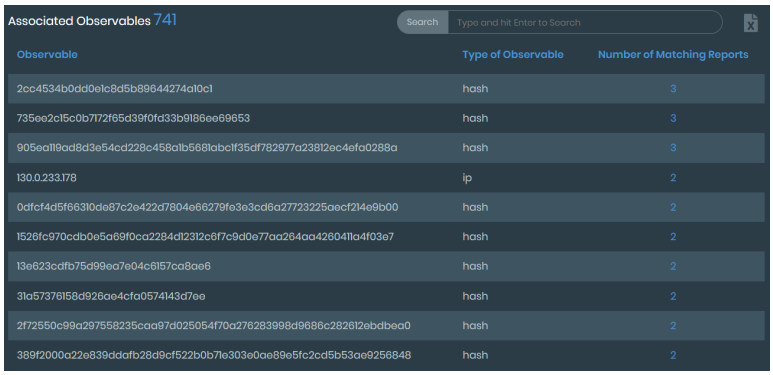
Exporting observables

When a report has associated observables, they are displayed at the bottom of the report in the *Associated Observables* section.

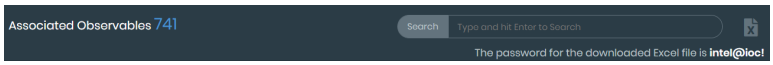
You can download the list of observables in Microsoft Excel format. The downloaded file is password protected. FortiRecon provides the password you need to open the file in Microsoft Excel.

To export observables:

1. View a report. See Viewing analyst reports on page 141.
2. Scroll down to the *Associated Observables* section.
   In the following example, the report has 741 associated observables:



3. On the right, click the *Download Observables* button.
   The password for the download is displayed. In the following example, the password is *intel@ioc!*.



The excel file is downloaded to your computer.

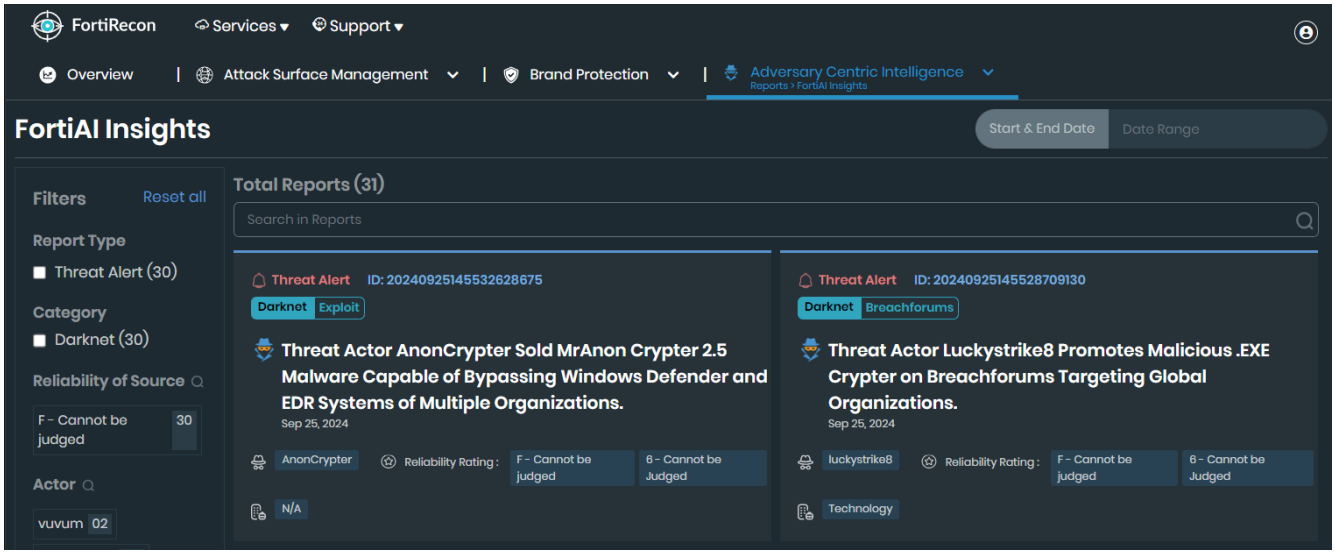
4. Open the Excel file.
   You are prompted for the password.
5. Type the password from FortiRecon, and click *OK*. The Excel file opens.

FortiAI Insights

The *Adversary Centric Intelligence* > *Reports* > *FortiAI Insights* page displays threat intelligence reports generated by our proprietary artificial intelligence, FortiAI. These reports provide enhanced threat understanding, proactive risk assessment, and faster incident response.

From *Adversary Centric Intelligence* > *Reports* > *FortiAI Insights*, you can:

- View, download, or share reports. See Viewing FortiAI Insights reports.
- Apply filters to the list of reports to hone in on specific reports. See Filtering FortiAI Insights reports.



Viewing FortiAI Insights reports

You can filter and search the list of FortiAI Insights reports using keywords. See Filtering FortiAI Insights reports.

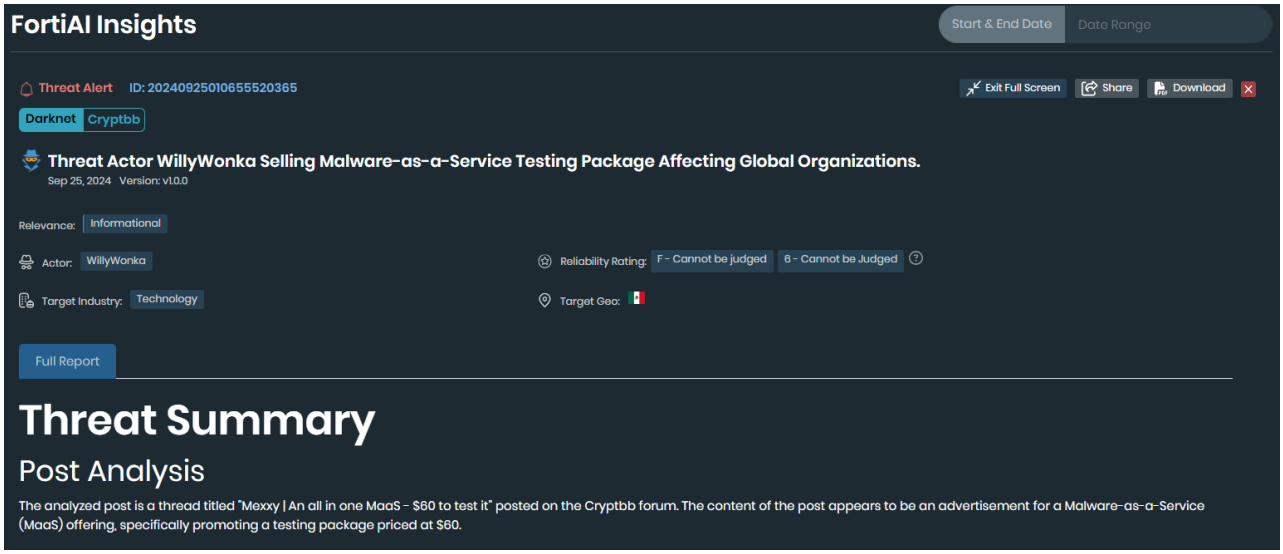
When you open a report, its details are displayed in the right pane. You can also download the report as a PDF or share it with others.

To view FortiAI Insights reports:

1. Go to *Adversary Centric Intelligence* > *Reports* > *FortiAI Insights*.
2. Click a report title to display the report details in right pane. The following information is displayed.
   - *Threat ID*: A unique identifier for the report.
   - *Source*: The origin of the threat intelligence.

- *Report Title*: A concise description of the report's content.
- *Report Date*: The date the report was generated.
- *Threat Actor*: The identified entity responsible for the threat.
- *Reliability Rating*: An assessment of the report's credibility. Click the help icon for information on how reliability ratings are assigned.
- *Target Industry*: The specific industry or sector targeted by the threat.
- *Target Geo*: The geographical region affected by the threat.
- *Full Report*: A detailed overview of the threat, including post-analysis, threat actor details, affected organizations, key indicators, and additional information.

3. Click *View Full Screen* to view the report in full-screen mode.
4. Click the *Share* to copy the report link or share the link in an email.
5. Click the *Download* link to download a PDF of the report.

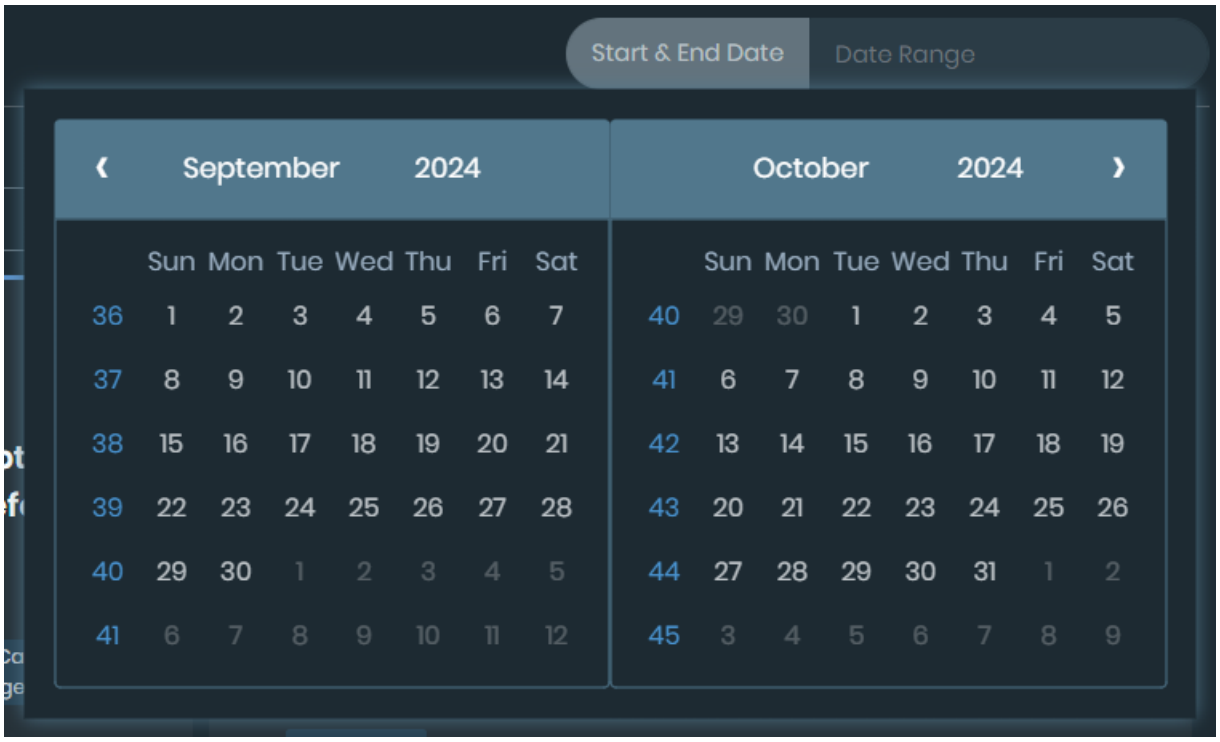


Filtering FortiAI Insights reports

Reports can by filtered by date range, keywords, and categories of filters.

To filter reports:

1. Go to *Adversary Centric Intelligence* > *Reports* > *FortiAI Insights*.
2. Filter reports by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.



   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range.
   Only reports from the date range are displayed.
   d. Click the *Filter Report by Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Search in Reports* box, type a keyword, and press *Enter*.
   The reports are filtered to display only reports with the keyword.
   b. Click the *X* beside the keyword to remove the filter.
4. Filter reports by categories:
   a. In the *Filters* pane on the left side, the following filter categories are displayed:
      - *Report Type*
      - *Category*
      - *Reliability of Source*
      - *Actor*
      - *Target Geography*
      - *Motivation*
   b. Select the available filters in the category you want to filter.
   To clear all the selected filters click *Reset All*. To clear any individual selected filter, select it again to deselect.

Card Fraud

The *Adversary Centric Intelligence* > *Card Fraud* page widget is only displayed for banking organizations that issue credit or debit cards.

The *Adversary Centric Intelligence* > *Card Fraud* page displays information about credit or debit cards that are for sale on darknet marketplaces. From the *Card Fraud* page, you can:

- View a summary of the total number of leaked cards as well as information about each leaked card. See Viewing leaked card information on page 150.
- Filter the information. See Filtering leaked card information on page 150.
- Download the list of leaked cards to Microsoft Excel format. See Exporting a list of leaked cards on page 151.

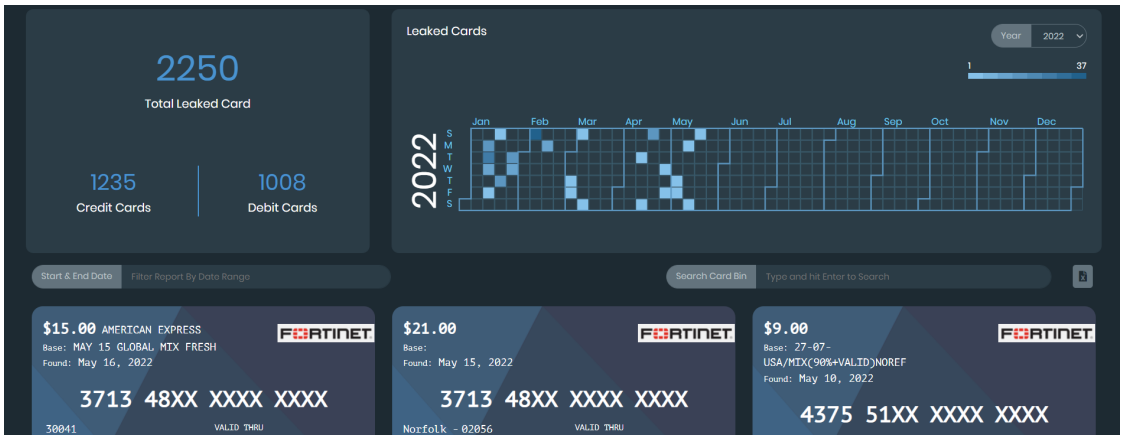
Viewing leaked card information

The *Adversary Centric Intelligence* > *Card Fraud* page displays information about the number of leaked cards as well as details about the leaked cards for a specific date range.

To view leaked card information:

1. Go to *Adversary Centric Intelligence* > *Card Fraud*. The *Card Fraud* page is displayed.

   The *Total Leaked Card*, *Credit Cards*, and *Debit Cards* numbers are for the default date range. Details about the leaked cards are displayed below.



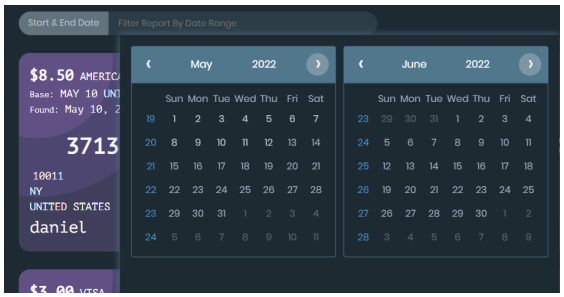
2. You can filter the displayed information. See Filtering leaked card information on page 150.

Filtering leaked card information

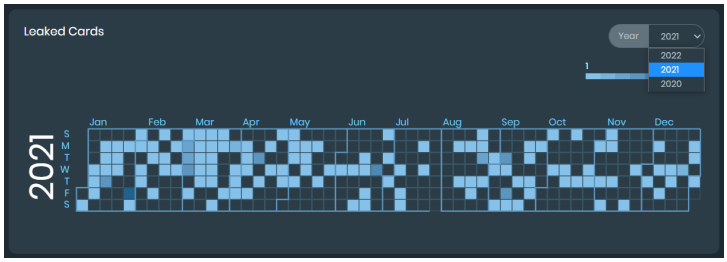
You can filter information about leaked cards by year, date range, and bank identification number (BIN).

To filter leaked card information:

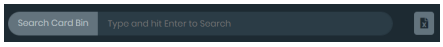
1. Go to *Adversary Centric Intelligence* > *Card Fraud*.
2. Filter reports by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.



   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range. Only reports from the date range are displayed.
   d. Click the *Filter Report by Date Range* box, and click *X* to remove the date range filter.
3. Filter by year:
   a. In the *Leaked Cards* widget, select a year from the dropdown list.



4. Filter by card BIN:
   a. In the *Search Card Bin* box, type a BIN, and press *Enter*.

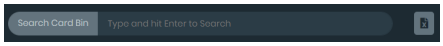


Exporting a list of leaked cards

You can download the list of leaked cards to a Microsoft Excel file.

To export leaked cards:

1. Go to *Adversary Centric Intelligence* > *Card Fraud*.
2. Beside the *Search Card Bin* box, click the *Export Leaked Cards* button.



   The *Leaked Card.xlsx* file is downloaded.
3. Open the file in Microsoft Excel.

Stealer Infections

The *Adversary Centric Intelligence* > *Stealer Infection* page includes information about possible infected systems that are affiliated with your employees or end-users that are listed for sale on credential stealer darknet marketplaces. The compromised system information is organized into two tabs:

1. **Leaked** - The *Compromised Systems(Leaked)* tab displays the stolen data that has been shared over Darknet forums, Telegram channels, Tor sites or any other medium where the threat actor operates. See Viewing leaked compromised systems.
2. **On Sale** - The *Compromised Systems(On Sale)* tab displays the stolen data that is currently being offered for sale on various Darknet marketplaces. See Viewing on sale compromised systems.

On the *Stealer Infection* page, you can:

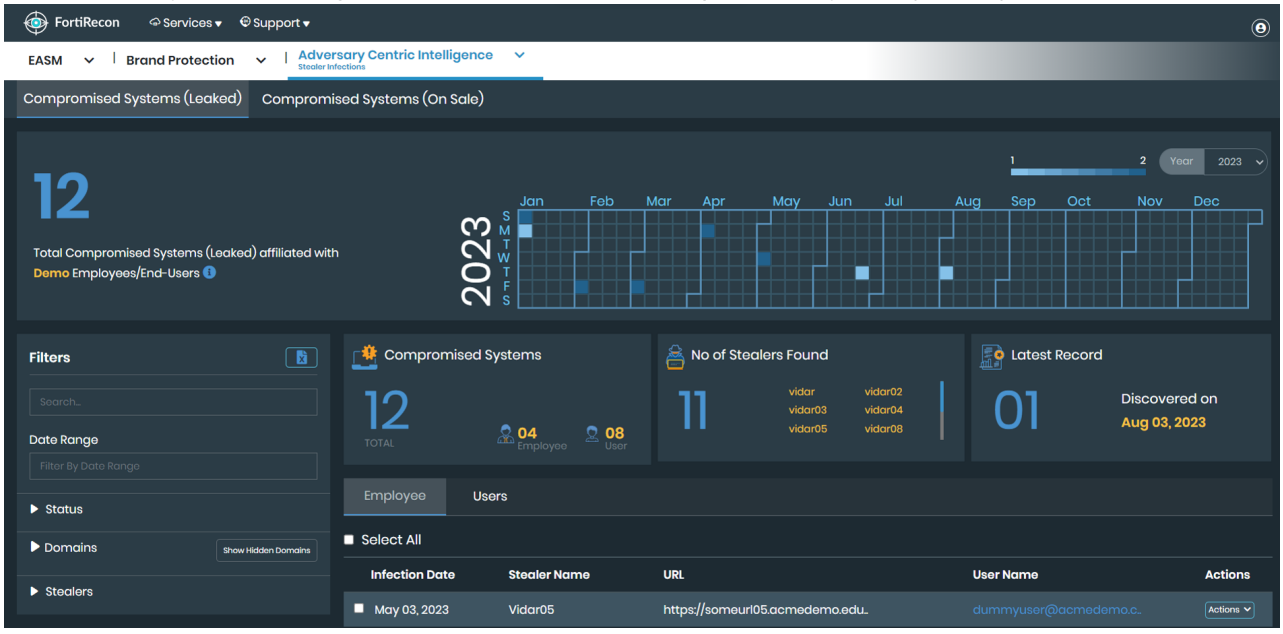
- Filter stealer infection information. See Filtering stealer infection information on page 155.
- Export market place data. See Exporting stealer infections data on page 157.

Viewing leaked compromised systems

The *Adversary Centric Intelligence* > *Stealer Infections* > *Compromised Systems(Leaked)* page displays information about possible infected systems that are affiliated with your employees or end-users that has been shared over Darknet forums, Telegram channels, Tor sites or any other medium where the threat actor operates.

To view leaked compromised systems information:

1. Go to *Adversary Centric Intelligence* > *Stealer Infections* > *Compromised Systems(Leaked)*.



2. Use the following widgets to review information about leaked compromised systems:

Total Compromised Systems (Leaked) affiliated with <organization name>	Displays the total number of compromised systems leaked affiliated with your organization. The calendar displays a summary of the leaked stealer events in the selected calendar year. Colored blocked indicate a stealer event. Light colors blocks indicate few affected credentials, and dark colored blocks indicate many affected credentials. Hover your mouse over each block to view the discovery date and the number of affected credentials.
Compromised Systems	Displays the total number of compromised systems including affected employees and end-users count.
No of Stealers Found	Displays the number of stealers found and the names of the stealers.
Latest Record	Displays the latest number of stealer events and the date that the event was discovered.
Employee	Displays a list of affected employees information.
Users	Displays a list of affected end-users information.

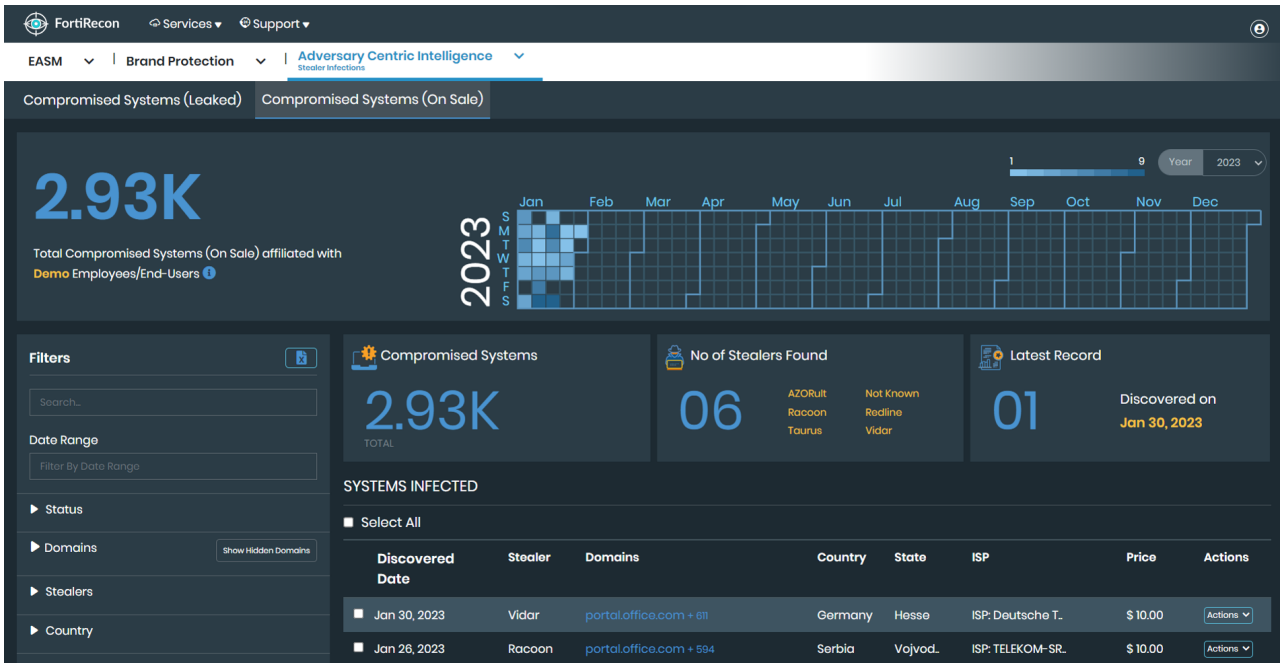
The values in all widgets are updated based on the filters applied, except for *Total Compromised Systems(Leaked) affiliated with <organization name>* value.

Viewing on sale compromised systems

The *Adversary Centric Intelligence* > *Stealer Infections* > *Compromised Systems(On Sale)* page displays information about possible infected systems that are affiliated with your employees or end-users and are for sale on darknet market places.

To view on sale compromised systems information:

1. Go to *Adversary Centric Intelligence* > *Stealer Infections* > *Compromised Systems(On Sale)*.



2. Use the following widgets to review information about on sale compromised systems:

Total Compromised Systems (On Sale) affiliated with <organization name>	Displays the total number of compromised systems on sale affiliated with your organization. The calendar displays a summary of the on sale stealer events in the selected calendar year. Colored blocked indicate a stealer event. Light colors blocks indicate few affected credentials, and dark colored blocks indicate many affected credentials. Hover your mouse over each block to view the discovery date and the number of affected credentials.
Compromised Systems	Displays the total number of compromised systems.
No of Stealers Found	Displays the number of stealers found and the names of the stealers.
Latest Record	Displays the latest number of stealer events and the date that the event was discovered.
Systems Infected	Displays a list of infected systems.

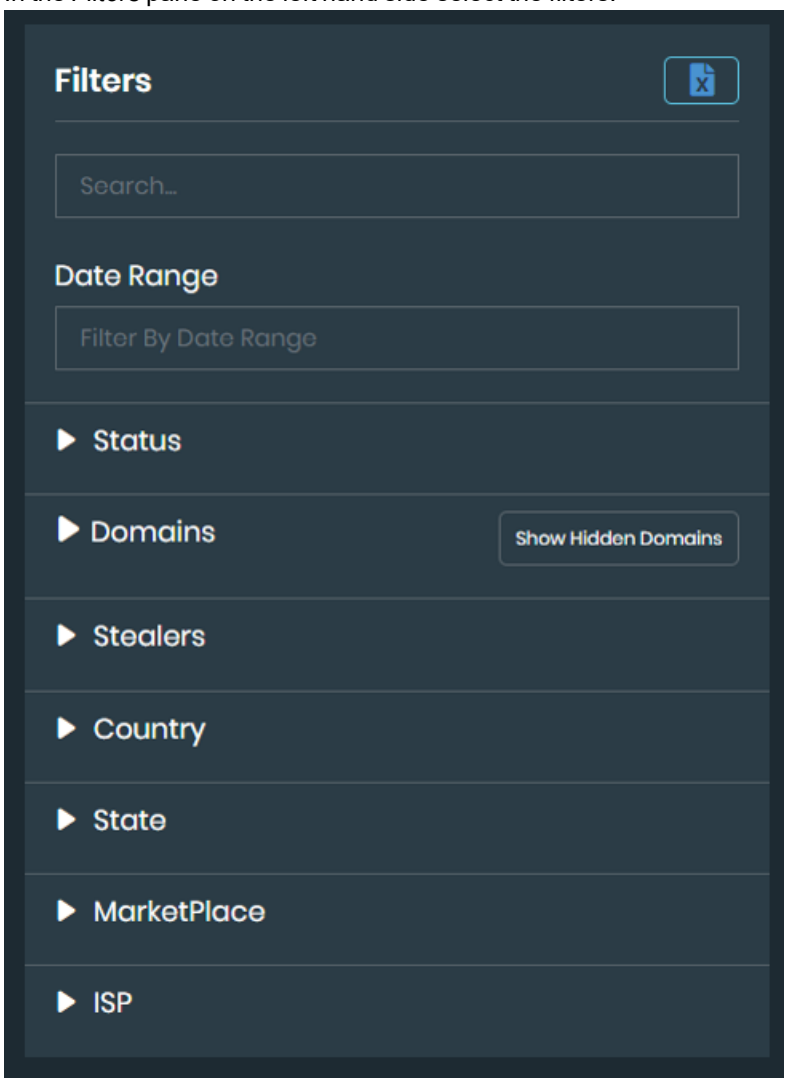
The values in all widgets are updated based on the filters applied, except for *Total Compromised Systems(On Sale) affiliated with <organization name>* value.

Filtering stealer infection information

You can use several methods to filter information in the *Stealer Infections* .

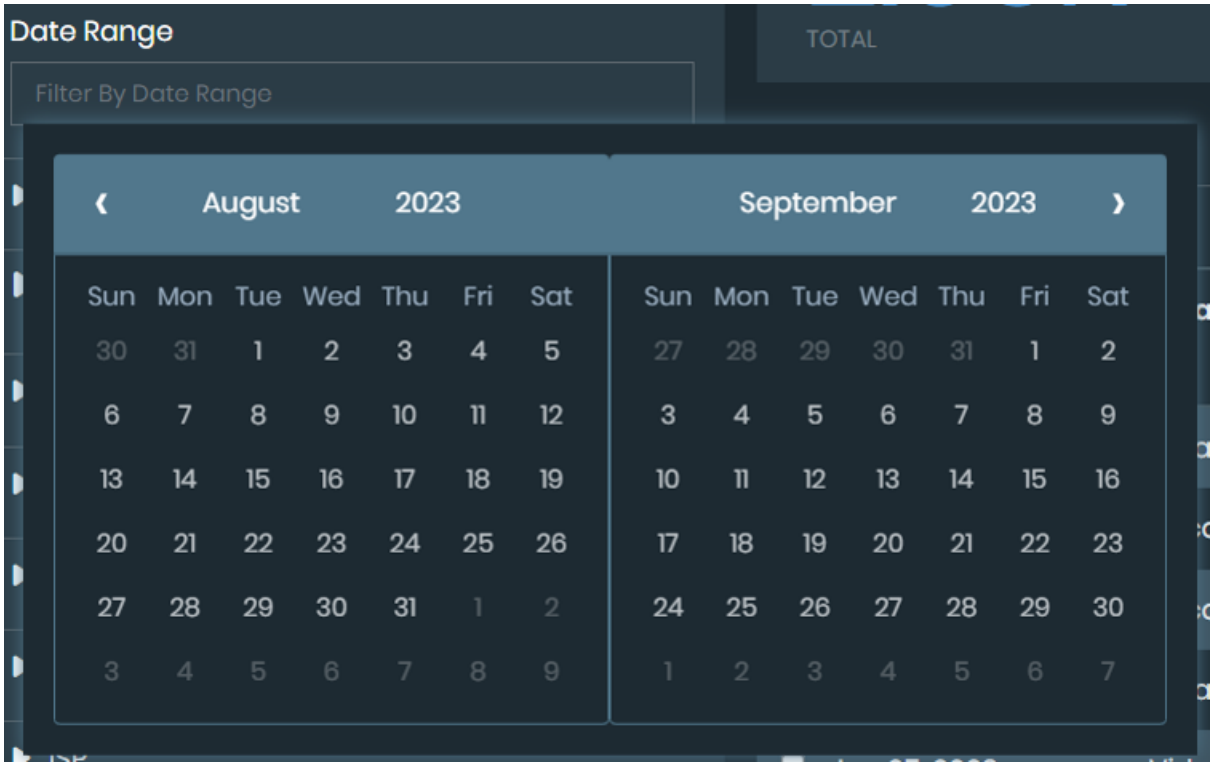
To filter stealer infection information:

1. Go to *Adversary Centric Intelligence* > *Stealer Infections*.
2. Select the desired tab *Compromised Systems(Leaked)* or *Compromised Systems(On Sale)*.
3. In the *Filters* pane on the left hand side select the filters.

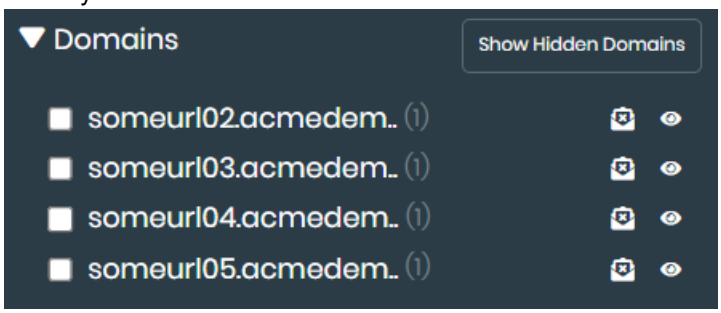


4. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
      The information is filtered.
   b. Clear the keyword and press *Enter* to remove the filter.

5. Filter information by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.

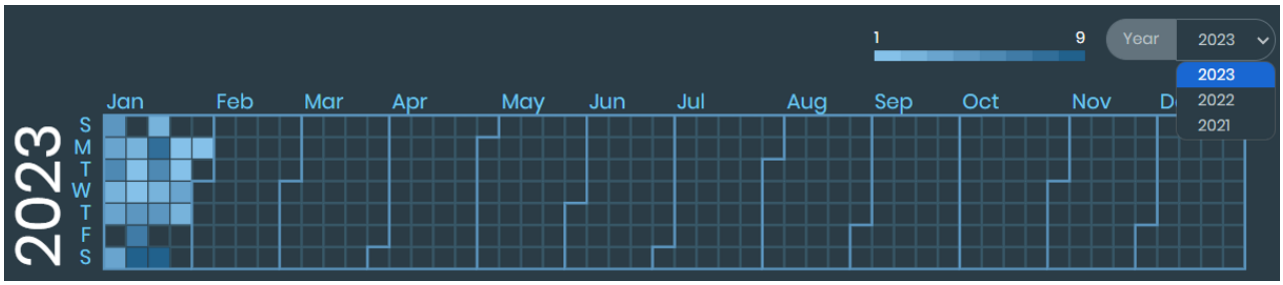


   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range.
   Only information from the date range is displayed.
   d. Click the *X* in the *Start & End Date* box to remove the date range filter.
6. Click *Active* or *Resolved* to filter by status.
7. Filter by domains.



   a. Click desired domains to filter.
   b. Click  icon next to desired domain to unsubscribe and stop email notifications.
   c. Click  icon next to desired domain to hide the domain.
   d. Click *Show Hidden Domains* to view hidden domains. Click  icon next to the desired hidden domain to unhide.
8. Click stealers to filter the data based on a specific stealers.

9. The following additional filters are available for *Compromised Systems(On Sale)* page. Click desired values to filter.
   - *Country*
   - *State*
   - *Marketplace*
   - *ISP*
10. Filter the events by year using *Calendar* widget:

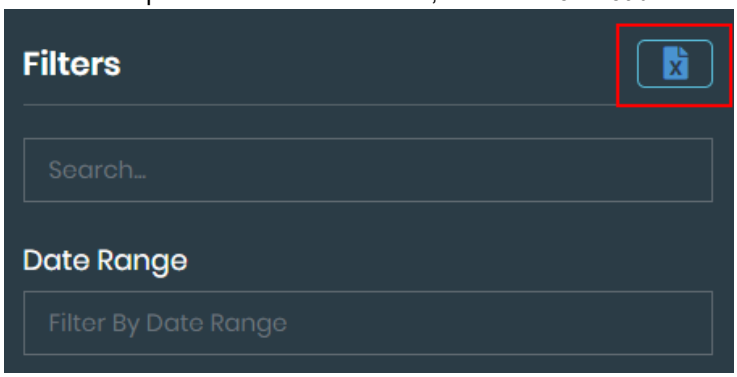


Exporting stealer infections data

You can download the stealer infections information to an *All Market Place.xlsx* file in Microsoft Excel format.

To export stealer infections information:

1. Go to *Adversary Centric Intelligence* > *Stealer Infections*.
2. Select the desired tab *Compromised Systems(Leaked)* or *Compromised Systems(On Sale)*.
3. (Optional) Filter the data. See Filtering stealer infection information on page 155.
4. In the Filters pane on the left hand side, click the *Download* icon.



5. An *All Market Place.xlsx* file is downloaded.

OSINT Cyber Threats

Open Source Intelligence (OSINT) is method of gathering threat intelligence from publicly available sources. Over time, OSINT coverage has changed to a great extent. Previously, it only covered sources such as Blogs, news, business websites, social networks, and so on.

The *Adversary Centric Intelligence* > *OSINT - Cyber Threats* page provides you the ability to stay up to date with information published in open source platforms, such as social media, GitHub repositories, and so on. Information for review is based on specific criteria, including:

- Exploited vulnerabilities
- Zero day vulnerabilities
- Global events

On the *OSINT - Cyber Threats* page, you can:

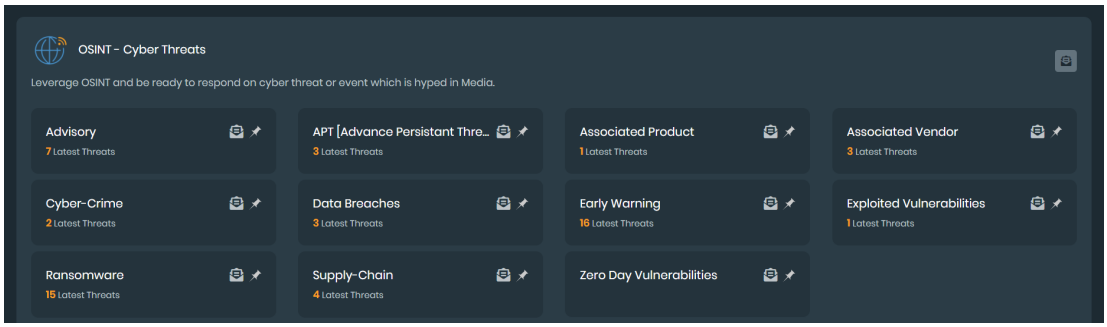
- Review threat events. See Reviewing threats on page 158.
- Pin threat events to the top of the list. See Pinning events on page 159.
- Subscribe to threat event notifications. See Subscribing to event notifications on page 159.
- Subscribe other FortiRecon users to event notifications. See Adding subscriptions on page 161.

Reviewing threats

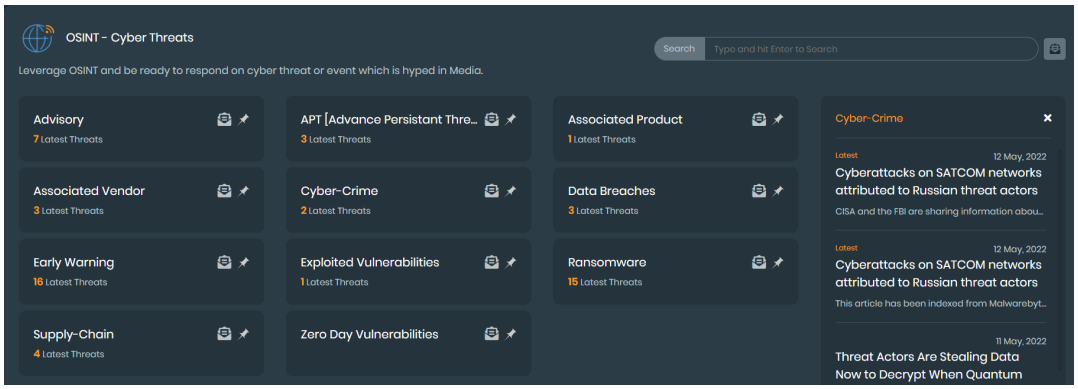
You can view more information about each threat.

To review threats:

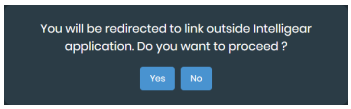
1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*. The list of events is displayed.



2. Click an event title, such as *Cyber-Crime*. The list of events is displayed on the right side.
In the following example, *Cyber-Crime* is selected:



3. On the right, click the event to display more information about it outside the FortiRecon portal.
A confirmation dialog is displayed.



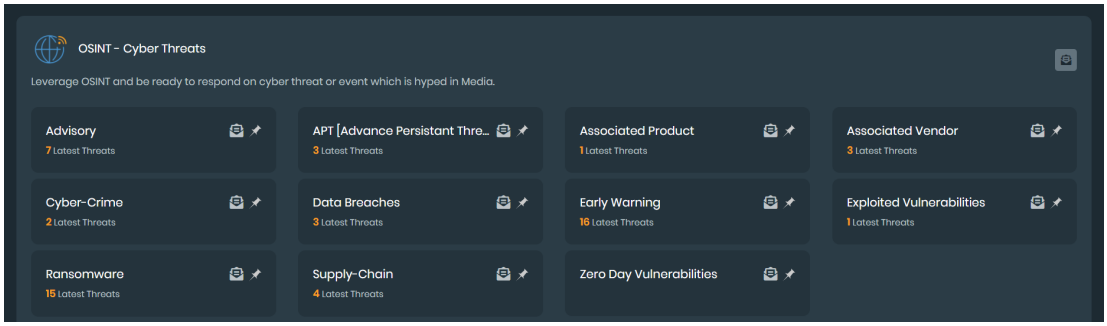
4. Click *Yes* to open the link in a new tab in your browser.

Pinning events

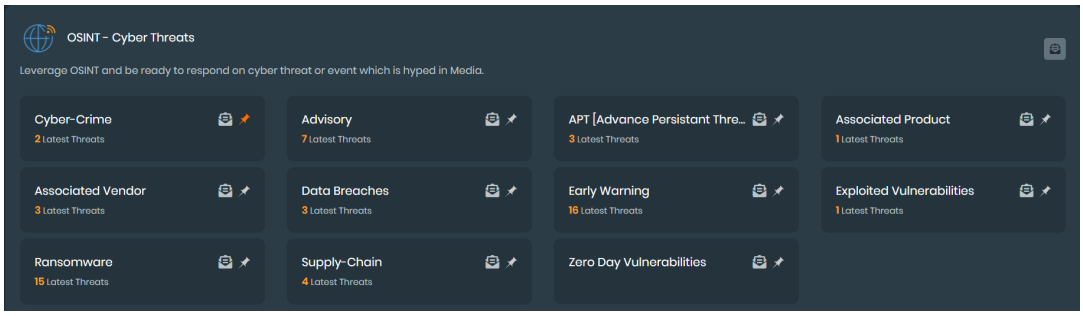
You can pin events to the top of the list. Pinned events have an orange *Pin* icon. Unpinned events have a white *Pin* icon.

To pin events:

1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*. The list of events is displayed.



2. Click the *Pin* icon beside an event to turn the pin orange and pin the event to the top of the list. In the following example, *Cyber-Crime* is pinned to the top of the list.



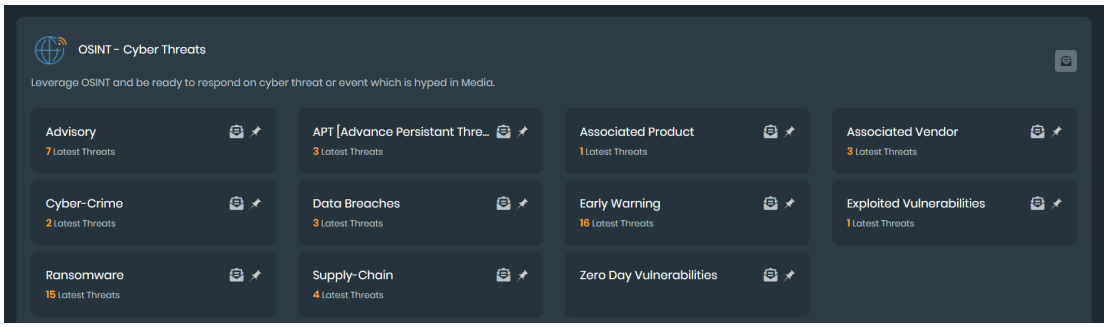
Click the *Pin* icon again to turn the pin white and unpin the event from the top of the list.

Subscribing to event notifications

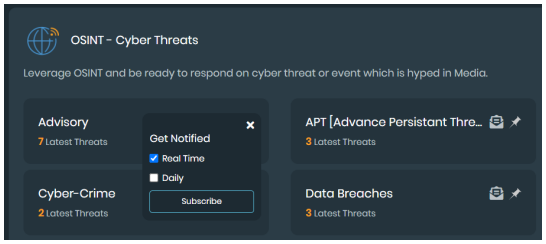
You can enable subscriptions to receive notifications for one or more threat events. You can also change subscriptions and unsubscribe.

To subscribe to event notifications:

1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*. The list of events is displayed.



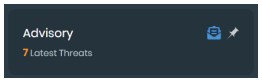
2. For an event, click the *Subscribe* icon. The subscription options are displayed for the event.
In the following example, subscription options are displayed for the *Advisory* event:



3. Select one of the following options to specify when to receive the notification:

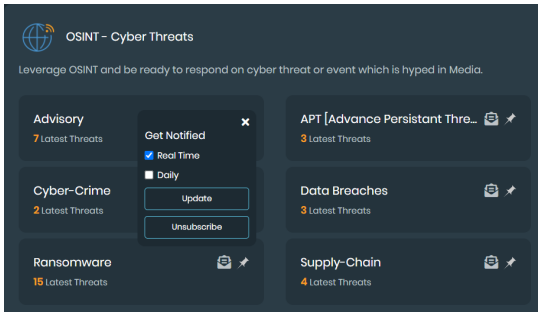
Real time	Select to receive a notification when a new threat event is published.
Daily	Select to specify the time each day to receive a notification about new threat events.

4. Click *Subscribe*.
The *Subscribe* icon turns blue.



To change event notifications:

1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*. The list of events is displayed.
2. Click a blue *Subscribe* icon. The subscription options are displayed.



3. Change when you get notified, and click *Update*.

To unsubscribe from event notifications:

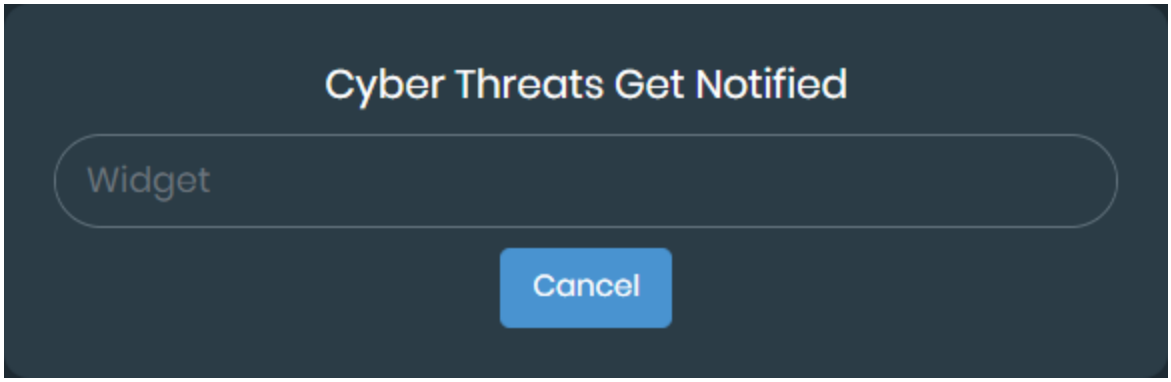
1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*. The list of events is displayed.
2. Click a blue *Subscribe* icon. The subscription options are displayed.
3. Click *Unsubscribe*.
   The *Subscribe* icon turns white, and notifications are turned off.

Adding subscriptions

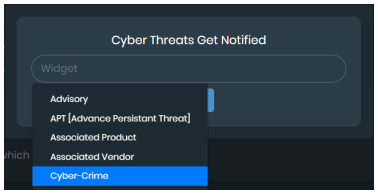
FortiRecon users with Admin privilege can set up subscriptions for other FortiRecon users to receive notifications about events.

To add subscriptions:

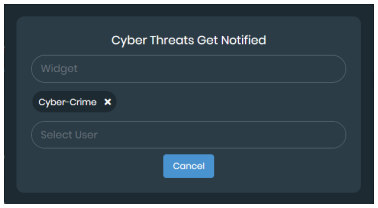
1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*, and click the *Add Subscription* button. The *Cyber Threats Get Notified* dialog is displayed.



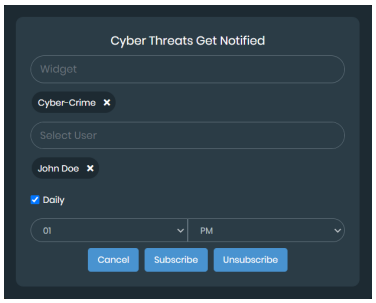
2. Click the *Widget* box, and select the threat events.
   In the following example, *Cyber-Crime* is selected.



   The *Select User* box is displayed.



3. In the *Select User* box, select a user.



   The *Daily* check box is displayed. By default users receive notifications in real-time as events occur.
4. Select *Daily* specify what time each day the user should receive the notification.
   Clear the *Daily* check box to receive notifications in real time.
5. Click *Subscribe*.

Vulnerability Intelligence

The *Adversary Centric Intelligence* > *Vulnerability Intelligence* page displays information on vulnerability exposure to help prioritize vulnerability patching. From the *Vulnerability Intelligence* page, you can:

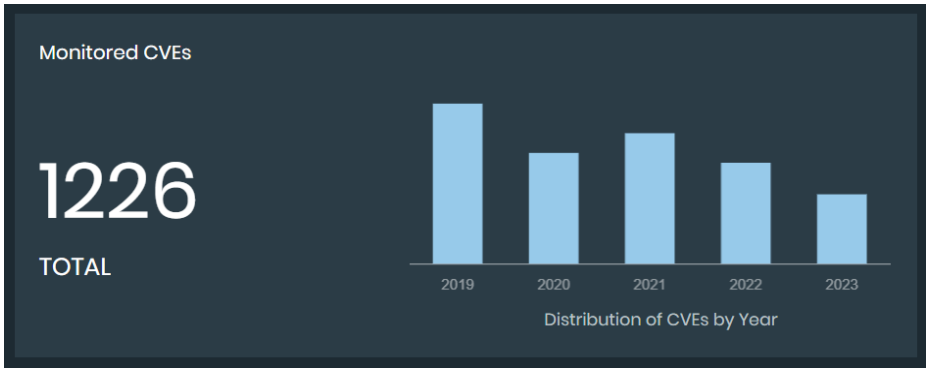
- Review known CVEs. See Vulnerability exposure on page 162.
- Review the notable global CVEs. See Global notable vulnerabilities on page 165.
- View specific CVE reports. See Viewing and filtering CVE reports on page 166.
- Export a list of CVEs. See Exporting CVEs on page 168.
- Bulk add CVEs to monitor. See Manually adding CVEs on page 168.

Vulnerability exposure

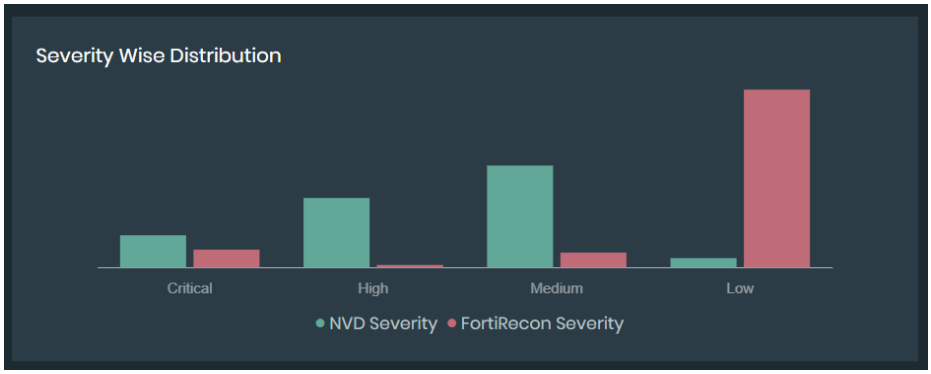
Monitored CVEs can be reviewed at a high level from the *Adversary Centric Intelligence* > *Vulnerability Intelligence* page in the *Vulnerability exposure* section:

Clicking on any chart element or legend item will filter the view and navigate you to a CVE details page pre-populated with the chosen filter.

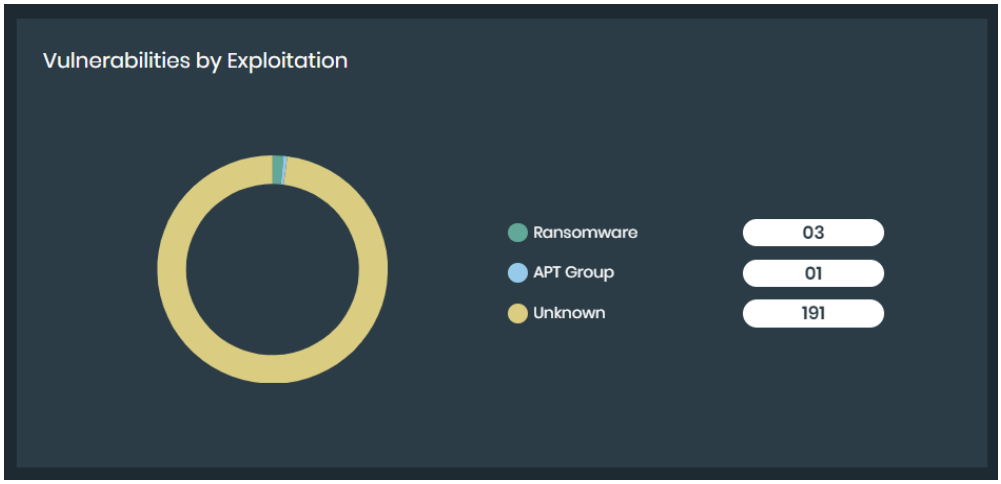
- *Monitored CVEs* : This tile displays the total count of monitored CVEs and distribution of CVEs by year graph.



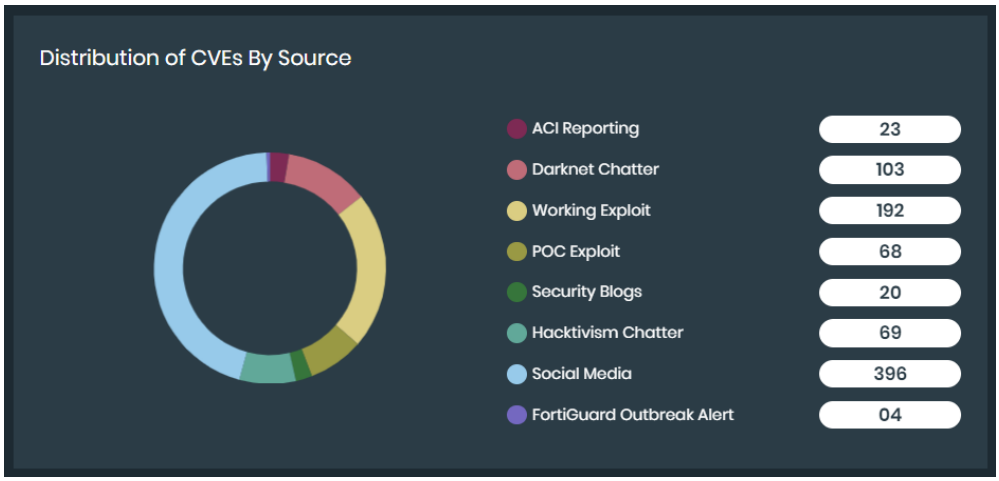
- *Severity Wise Disribution*: This tile displays a graph of CVEs to show the total count of CVEs per rating, from *Low* to *Critical* using both NVD and FortiRecon severity classifications.



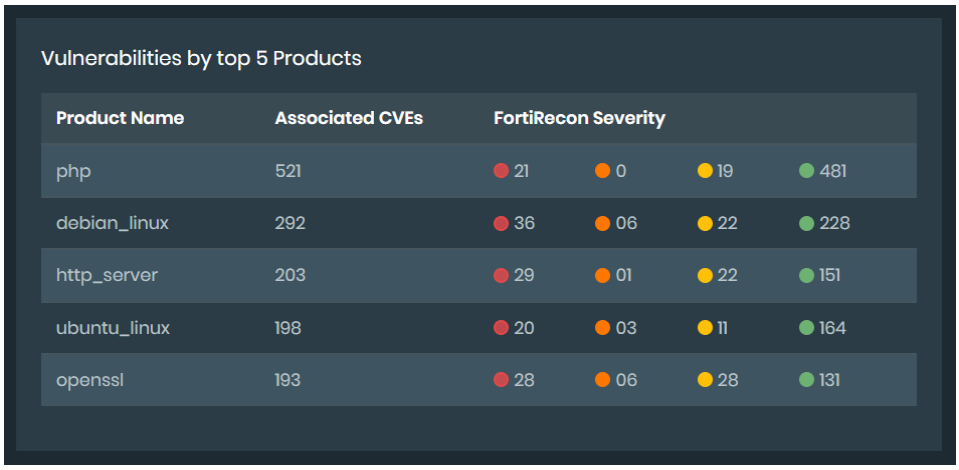
- *Vulnerabilities by Exploitation*: This tile displays the distribution of vulnerabilities based on the availability of known exploits.



- *Distribution of CVEs By Source*: This tile displays the breakdown of CVEs based on their originating source.



- *Vulnerabilities by top 5 Products*: Displays a list of the products with the most CVEs monitored and the severity range from *Low* to *Critical*.



- *Vulnerabilities by top 5 Vendors*: Displays a list of the vendors with the most CVEs monitored and the severity range from *Low* to *Critical*.

- *CVEs from EASM Module*: Displays a list of automatically monitored CVEs. Select the *View All* button to view more information. You sort the data by selecting *Date*, *FortiRecon Severity*, or *NVD Severity* from the dropdown. See Viewing and filtering CVE reports.

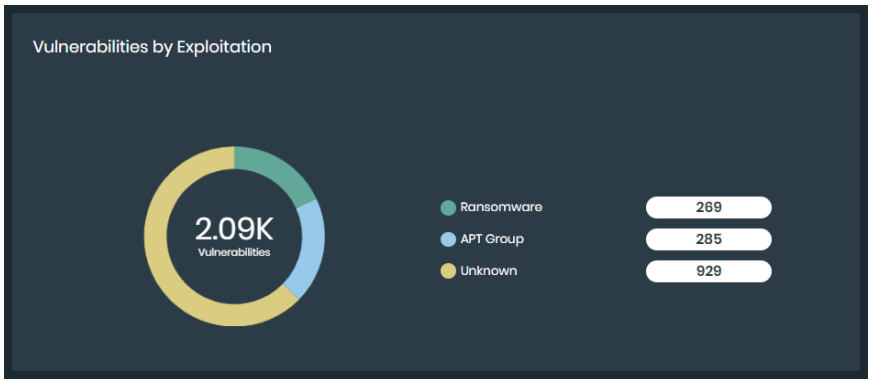
- *CVEs added Manually*: Displays a list of CVEs added by the user.

Global notable vulnerabilities

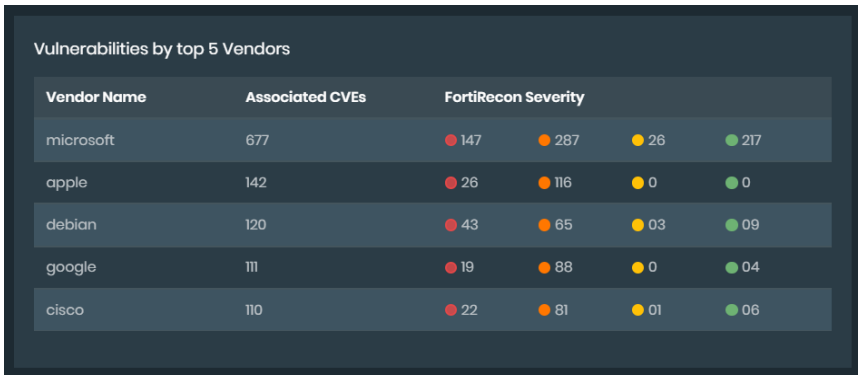
Monitored CVEs can be reviewed at a high level from the *Adversary Centric Intelligence* > *Vulnerability Intelligence* page in the *Global notable vulnerabilities* section:

Clicking on any chart element or legend item will filter the view and navigate you to a CVE details page pre-populated with the chosen filter.

- *Vulnerabilities by Exploitation*: This tile displays the distribution of vulnerabilities based on the availability of known exploits.



- *Vulnerabilities by top 5 Vendors*: Displays a list of the vendors with the most notable CVEs monitored and the severity range from *Low* to *Critical*.



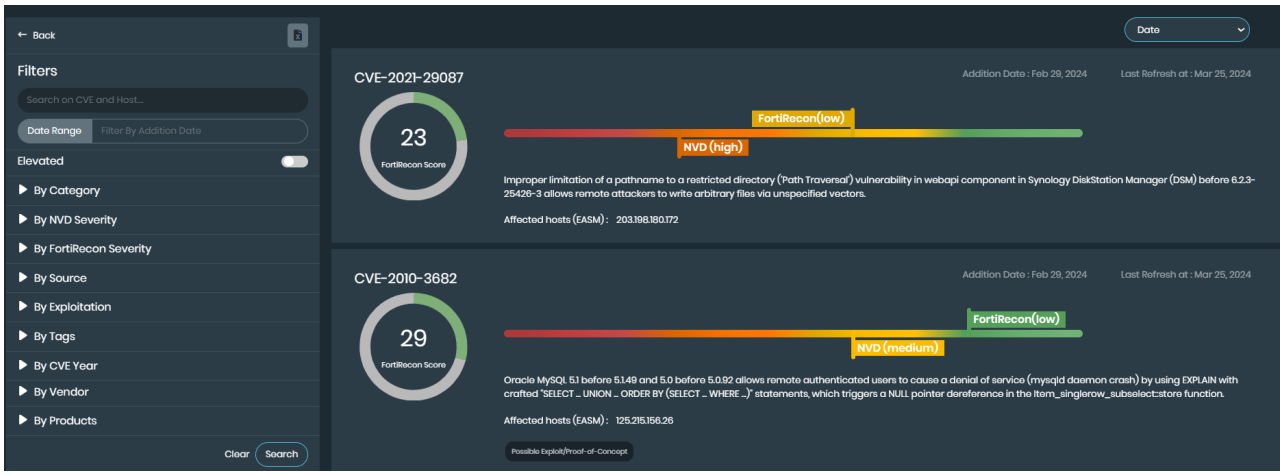
- *Latest 10 Notable CVEs*: Displays a list of the latest notable CVE monitored and the severity range from *Low* to *Critical*. You sort the data by selecting *Date*, *FortiRecon Severity*, or *NVD Severity* from the dropdown. Select the *View All* to view more information. See Viewing and filtering CVE reports.

Viewing and filtering CVE reports

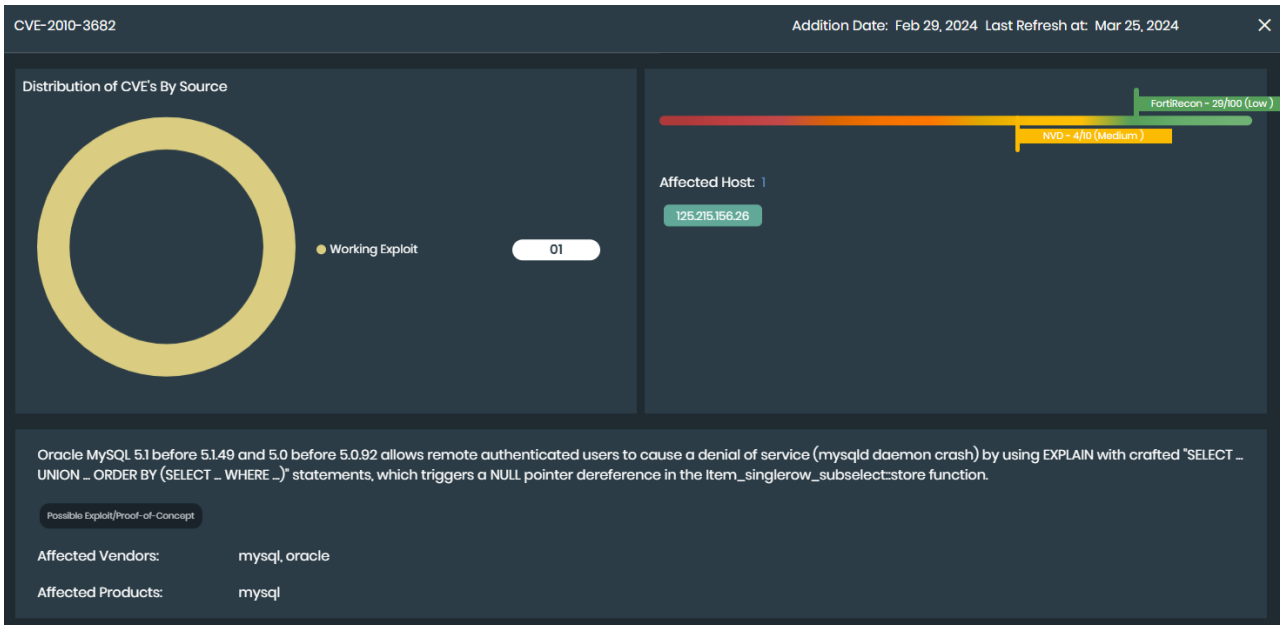
You can review detailed CVE reports in the *Adversary Centric Intelligence* > *Vulnerability Intelligence* page by selecting the *View All* button from the *Vulnerability exposure* > *CVEs from EASM Module*, *Vulnerability exposure* > *CVEs added Manually*, or *Global notable vulnerabilities* > *Latest 10 Notable CVEs* sections.

To filter reports:

1. Go to *Adversary Centric Intelligence* > *Vulnerability Intelligence*.
2. Select *View All* button. The CVE cards page is displayed. You sort the data by selecting *Date*, *FortiRecon Severity*, or *NVD Severity* from the dropdown.



3. Filter information by a date range:
   a. Click *Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range.
   d. Click the *X* to remove the date range filter.
4. Search for keywords:
   a. In the *Search* box, type a keyword.
5. Enable *Elevated* to search for CVEs that have had the severity increased.
6. Filter reports by information:
   a. Select the information dropdown menus:
      - *By Category*
      - *By Addition*
      - *By Severity*
      - *By CVE Year*
      - *By Vendor*
      - *By Products*
   b. Select one or more filters.
7. Click *Search*. The CVE reports that match the filters are displayed.
8. Select the CVE ID to view the full, detailed report.



Exporting CVEs

You can export a list of all or specific CVEs from the CVE cards page to an Excel file. Information in the file includes:

- CVE ID
- Truview Score
- Truview Severity
- NVD Severity
- Description
- Published date

To export CVEs:

1. Go to *Adversary Centric Intelligence* > *Vulnerability Intelligence*.
2. Select *View All* button. The CVE cards page is displayed.
3. Filter for the reports you want included in the Excel file. See Viewing and filtering CVE reports on page 166.
4. Click *Export CVE List*. An Excel file is downloaded to your device.

Manually adding CVEs

You can bulk add CVEs to monitor in the *Vulnerability Exposure* > *CVEs added Manually* tab on the *Adversary Centric Intelligence* > *Vulnerability Intelligence* page.

To manually add CVEs:

1. Go to *Adversary Centric Intelligence* > *Vulnerability Intelligence*.
2. Click *Manage CVEs Watchlist*. The *Manage CVEs* dialog is displayed.

3. Enter the CVE IDs in the text field.
4. Click *Submit*.

Ransomware Intelligence

The *Adversary Centric Intelligence* > *Ransomware Intelligence* page helps with supply chain monitoring and displays information on past and potential ransomware incidents. The information in this module is captured from blogs and sites operated by ransomware operators. The names of victims or potential victims mentioned in this section are purely based on information provided on these sites and blogs. The authenticity of these claims must be validated by your organization.

From the *Ransomware Intelligence* page, you can:

- View past and potential ransomware incidents. See Viewing ransomware intelligence on page 169.
- Filter ransomware incident information. See Filtering ransomware intelligence on page 175.
- Export information on ransomware incidents to an Excel file. See Exporting ransomware information on page 176.
- Create, edit, and monitor a ransomware watchlist. See Managing My Watchlist on page 177.

Viewing ransomware intelligence

The *Ransomware Intelligence* page contains multiple sections that display high level information on the ransomware threat landscape.

- Ransomware Trends
- Ransomware Threat Campaigns
- Watchlist
- Latest Ransomware Victims
- Latest Initial Access Broker (IAB) Victims

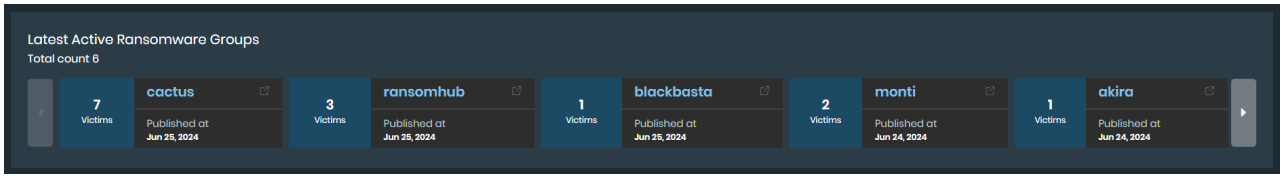
Ransomware Trends

This section provides a high-level view of global ransomware activity.

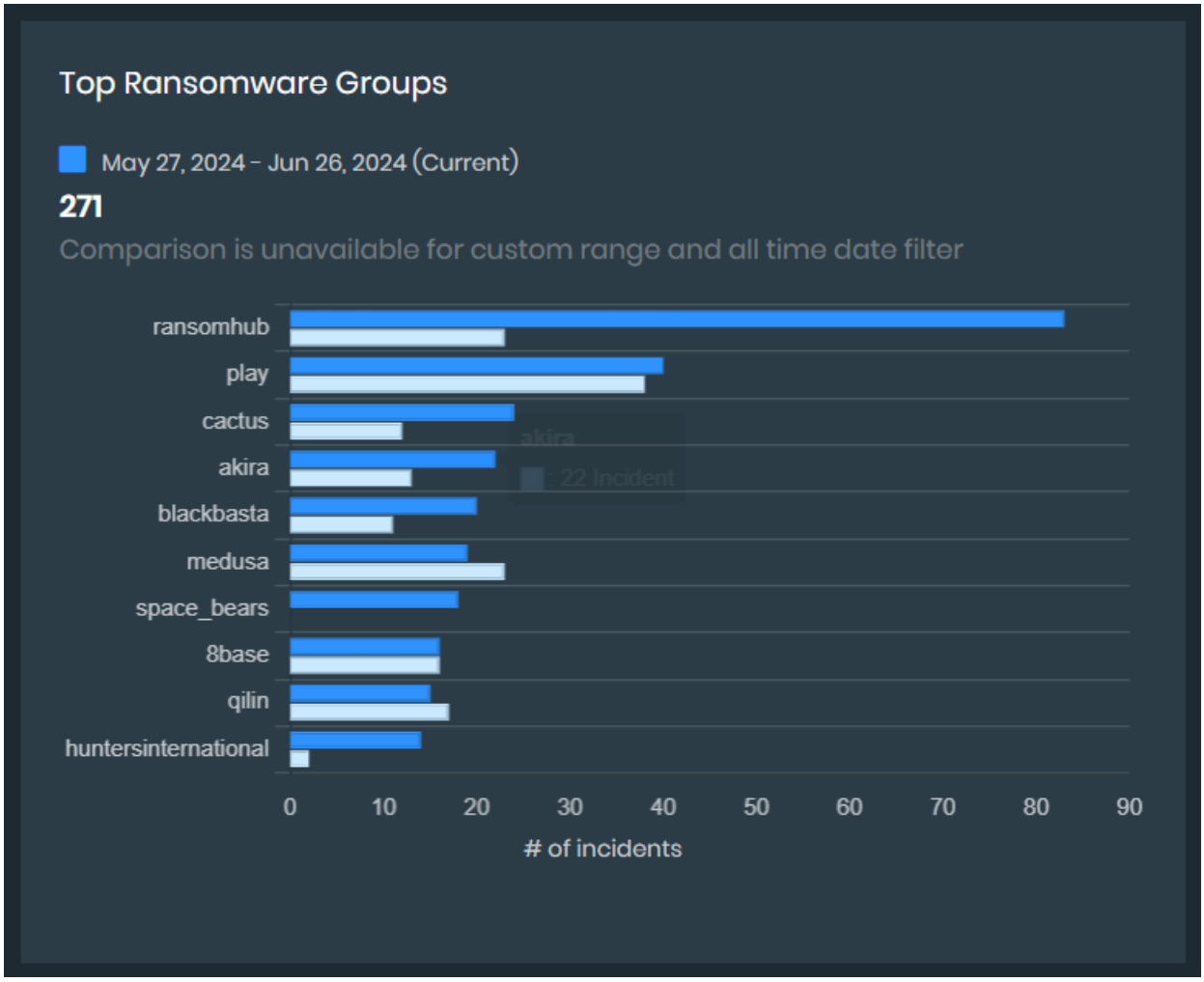
You can filter the data displayed in *Ransomware Trends* using the *Ransomware Group* and *Date* filters.

- *Summary*: A summary of total number of ransomware groups tracked, ransomware victims, most active ransomware groups, top targeted sector, and top victimized countries.

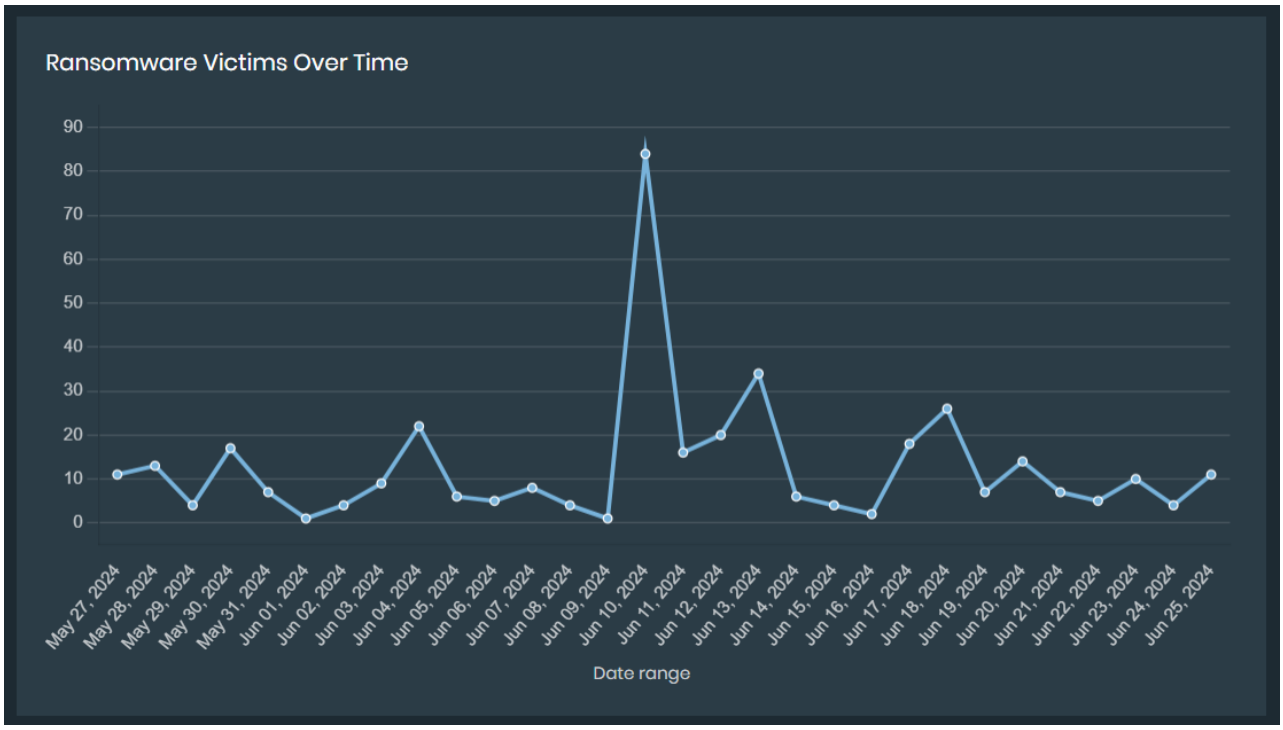
- *Latest Active Ransomware Groups*: A list of known, active ransomware groups, including victim count, group name, and published date. Click link icon to view ransomware victims affected.



- *Top Ransomware Groups*: A bar chart that compares the current number of incidents for each ransomware group with the number of incidents over a period of time. You can select the time period using the date filter.

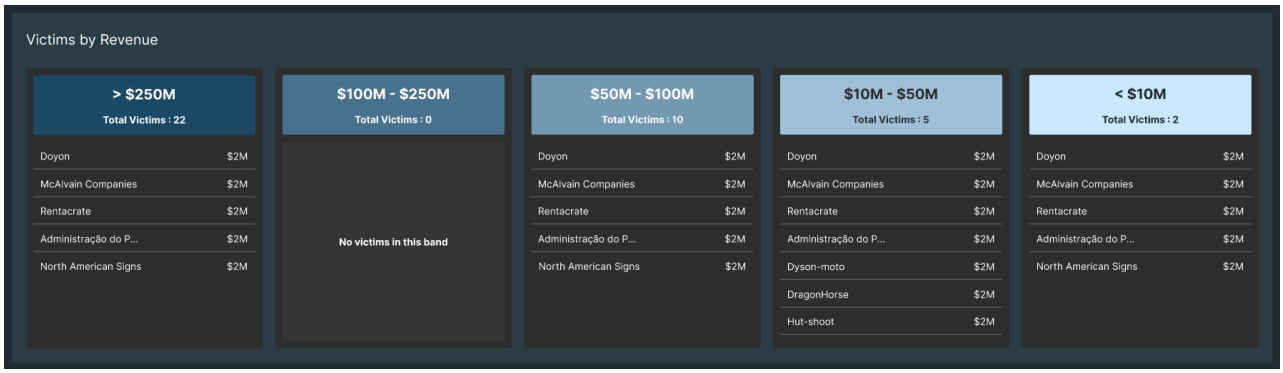


- *Ransomware Victims Over Time*: A line graph that tracks the number of ransomware victims identified over time.



- *Top 10 Countries/Sectors by Victims*: A heat map displaying the distribution of ransomware victims across different countries and sectors. Use the *Show By* dropdown to switch between a country or sector view.

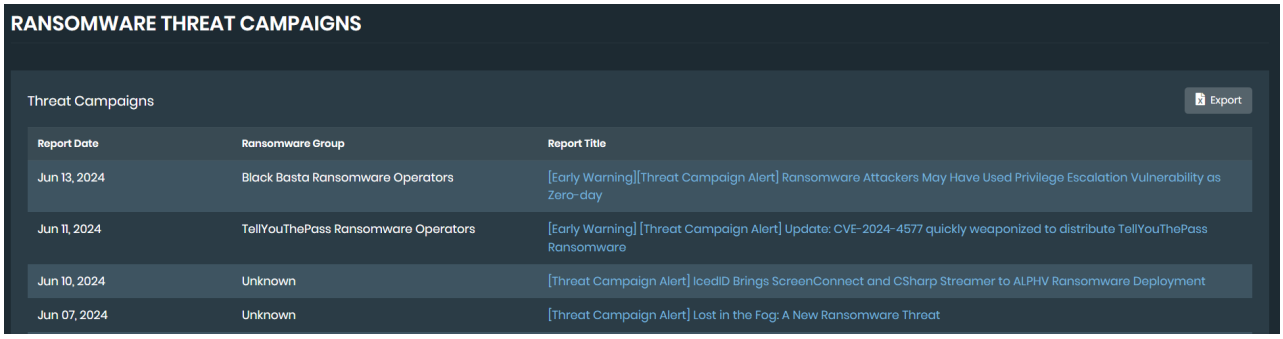
- *Victims by Revenue*: A list of organizations impacted by ransomware attacks, along with their estimated revenue.



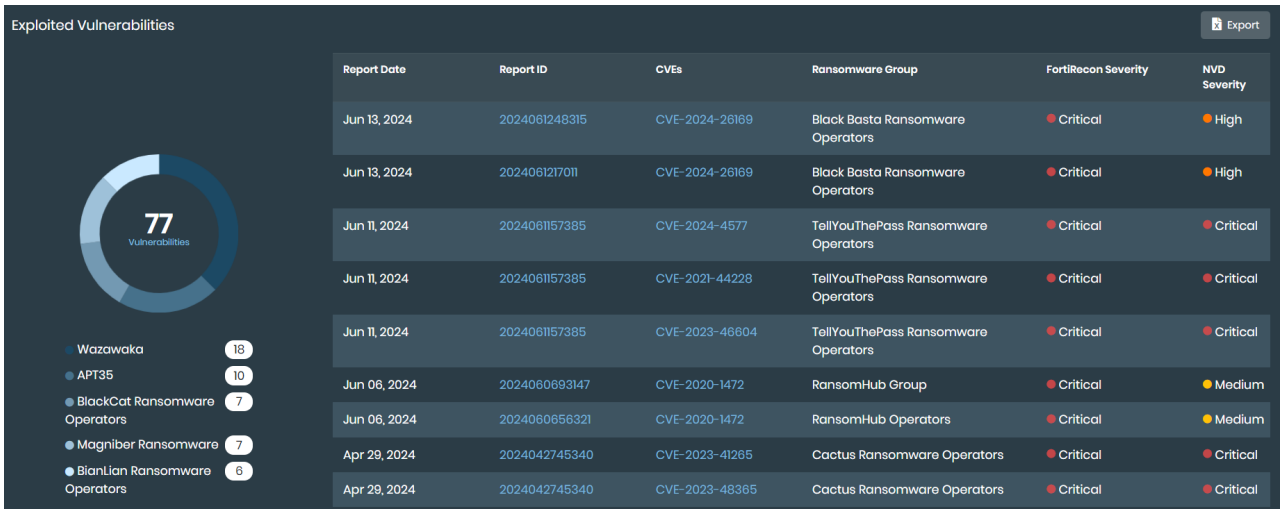
Ransomware Threat Campaigns

This section provides information on specific ransomware attacks.

- *Threat Campaigns*: A list of ransomware campaigns including report date, ransomware group and link to the report. Click *Export* to export the data.

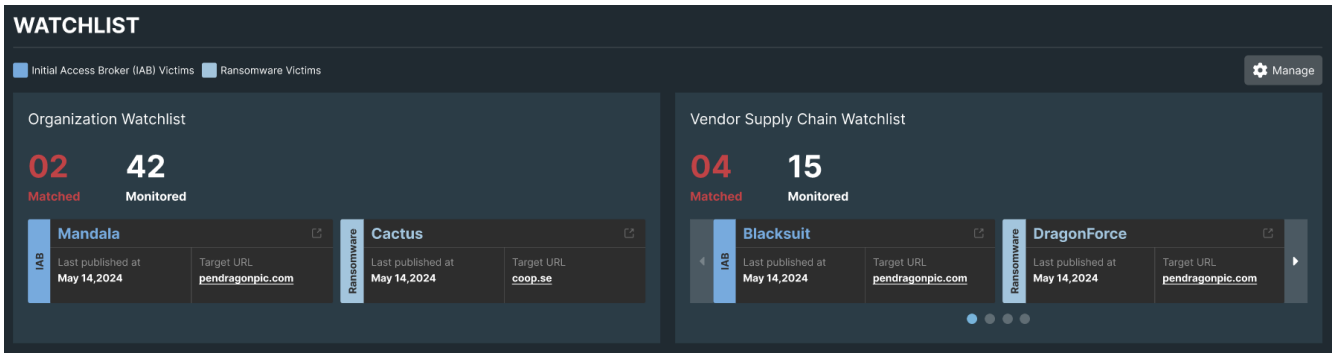


- *Exploited Vulnerabilities*: A list of exploited vulnerabilities including CVE, ransomware group, FortiRecon and NVD severity information.
  - Click *Report ID* to view the report
  - Click *CVE* to view the detailed information on *Vulnerability Intelligence* page with selected CVE as filter.
  - Click *Export* to export the data.



Watchlist

A list of monitored organization and vendors. If an asset matches a monitor, an alert will be triggered. Add or edit your watchlist by selecting *Manage*. See Managing My Watchlist.

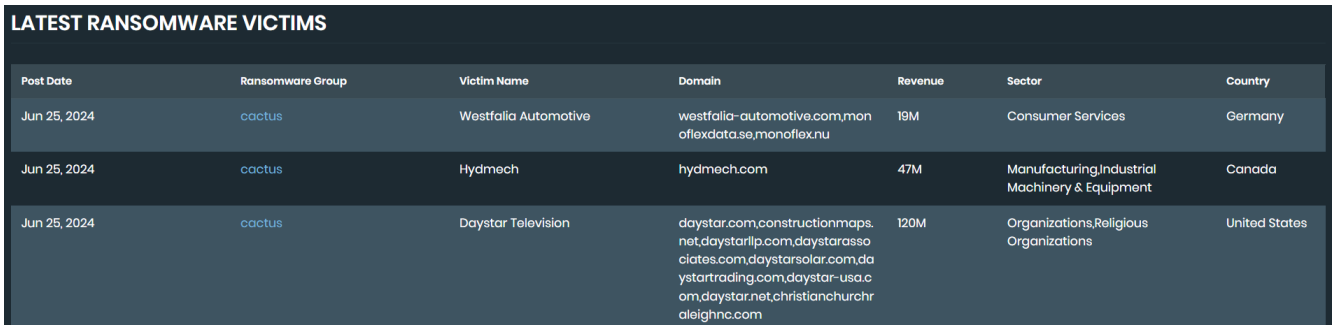


Latest Ransomware Victims

A list of the most recent victims of ransomware victims, including information on the victim revenue, sector, and country. Click *View All* to view more victims.

In the *Latest Ransomware Victims* page, click *Show Details* next to ransomware entry to view the post.

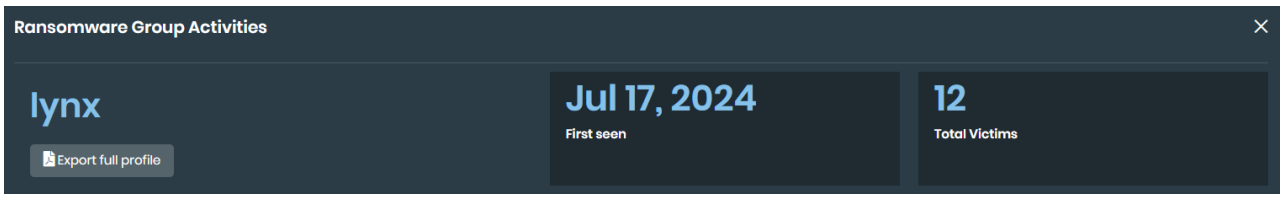
Click ransomware group name to view detailed information. See Ransomware Group Activities.



Ransomware Group Activities

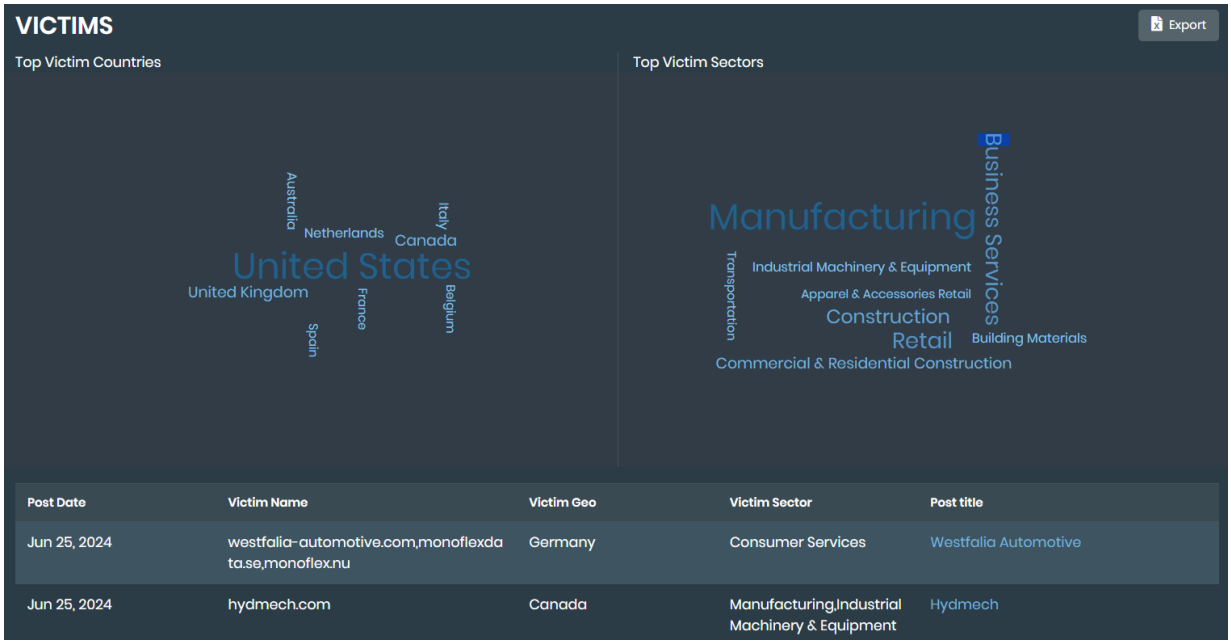
This page provides detailed information about a specific ransomware group, including its activity, victims, exploited vulnerabilities, and technical indicators. It includes following sections.

- The overview section provides information of the ransomware group's activity level, including the date it was first identified and the total number of victims identified to be impacted. Click *Export full profile* to download detailed ransomware group information in PDF format. Once the export is complete, you can download the file from the *Profile* > *Downloads* page.



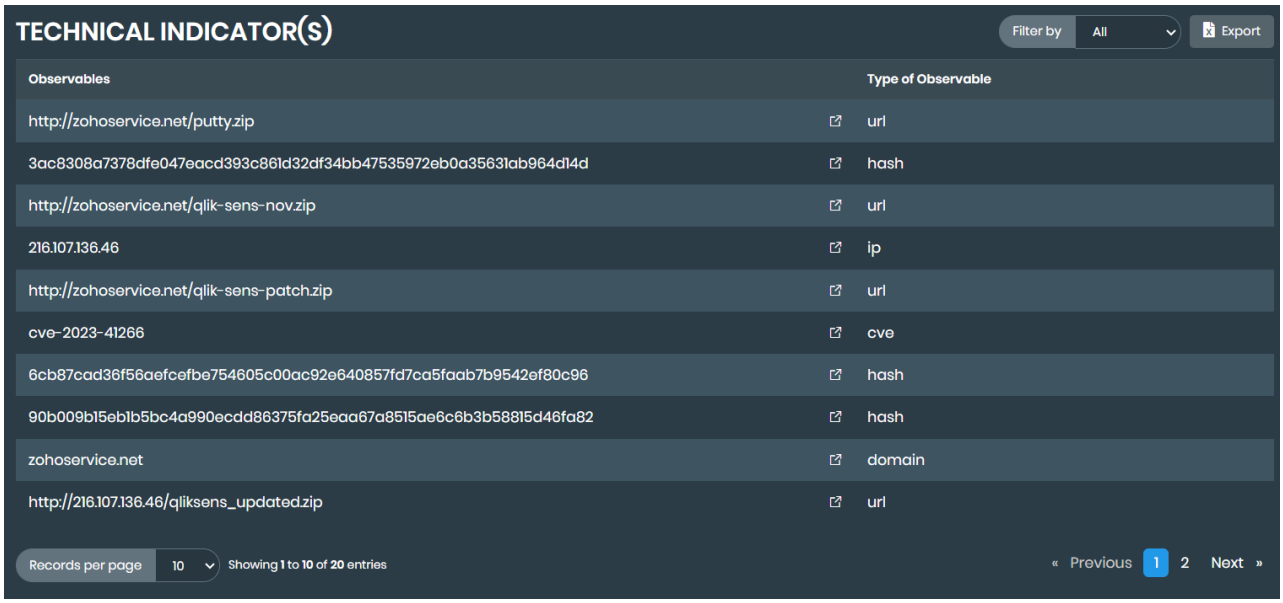
- The *Victims* section includes the following information.
  - *Top Victim Countries*: This word cloud displays the most frequently targeted countries by the group. The size of a country name corresponds to the number of victims in that location.

- *Top Victim Sectors*: This word cloud visualizes the sectors most impacted by the group's attacks. The size of a sector name reflects the number of victims within that sector.
- *Victims List*: This table lists identified victims of the ransomware group.



- *Exploited Vulnerabilities*: This section displays a list of exploited vulnerabilities including CVE, ransomware group, FortiRecon and NVD severity information.
  - Click *Report ID* to view the report
  - Click *CVE* to view the detailed information on *Vulnerability Intelligence* page with selected CVE as filter.
  - Click *Export* to export the data.

- *Technical Indicators*: This section provides a list of technical indicators (observables) associated with the ransomware group's activity. You can filter the data by observable type. Click *Export* to export the data.



Latest Initial Access Broker (IAB) Victims

A list of latest victims compromised by Initial Access Brokers (IABs). IABs often provide access to compromised networks, which can be exploited by ransomware attackers.

Click *View All* to view more victims. In the *Initial Access Broker (IAB) Victims* page, click *Associated Reporting* to view the detailed report.

Filtering ransomware intelligence

You can filter the information displayed on the *Ransomware Intelligence* > *Ransomware Trends*, *Ransomware Intelligence* > *Latest Ransomware Victims*, *Ransomware Intelligence* > *Potential Ransomware Victims*, and *My Watchlist* pages.

To filter information on ransomware trends:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence* > *Ransomware Trends*.
2. Specify your filters:
   - Select a group from *Ransomware group* dropdown.
   - Select the required time period from the *Date* filter.

   The *Ransomware Trends* section will update.

To filter information on the latest ransomware victims:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Latest Ransomware Victims* section, click *View All*. The *Latest Ransomware Victims* page is displayed.
3. Specify your filters:
   - Enter a keyword in the *Search* field.
   - Select a start and end range from the *Date Range* field.
   - Select specific filters from the list of categories.
4. Click *Search*. The list of victims that match your filters are displayed.

To filter information on Initial access broker victims:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Latest Initial Access Brokers(IAB) Victims* section, click *View All*. The *Initial Access Brokers(IAB) Victims* page is displayed.
3. Specify your filters:
   - Enter a keyword in the *Search* field.
   - Select a start and end range from the *Date Range* field.
   - Select specific filters from the list of categories.
4. Click *Search*. The list of victims that match your filters are displayed.

To filter your watchlist:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Watchlist* section, click *Manage*. The *My Watchlist* page is displayed.
3. Select a watchlist to filter:
   - *Organization Watchlist*
   - *Vendor Watchlist*
4. In *Organization Watchlist* tab, click the desired radio button to filter the results:
   - *All*: Show all the assets.
   - *EASM*: Show only assets that were automatically added to the watchlist by EASM.
   - *Manual*: Show only assets that were manually added to the watchlist.

   The watchlist will display any assets that match the set filters.

Exporting ransomware information

You can export a list of recent ransomware victims into an Excel file. The spreadsheet will include information on:

- Victim Name
- Affected Domains
- Revenue
- Sector
- Country
- Date
- Description

To export all of the ransomware victims:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. Scroll to the victim list you want to export:
   - *Latest Ransomware Victims*
   - *Latest Initial Access Broker (IAB) Victims*
3. Click *View All*. The list of victims is displayed.
4. Click the *Export List* icon. The file is downloaded to your computer.

To export specific ransomware victims:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. Scroll to the victim list you want to export:
   - *Latest Ransomware Victims*
   - *Latest Initial Access Broker (IAB) Victims*
3. Click *View All*. The list of victims is displayed.
4. Specify your filters. See Filtering ransomware intelligence on page 175.
5. Click the *Export List* icon. The file is downloaded to your computer.

Managing My Watchlist

Users can monitor certain vendor and organization names in the *My Watchlist* page in the *Vendor Watchlist* and *Organization Watchlist*, respectively. If a match for a monitored asset appears, it triggers an alert. Vendors and organizations can be added to the watchlist manually by users or automatically by EASM.

To filter the monitored assets, see Filtering ransomware intelligence on page 175.

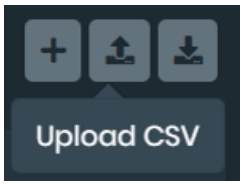
To create a new asset to manage:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Watchlist* section, click *Manage*. The *My Watchlist* page is displayed.
3. Click + icon. The *Create Watchlist* dialog is displayed.

4. Select the watchlist to add to from the *Select Watchlist* dropdown.
5. Enter a name for the monitored asset.
6. Enter the domain name of the monitored asset.
7. Click *Submit*. The asset is displayed on the assigned watchlist.

To add vendors in bulk:

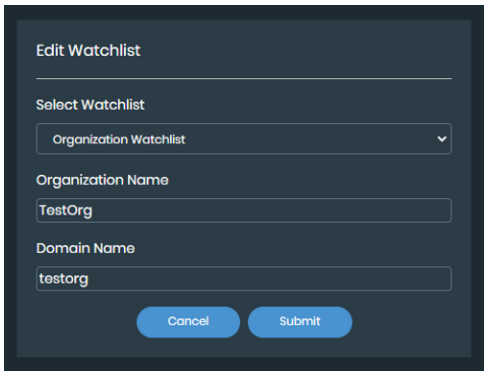
1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Watchlist* section, click *Manage*. The *My Watchlist* page is displayed.
3. Click *Upload CSV* icon to upload the .csv files containing the vendors list. Browse and select the file. Click **Open**.



Note: Ensure that the format in which the vendors data is stored matches with the required format. To view the required format click *Download Sample CSV* icon, select the watchlist type from the drop down and click *Download*.

To edit a monitored asset:

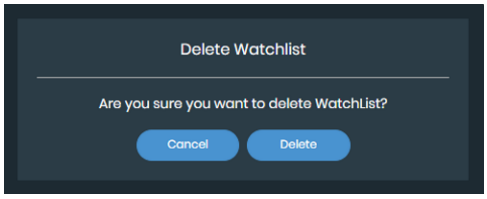
1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Watchlist* section, click *Manage*. The *My Watchlist* page is displayed.
3. Find the asset you want to edit and click *Edit icon*. The Edit Watchlist dialog is displayed.



4. Edit the asset details and click *Submit*.

To delete a monitored asset:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Watchlist* section, click *Manage*. The *My Watchlist* page is displayed.
3. Click *Delete icon*. A confirmation dialog is displayed.



4. Select *Delete*.

Vendor Risk Assessment

The *Adversary Centric Intelligence* > *Vendor Risk Assessment* page is designed to create a watchlist of vendors that allows you to assess the security hygiene level of each vendor. From the *Vendor Risk Assessment* page, you can:

- Add new vendors to the watchlist. See Adding a new vendor to the watchlist on page 179.
- View the security hygiene assessment of a vendor. See Viewing the vendor risk assessment on page 180.

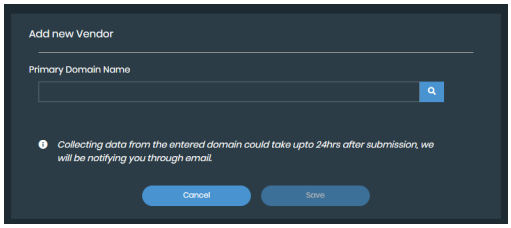
Adding a new vendor to the watchlist

You can add new vendors to the watchlist to generate a risk assessment report and identify the overall estimate risk exposure rating. Vendors can be added to the watchlist using the primary domain. Once the domain name has been submitted, collecting data and generating the risk assessment can take up to 24 hours.

If the overall estimated risk exposure rating of a vendor changes to *High*, an alert notification will be sent.

To add a new vendor to the watchlist:

1. Go to *Adversary Centric Intelligence* > *Vendor Risk Assessment*.
2. Click *Add Vendor*. The *Add new Vendor* dialog is displayed.



3. Enter the vendor domain in the *Primary Domain Name* field.

4. Click the search icon. Vendor information will be displayed.
5. Click *Save*. The vendor risk assessment will begin to generate.

By default, you can add a maximum of 25 vendors to watchlist. To monitor additional vendors, you can purchase a separate license.

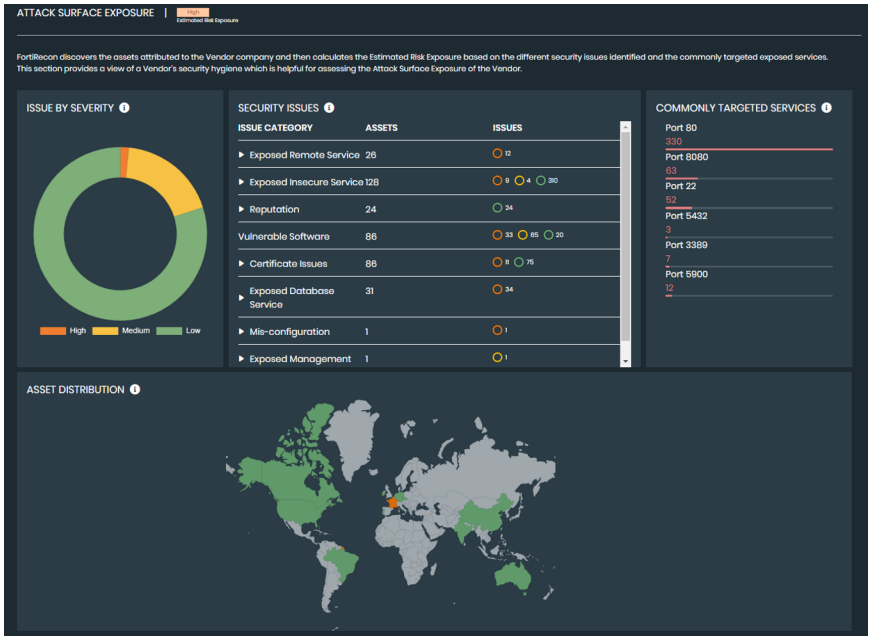
Removing a vendor from the watchlist

To remove a vendor from the watchlist, click *Remove* on its watchlist card.

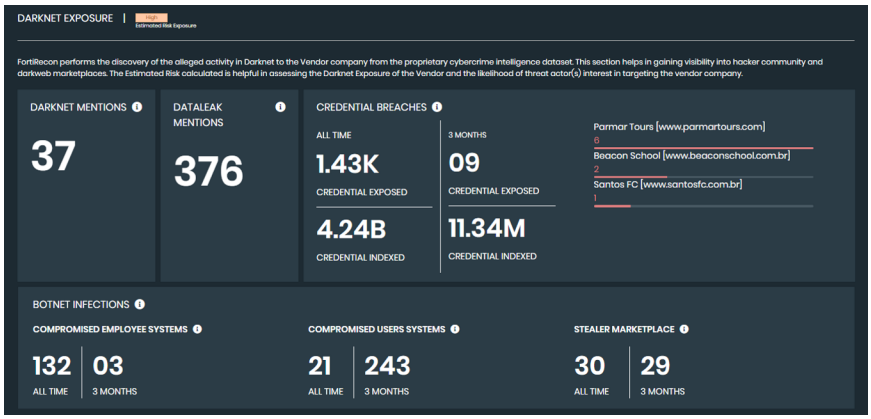
Viewing the vendor risk assessment

The vendor risk assessment organizes the generated vendors data into:

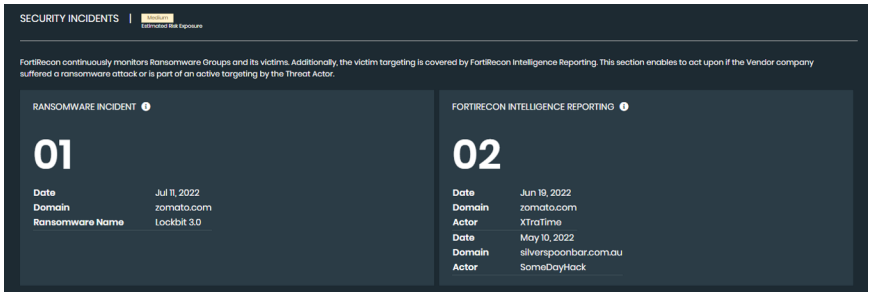
- *Attack Surface Exposure*: Provides an overview of the vendor company's assets and current security hygiene to assess the estimated risk exposure.



- *Darknet Exposure*: Provides an overview of potential activity in hacker communities and darkweb marketplaces toward the vendor company. The estimated risk can be used to assess the likelihood of threat actors' interest in targeting the vendor company.



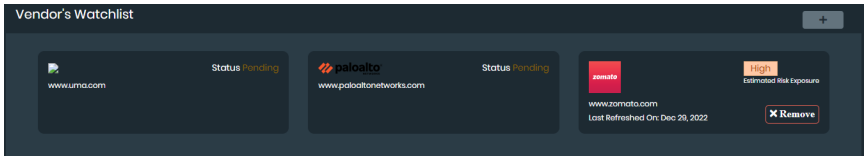
- *Security Incidents*: Provides an overview of ransomware incidences and intelligence reporting so that action can be taken if the vendor company suffers a ransomware attack or is targeted by a threat actor.



Each of these sections is further divided into widgets that allow you to review detailed risk data in order to make informed decisions.

To view a vendor risk assessment:

1. Go to *Adversary Centric Intelligence* > *Vendor Risk Assessment*.



2. Select the vendor that you want to review. The *Vendor Risk Assessment* opens.

You cannot review vendor information while the *Status* is *Pending*.

---

3. Review the banner for high-level information on the vendor and the *Overall Estimated Risk Exposure*.

4. Review the *Attack Surface Exposure*:

Issue by Severity	The distribution of security issues by severity on the vendor's attack surface.
Security Issues	The type of security issues identified and the assets affected, distributed by severity. Select a dropdown arrow in the *Issue Category* for further breakdown of the assets.
Commonly Targeted Services	The services on the vendor's attack surface that are commonly targeted and the number of assets exposing the service.
Asset Distribution	A geographical distribution of the vendor's assets.

5. Review the *Darknet Exposure*:

Darknet Mentions	The number of mentions of the vendor's name or domain on platforms where threat actors perform active discussions.
Dataleak Mentions	The number of mentions of the vendors name or domain on datasets leaked by threat actors.
Credential Breaches	An overview of credentials affiliated with the vendor's domain that have been identified in third party data breaches.
Botnet Infections	An overview of botnet campaigns used to steal credentials from end users: • *Compromised Employee Systems*: The number of usernames from the shared infected system logs containing the email address domain affiliated with the vendor. • *Compromised Users Systems*: The number of credentials shared from the infected system logs containing the URL or application visited on the infected system matching the vendor's domain. These systems can be end users or employees. • *Stealer Marketplace*: The number of credentials stolen by threat actors containing the URL or application visited on the infected system matching the vendor's domain. These logs are being listed for sale on prominent stealer marketplaces.

6. Review the *Security Incidents*:

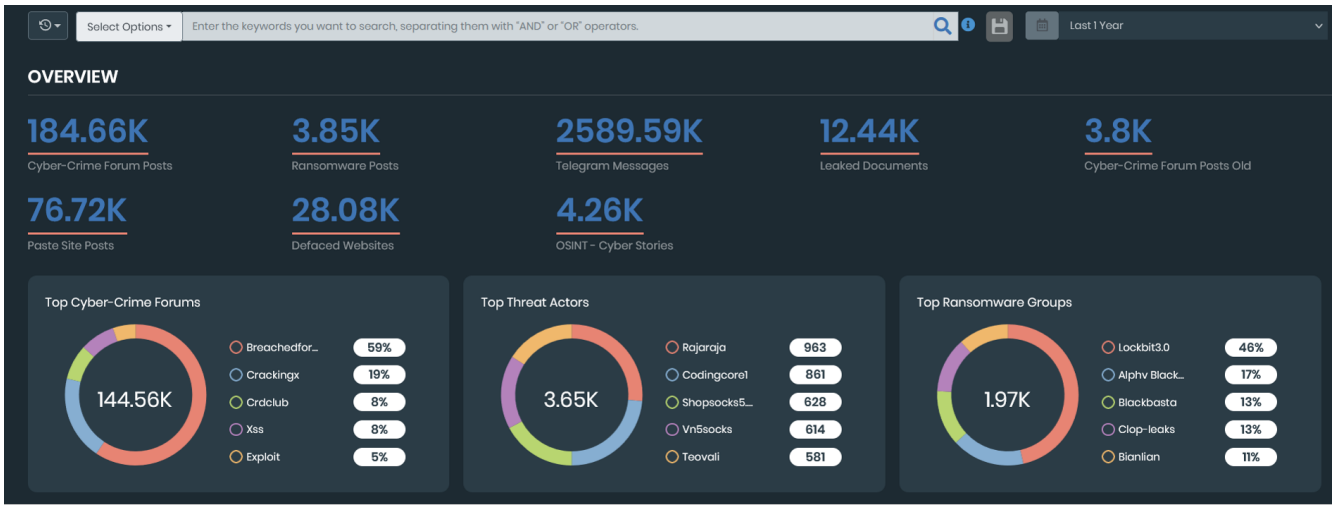
Ransomware Incident	The vendor name or domain appeared on the victim list by a ransomware group.
FortiRecon Intelligence Reporting	FortiRecon ACI reporting contains mention of the vendor's name or domain.

Intelligence Collection Lookup

The *Adversary Centric Intelligence* > *Intelligence Collection Lookup* page allows you to search the comprehensive intelligence collection, including cyber-crime forums, ransomware posts, Telegram messages, leaked documents, and more using a simple query syntax. From the *Intelligence Collection Lookup* page, you can:

Create and save search queries. See Search Query.

Review the search results. See Search Results.



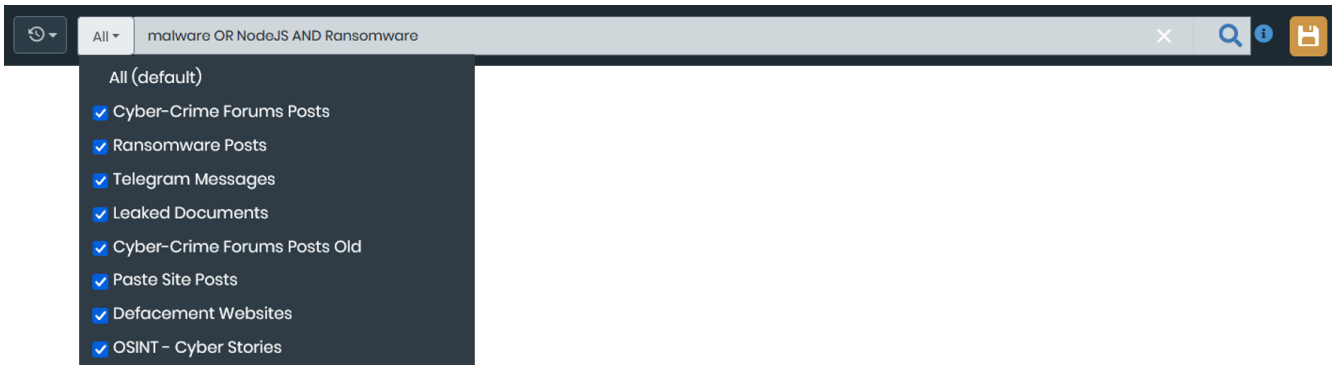
Search Query

You will able to search from the available intelligence sources using search query including keywords and operators.

Creating and running a search query

To create and run a search query:

1. Navigate to *Adversary Centric Intelligence* > *Investigation* page.
2. Enter the search query using keywords and operators you want to search in the search box. For supported query syntax, see Search Query Syntax.
3. Select the required sources, from the list. Supported sources include the following:
   - *All(default)*
   - *Cyber-Crime Forums Posts*
   - *Ransomware Posts*
   - *Telegram Messages*
   - *Leaked Documents*
   - *Cyber-Crime Forums Posts Old*
   - *Paste Site Posts*
   - *Defacement Websites*
   - *OSINT- Cyber Stores*
4. Click search icon.



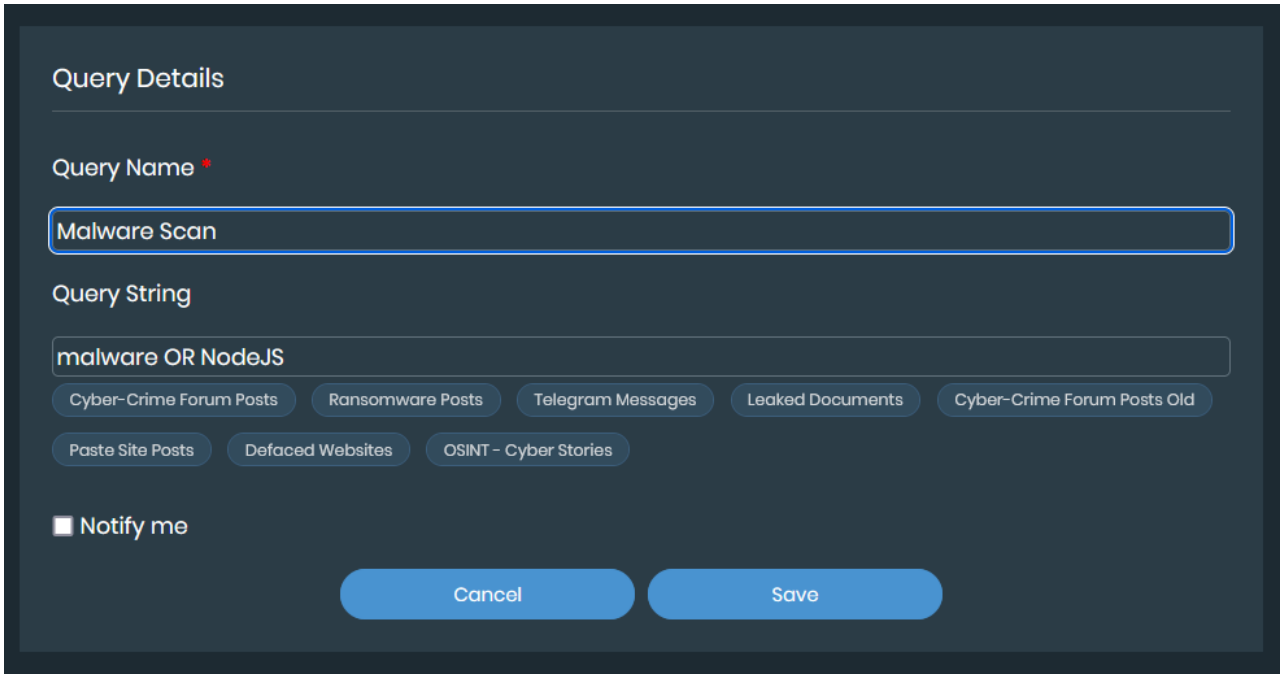
Saving a search query

You will be able to save your custom search queries for future use and to get notified. There are two types of saved queries:

- **System queries** - These queries are automatically generated for each organization based on their organization name, brand names, and primary domain. System queries cannot be edited.
- **User queries** - You can save custom search queries that are specific to your requirements.

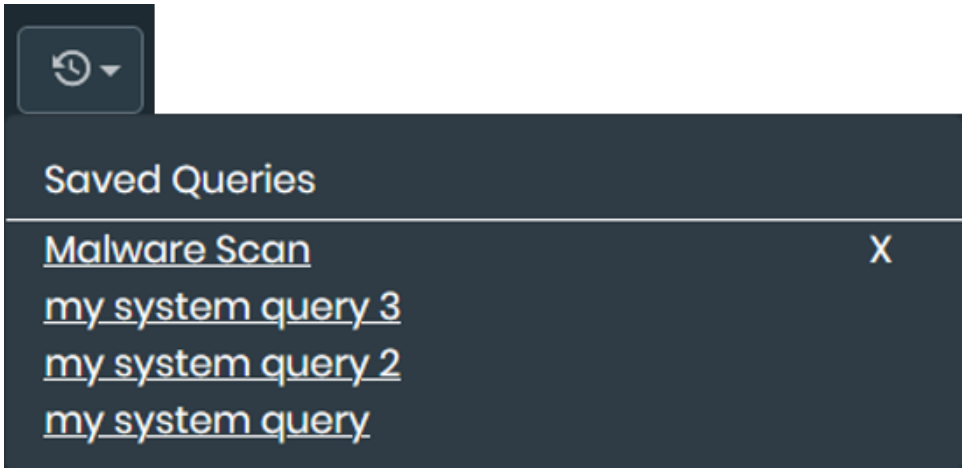
To save a user search query:

1. Navigate to *Adversary Centric Intelligence* > *Investigation* page.
2. Enter and run the search query.
3. Click *Save* icon.
4. In the Query Details window, provide the *Query Name*.
5. Select *Notify* checkbox, if you want to enable notifications for the query.
6. Click *Save*.



To run a saved search query:

1. Navigate to *Adversary Centric Intelligence* > *Investigation* page.
2. Click Saved Queries icon.
3. Select the required saved search query.



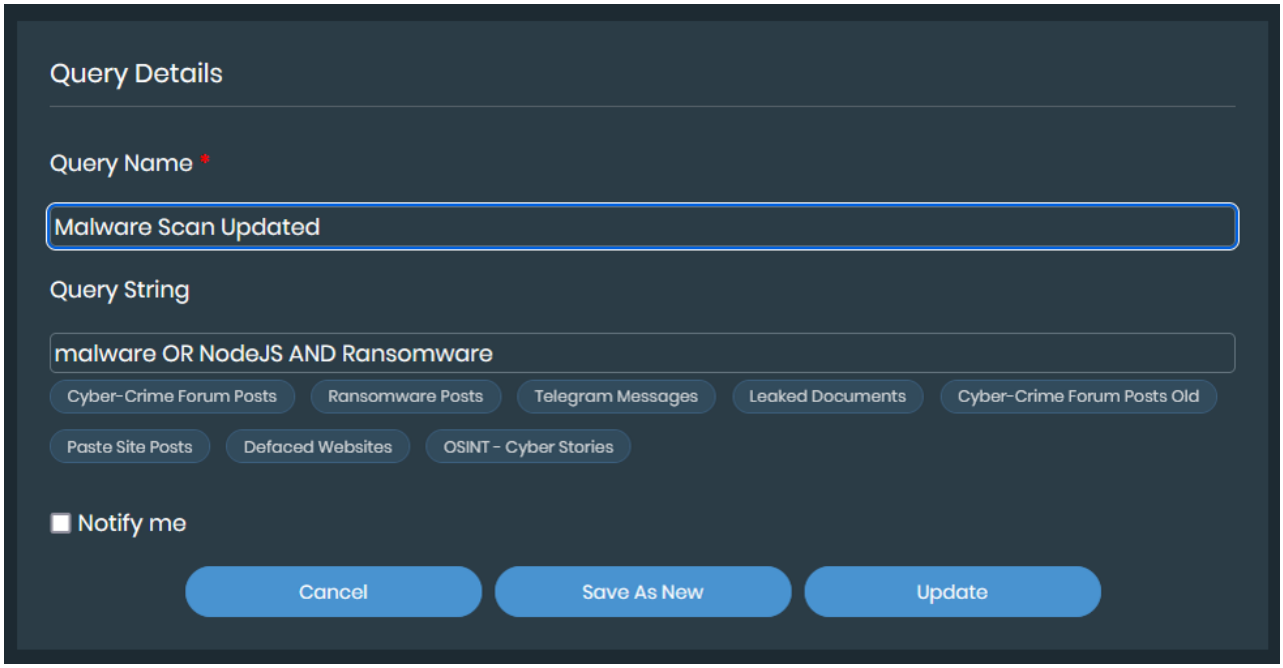
To delete a saved search query:

1. Navigate to *Adversary Centric Intelligence* > *Investigation* page.
2. Click Saved Queries icon.
3. Click *X* icon.

To update a saved search query:

1. Select the saved search query.
2. Update the search query in the search box if required.
3. Click *Save* icon.
4. Update the *Query Name* if required.

5. Click *Update* to update the existing search query or click *Save As New* to save as a new search query.



Search Query Syntax

Lucene query language is used to search for specific posts/messages. Following are the examples for using the query language.

Use Case	Query
To filter messages for exact domain match.	"knowbe4.com"
To filter messages for wildcard match containing the domain name.	*google.com
To filter messages for specific keyword with exact match.	"Cyber"
To filter messages for keyword with wildcard match.	*Cyber*
To find matches for multiple keywords.	("bank" OR "banco" OR "ATM malware")
To find matches for multiple keywords with AND condition	("stealer" OR "worm" OR "malware") AND ("bank")
To find matches for multiple keywords while excluding some keywords.	(healthcare OR medical*) NOT ("healthy" OR "Medical Cannabis")

Following operators and modifiers are supported.

Operators and Modifier	Description
AND	Use this option to find both terms that exist in the text.
OR	Use this option to find at least one term that exists in the text.
NOT	Use this option to exclude that exists in the text.
*	Use this option to perform wildcard search.

Search Results

Once you run either a system or a custom search query, the filtered results are displayed. The default display period for the results is *1 year*. There are two sections available for viewing search results.

- Overview
- Detailed Results

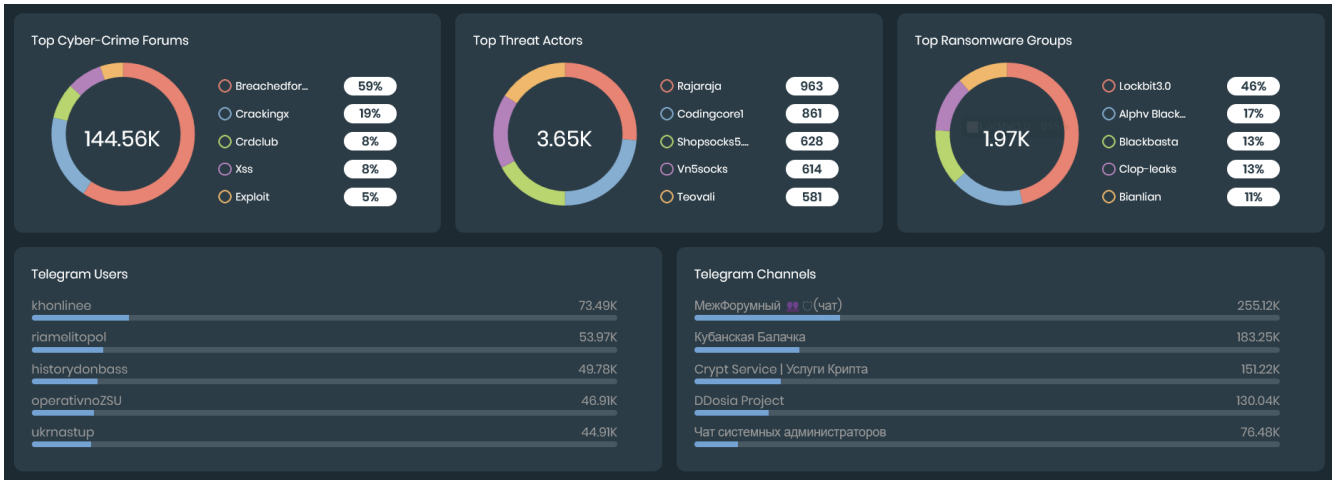
To modify the result period, click date drop-down menu and choose the desired time period.

Overview

The overview section provides the cumulative count of the following fields discovered in the search.

- *Cyber-Crime Forums Posts*
- *Ransomware Posts*

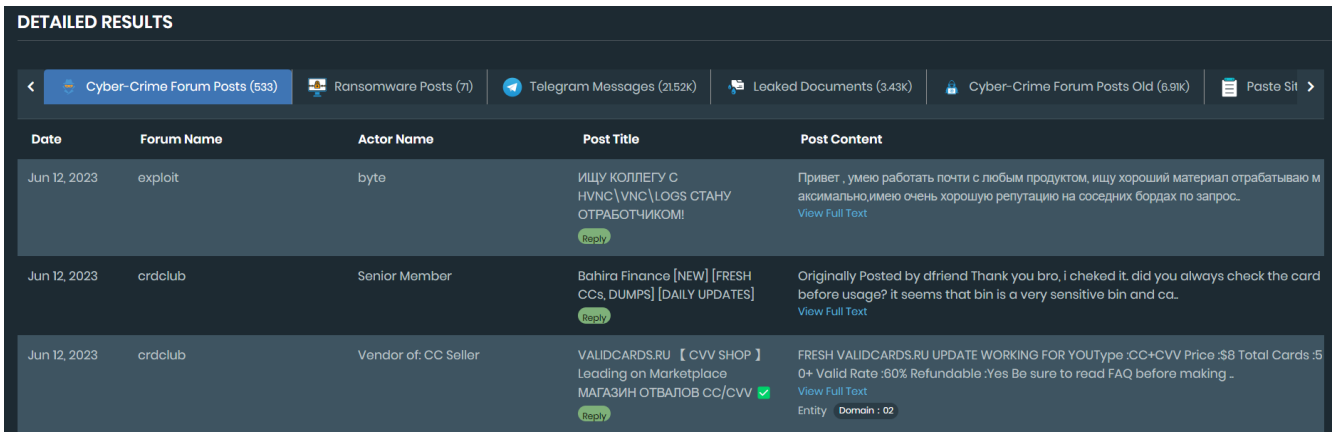
- *Telegram Messages*
- *Leaked Documents*
- *Cyber-Crime Forums Posts Old*
- *Paste Site Posts*
- *Defacement Websites*
- *OSINT- Cyber Stores*



The overview section also includes the following chart widgets:

- *Top Cyber-Crime Forums*: Displays the top 5 forums from Darknet posts.
- *Top Threat Actors*: Displays the top 5 threat actors contributing to Darknet posts.
- *Top Ransomware Groups*: Displays the top 5 groups from Ransomware posts.
- *Telegram Users*: Displays the top 10 users with Telegram posts.
- *Telegram Channels*: Displays the top 10 channels with Telegram posts.

Detailed Results



The detailed results section displays the detailed information of the discovered search results. The following data is displayed for each source.

Intelligence Source	Fields Displayed
Cyber-Crime Forum Posts	• Date • Forum Name • Actor Name • Posts Title • Post Content Click *View Full Text* or *Entity* type to view the full content. The extracted entities if any including *domain, URL, CVE, email,* or *IP* are displayed in the full content window.
Ransomware Posts	• Date • Ransomware • Name • Title • Victim Company • Victim Country • Victim Sector • Posts Content Click *View Full Text* or *Entity* type to view the full content. The extracted entities if any including *domain, URL, CVE, email*, or *IP* are displayed in the full content window.
Telegram Messages	• Date • Username • Channel • Message
Leaked Documents	• Date • Leak Name • File Name • File Data Click *View Full Text* to view the full content.
Cyber-Crime Forum Posts Old	• Date • Forum • Name • Actor Name • Posts Title • Posts Content Click *View Full Text* or *Entity* type to view the full content. The extracted entities if any including *domain, URL, CVE, email,* or *IP* are displayed in the full content window.
Paste Site Posts	• Date • Author Name

Intelligence Source	Fields Displayed
	• Title • Content Click *View Full Text* to view the full content. Click link icon to view the site posts in detail.
Defaced Websites	• Date • Source • Notifier • Domain Click link icon to view the website.
OSINT - Cyber Stories	• Date • Title • Content Click *View Full Text* or *Entity* type to view the full content. The extracted entities if any including *domain, URL, CVE, email,* or *IP* are displayed in the full content window. Click link icon to read the full article.

Investigation

The *Adversary Centric Intelligence* > *Investigation* page displays information about investigations into security events. From the *Investigation* page, you can:

- Review the reputation of IPv4 addresses. See Reviewing IP address reputation on page 190.
- Review the reputation of a domain. See Reviewing domain reputation on page 191.
- Review a file hash. See Reviewing a file hash on page 191.
- Review a CVE. See Reviewing a CVE on page 191.

Reviewing IP address reputation

You can use the *IP Reputation* search bar to search for IPv4 addresses.

To review IP address reputation:

1. Go to *Adversary Centric Intelligence* > *Investigation* > *IP Reputation*. The *IP Reputation* tab is displayed.

2. Type the IPv4 address, and press *Enter*.

Reviewing domain reputation

You can use the *Domain Reputation* search bar to search for domains.

To review domain reputation:

1. Go to *Adversary Centric Intelligence* > *Investigation* > *Domain Reputation*. The *Domain Reputation* tab is displayed.

2. Type the domain name, and press *Enter*.

Reviewing a file hash

You can use the *File Hash* search bar to search for a file hash.

To review a file hash:

1. Go to *Adversary Centric Intelligence* > *Investigation* > *Hash Lookup*. The *Hash Lookup* tab is displayed.

2. Type the file hash, and press *Enter*. The results are displayed.

Reviewing a CVE

You can use the *CVE* search bar to search for a CVE.

To review a CVE:

1. Go to *Adversary Centric Intelligence* > *Investigation* > *CVE*. The *CVE* tab is displayed.

2. Type the CVE, and press *Enter*. Information about the CVE is displayed.

Profile settings

The *Profile Settings* page allows you to personalize your FortiRecon account and provide information on your organization.

You can access *Profile Settings* from the menu in the top-right corner of FortiRecon. See Accessing profile settings on page 192.

The *Profile Settings* module contains the following pages:

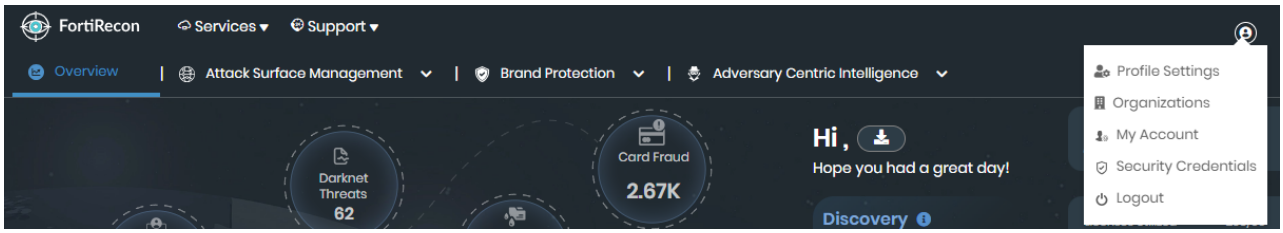
Profile	Displays information about your personal FortiRecon account. You can edit user idle timeout setting, view account details, and copy your API key for sharing. See Profile on page 193.
Users	Displays account information for members of your organization. Administrators can add, edit, and delete user accounts. See Users on page 196
Access Templates	Allows the creation and editing of access templates. Access templates control the modules and sub modules available to users on FortiRecon. See Access templates on page 198.
Audit Logs	Displays logs of all user actions performed within FortiRecon. See Audit Logs.
Downloads	Displays a list of all the files downloaded from FortiRecon in that last 30 days. You can download the files to your computer or delete unnecessary files. See Downloads on page 202.
Integrations	Displays the webhook integrations with Microsoft Teams and Slack. You can create, edit, disable, and delete integrations. See Integrations on page 203.
Seeds	Displays the domains, card BINs, and mobile applications of your organization that are being monitored by FortiRecon. See Seeds on page 206.
Notification Center	Displays the current notification settings for all the modules assigned to you. You can view, search, and enable or disable notifications. See Notification Center on page 207.

Accessing profile settings

You can access the *Profile Settings* from any page by selecting the menu in the top-right corner.

To access profile settings:

1. Hover over the profile menu in the top-right corner, and select *Profile Settings*.



The *Profile* page is displayed.

Profile

The *Profile* page provides information on your personal account information and allows you to customize settings. From the *Profile Settings* > *Profile* tab, you can:

- Edit user idle timeout setting. See Editing user idle timeout on page 193.
- View information about your subscription, such as registered domains, target industries and geography, keywords, and your API key. See Subscription Details on page 194.
- Copy your API key for sharing. See Sharing the API key on page 195.

Editing user idle timeout

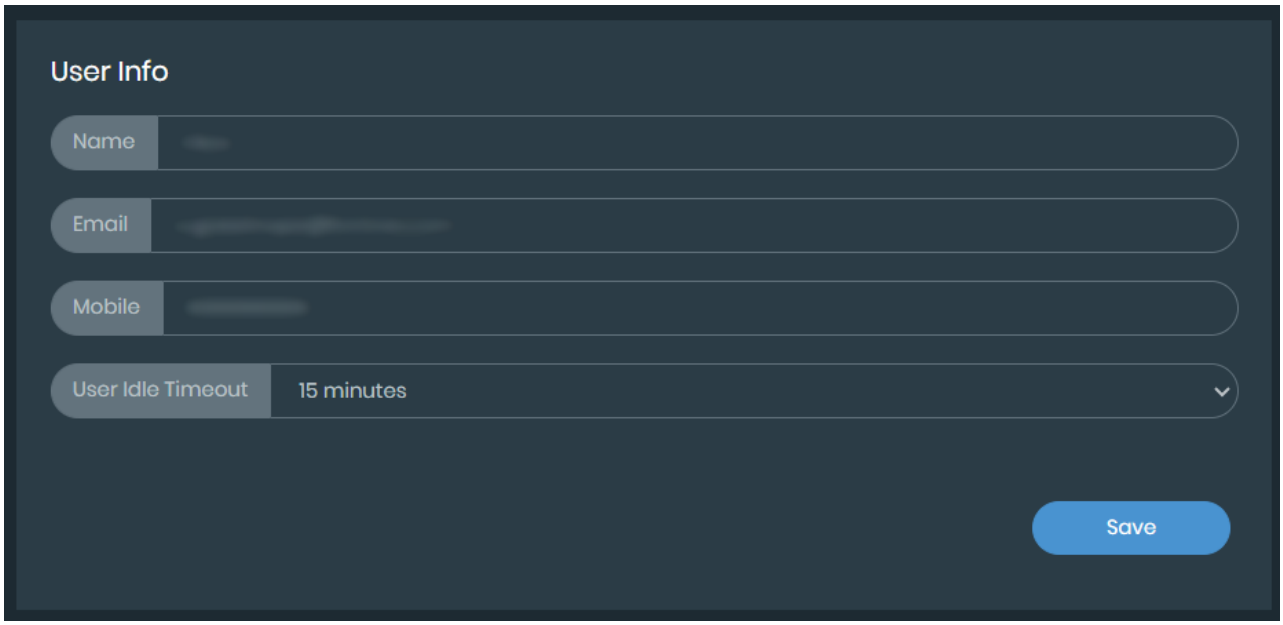
You can edit user idle timeout on the *Profile* page. To edit your personal information and other FortiRecon account users, see Editing users on page 197.

To edit personal user information:

1. Go to *Profile Settings* > *Profile*.
2. Select the timeout period you want from the *User Idle Timeout* dropdown.

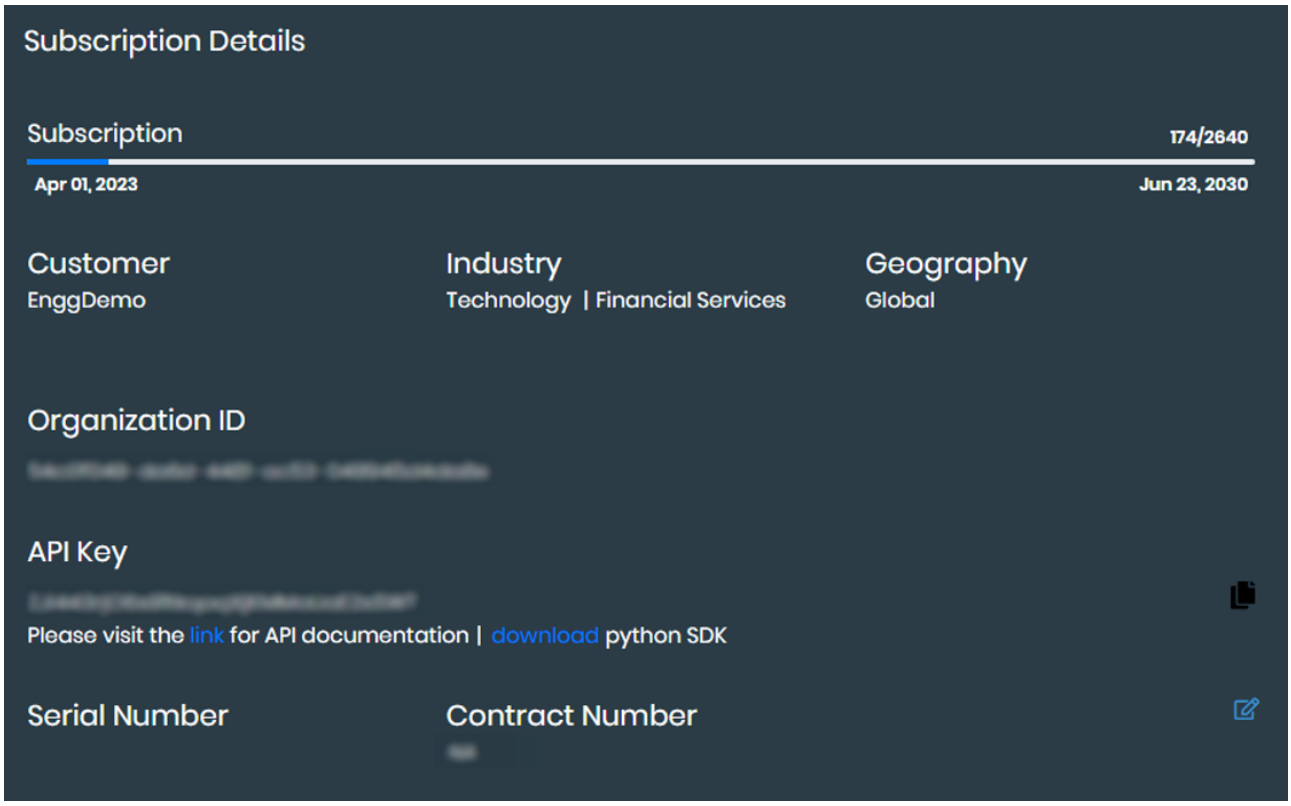
3. Click *Save*.

By default, user idle timeout is set to *15 minutes*.



Subscription Details

Subscription Details provides information on your subscription, including organization ID, license serial number, contract information, and your API key.



To view subscription details:

1. Go to *Profile Settings* > *Profile*.
2. Scroll to *Subscription Details* to view information on your:
   - Subscription
   - Customer
   - Industry
   - Geography
   - Organization ID
   - API Key

   To access the API documentation or download the Python SDK package, click on the links below the API key.

   - Serial Number
   - Contract Number

Sharing the API key

You can copy your API key to your clipboard to share with others or use in other software.

To copy your API key:

1. Go to *Profile Settings* > *Profile*.
2. Click *Copy* in *Subscription Details*. The API key is copied to your clipboard.

Users

Multiple FortiRecon accounts can be created for an organization in the *Users* pages. The following roles are available for FortiRecon accounts:

- User: Has access limited to what is included in the assigned access template.
- Admin: Has administrative access over other accounts.

Only administrators can add and make changes to other accounts.

From the *Profile Settings* > *Users* page, you can:

- View all user accounts for your organization. See Viewing user accounts on page 196.
- Add new users. See Adding users on page 197.
- Edit existing users. See Editing users on page 197.
- Delete users. See Deleting users on page 198.

Viewing user accounts

You can view all of the current users for your organization on the *Users* page. User information listed for all users includes:

- Name
- Role
- Email
- Phone Number

To view user accounts:

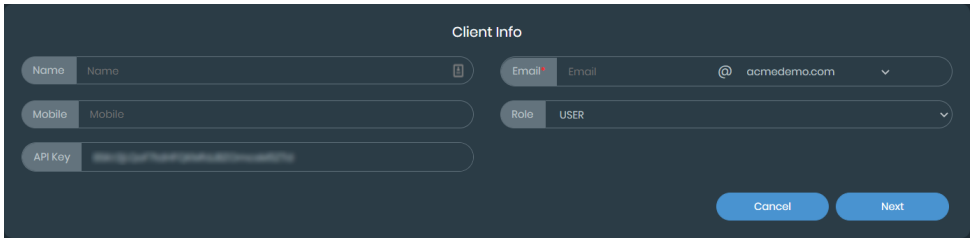
1. Go to *Profile Settings* > *Users*.
2. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a name or email, and press *Enter*.
      The user accounts are filtered to display only accounts with the keyword.
   b. Click the *X* beside the keyword to remove the filter.

Adding users

Administrators can add new user accounts. Before you add new users, define access templates to select in the user accounts. See Access templates on page 198.

To add a user account:

1. Access *Profile Settings*, and click the *Users* page. The users are displayed.
2. Click the *Add User* button. The *Client Info* page is displayed.



3. On the *Client Info* page, complete the following options, and click *Next*.

Name	Type a name for the user.
Mobile	Type the mobile phone number for the user.
API Key	Displays the automatically generated API key for the user.
Email	Type the email address, and select the domain for the user.
Role	Select one of the following roles: • User: gives the user access to the modules defined to their account. • Admin: gives the user access to the modules defined to their account and administrative access over other accounts.

The *Permissions* page is displayed

4. Select a *User Template* from the dropdown. The *Main Modules*, *Sub Modules*, and *Access* are adjusted to the template's settings.
5. Click *Save*. The user is created.

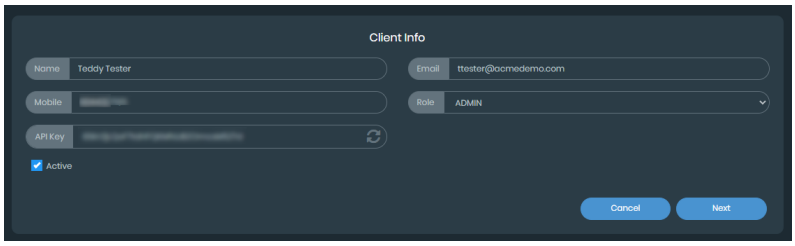
Editing users

All organization members with FortiRecon accounts are listed on the *Users* page. Administrators can edit the information of other members.

You cannot edit an email address.

To edit a user account:

1. Go to *Profile Settings* > *Users* and find the account you want to edit.
2. Click *Edit*. The *Client Info* page is displayed.



3. On the *Client Info* page, complete any of the following options as needed, and click *Next*.

Name	Type a new name for the user.
Mobile	Type a new mobile phone number for the user.
API Key	Select *Re-generate API* to create a new *API Key*. This can be done when it is suspected that the API Key has been compromised or leaked.
Role	Select a new role from the *Role* dropdown.

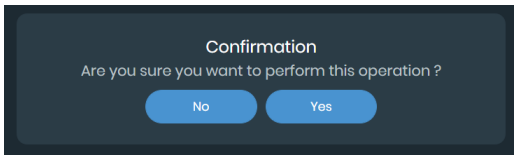
   The *Permissions* page is displayed.
4. Select a new *User Template* from the dropdown, if needed. The *Main Modules*, *Sub Modules*, and *Access* are adjusted to the template's settings.
5. Click *Save*. The user information and access permissions are updated.

Deleting users

Administrators can delete the account of another member on the *Users* page.

To delete a user account:

1. Go to *Profile Settings* > *Users* and find the account you want to delete.
2. Click *Delete*. A confirmation message is displayed.



3. Click *Yes*. The account is deleted.

Access templates

Access templates are used for controlling user accounts. When you create an access template, you can define what modules and sub modules a user can access, and then you can assign the access template to user accounts. See Adding users on page 197

From the *Profile Settings* > *Access Template* page, you can:

- View available access templates. See Viewing access templates on page 199.
- Add a new access template. See Adding a template on page 199.

- Edit an existing access template. See Editing a template on page 200.

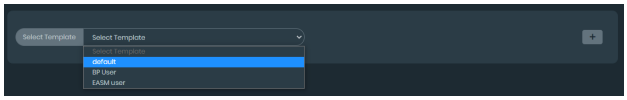
Viewing access templates

You can view the settings assigned to an access template in the *Access Templates* page. Assigned *Main Modules*, *Sub Modules*, and *Access* settings appear in the following formats:

- Grey: The Sub Module is a default setting that is always included if the Main Module is selected.
- Blue: The feature has been intentionally selected from the optional features.

To view an access template:

1. Go to *Profile Settings* > *Access Templates*.
2. Click the *Select Template* dropdown. A list of existing access templates is displayed.



3. Select the template you want to view. The template is displayed.

Adding a template

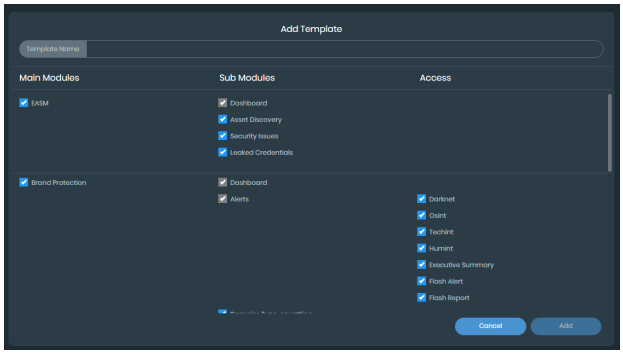
You can create new templates in the *Access Templates* page, and they can include any of the *Main Modules*, specific *Sub Modules*, and *Access* settings.

While all *Access* settings are optional, the following *Sub Modules* are mandatory when the associated *Main Module* has been selected:

Main Module	Mandatory Sub Modules
EASM	Dashboard
Brand Protection	Dashboard and Alerts
Adversary Centric Intelligence	Dashboard and Reports

To create an access template:

1. Go to *Profile Settings* > *Access Templates*.
2. Click *Add Template*. The *Add Template* page is displayed.



3. Enter a name in the *Template Name* text box.
4. Select the *Main Modules*, *Sub Modules*, and *Access* fields to enable user access to them.
5. Clear the *Main Modules*, *Sub Modules*, and *Access* fields to disable user access to them.
6. Click *Add*. The template is created.

Editing a template

You can edit a template that has previously been created to add or remove *Modules*, *Sub Modules*, and *Access* settings.

To edit an access template:

1. Go to *Profile Settings* > *Access Templates*.
2. From the *Select Template* dropdown, select the template you want to edit . The template is displayed.
3. Enter a new name in the *Template Name* text box, if needed.
4. Select the new *Main Modules*, *Sub Modules*, and *Access* fields to enable access to them.
5. Clear the *Main Modules*, *Sub Modules*, and *Access* fields to disable access to them.
6. Click *Save*. The template is updated.

Audit Logs

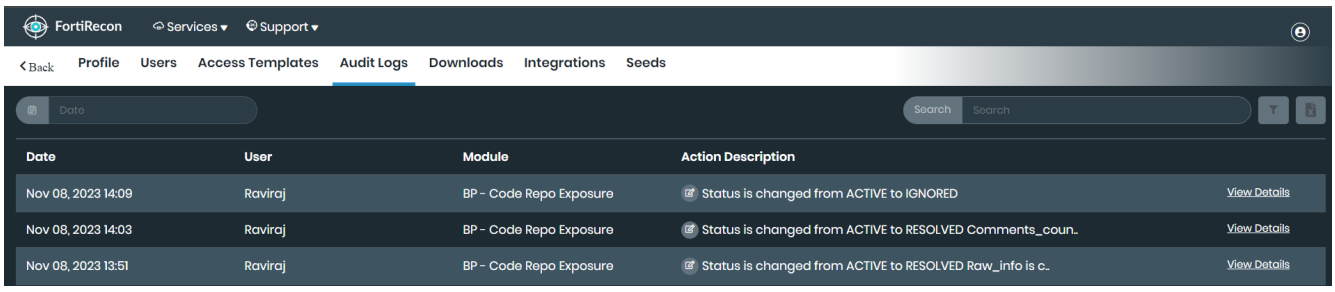
The Audit Logs page provides a comprehensive overview of all activities performed within FortiRecon, allowing you to track user actions, monitor changes made to your organization's data, and maintain compliance with security regulations.

From *Profile Settings* > *Audit Logs* tab, you can:

- View the audit logs. See Viewing the audit logs.
- Apply filters to the list of audit logs to view specific logs. See Filtering audit logs.
- Export audit logs to an Excel file. See Exporting audit logs.

Viewing audit logs

Audit logs capture detailed information about every action taken within FortiRecon, including the date and time of the action, the user responsible, FortiRecon module, and the action description.

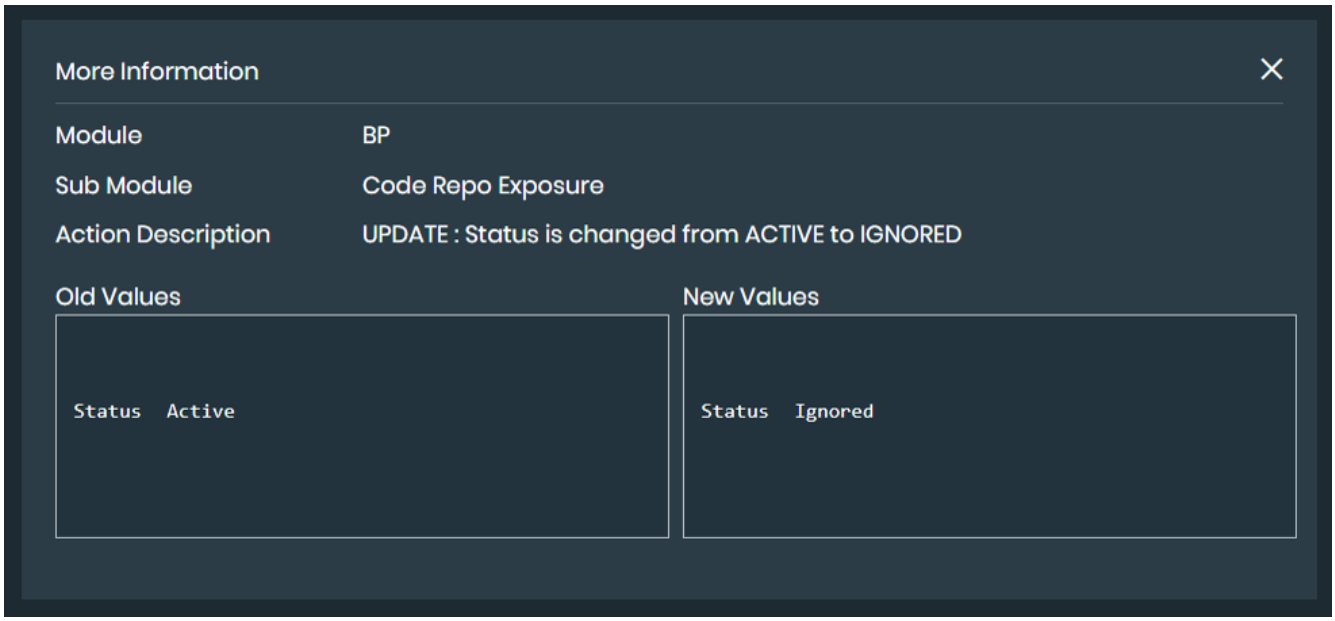


To view audit logs:

1. Go to *Profile Settings* > *Audit Logs*.
2. Apply the required filters. See Filtering audit logs.
3. Click *View Details* next to a desired audit log to view detailed information.

More Information window displays detailed audit log information including:

- *Module*
- *Sub Module*
- *Action Description*
- *Old Values*
- *New Values*



Filtering audit logs

By default, the *Profile Settings* > *Audit Logs* page displays all audit logs, starting with most recent log. You can use filters to display specific logs.

To filter audit logs:

1. Go to *Profile Settings* > *Audit Logs*.
   a. Filter audit logs by a date range:
   b. Click *Date* field. Two calendars are displayed.
   c. In the left calendar, select a month, year, and day to specify the start date of the range.

d. Select a month, year, and day to specify the end date of the range.
e. Only audit logs from the date range are displayed.
f. Click the *Date* field, and click *X* to remove the date range filter.

2. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
   b. The audit logs are filtered to display only logs with the keyword.
   c. Click the *X* beside the keyword to remove the filter.
3. To filter the audit logs by *Module, Sub Module*, or *User*, click the *Filter* icon, select the desired filters, and then click *Apply Filters*. To clear the applied filters, click the *Filter* icon and deselect the filters.

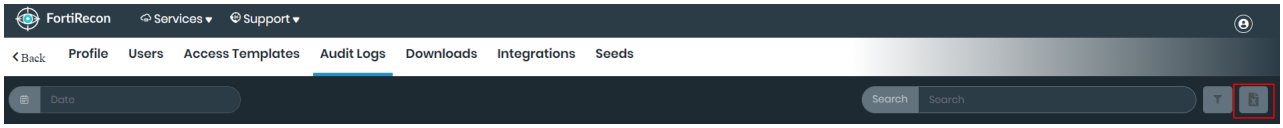
Exporting audit logs

You can export a list of audit logs into an Excel file. The spreadsheet will include the information on:

- Date
- User
- Module
- Sub Module
- Action Description

To export the audit logs:

1. Go to *Profile Settings* > *Audit Logs*.
2. Optionally, apply the required filters to export specific logs. See Filtering audit logs.
3. Click *Download* icon. The file is downloaded to your computer.



Downloads

Files downloaded from *EASM*, *Brand Protection*, and *Adversary Centric Intelligence* are saved in the *Downloads* page. Files are saved in a list with the most recently downloaded files at the top.

From the *Profile Settings* > *Downloads* page, you can:

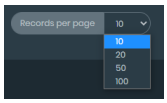
- View all downloads from the past 30 days. See Viewing downloads on page 202.
- Retrieve downloads from the past 30 days. See Retrieving downloads on page 203.
- Delete downloads. See Deleting downloads on page 203.

Viewing downloads

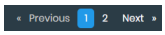
You can view all of your downloads from the past 30 days.

To view downloads:

1. Go to *Profile Settings* > *Downloads*. The most recent downloads are displayed.
2. From the *Records per page* dropdown list, select the number of downloads to display on the page.



3. Navigate between pages by selecting *Previous* and *Next*.



Retrieving downloads

You can retrieve downloaded files in the *Downloads* page.

To retrieve a downloaded file:

1. Go to *Profile Settings* > *Downloads* and find the file you want.
2. Click the file in the *Download* column. The file is downloaded to your computer.

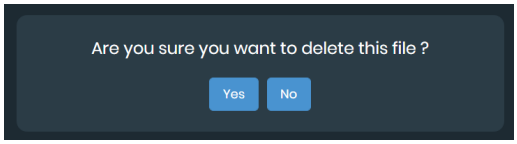
If a file is not finished downloading, an update message is displayed when you hover your mouse over the file. You cannot click the file until it is finished downloading.

Deleting downloads

Downloaded files are automatically deleted after 30 days. However, you can manually delete files if needed.

To delete downloaded files:

1. Go to *Profile Settings* > *Downloads* and find the file.
2. Click the delete icon in the *Actions* column. A confirmation message is displayed.



3. Click *Yes*. The file is deleted.

Integrations

You can use webhook integration to receive automated alert and report notifications over Microsoft Teams and Slack. For example, if you have flash reports configured for a Slack integration, when a flash report appears on FortiRecon, you receive an automated notification on your Slack account.

From the *Profile Settings* > *Integrations* page, you can:

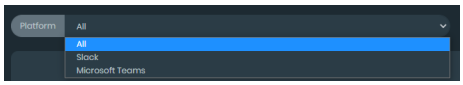
- View the details of existing integrations. See Viewing integration details on page 204.
- Create new integrations. See Adding integrations on page 204.
- Edit existing integrations. See Editing integrations on page 205.
- Disable integrations. See Disabling integrations on page 206.
- Delete integrations. See Deleting and disabling integrations on page 206.

Viewing integration details

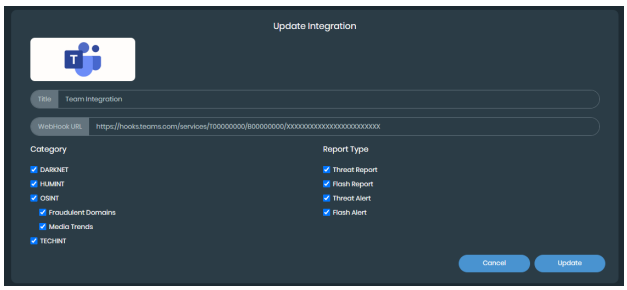
You can view the details of an integration in the *Integrations* page.

To view the details of an integration:

1. Go to *Profile Settings* > *Integrations*.
2. Find the integration you want to view:
   a. Search for keywords:
      i. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
      The integrations are filtered to display only integrations with the keyword.
      ii. Click the *X* beside the keyword to remove the filter.
   b. Search by platform:
      i. Select the *Platform* dropdown. A list of available integration platforms is displayed.



      ii. Select the platform you want to view.
      The integrations are filtered to display only integrations for that platform.
3. Click the name or icon of the integration. The *Update Integration* page displays the integration details.



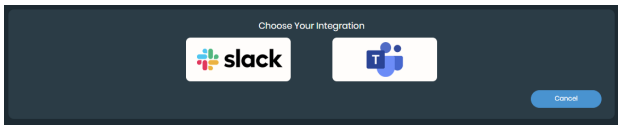
Adding integrations

You can add multiple webhook integrations to your account in FortiRecon.

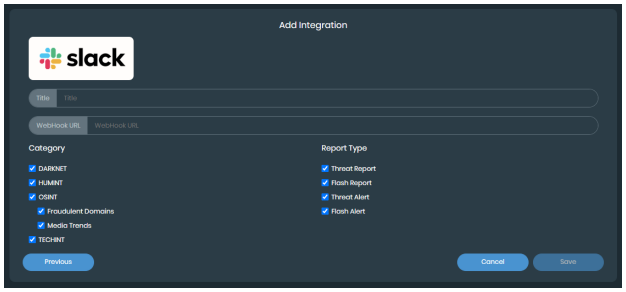
You must retrieve the webhook URL from Microsoft Teams and Slack before adding an integration to FortiRecon. See Microsoft Teams Webhooks and Connectors and Slack API Sending messages using Incoming Webhooks for more information.

To add an integration:

1. Go to *Profile Settings* > *Integrations*.
2. Click *Add Integrations*. The *Choose Your Integration* page is displayed.



3. Select the software you want to integrate with. The *Add Integration* page is displayed.



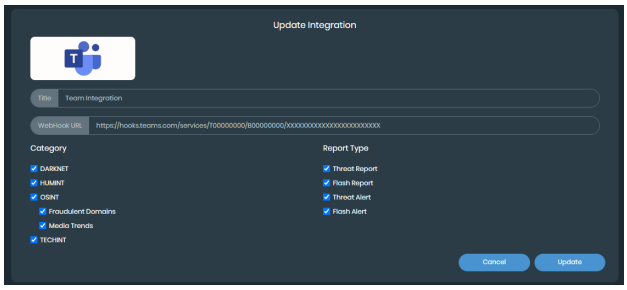
4. Enter the name of the integration in the *Title* text box.
5. Paste the webhook URL from the software into the *WebHook URL* text box.
6. Select the *Category* and *Report Type* fields that you want to include in the integration.
7. Clear any fields that you want to exclude from the integration.
8. Click *Save*. The integration is added.

Editing integrations

You can change the features and details of a webhook integration from the *Integrations* page.

To edit an integration:

1. Go to *Profile Settings* > *Integrations* and locate the integration.
2. Click the name or icon of the integration. The *Update Integration* page is displayed.



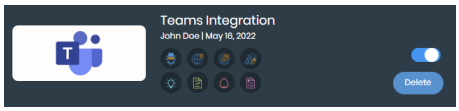
3. Edit the *Title* and *WebHook URL* text boxes, as needed.
4. Select the *Category* and *Report Type* fields that you want to include in the integration.
5. Clear any fields that you want to exclude from the integration.
6. Click *Update*. The webhook integration is updated.

Disabling integrations

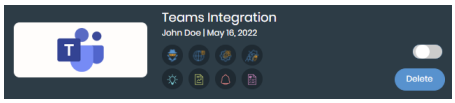
You can temporarily disable unused integrations, and then enable them again in the future. The integration toggle allows you to enable and disable an integration as needed.

To disable an integration:

1. Go to *Profile Settings* > *Integrations* and find the integration.



2. Select the toggle to disable the integration. The notifications are no longer sent to the software.



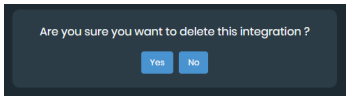
3. Select the toggle again to enable the integration.

Deleting and disabling integrations

You can delete unneeded webhook integrations.

To delete an integration:

1. Go to *Profile Settings* > *Integrations* and find the integration.
2. Click *Delete*. A confirmation message is displayed.



3. Click *Yes*. The integration is deleted.

Seeds

You can view your organization information in *Profile Settings* > *Seeds* page. *Seeds* page displays the information captured by FortiRecon during the following scenarios:

- Information you provide during onboarding.
- Any assets you add from *EASM* > *Asset Discovery* > *Bulk Add/Remove Assets*.

The Seeds section is read-only. If you want to remove an asset (ASN /IP address /IP range/ domain/ sub domain) from Seeds, you must remove it from *EASM* > *Asset Discovery* > *Bulk Add/Remove Assets*.

Because Seeds is your initial input, the EASM module uses it to discover additional assets and populate them in *EASM* > *Asset Discovery*. The assets in *EASM* > *Asset Discovery* are then used to populate the data in Brand Protection and ACI modules.

From the *Profile Settings* > *Seeds* page, you can:

- View your organization's registered assets. See Viewing your assets on page 207.

Viewing your assets

On the *Seeds* page, you can view the domain names, ASN, IP prefix, sub domains, card BINs, mobile apps, and social media profiles of your organization that are being monitored by FortiRecon. You can toggle between the following pages to view your organization's assets:

- Domains
- ASN
- IP Prefix
- IP Address
- Sub Domain
- Card BIN
- Owned Mobile Applications
- Social Media

To view your organization's assets:

1. Go to *Profile Settings* > *Seeds*.
2. Navigate between asset types by selecting desired tab.
3. Search for assets:
   - Navigate to one of the tabs, and search for a keyword in the *Search* box to look for entries specific to that asset type.

Notification Center

The *Notification Center* provides a centralized location for managing email notification settings within FortiRecon. You can view current settings, search for notifications, and enable or disable notifications based on your preferences. Administrators have additional privileges to view and modify notification settings for individual users.

All notifications are enabled by default.

From the *Profile Settings* > *Notification Center* page, you can:

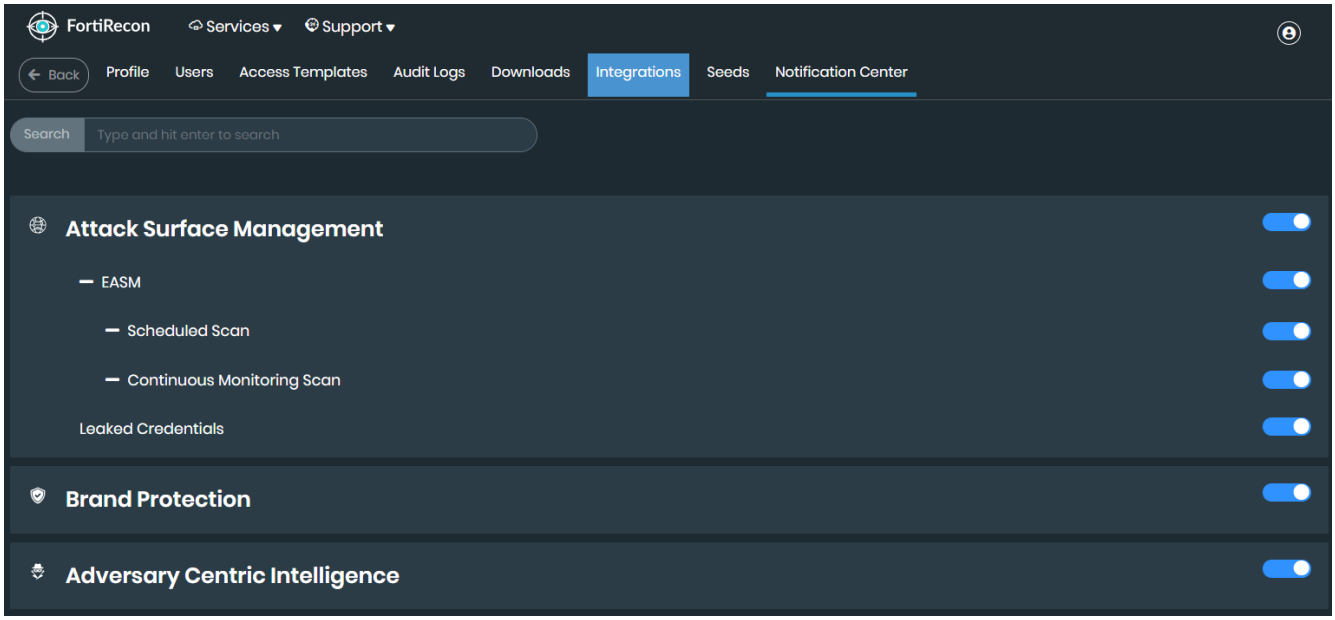
- View and edit your current notification settings. See Viewing and managing notification settings.
- Customize notifications in Adversary Centric Intelligence module. See Customizing notifications.
- Modify notification settings for other users as an Administrator. See Managing notifications as an administrator.

Viewing and managing notification settings

You can view and edit your current notification settings in *Profile Settings* > *Notification Center* page.

To view and edit notification settings:

1. Go to *Profile Settings* > *Notification Center*.
2. Search for a specific notification or select a module to view its available notification settings.
3. Toggle *enable/disable* to activate or deactivate notifications.



Customizing notifications

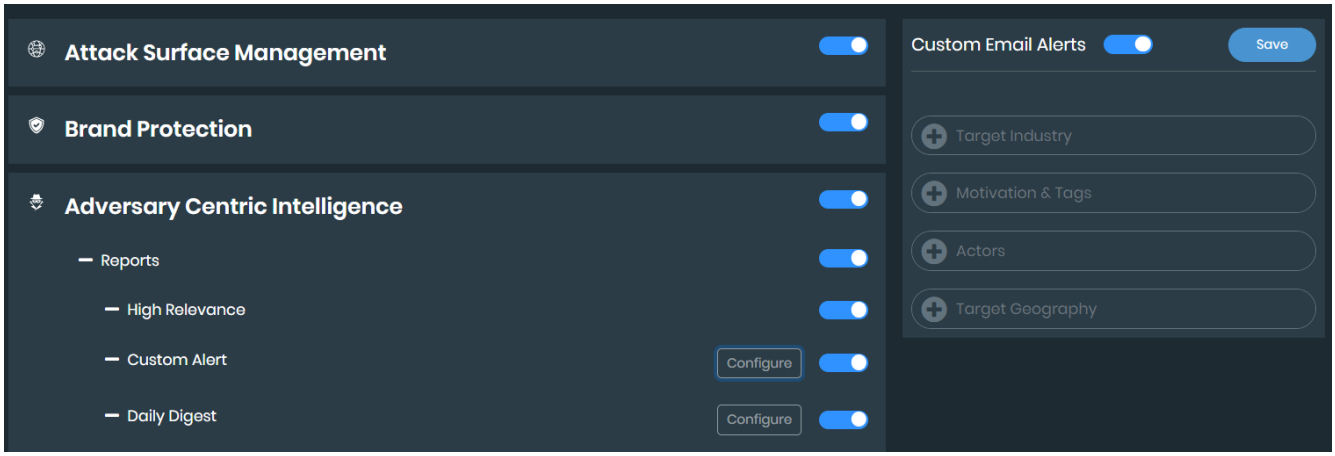
FortiRecon offers customization options for the following notifications. These configurations allow you to tailor your notifications to meet your requirements.

Module	Notification	Description
Adversary Centric Intelligence	Reports > Custom Alert	Customize by adding *Target Industry*, *Motivation & Tags*, *Actors*, and *Target Geography*.
	Reports > Daily Digest	Select the *Category*, *Report Type*, and *Time*.
	Stealer Infections > Compromised System (Leaked)	Select *Employee* and *User* domains.
	Stealer Infections > Compromised System (On Sale)	Select *Domain*.
	Cyber Threats > List of Widgets	Select from the list of available widgets.

Module	Notification	Description
	Intelligence Collection Lookup > List of Queries	Select from the list of available queries.

To customize notifications:

1. Go to *Profile Settings* > *Notification Center*.
2. Search for a supported customizable notification or select a module to view its available notifications.
3. Click *Configure* next to the desired notification.
4. Provide the necessary details.
5. Click *Save*.

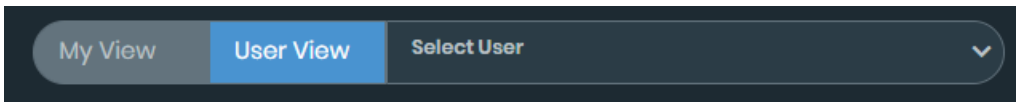


Managing notifications as an administrator

As an administrator, you have the privilege to view and modify notification settings for other users within your organization. This allows you to ensure that users receive notifications relevant to their roles and responsibilities.

To edit notification settings for other users:

1. Go to *Profile Settings* > *Notification Center*.
2. Select the *User View* option in top right corner.



3. Choose a user from the *Select User* dropdown.
4. Search for a specific notification or select a module to view its available notification settings.
5. Toggle *enable/disable* to activate or deactivate notifications.
6. Click *My View* to switch back to your own notification settings.

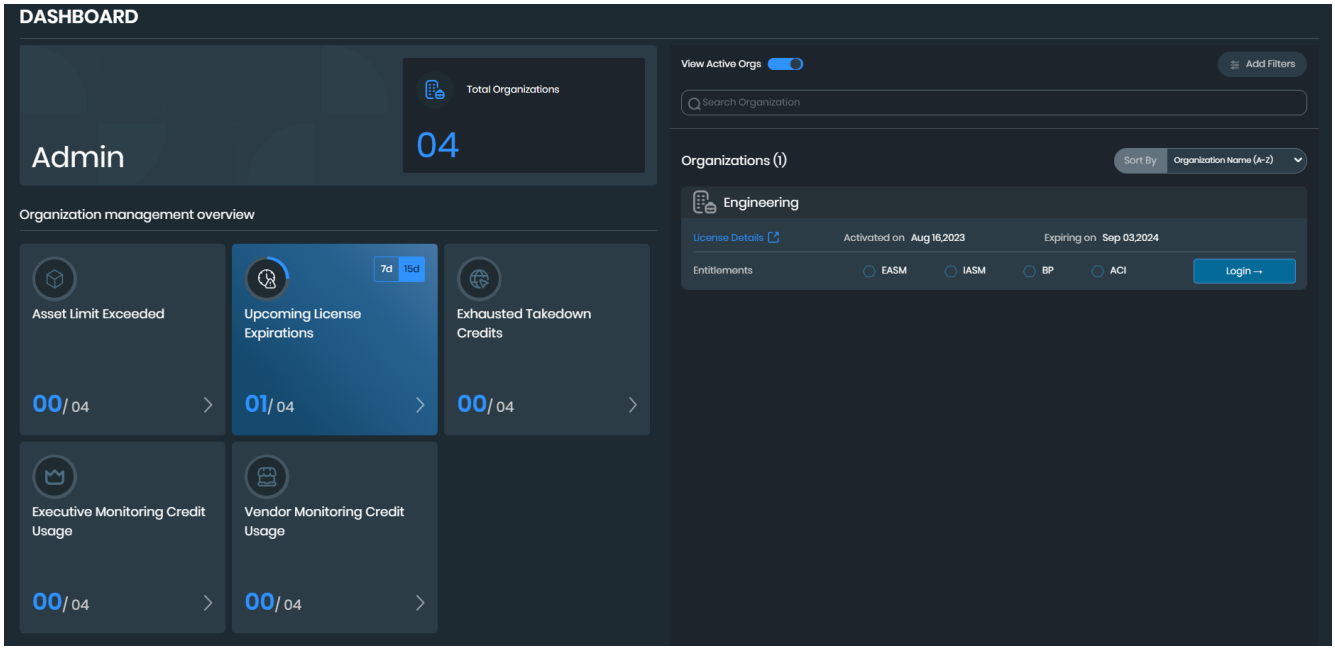
Any notification setting modified by an administrator can also be modified by the user.

Organization Dashboard

The Organization dashboard page provides a centralized view of all organizations you belong to and their associated licensing details.

You can select a specific organization and log in to access its corresponding FortiRecon portal. To switch between organizations, you can access *Organization* dashboard from the menu in the top-right corner of FortiRecon.

- Filtering organizations
- Viewing licensing details



Filtering organizations

To refine your view of organizations, you can use the following filtering options:

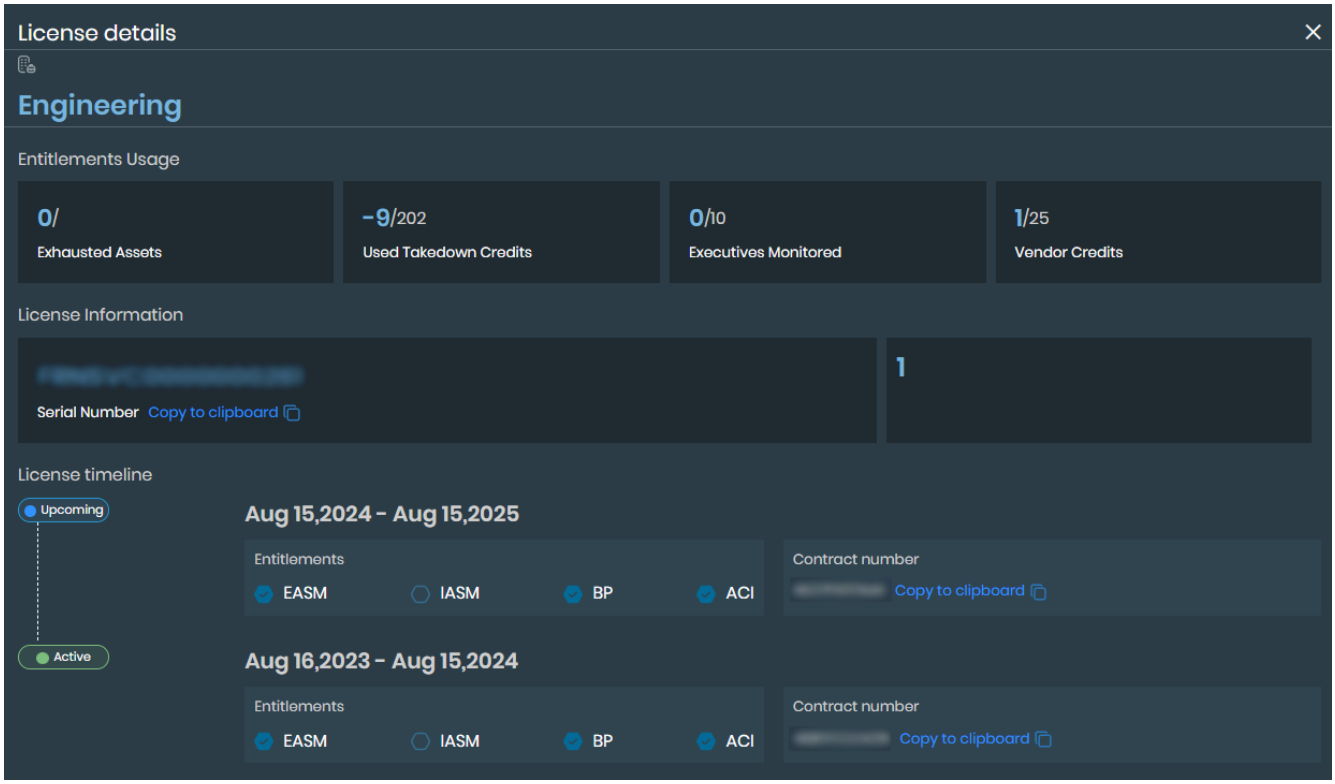
1. Toggle *View Active Orgs* to show or hide all active organizations.
2. Use search bar to search for a specific organization by name.
3. Click *Add Filters* to apply filters based on *Region*, *Country*, *Subscription Status*, and *Entitlements*.
4. Select predefined filters in *Organization management overview* section to filter organizations with *Asset Limit Exceeded*, *Upcoming License Expirations (7d or 15d)*, *Exhausted Takedown Credits*, *Executive Monitoring Credit Usage*, or *Vendor Monitoring Credit Usage*.
5. Use *Sort By* drop down to sort the filtered organizations.

- The *Provision Organization* option and *Add Filter* > *Provision Status* filter are only available to pAdmin user.
- If *New* filter is selected in *Add Filter* > *Provision Status*, all the other filters will be disabled.

Viewing licensing details

To view detailed licensing information for a specific organization, click *License Details* on the *Organization* dashboard page. The *License details* page displays the following information:

- Entitlements usage information including utilization count for *Exhausted Assets*, *Used Takedown Credits*, *Executives Monitored*, and *Vendor Credits*.
- License information including serial number and number of active contracts.
- License timeline displays *Active* and *Upcoming* license information, including contract period, entitlements, and contract number for each contract.



www.fortinet.com