User Guide

FortiRecon 26.1.0

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

February 20, 2026
FortiRecon 26.1.0 User Guide
75-261-1254425-20260220

TABLE OF CONTENTS

Change Log **8**
Introduction **9**
Requirements 10
Acceptable FortiRecon use cases 10
Default alerts 11
Monitoring Service Status 12
Licensing **13**
Standard FortiRecon Licensing 13
FortiRecon FortiFlex Licensing 14
Prerequisites 15
Transferring FortiPoints to FortiFlex Points 15
Creating a FortiRecon Configuration in FortiFlex 16
Creating a FortiRecon Entitlement in FortiFlex 18
Upgrading Trial License 19
Renewing Expired FortiRecon Licenses 20
Getting started **22**
Accessing FortiRecon portal **26**
Organization **28**
Prerequisites 28
Enabling Organization Portal 29
Creating an Organization 29
Creating an Organization Unit(OU) 31
Creating a Member Account 31
Creating a pAdmin account 33
Creating an OUAdmin account 35
Adding FortiRecon Licensing to Organization Unit (OU) 37
Transferring FortiPoints to FortiFlex points 38
Creating a FortiRecon configuration in FortiFlex 39
Creating a FortiRecon entitlement in FortiFlex 42
Provisioning FortiRecon 43
Managing Entitlements 46
User Roles 47
Overview **49**
Viewing Digital Risk Posture 50
Digital Footprint Map 50
License Details 54
Trends Reporting 54
Top Threat Actors 54
Activities 55
Viewing MITRE ATT&CK Framework 55
Downloading Executive Report 57

Attack Surface Management **58**
EASM 59
EASM Dashboard 59
EASM Security Issues 63
EASM Asset Discovery 68
Web Application Assessment 77
EASM Asset Management 85
IASM 96
IASM Agent 97
IASM Dashboard 100
IASM Security Issues 104
IASM Asset Discovery 110
IASM Asset Management 112
Leaked Credentials 122
Viewing leaked credentials by year 122
Viewing leaked credential details 123
Viewing breached datasets 123
Exporting leaked accounts 125
Integrations 125
Adding integrations 125
Editing integrations 128
Brand Protection **129**
Dashboard 130
Viewing the domain threat summary 130
Viewing the brand abuse summary 131
Viewing the information exposure summary 131
Viewing the alert summary 132
Viewing the takedown credit summary 133
Domain Threats 133
Reviewing domain threats 134
Managing domain threats 135
Filtering domains 135
Digital watermark 136
Adding a new domain threat 137
Managing referrer logs 138
Social Media Threats 140
Reviewing social media threats 140
Managing social media threats 141
Filtering social media threats 141
Adding official profiles 142
Adding a new social media threat 143
Rogue Mobile Apps 144
Reviewing rogue applications 144
Filtering rogue applications 145
Adding official applications 146
Assigning application status 147
Taking down rogue apps 147
Exporting rogue applications 148

Executive Monitoring 149
Reviewing executive profile threats 149
Filtering executive profile threats 150
Adding executive profiles 150
Code Repo Exposure 152
Managing keywords 152
Reviewing attributes 154
Managing attributes 155
Filtering attributes 155
Open Bucket Exposure 156
Reviewing files 156
Managing files 157
Filtering files 157
Takedown 158
Authority Letters 159
Initiating Takedowns for IMs 163
Reviewing takedown requests 164
Filtering takedown requests 165
Revoking Takedown Requests 165
Adversary Centric Intelligence 167
Dashboard 167
Changing the dashboard date range 168
Viewing risk exposure summary 168
Viewing global threat report summary 170
Reports 171
Using FortiAI Assistant 172
Viewing reports 173
Filtering reports 175
Sharing reports 176
Card Fraud 176
Viewing leaked card information 177
Filtering leaked card information 177
Exporting a list of leaked cards 178
Stealer Infections 179
Viewing leaked compromised systems 179
Viewing on sale compromised systems 180
Filtering stealer infection information 181
Exporting stealer infections data 184
OSINT Cyber Threats 185
Reviewing threats 185
Pinning events 186
Subscribing to event notifications 187
Adding subscriptions 188
Vulnerability Intelligence 189
Vulnerability exposure 189
Global notable vulnerabilities 192
Viewing and filtering CVE reports 193
Exporting CVEs 195

Manually adding CVEs 195
Ransomware Intelligence 196
Viewing ransomware intelligence 196
Filtering ransomware intelligence 203
Exporting ransomware information 205
Managing My Watchlist 205
Vendor Risk Assessment 207
Adding a new vendor to the watchlist 207
Viewing the vendor risk assessment 208
Intelligence Collection Lookup 211
Search Query 211
Search Results 215
Investigation 218
Reviewing IP address reputation 219
Reviewing domain reputation 219
Reviewing a file hash 219
Reviewing a CVE 219
Security Orchestration 221
Getting Started 222
Configuring and Running a Standalone Playbook 223
Configuring and Running Contextual Playbooks 227
Home 229
Playbooks Overview 230
Playbooks Collections 230
Playbooks 230
Playbook Designer 232
Playbook Steps 235
Playbook Assets 245
Global Variables 245
Event Templates 245
Content Hub 247
Viewing Content Hub 248
Connectors 249
Widgets 250
Solution Packs 251
Agents 252
Execution Logs 252
Using Execution Logs 253
Tasks 256
Profile settings 257
Accessing profile settings 257
Profile 258
Editing user idle timeout 258
Subscription Details 259
Uploading Organization Logo 261
Sharing the API key 261
Users 261

Viewing user accounts 262
Adding users 262
Editing users 264
Deleting users 265
Configuring External IdP 265
Access templates 267
Viewing access templates 267
Adding a template 267
Editing a template 268
Audit Logs 269
Viewing audit logs 269
Filtering audit logs 269
Exporting audit logs 270
Downloads 270
Viewing downloads 271
Retrieving downloads 271
Deleting downloads 271
Integrations 272
Viewing integration details 272
Adding integrations 272
Editing integrations 273
Disabling integrations 273
Deleting and disabling integrations 273
Seeds 274
Viewing your assets 274
Business Names 275
Card BIN 277
Notification Center 279
Viewing and managing notification settings 279
Customizing notifications 280
Managing notifications as an administrator 281
Organization Dashboard 283

Change Log

Date	Change Description
2026-02-20	Initial release.
2026-02-23	Updated Upgrading IASM Agent topic.
2026-02-25	Updated Security Orchestration topic.
2026-03-06	Updated the following topics. • Filtering stealer infection information on page 181 • Investigation

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 59.
	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 96.
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 129.
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 167.

Security Orchestration	The *Security Orchestration* module helps you investigate and respond to security threat findings from Attack Surface Management, Brand Protection, and Adversary Centric Intelligence. This solution reduces the time responders require to prioritize and take appropriate actions by automating and streamlining security workflows. It provides preconfigured playbooks to help you get started quickly. You can also create playbooks using connectors, add playbook variables, and view execution logs. Install and connect agents if required. See Security Orchestration.
Profile Settings	The Profile Settings module allows you to personalize your FortiRecon account and provide information on your organization. See Profile settings on page 257.

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 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 Fortinet 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.

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 10 and Licensing.
- 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 207.

- Bank identification numbers (BINs) should only be added for the licensed entity and brand. See Card Fraud on page 176.

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.

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
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

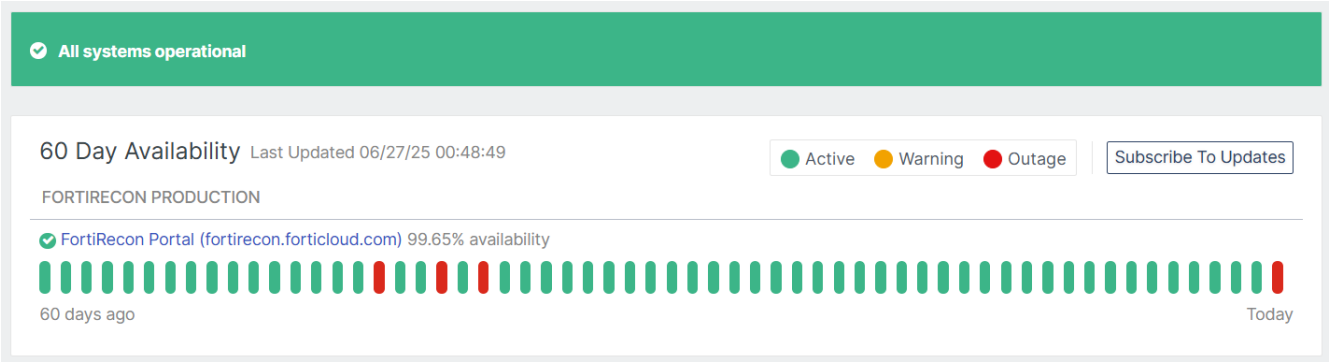
The FortiRecon Status page provides an overview of the current and historical availability of the FortiRecon service. You can receive and track notifications for incidents and downtime affecting the FortiRecon GUI and Rest APIs.

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

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.

The FortiRecon service uptime is displayed graphically for a period of 60 days. The downtime/outage events experienced by the service are indicated in colored bars; hover over the *Warning* or *Outage* bars to view the details. Click *Subscribe To Updates* and enter your email address to receive notifications.

Click *FortiRecon Portal* link to view detailed status statistics.



The *Scheduled Maintenance* section displays upcoming maintenance information.

The historical incidents are listed in *Maintenance History For Last 30 Days* section.

Licensing

You can license FortiRecon in two ways: by purchasing a standard FortiRecon license or by subscribing through the FortiFlex program.

- Standard FortiRecon Licensing
- FortiRecon FortiFlex Licensing
- Upgrading Trial License
- Renewing Expired FortiRecon Licenses

Standard FortiRecon Licensing

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. After registration you can continue with subscribing to FortiRecon, see Getting started.

Licenses are structured into core solution bundles and stackable add-on services.

Solution Bundles

You can choose from three primary solution bundles based on the required level of monitoring.

- *External Attack Surface Monitoring (EASM)*
- *EASM and Brand Protection (BP)*
- *EASM, BP, and Adversary Centric Intelligence (ACI)*

Default Entitlements

The following capacities are included as default entitlements with any of the solution bundles listed above:

- *Takedowns*: 2 credits
- *Executive Profiles*: 10
- *Vendors*: 25
- *Security Orchestration Playbooks*: 100 per month

Add-on Services

The following add-on services are available.

Add-on Service	Description
Internal Attack Surface Management (IASM)	Adds monitoring for internal assets. **Note:** Requires an active EASM license.

Add-on Service	Description
Takedown Service	Increases your capacity to request the removal of malicious content. Available in packs of 5, 10, or 50 Takedowns. Credits must be activated within one year and expire three years after activation.
Executive Monitoring	Expands monitoring for high-value targets. Available in stackable packs of 5, 10, or 50 additional Executives.
Vendor Monitoring	Increases third-party risk visibility. Available in stackable packs of 5, 10, or 50 additional Vendors.
Security Orchestration Playbooks	Increases monthly automation capacity by 2000 playbook executions per pack and is stackable.

For more details on specific SKUs and ordering information, please refer to the FortiRecon Data Sheet.

FortiRecon FortiFlex Licensing

You can subscribe to FortiRecon by using FortiFlex points.FortiFlex is a consumption-based licensing model that allows you to use FortiPoints to pay for Fortinet products and services, including FortiRecon.

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.

- Prerequisites
- Transferring FortiPoints to FortiFlex Points
- Creating a FortiRecon Configuration in FortiFlex
- Creating a FortiRecon Entitlement in FortiFlex

Prerequisites

Before using FortiFlex for FortiRecon, ensure you meet these requirements:

- Enroll in the *FortiFlex Enterprise* program to enable FortiFlex in *FortiCloud Marketplace*. FortiFlex currently supports only the prepay option.
- Purchase sufficient *FortiPoints* to cover the resources you plan to allocate for your FortiRecon deployments.

> - To purchase *FortiFlex Enterprise* 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.

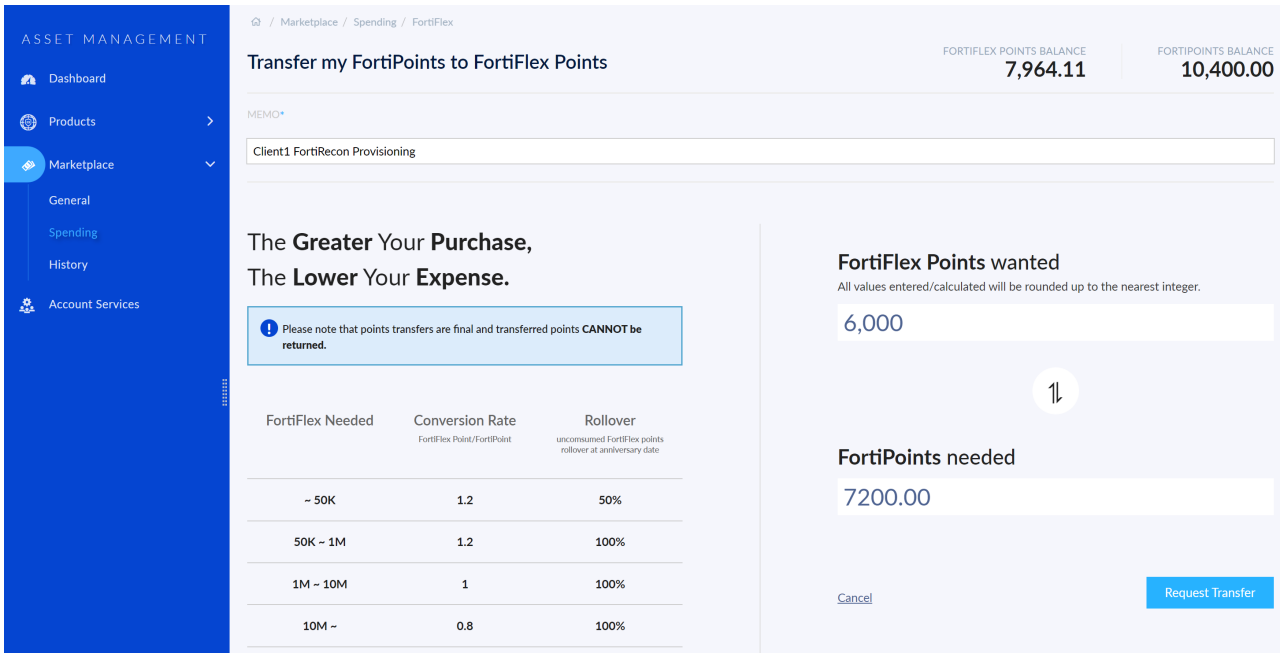
Transferring FortiPoints to FortiFlex Points

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 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

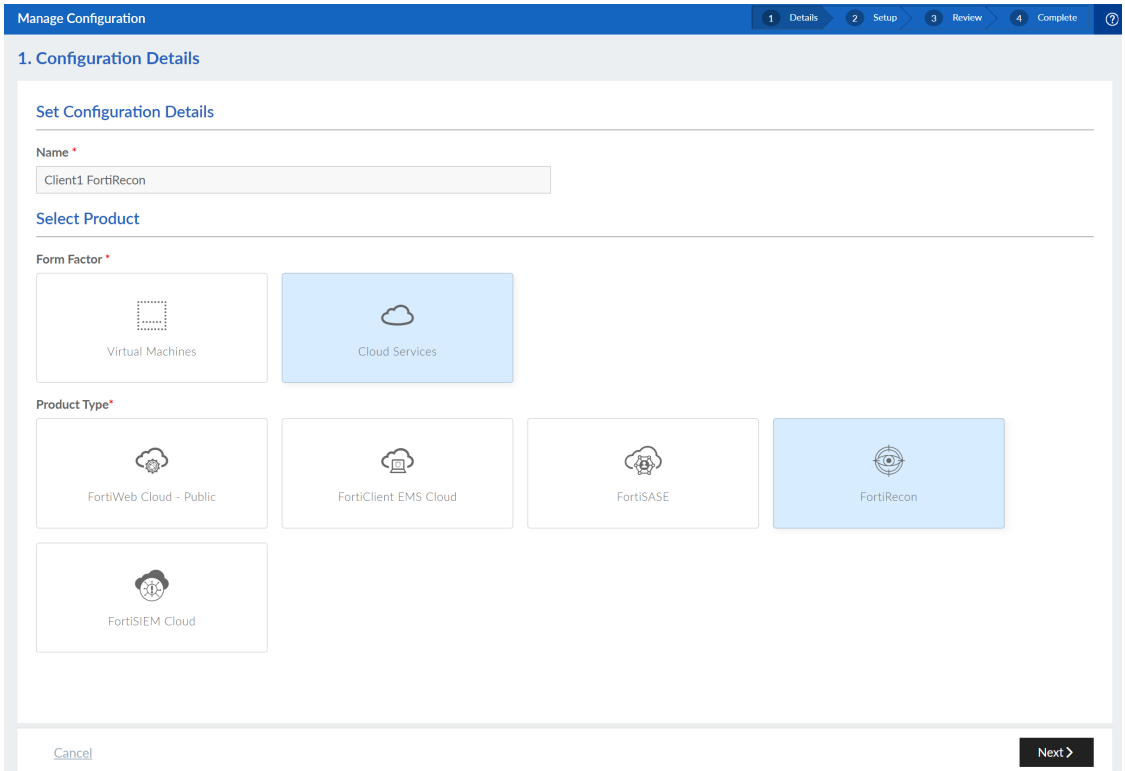
Configurations allow you to define and customize a FortiRecon service package, including the number of assets, internal networks, executives, and vendors to be monitored.

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 FortiCloud account.
   a. If logging in for the first time, email verification must be completed.
2. Go to *Services* > *FortiFlex*.
3. In FortiFlex, go to *Configurations*, and click *New Configuration*.
4. In the *Configuration Details* page, set the following configuration details and click *Next*.

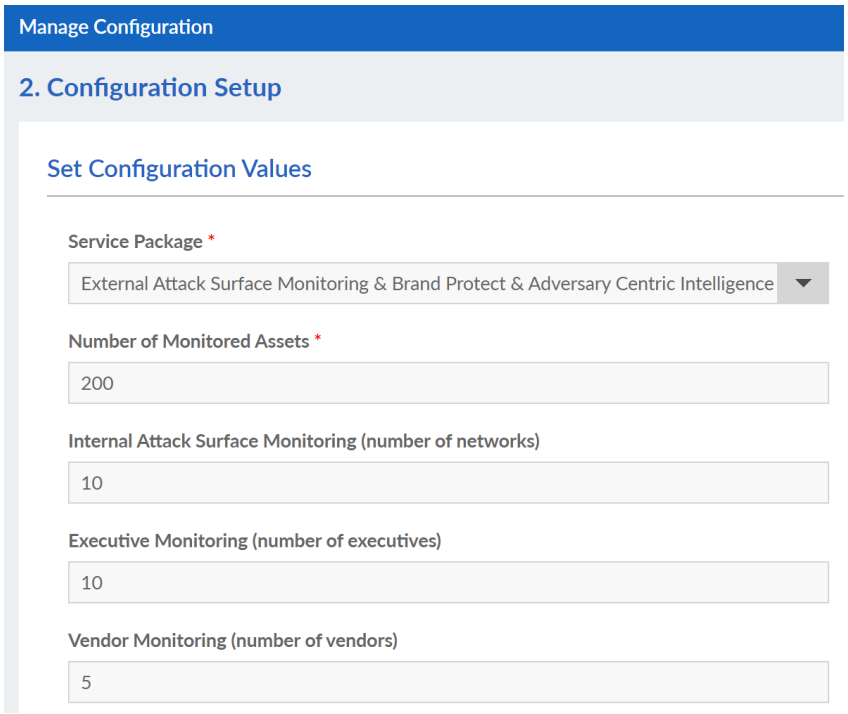
- *Name* - Enter a configuration name.
- *Form Factor* - Select *Cloud Services*.
- *Product Type* - Select *FortiRecon*.



5. 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.

6. Review the configuration details, and click *Submit*.
7. 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.

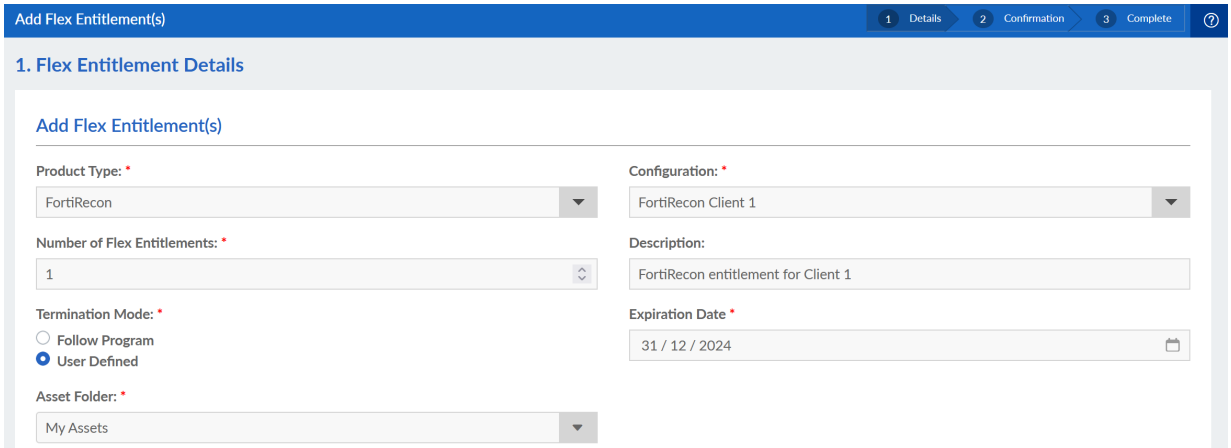
Perform the following steps to create a FortiRecon entitlement.

1. If not logged in, log in to https://support.fortinet.com/ using your FortiCloud account.
2. Go to *Services* > *FortiFlex*.
3. Go to *Flex Entitlements*, and click *New Flex Entitlement*. The *Add Flex Entitlement* page opens.
4. 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*.



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

After successful creation, copy the serial number for your new FortiRecon entitlement. Continue with subscribing to FortiRecon, see Getting started.

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

Upgrading Trial License

During your FortiRecon trial period, you have two options for upgrading to a full subscription, either by purchasing a standard license or by subscribing via FortiFlex.

Upgrading During the Trial Period

If your trial period is still active, you can upgrade your license by adding a purchased standard license or a FortiFlex entitlement.

To upgrade your license:

1. Go to **Profile Settings > Profile**.
2. Scroll to **Subscription Details**.
3. Click the edit icon next to **Contract Number**.

4. Enter the following information:
   - *License Serial*: Enter your FortiRecon license serial number (for standard licenses) or the serial number obtained from your FortiFlex entitlement.
   - *Email*: Enter the email address used to purchase the license or associated with your FortiCloud account for FortiFlex.
   - *Contract Number*: If you are upgrading with a standard FortiRecon license, enter the contract number. This field is not required for FortiFlex subscriptions.
5. Click **Save & Next**.
6. Enter your seed information. Based on the purchased license or FortiFlex configuration, you can add an additional domain or modify existing domain details. Select the **Add/Remove Assets** checkbox to add or remove assets as needed.

Upgrading After Trial Expiration

If your trial period has already expired, attempting to log in will display an expiration page. In this case, you can purchase a new standard license or create a FortiFlex entitlement and then perform these steps:

1. Log in to FortiRecon. The license expiration page is displayed. Provide the following details:
   - *License Serial*: Enter your FortiRecon license serial number (for standard licenses) or the serial number obtained from your FortiFlex entitlement.
   - *Contract Number*: If you are upgrading with a standard FortiRecon license, enter the contract number. This field is not required for FortiFlex subscriptions.
   - *Email*: Enter the email address used to register the contract or associated with your FortiCloud account for FortiFlex.
2. Click Verify.
3. FortiRecon sends a One Time Password (OTP) to your email. This OTP is valid for five minutes. Enter the OTP and click Validate. If needed, click the regenerate icon to receive a new OTP.
4. Once validated, enter the primary domain and click *Proceed*. A confirmation pop-up appears.
   - Click **Use existing account** to continue with your existing data.
   - Click **Create new account** to create a new account. If you select Create new account, the FortiRecon Provisioning form appears.

For more information on completing provisioning form, see Getting started.

> Creating a new account will delete all previous data.

Renewing Expired FortiRecon Licenses

If your current FortiRecon license has expired, purchase a new license or create a new FortiFlex entitlement, then perform the following steps to add it:

1. Log in to FortiRecon. The license expiration page is displayed. Enter the following information.
   - *License Serial*: Enter your new FortiRecon license serial number (for standard licenses) or the serial number obtained from your new FortiFlex entitlement.

- *Contract Number*: If you are renewing with a standard FortiRecon license, enter the contract number. This field is not required for FortiFlex subscriptions.
- *Email*: Enter the email address used to register the contract or associated with your FortiCloud account for FortiFlex.

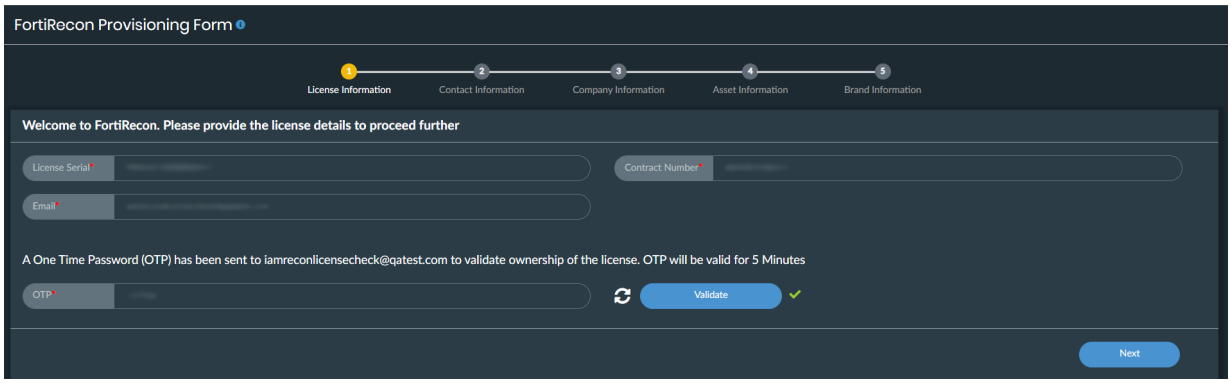
2. Click *Verify*.
3. A One Time password (OTP) will be sent to your email and is valid for five minutes. Enter the OTP and click *Validate*. Click regenerate icon to generate a new OTP if needed.
4. Once validated, enter the primary domain and click *Proceed*.

Getting started

After you acquire a FortiRecon license or entitlement, you can subscribe and start the service. For more information on licensing, see Licensing

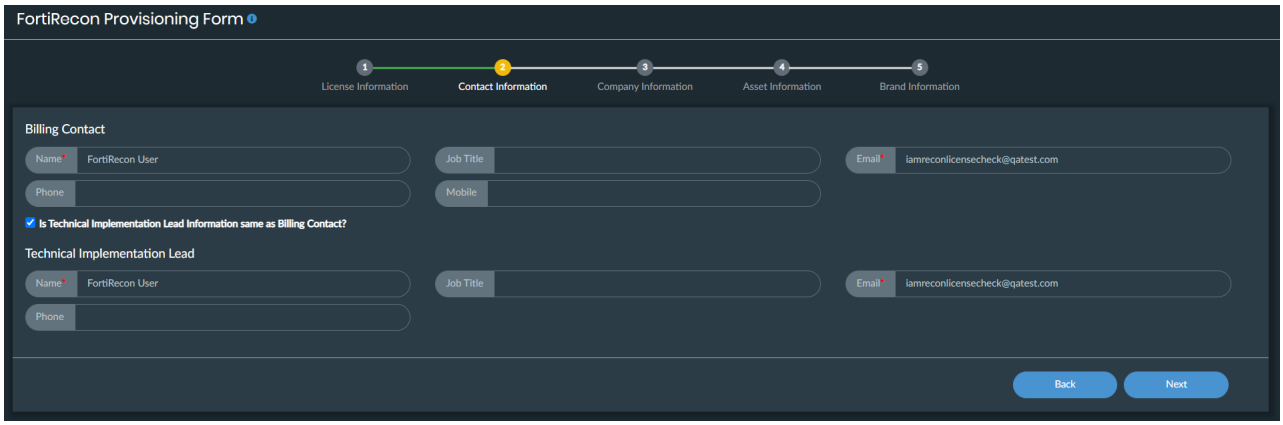
To subscribe to FortiRecon:

1. After registering your standard license (see Standard FortiRecon Licensing) or obtaining your FortiFlex serial number (see FortiRecon FortiFlex Licensing), go to FortiRecon at https://fortirecon.forticloud.com.
2. Click *Login*. The FortiCloud login page is displayed. Enter your FortiCloud credentials.
3. After you log in to FortiRecon for the first time, the *FortiRecon Provisioning Form* page is displayed.
4. *License Information*.
   a. Enter the following information.
      - *License Serial*: Enter your FortiRecon license serial number (for standard licenses) or the serial number obtained from your FortiFlex entitlement.
      - *Contract Number*: If you are using a standard FortiRecon license, enter the contract number. This field is not required for FortiFlex subscriptions.
      - *Email*: Enter the email address used to register the contract or associated with your FortiCloud account for FortiFlex.
   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. Once verified, click *Next*.



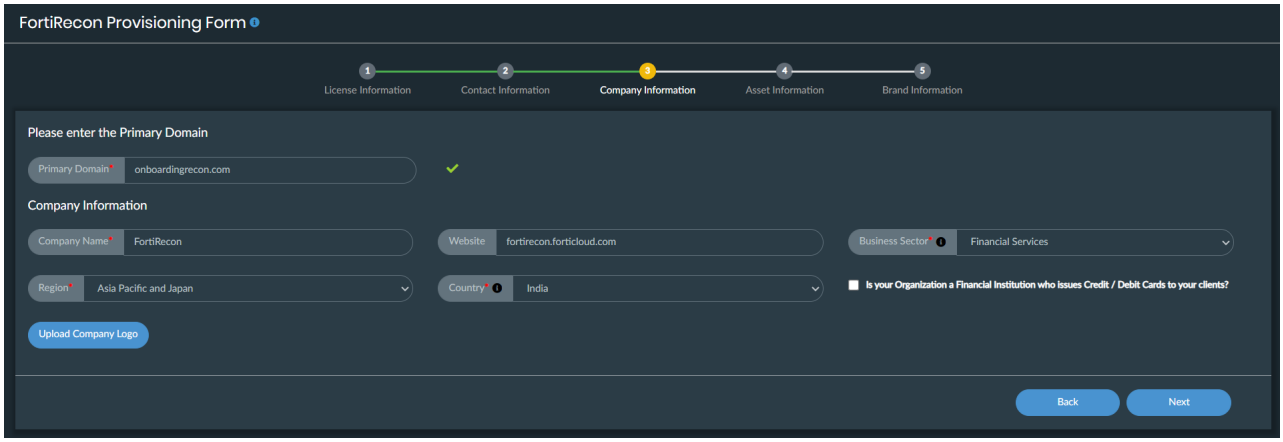
5. *Contact Information*.
   a. Enter the contact information of the billing contact in the *Billing Contact* fields.
   b. Enter your contact information in the *Technical Implementation Lead* fields. Select *Is Technical Implementation Lead Information same as Billing Contact* checkbox if applicable.

> 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.

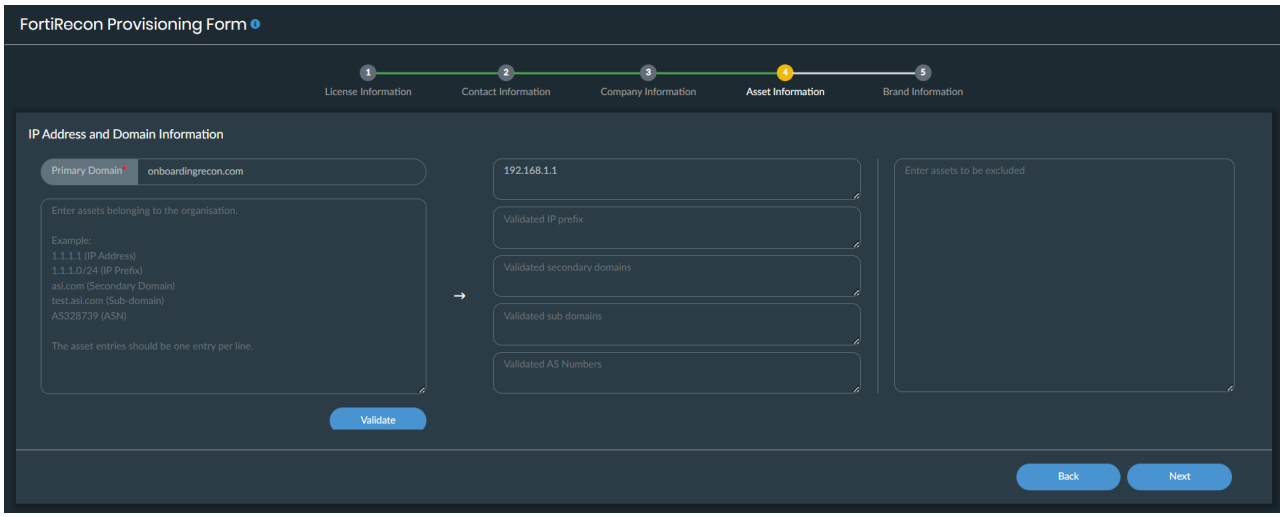


6. *Company Information*.
   a. Enter the primary domain. If the domain already exists, a confirmation prompt appears.
      - *Use existing account*: Click to continue with existing data. The license will be added to the existing organization.
      - *Create new account*: Click to create a new account. **Note**: Creating a new account will delete all previous data.

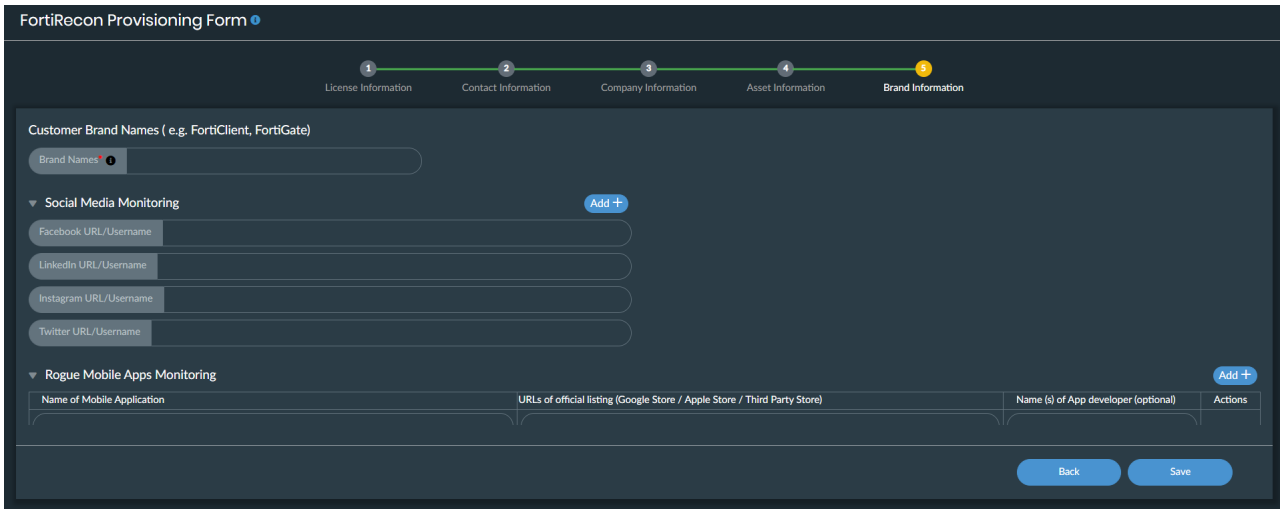
        If you create a new account, an authorization code valid for 24 hours is generated. Contact Fortinet support to obtain the authorization code and delete the existing information.
   b. Once primary domain validated, enter your organization's information in the *Company Information* fields. Click *Upload Company Logo* to browse and upload your organization's logo.
   c. If your organization is a Financial Institution issuing credit or debit cards, select the checkbox. This will enable the *Card Information* step.



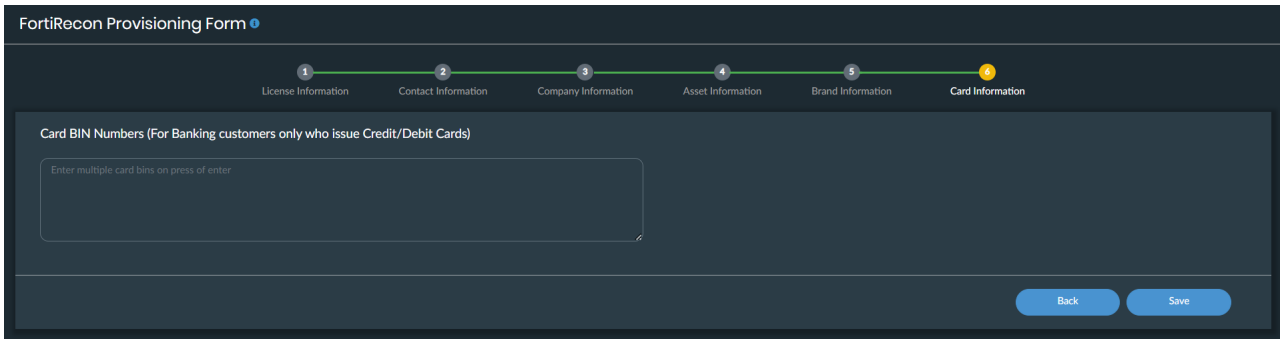
7. *Asset Information*. Enter your organization's assets information including primary, secondary and sub domains, IP addresses, IP range, ASN, assets to be excluded from monitoring.



8. *Brand Information*. Enter your brand names, social media profile and mobile applications to be monitored. Click *Save*.



9. *Card Information*. Enter Card BIN numbers. This is only for financial institutions who issue credit or debit cards.



10. Click *Save*. Your information will be sent to the FortiRecon team for review and provisioning. You will be redirected to FortiRecon portal.
11. Wait for the FortiRecon team to analyze your assets and populate the FortiRecon portal for you.

12. When you receive an email from the FortiRecon team, you can access the FortiRecon portal and review the analysis.

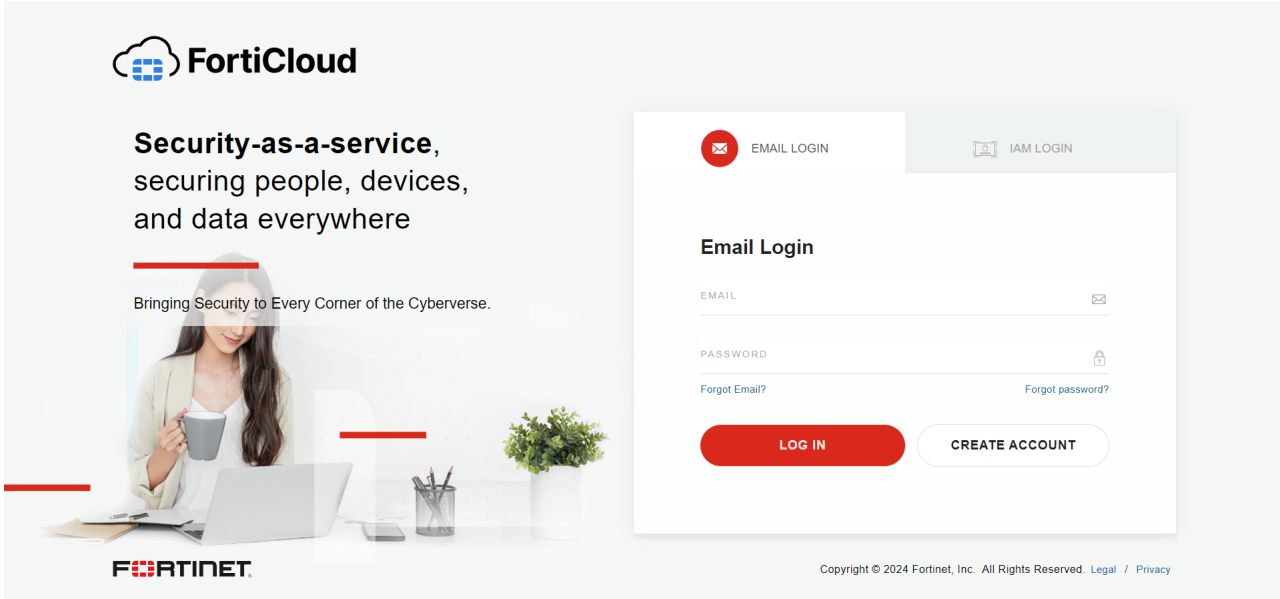
Accessing FortiRecon portal

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:

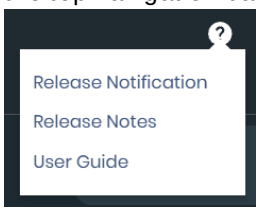
1. Go to FortiRecon at https://fortirecon.forticloud.com.

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



3. Enter your FortiCloud credentials.

4. Click *Login*. The *Release Notification* window displays the latest features upon login. You can also access this information, along with links to the *User Guide* and *Release Notes*, via the *Help*(question mark) icon in the top navigation bar.



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

5. Click *Back*. The *Overview* page is displayed. See Overview.

Organization

FortiRecon supports FortiCloud Organization, which lets you create and manage FortiRecon for multiple sub-organizations using a multitenant approach. You can create an Organizational Unit (OU) for each sub-organization and then provision FortiRecon for that OU. Each OU requires a dedicated FortiRecon license.

Perform the following steps to create an organization.

1. Prerequisites
2. Create a new organization.
3. Create an Organization Unit(OU).
4. Create a Member Account.
5. Create a pAdmin account.
6. Create an OU Admin account.
7. Add FortiRecon license to an Organization Unit(OU).
8. Provision FortiRecon.

To onboard and manage clients to FortiRecon, Managed Security Service Providers (MSSPs) can refer to FortiRecon for Managed Security Services Providers (MSSPs).

Prerequisites

Before creating the organization, ensure you have completed the following.

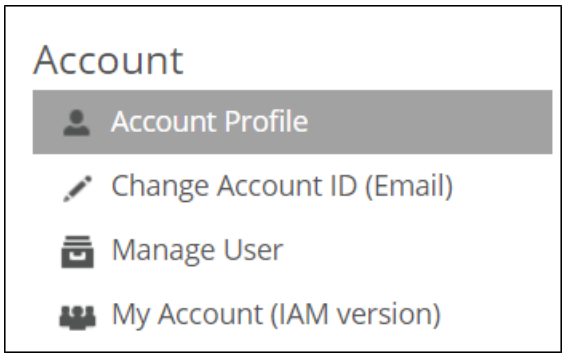
- The organization *Root Account* must have access to a basic *Fortinet Developer Network (FNDN)* subscription. See Creating a FortiCloud account to create a new FortiCloud account and Accessing Fortinet Developer Network to access FNDN.
- Enable the *Organizations* portal within the FortiCloud account. See Enabling Organization Portal.
- Purchase a FortiRecon standard license. Or, if you want to use the FortiFlex method for licensing:
  - Enroll in *FortiFlex Enterprise*program to enable FortiFlex in *FortiCloud Marketplace*.
  - Purchase sufficient *FortiPoints* to cover the resources allocated to client deployments.

- To purchase a *FortiFlex Enterprise*, 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.
- Each Organizational Unit (OU) requires a dedicated FortiRecon license, either a FortiFlex or standard license.

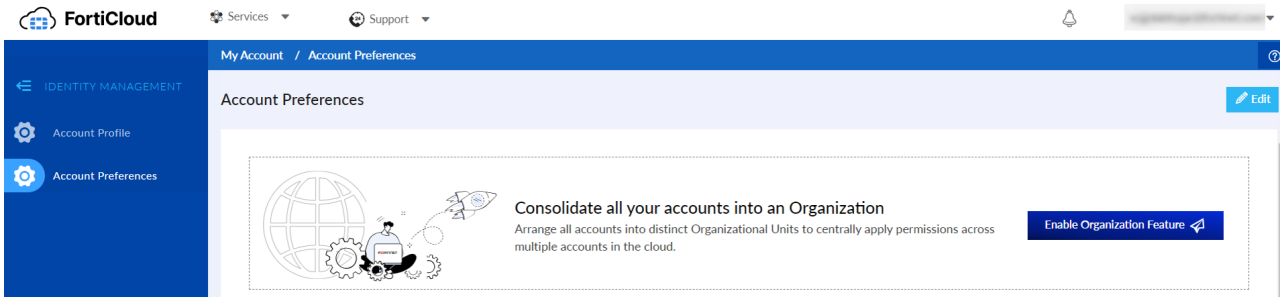
Enabling Organization Portal

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*.

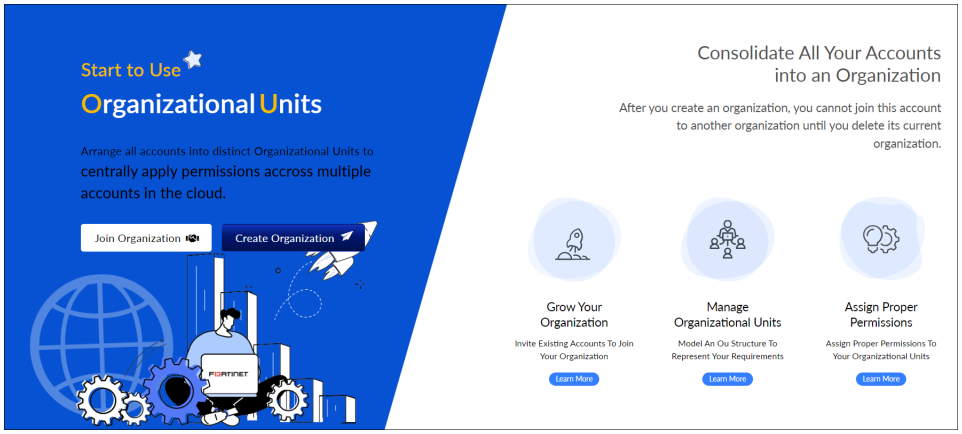


Creating an Organization

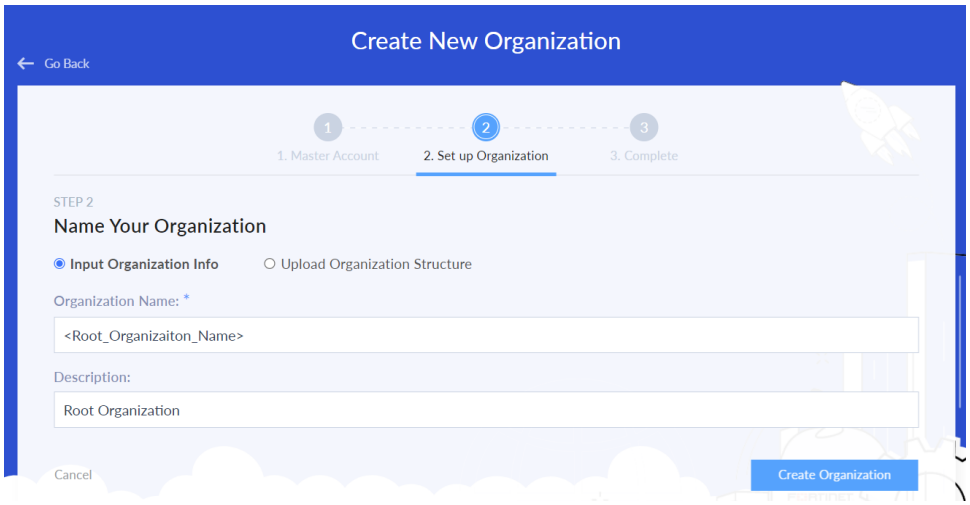
When you create an Organization your account becomes the *Root Account* for the organization.

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:

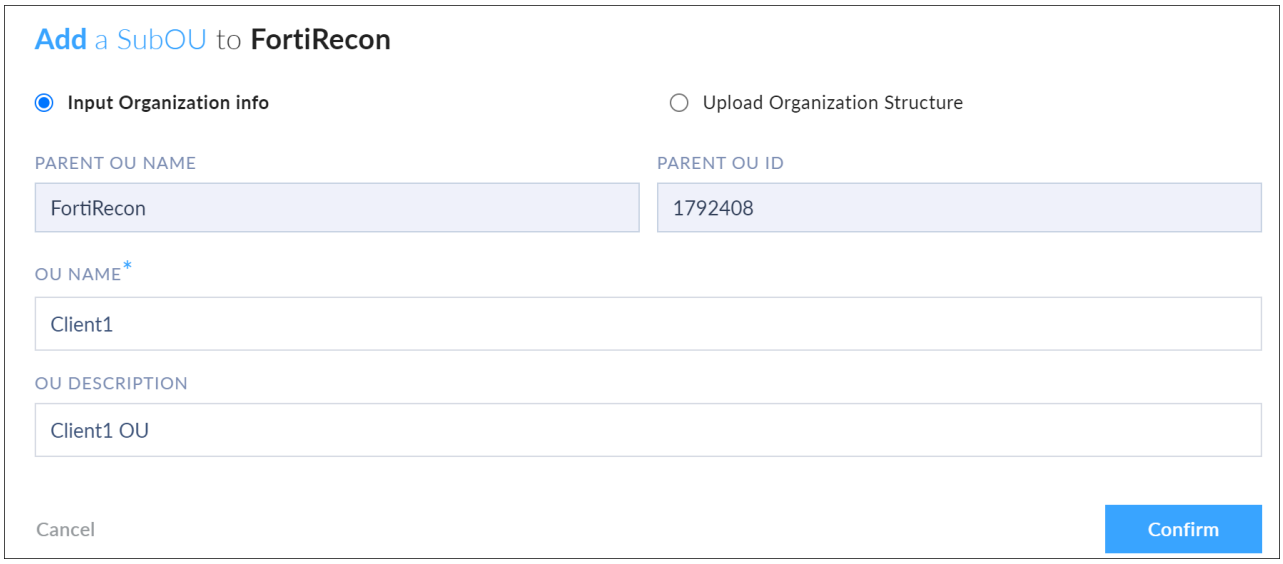
1. On the Set up Organization page, click *Upload Organization Structure*.
2. Download the Bulk Import template.
3. Use the template instructions to enter the OU information and create the organization hierarchy.
4. After you have completed the template, click *Organization Structure File Upload*, and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

Creating an Organization Unit(OU)

Organizational Units (OUs) are folders used to organize your sub-organizations 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.

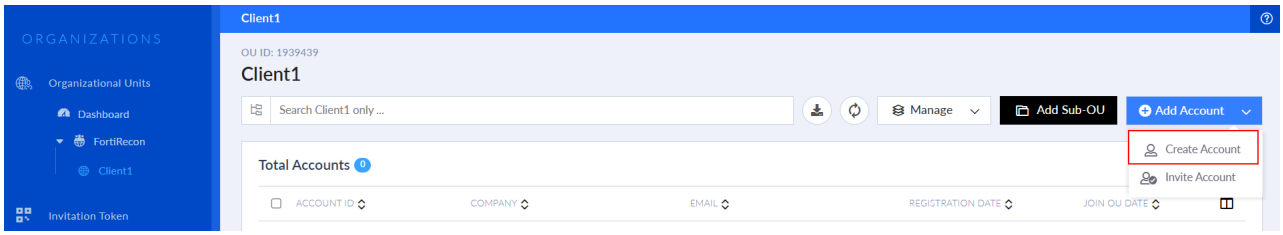


Creating a Member Account

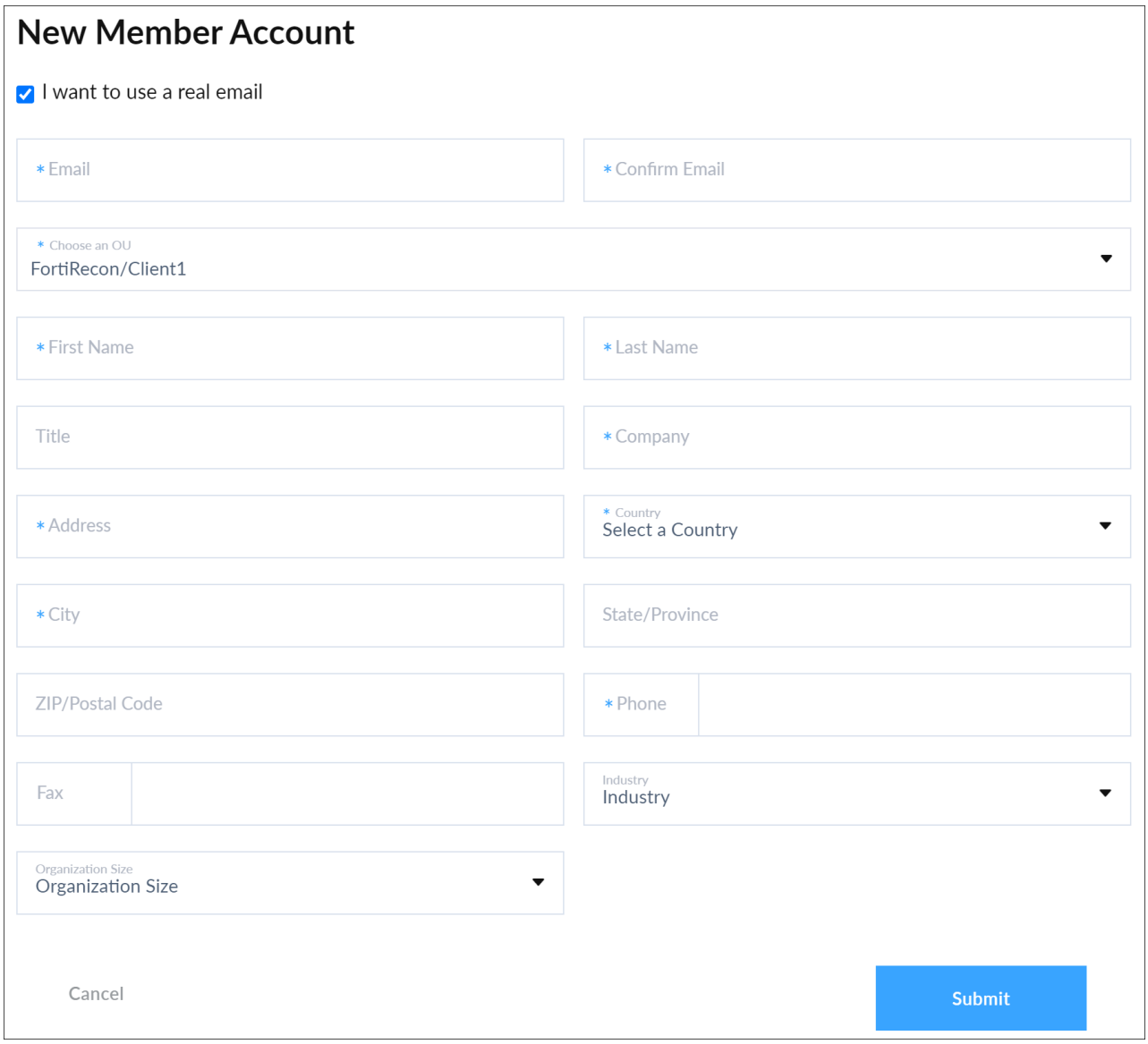
A Member Account is a FortiCloud account that joins an Organization. New Member Accounts can be created directly within the *Root account Organization* or a *SubOU*.

Perform the following steps to create a member account.

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



3. Select *I want to use a real email* to input the email address. Fields are displayed to enter the email address.
4. Select the 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 sub-organization information.
6. Click *Submit*. A confirmation message is displayed.

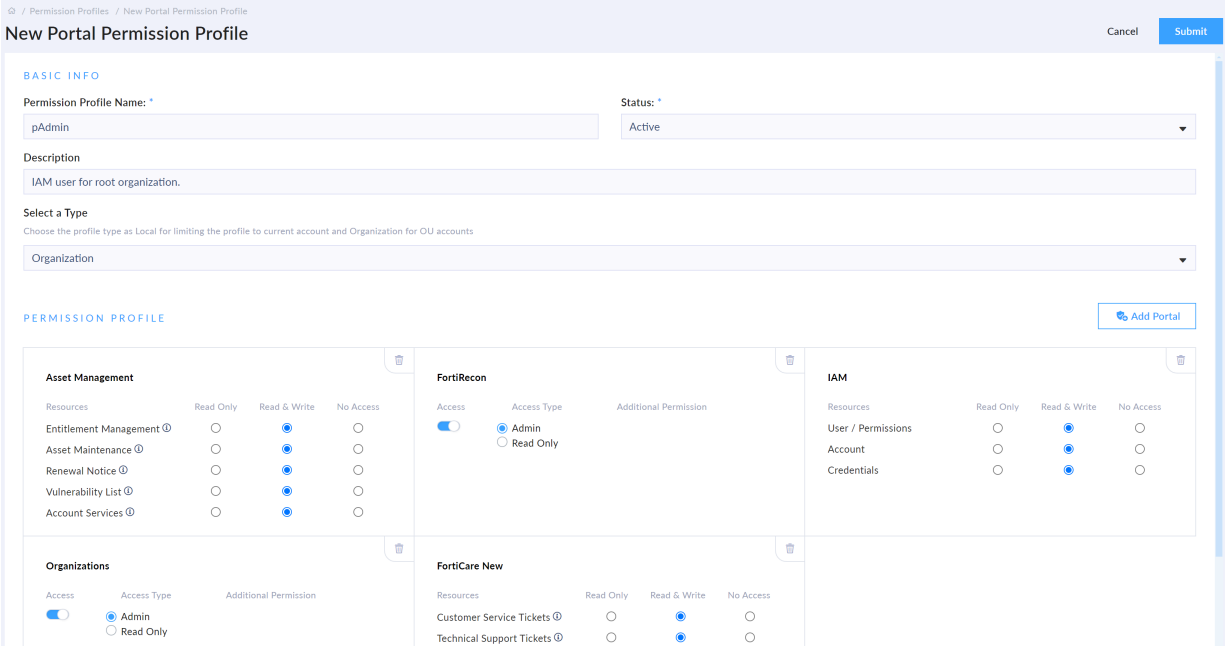
For more information on creating member account, see FortiCloud Services > Organization Portal > Creating new Member Accounts.

Creating 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 FortiRecon. 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*.

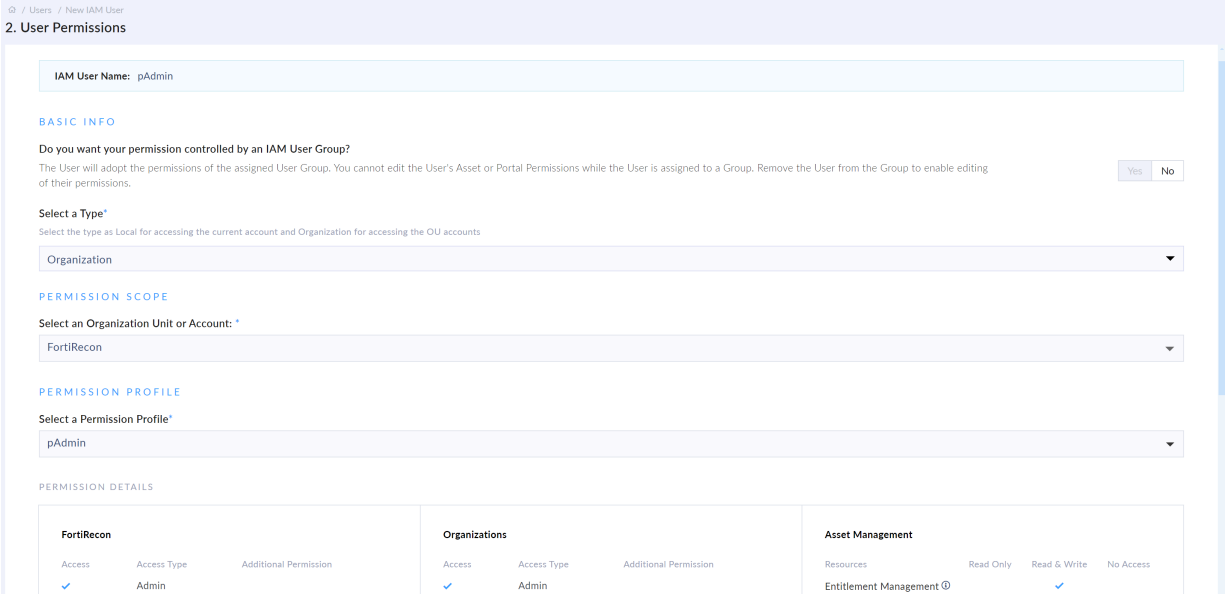


For more information, see Permission profiles within Organizations in the *Identity & Access Management*.

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 root account email address. The account used to create the organization is the root account.
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.

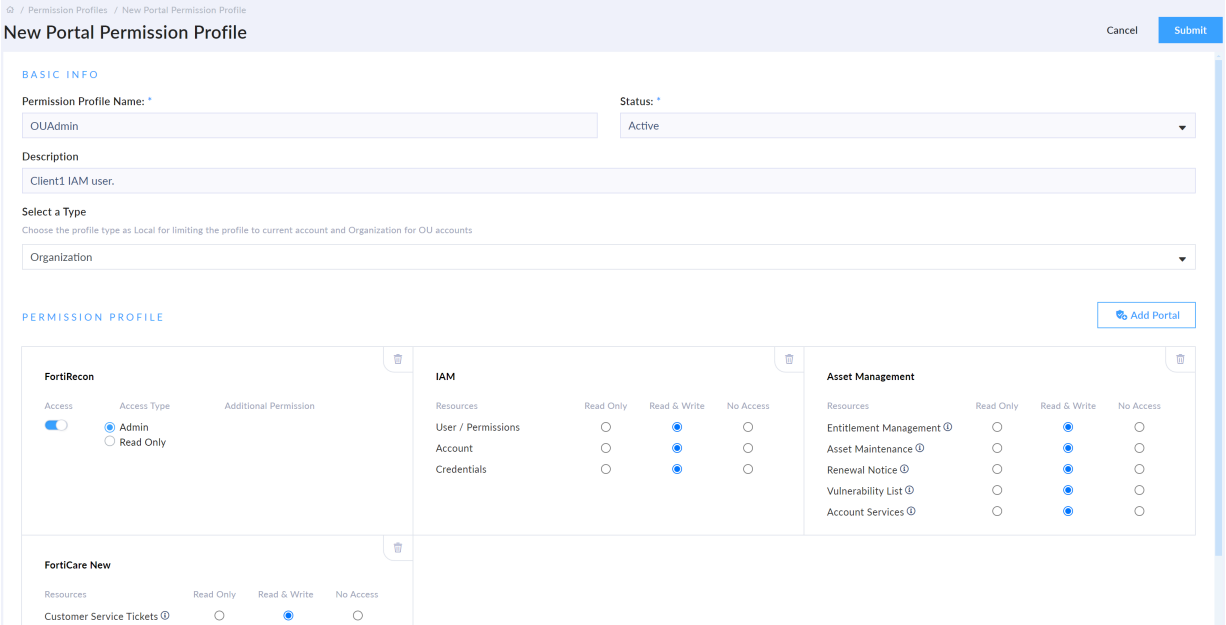
> For more information, see Creating users, user groups, and roles within Organizations in the *Identity & Access Management*.

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 sub-organization administrator 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*.

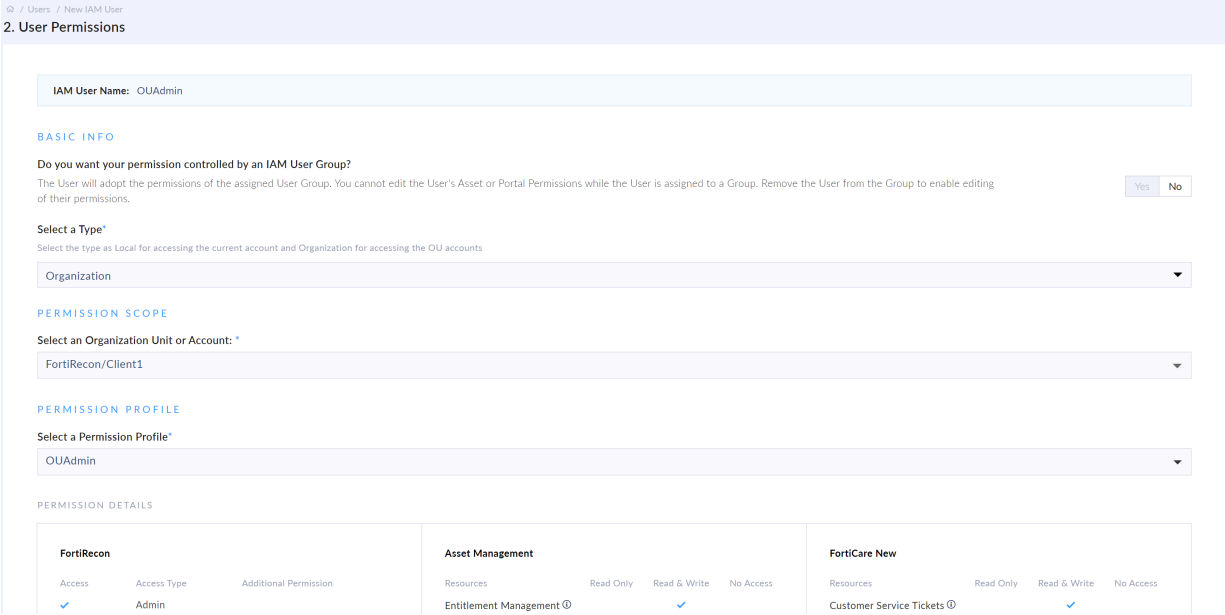


For more information, see Permission profiles within Organizations in the *Identity & Access Management*.

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 member account email address. This email must match the one used when you created the member account.
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. Set the type to *Organization*.
   d. Set the *Permission Scope* to the respective *OU* of the sub-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.

> 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 sub-organization administrator.

- **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.

Adding FortiRecon Licensing to Organization Unit (OU)

You can use either the Standard or FortiFlex licensing method for each Organizational Unit (OU). See Licensing.

Standard Licensing

Perform the following steps to add a standard license.

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 sub-organization member account.

3. Register the purchased license. For more information about registering products on FortiCloud, see the *FortiCloud Account Services > Registering products* documentation.

   After registration, you can continue by provisioning FortiRecon , see Provision FortiRecon.

FortiFlex Licensing

Perform the following steps to add a license using FortiFlex.

1. Transferring FortiPoints to FortiFlex points
2. Creating a FortiRecon configuration in FortiFlex
3. Creating a FortiRecon entitlement in FortiFlex

After creating entitlement, you can continue by provisioning FortiRecon , see Provision FortiRecon. To manage entitlements, see Managing Entitlements.

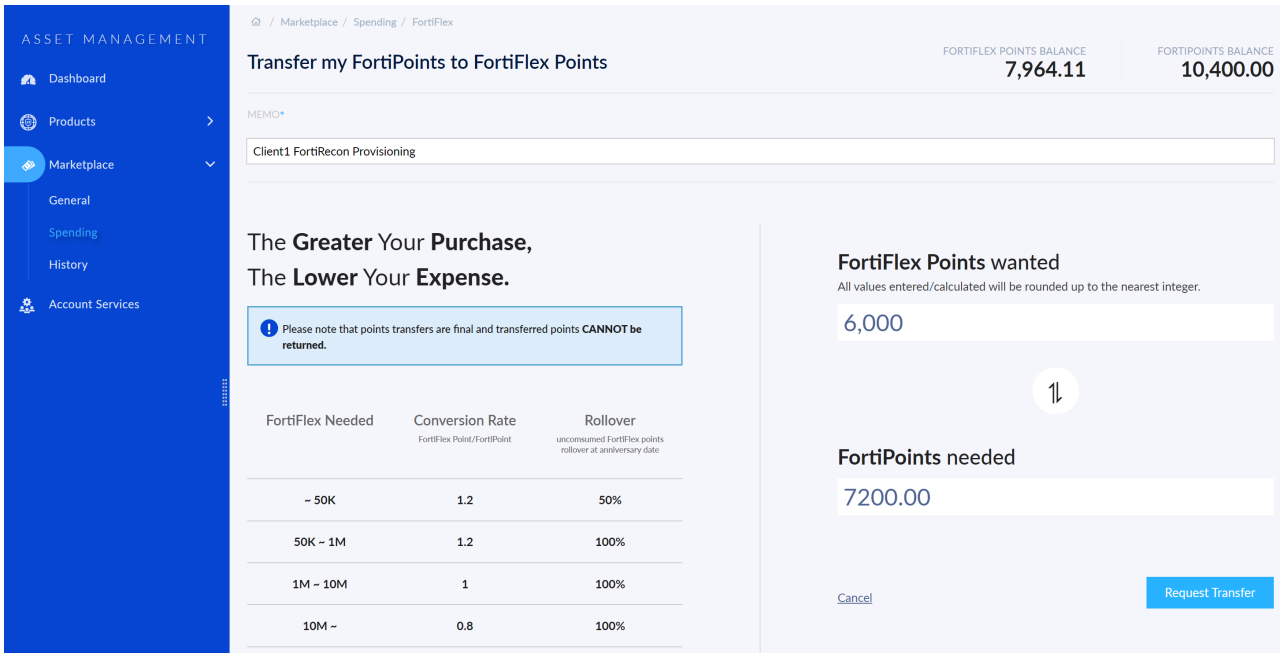
Transferring FortiPoints to FortiFlex points

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.

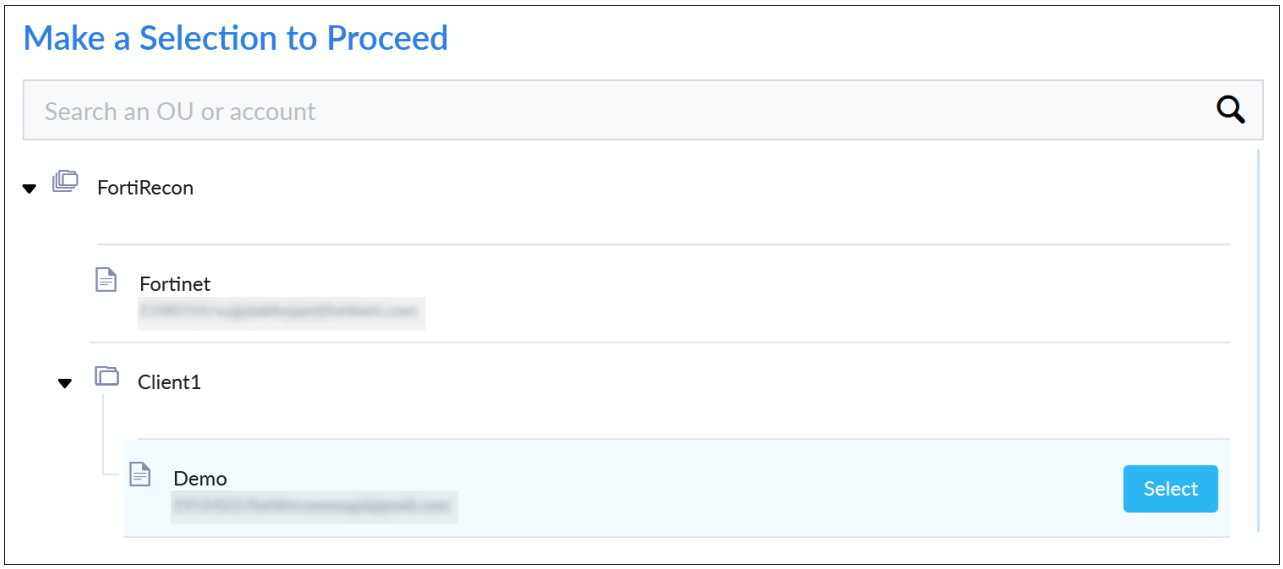
Creating a FortiRecon configuration in FortiFlex

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

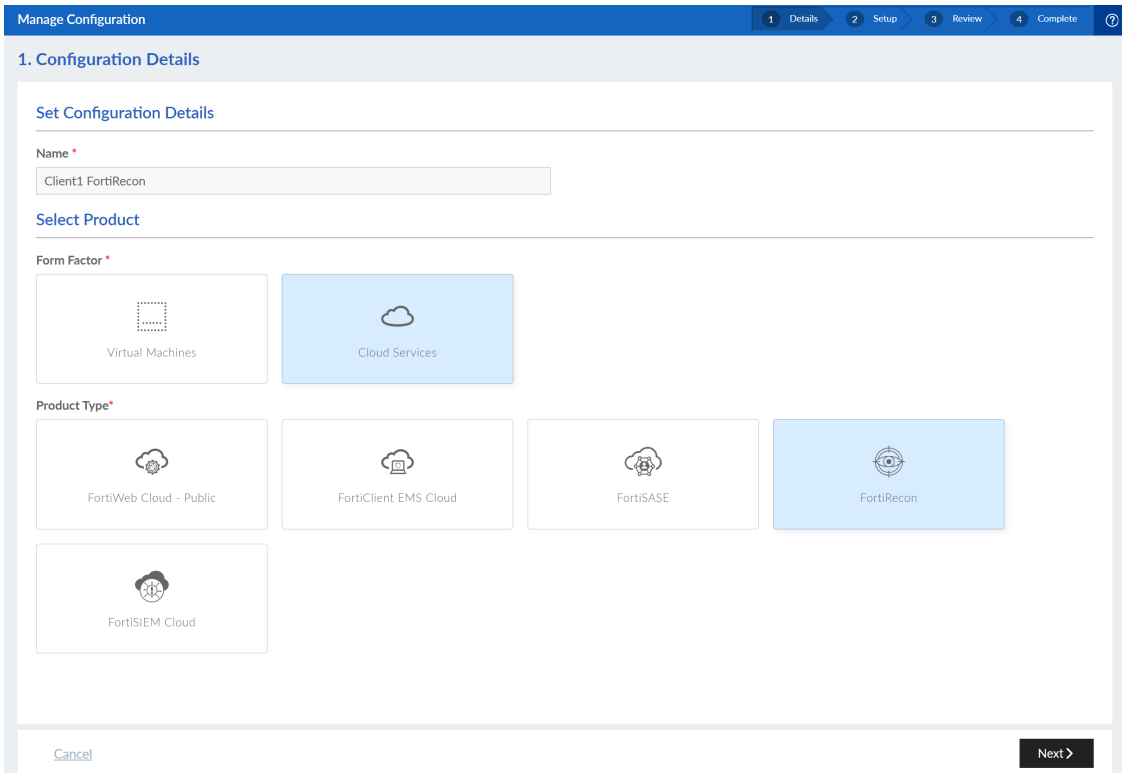
You can use the FortiFlex points calculator to estimate the total number of points that will be consumed before you create the configuration. See Points calculator in *FortiFlex Administration Guide*.

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 sub-organization member account.

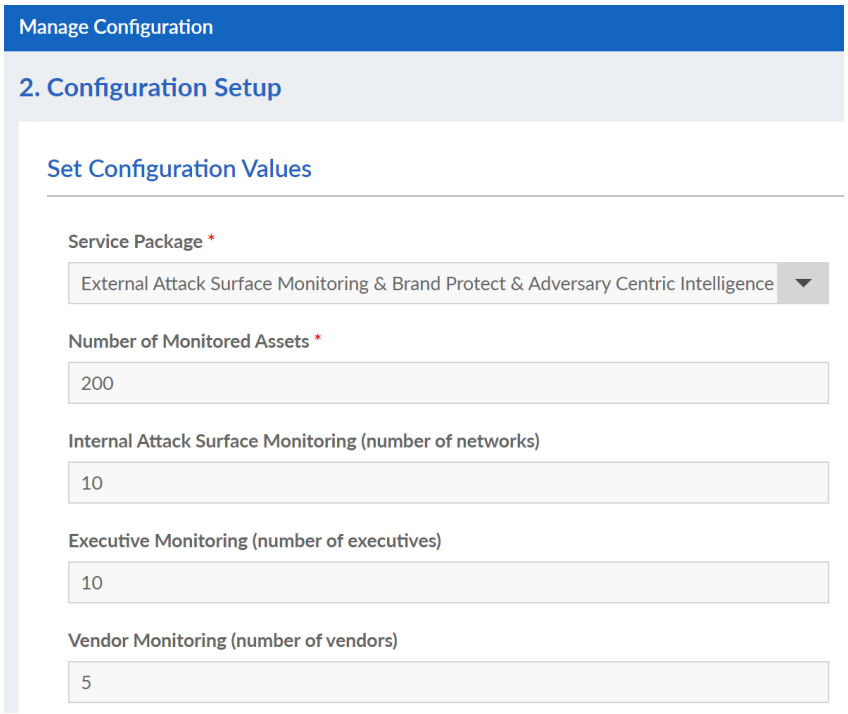


3. Go to *Services* > *FortiFlex*.
4. In FortiFlex, go to *Configurations*, and click *New Configuration*.
5. In the *Configuration Details* page, set the following configuration details and click *Next*.
   - *Name* - Enter a configuration name.
   - *Form Factor* - Select *Cloud Services*.
   - *Product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

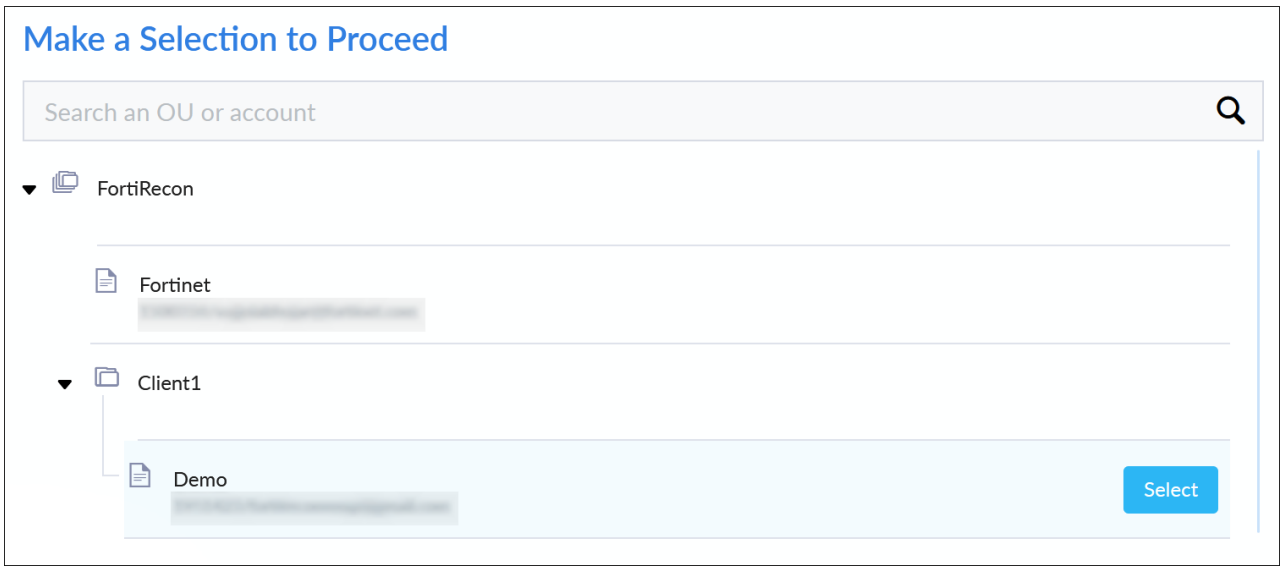
For more information, see Creating a Cloud service configuration in *FortiFlex Administration Guide*.

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.

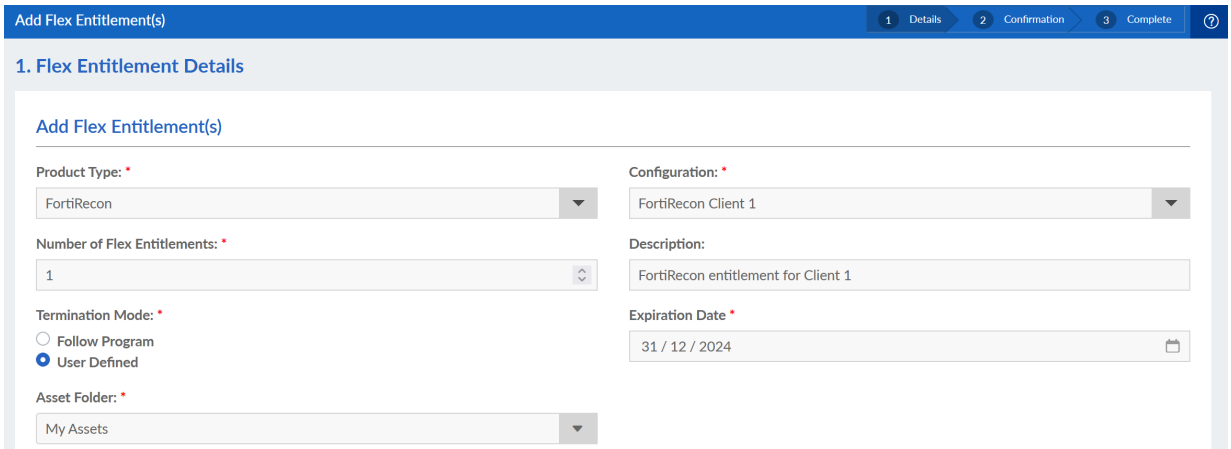
1. If not logged in, log in to https://support.fortinet.com/ using your *pAdmin*account.
2. In the Make Selection page, select the sub-organization member account.



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*.

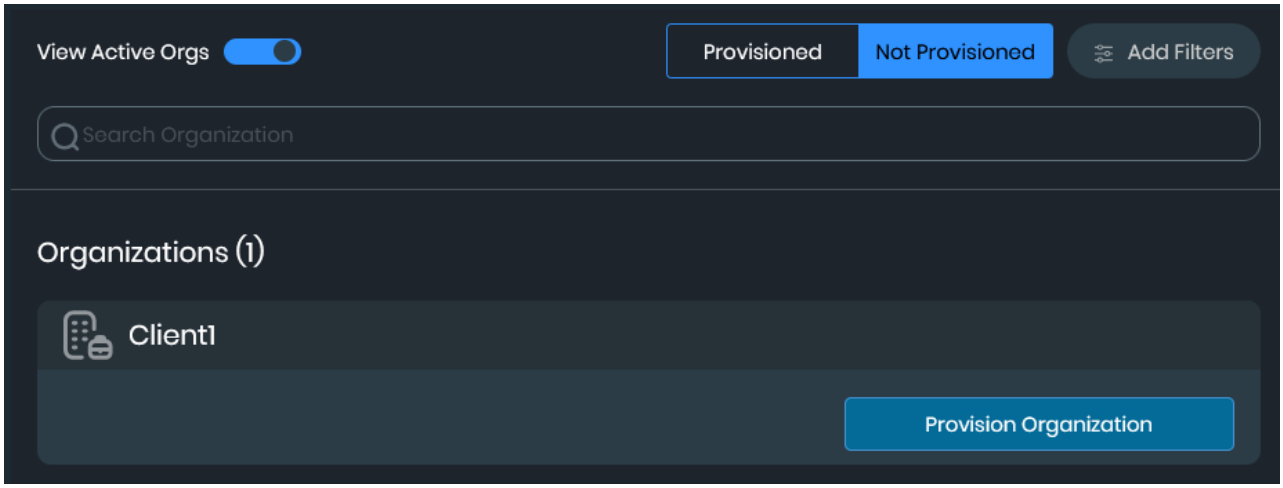
For more information on, see Creating Cloud service entitlements in *FortiFlex Administration Guide*.

Provisioning FortiRecon

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

Perform the following steps to provision FortiRecon.

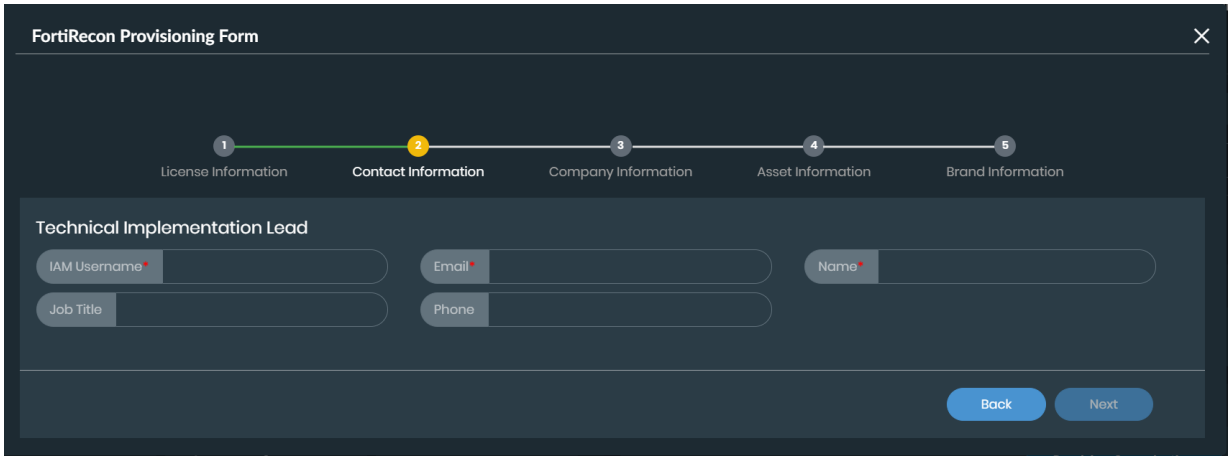
1. Login to FortiRecon portal using pAdmin credentials.
2. If logging in for the first time, email verification must be completed.
3. After verifying the email successfully, reload the FortiRecon portal. The FortiRecon*Organization* dashboard is displayed.
4. Enable the *View Active Orgs* toggle and 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.

a. *License information* will be auto fetched. Click **Next**.

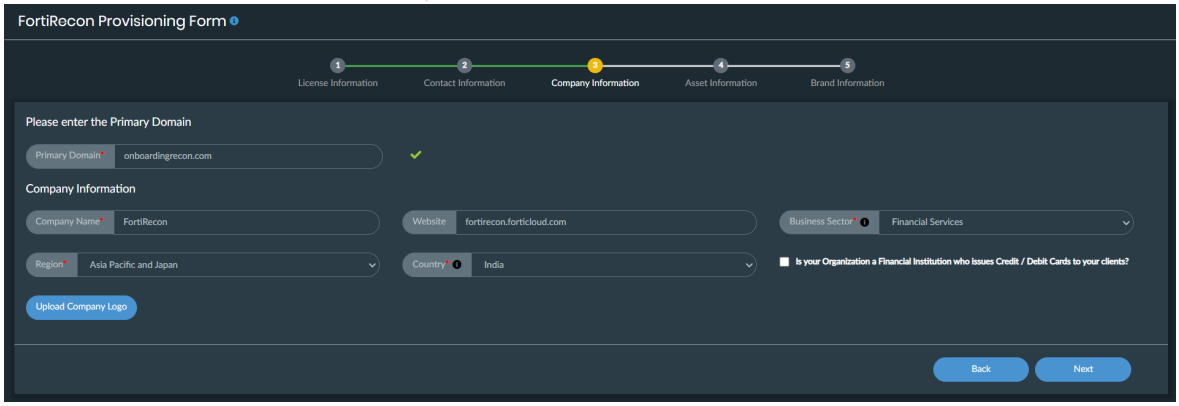
b. In *Contact Information* section, enter the IAM username that belongs to the IAM user added to this OU, and upon entering the IAM username, other fields such as email and name will be automatically filled.



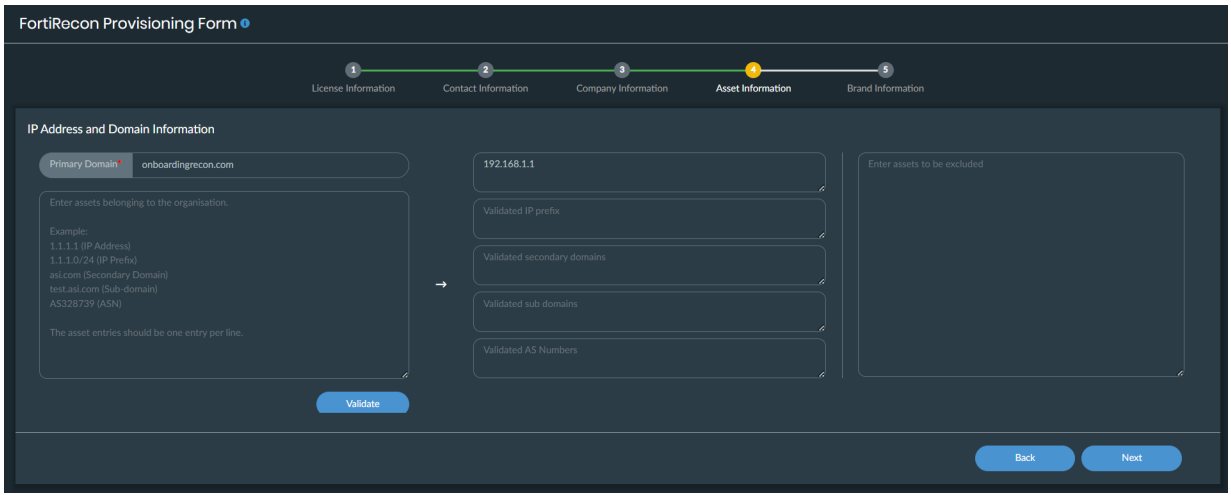
c. In *Company Information*, enter the primary domain. If the domain already exists, a prompt appears. Contact *Fortinet Support* to proceed further.

   i. Once primary domain validated, enter your organization's information in the *Company Information* fields. Click *Upload Company Logo* to browse and upload your organization's logo.

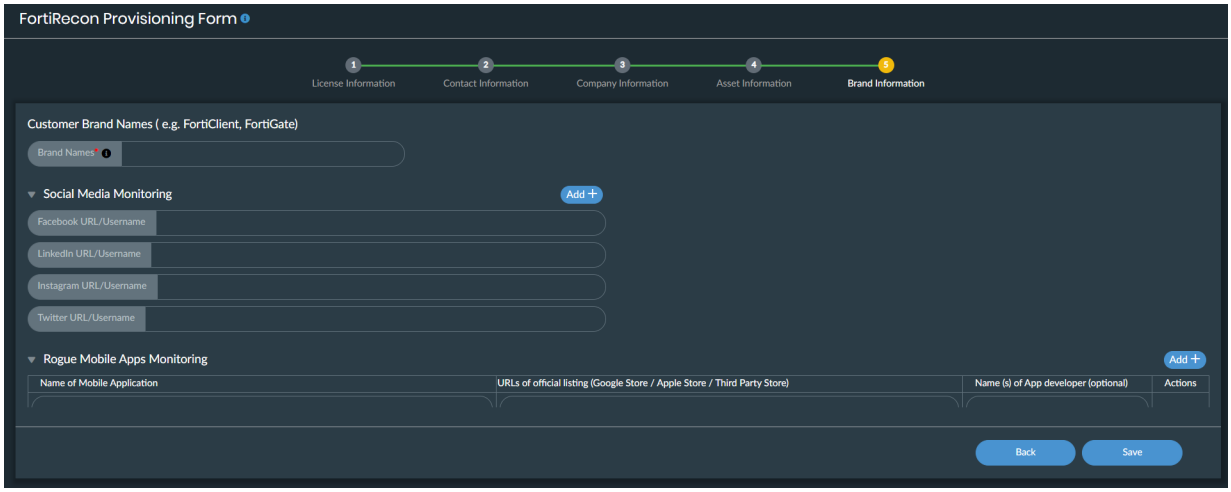
   ii. If your organization is a Financial Institution issuing credit or debit cards, select the checkbox. This will enable the *Card Information* step.



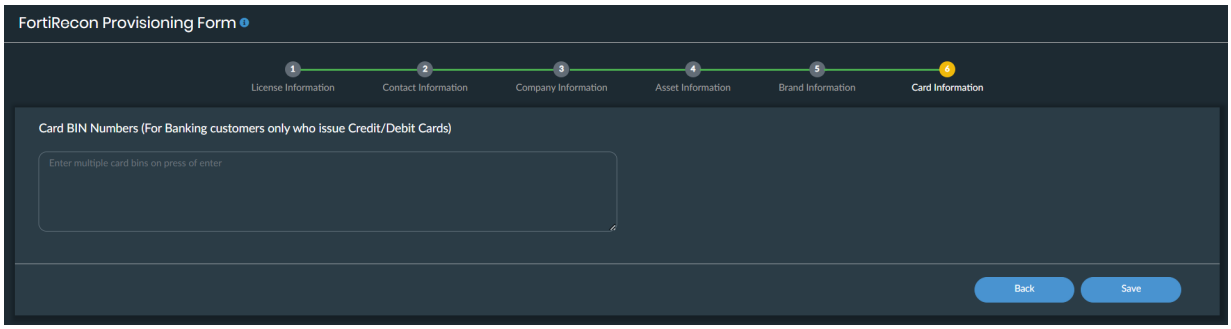
d. *Asset Information*. Enter your organization's assets information including primary, secondary and sub domains, IP addresses, IP range, ASN, assets to be excluded from monitoring.

e. 

f. *Brand Information*. Enter your brand names, social media profile and mobile applications to be monitored. Click *Save*.

g. 

h. *Card Information*. Enter Card BIN numbers. This is only for financial institutions who issue credit or debit cards.



i. Click *Save*. Your information will be sent to the FortiRecon team for review and provisioning.

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.

Sub-organization administrators can create and manage IAM users. See Users.

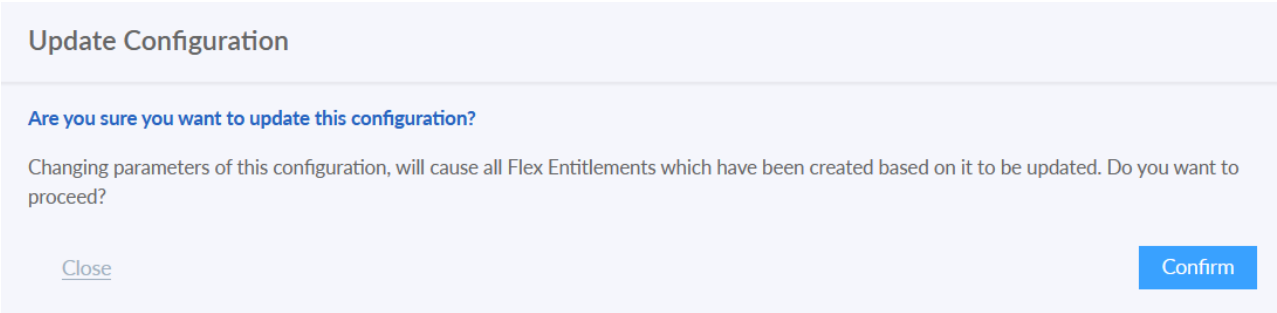
Managing Entitlements

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 sub-organization 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.

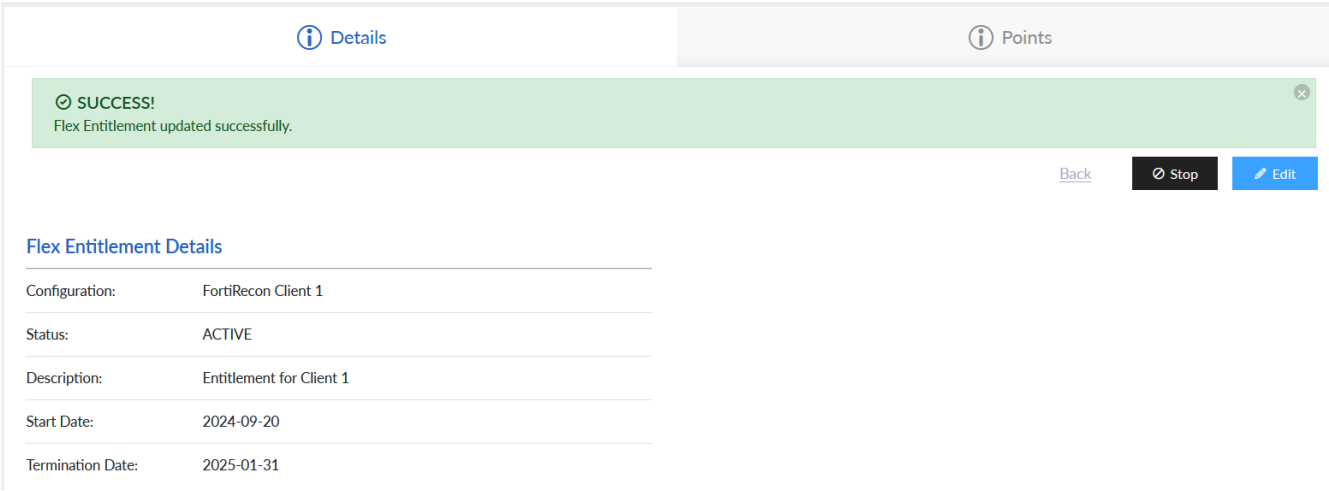


It may take up to 3 hours for any modifications to take effect in FortiRecon.

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 sub-organization 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.

Role	Access	Permission Scope	Description
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 FortiCloud.		
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.

> You will receive notification email when asset usage exceeds 100% and access to all modules except *Attack Surface Management > Asset Discovery* is blocked when usage reaches 150%. You can either reduce asset usage or contact *Fortinet Support* to purchase additional licenses.

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.

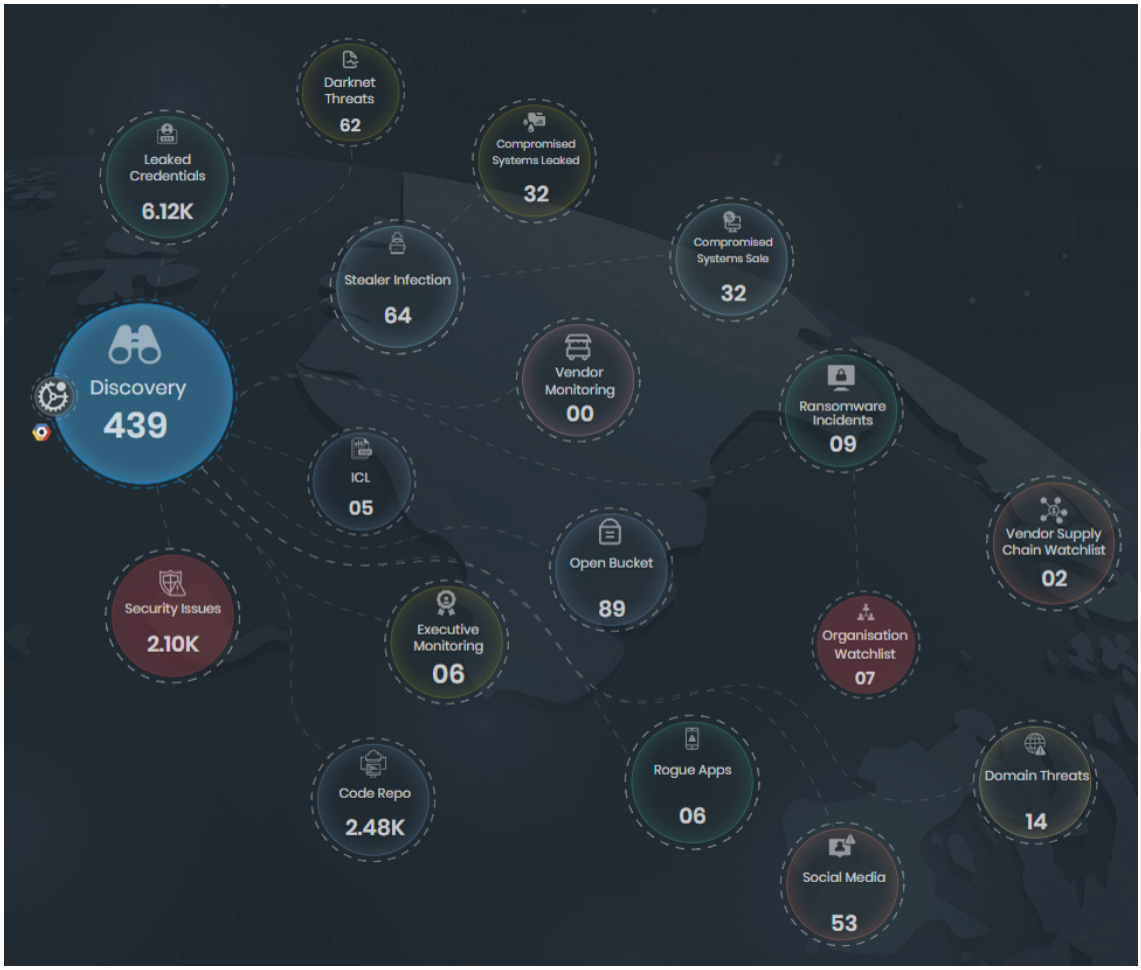
Viewing Digital Risk Posture

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

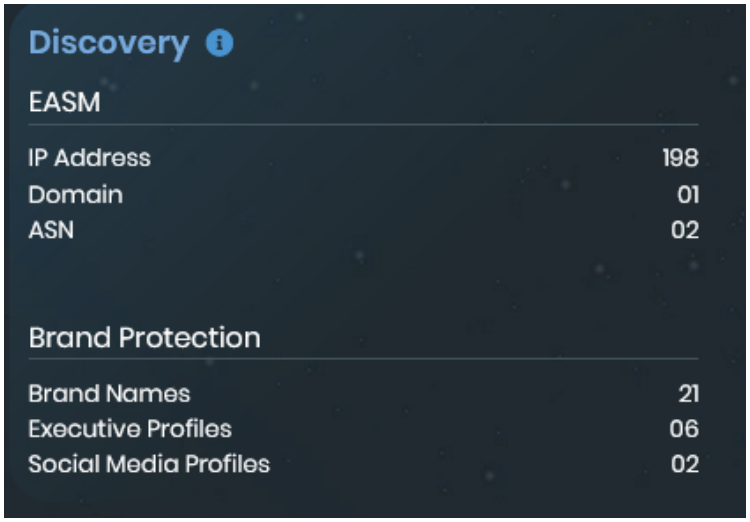
- Digital Footprint Map
- License Details
- Trends Reporting
- Top Threat Actors
- Activities

Digital Footprint Map

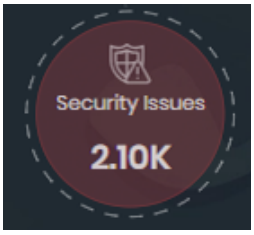
The digital footprint map is an interactive visualization tool that enables you to quickly identify and prioritize critical threats across *Attack Surface Management (ASM)*, *Brand Protection (BP)*, and *Adversary Centric Intelligence (ACI)* modules.



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.

Bubble	Description	License Required
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.	
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.	
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.	

Bubble	Description	License Required
Darknet Threats	Displays the total count of the intelligence reports available. Click the bubble to view the count for each category.	FortiRecon EASM, BP, and ACI.
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.

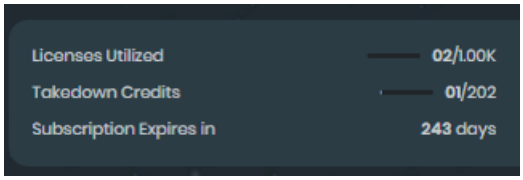
License Details

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.

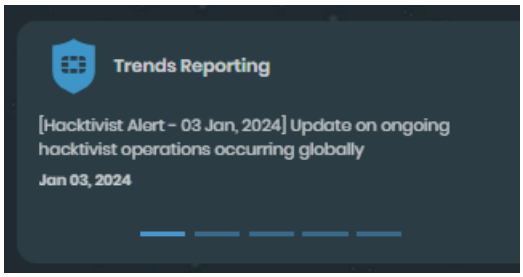
Subscription Expires in - Displays remaining days until your FortiRecon subscription expires.



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.

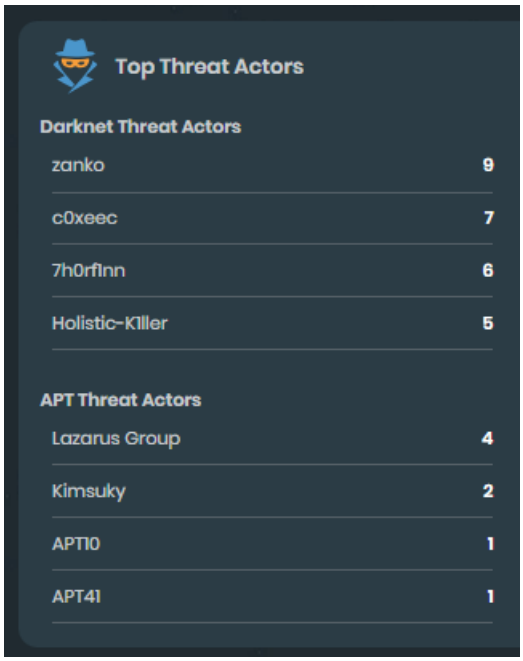
Click any report to view the detailed information.



Top Threat Actors

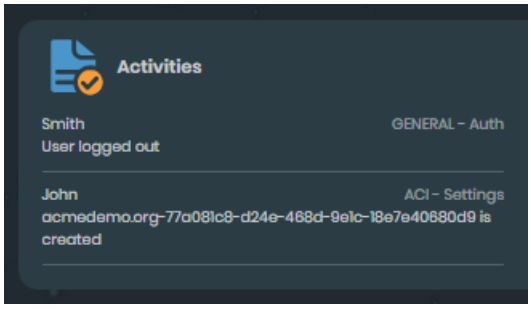
The *Top Threat Actors* widget displays the top five threat actors and Advanced Persistent Threat (APT) groups.

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



Activities

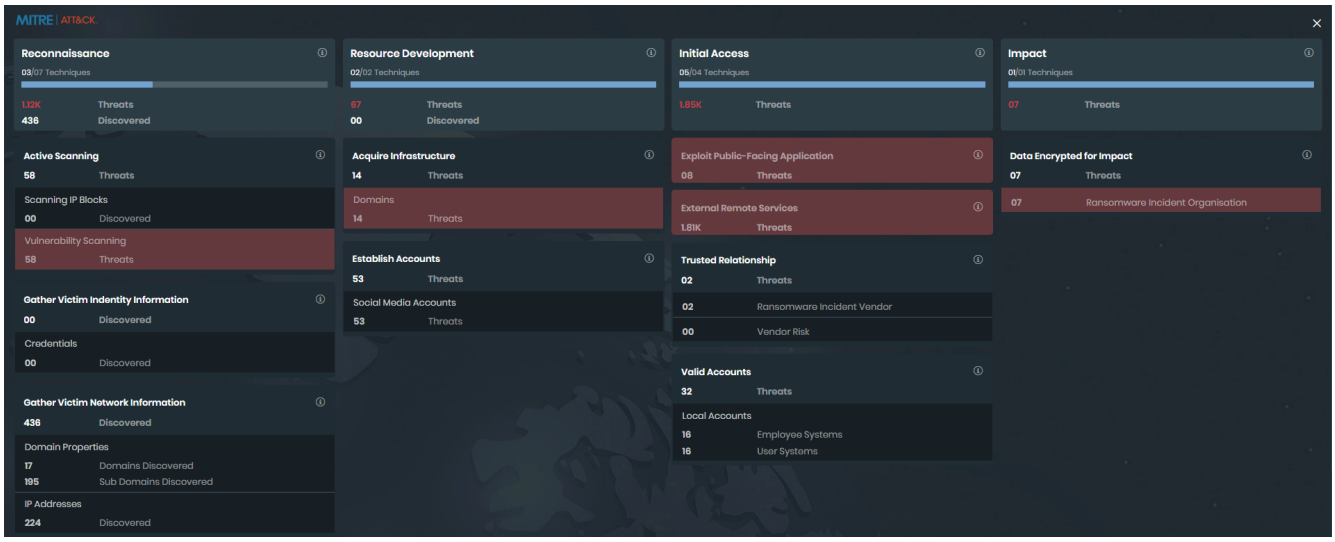
The *Activities* widget displays a log of recent activities performed within FortiRecon.



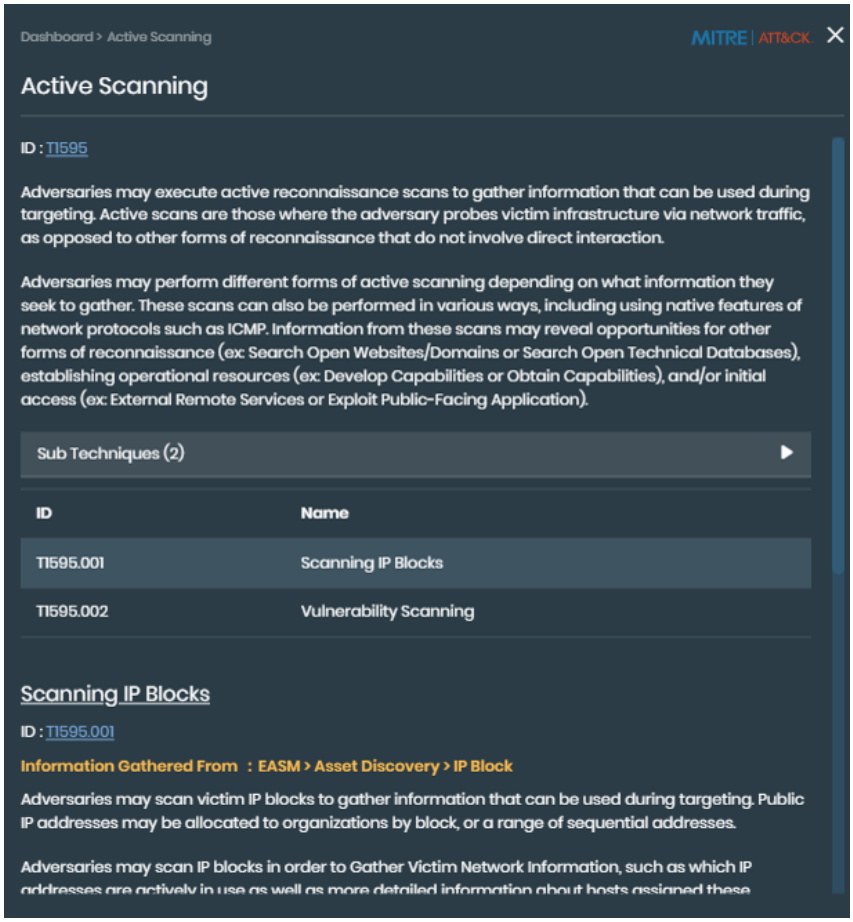
Viewing MITRE ATT&CK Framework

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.

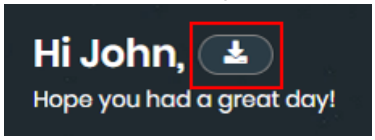


Downloading Executive Report

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 271.

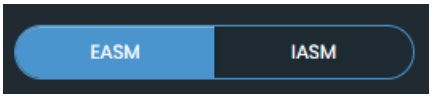
Attack Surface Management

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 :

- You will receive notification email when asset usage exceeds 100% and access to all modules except *Attack Surface Management* > *Asset Discovery* is blocked when usage reaches 150%. You can either reduce asset usage or contact *Fortinet Support* to purchase additional licenses.
- 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.
Web Application Assessment	Displays a summary of your web applications that have been analyzed by the lightweight, unauthenticated assessment. You can review and filter identified vulnerabilities and exposed endpoints for each asset. See Web Application Assessment.
Asset Management	Displays tags and groups used to filter and link assets. Also, you can configure IASM. See EASM Asset Management or IASM Asset Management.
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 122.

Integrations	Displays the added integrations for *AWS, Azure, Google Cloud Platform, FortiDAST*, and *FortiGate*. See Integrations on page 125.

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.

- EASM Dashboard
- EASM Security Issues
- EASM Asset Discovery
- EASM Asset Management

EASM Dashboard

The *Attack Surface Management* > *Dashboard* > *EASM* 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 59.
- View a summary of potential security issues related to your organization. See Viewing security issues summary on page 60.
- 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 61.
- Download the dashboard content to your hard drive. See Downloading the EASM dashboard details on page 62.

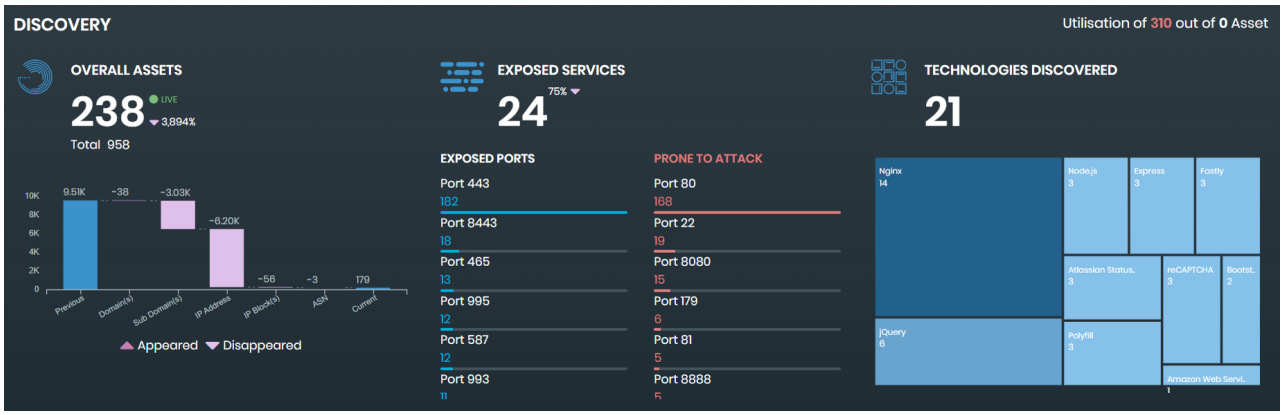
Viewing discovered assets summary

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 EASM Asset Discovery on page 68.

Viewing security issues summary

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

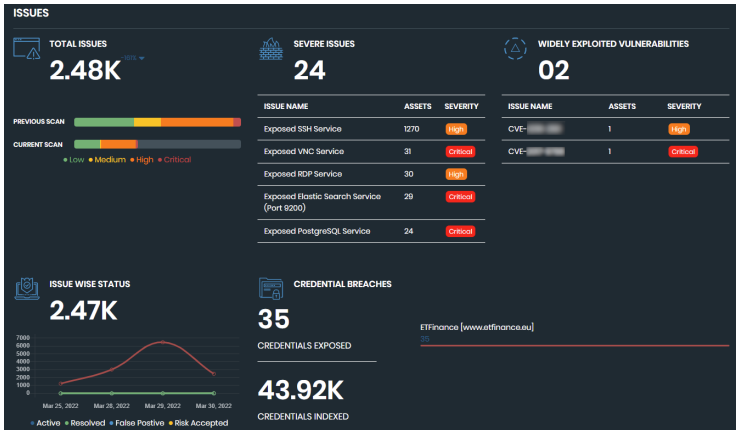
- Total Issues
- Severe Issues
- Widely Exploited Vulnerabilities
- Issue Wise Status

- 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.

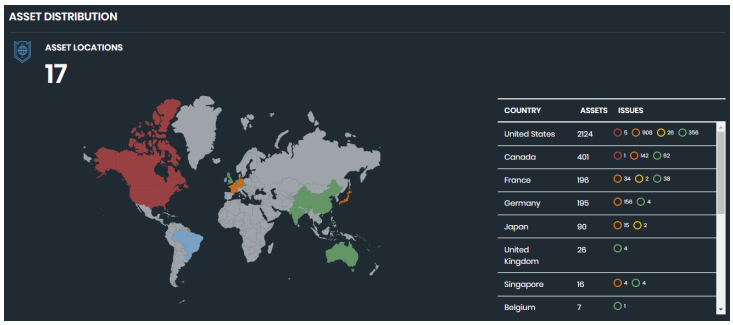
3. Click an issue or vulnerability to display more details on the *Security Issues* page. See EASM Security Issues on page 63.

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 EASM Security Issues on page 63.

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 271.

EASM Security Issues

The *Attack Surface Management* > *Security Issues* > *EASM* 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 63.
- Apply filters to the list of security issues to hone in on specific issues. See Filtering security issues on page 65.
- 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 66.
- Add a comment to explain status changes made to security issues. See Adding a comment to a security issue on page 67.
- Export security issues to an Excel file. See Exporting security issues.

Viewing security issues

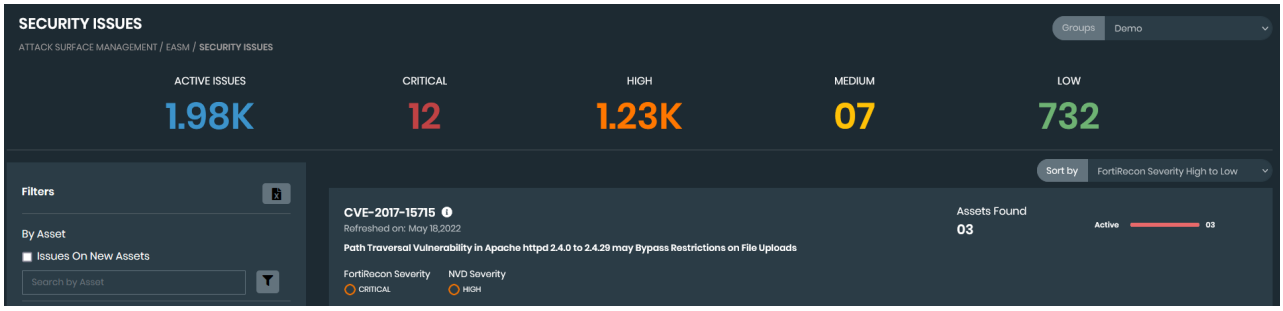
The *Attack Surface Management* > *Security Issues* page displays the number of active security issues and how many of the active security issues are rated critical, high, medium, and low based on FortiRecon severity rating. Color indicates the severity of a security issue:

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.

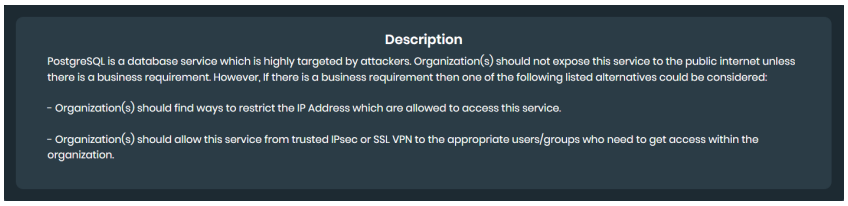
You can use search and filters to change the list of reports that are displayed, and then click each report to display its details.

To view security issues:

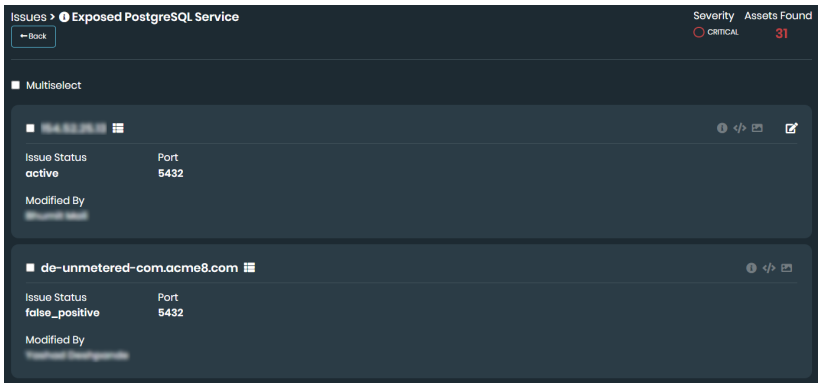
1. Go to *Attack Surface Management* > *Security Issues*. Choose *EASM* using toggle, the respective security issues are displayed.
   The *Issues* bar across the top displays the number of active security issues and the number of active security issues that are rated critical, high, medium, and low 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 identified CVEs, a brief description is displayed.
4. For each report, click the *i* icon to display a description of the issue and suggested remediation steps.



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



6. 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.
7. When available, click the following icons:

Additional Information	Displays additional information about the security issue.
Raw Data	Displays raw data about the security issue.
Actions	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 66. Click **Run Automation** to run playbooks. See Security Orchestration.

8. Click the *Back* button.

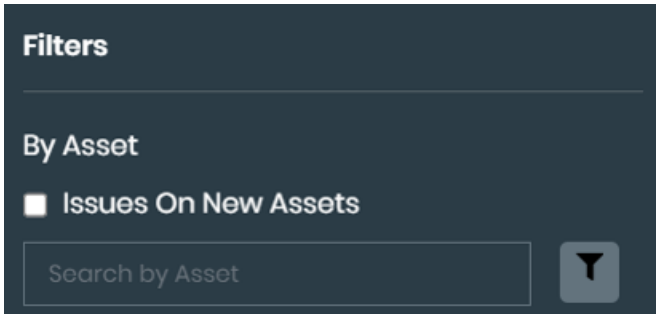
Filtering security issues

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:

Filter	Options
Status	Select one of the following statuses: • *Active* • *Resolved* • *Risk accepted* • *False positive*
FortiRecon Severity	Select one or more of the following severity statuses: • *Critical* • *High* • *Medium* • *Low*
NVD Severity	**Note**: Ensure *Vulnerable Software* category is selected to enable this filter. Select one or more of the following severity statuses: • *Critical* • *High*

Filter	Options
	• *Medium* • *Low*
Category	Select one or more of the categories. The list of categories changes based on the displayed security issues.
Tags	Select one or more tags.

The list of filtered security issues is displayed.

5. In the *Filters* list, click *Clear* to remove all filters.
6. The *Archived Results (All Time)* section displays all results previously marked as *False Positive* or *Risk Accepted*. To revert an archived action and return a result to an *Active* state, locate the result in the *False Positive* or *Risk Accepted* lists and change the status back to *Active*.

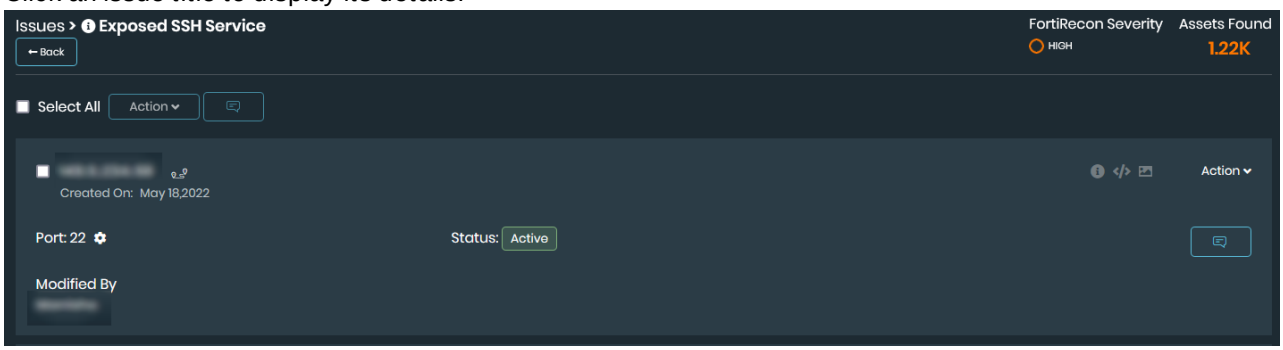
Changing the status of security issues

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.
   The list of filtered security issues is displayed.
3. Click an issue title to display its details.



4. Click *Action* 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*.

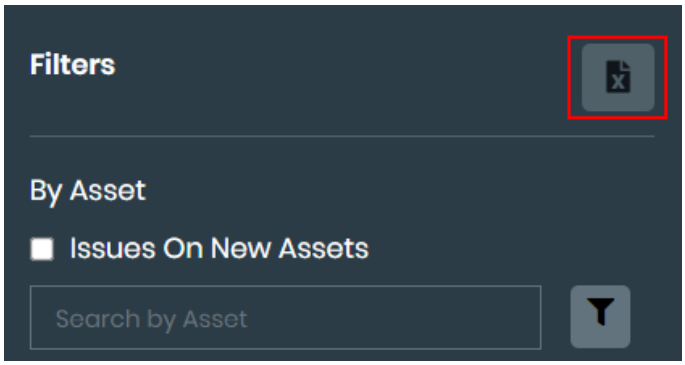
Exporting security issues

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.



EASM Asset Discovery

The *Attack Surface Management* > *Asset Discovery* > *EASM* 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 68.
- Mark discovered assets as false positives to remove them from the next scheduled FortiRecon scan. See Marking assets as false positives on page 70.
- Manually add assets to FortiRecon to include them in the next scheduled scan. See Adding assets manually on page 71.
- Manually remove assets from the next scheduled FortiRecon scan. See Removing assets manually on page 72.
- Assign tags to assets for focused filtering. See Assigning tags on page 72.

  > Tags are created in *Attack Surface Management* > *Asset Management*. Assets can also be assigned to tags in bulk in the *Asset Management* page. See EASM Asset Management on page 85.

- Perform a FortiDAST vulnerability scan on assets. See Performing a FortiDAST scan on page 73.
- View DNS health report for your domains. See DNS Health Report on page 75.
- Export a list of assets to an Excel file. See Exporting assets.

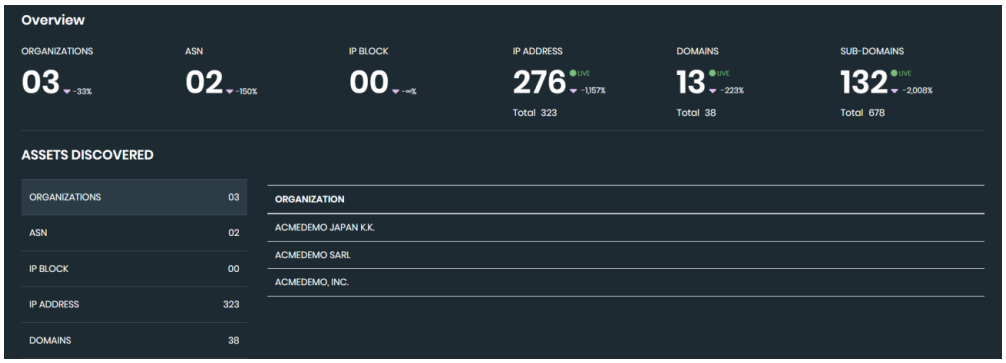
Viewing asset details

The *Attack Surface Management* > *Asset Discovery* > *EASM* 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:

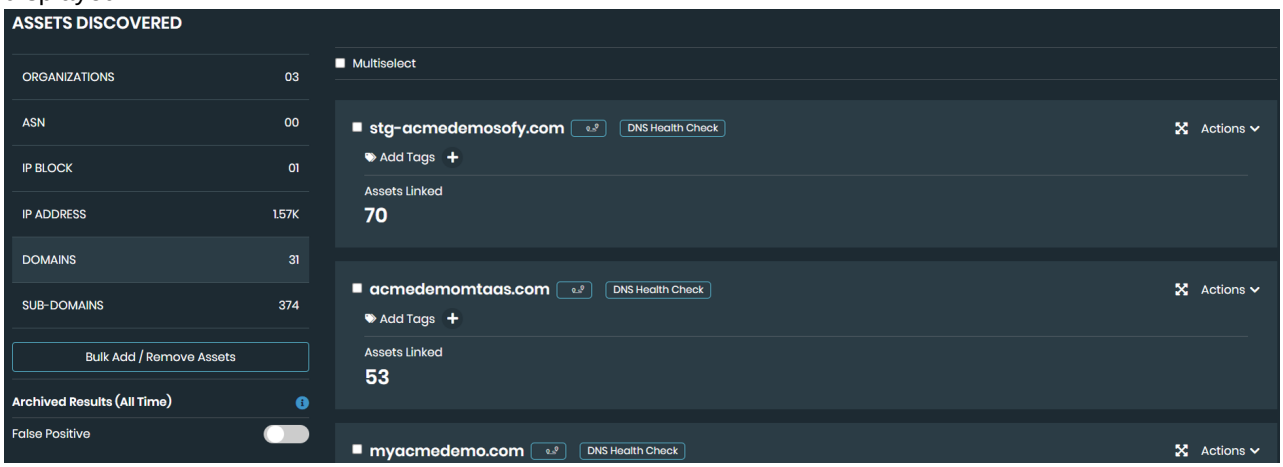
1. Go to *Attack Surface Management* > *Asset Discovery*.
2. Choose *EASM* using toggle. The number of discovered assets display in an *Overview* section across the top and in an *Assets Discovered* list on the left side of the page.



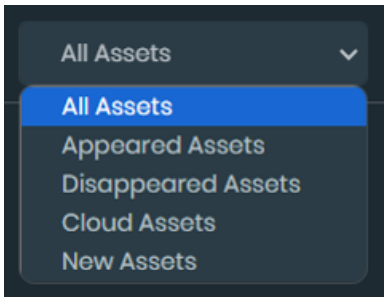
The following information is available:

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.

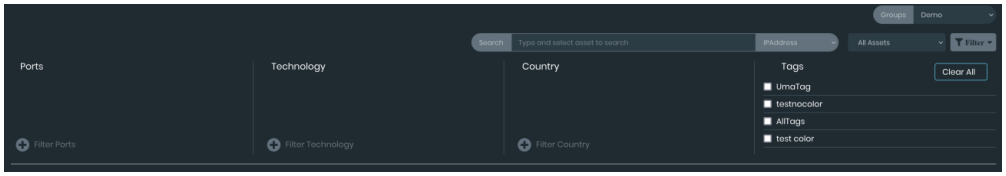
b. Select *Disappeared Assets* to show assets that disappeared in the latest scan.

c. Select *Cloud Assets* to show cloud-based assets.

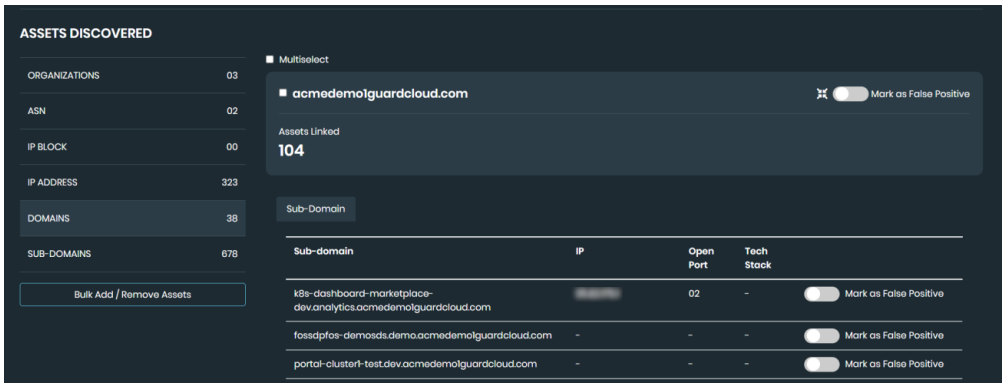
> Cloud assets can only be filtered if the AWS cloud environment has been integrated. See Integrations on page 125.

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 70.

8. Enable the **False Positive** toggle to show only assets marked as false positives. You can then use the search bar to find specific assets within this filtered list.

Marking assets as false positives

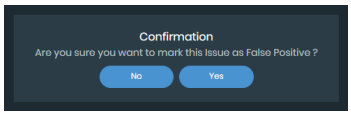
You can manually mark any of the following discovered assets as false positives to remove them from the next scheduled FortiRecon scan:

- 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*.

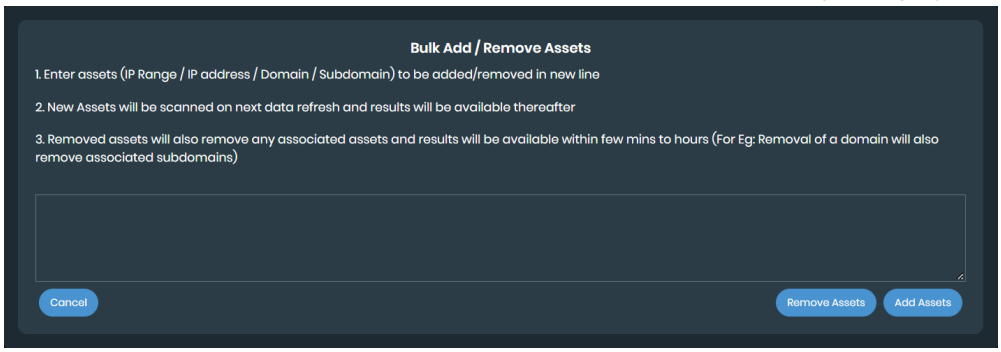
Adding assets manually

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.

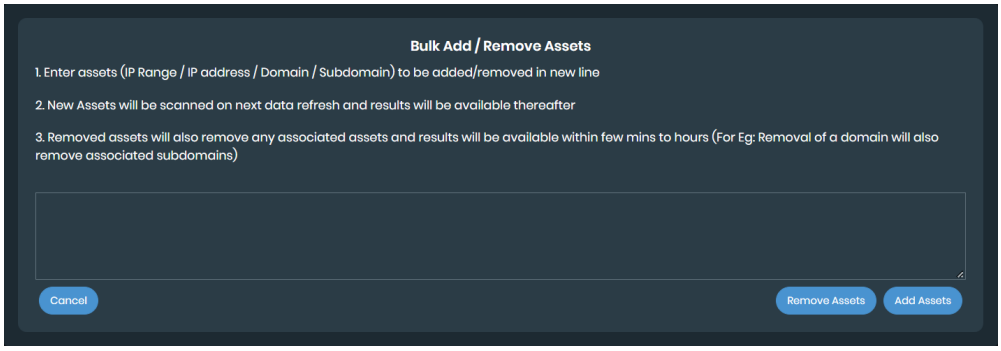
Removing assets manually

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

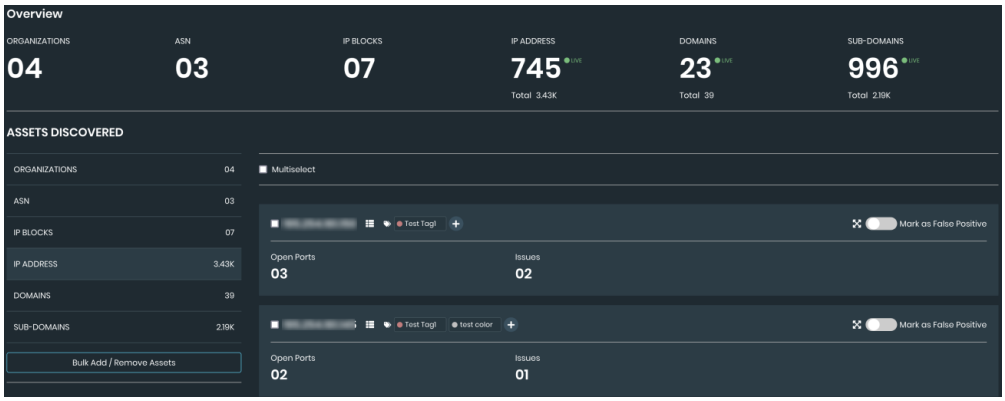
Tags can be assigned to assets for focused filtering in the *EASM* > *Asset Discovery* page. For more information on tags, see EASM Asset Management on page 85.

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 86.

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



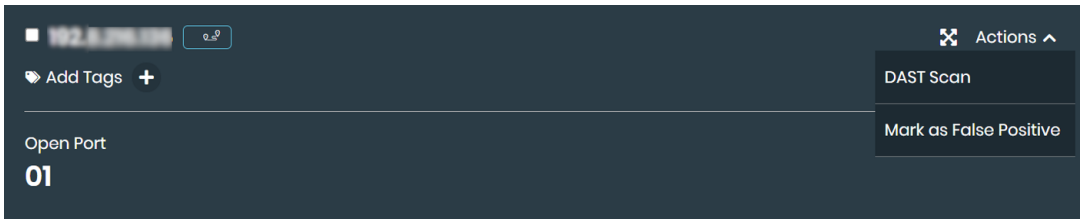
Performing a FortiDAST scan

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

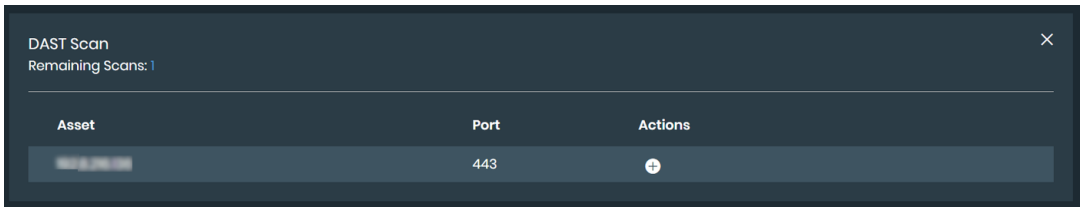
Guide for more information on how the integration and scanning works.

To scan an asset with FortiDAST:

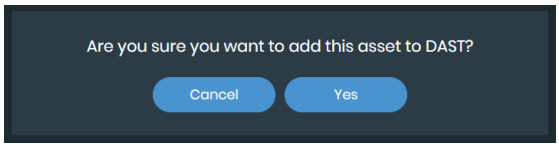
1. Add a FortiDAST integration to FortiRecon. See Adding integrations on page 125.
2. Go to *Attack Surface Management* > *Asset Discovery*.
3. Navigate to the asset you want to scan.
4. Select *Actions* > *DAST Scan*.



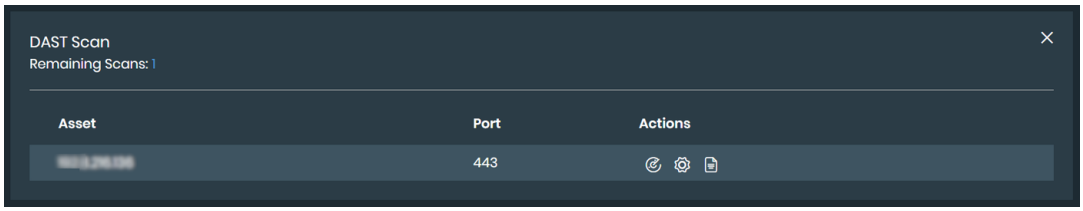
The *DAST Scan* dialog opens with number of *Remaining Scans* displayed.



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



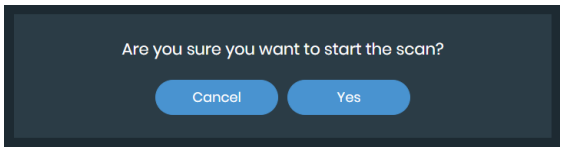
6. Click *Yes*. The *Scan*, *Config Scan*, and *View Result* buttons become available for the asset.



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

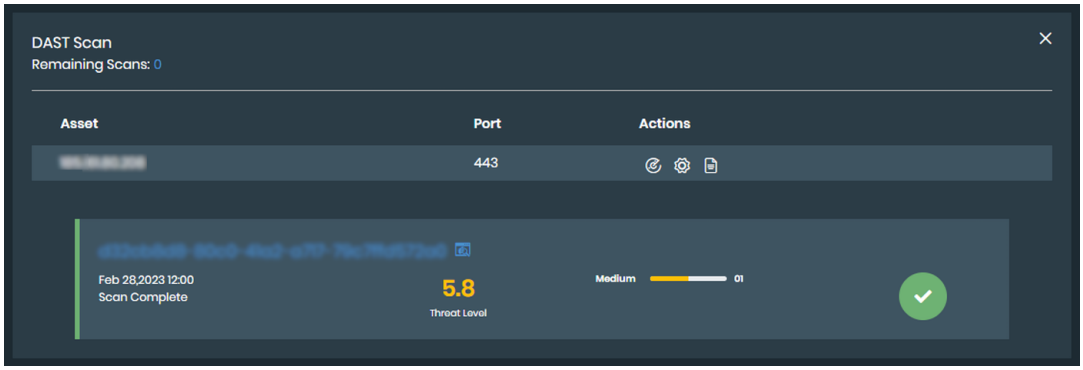
> Only master or sub users will be redirected to FortiDAST to complete the configuration. Other users will be prompted with a dialog on how to proceed.

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.



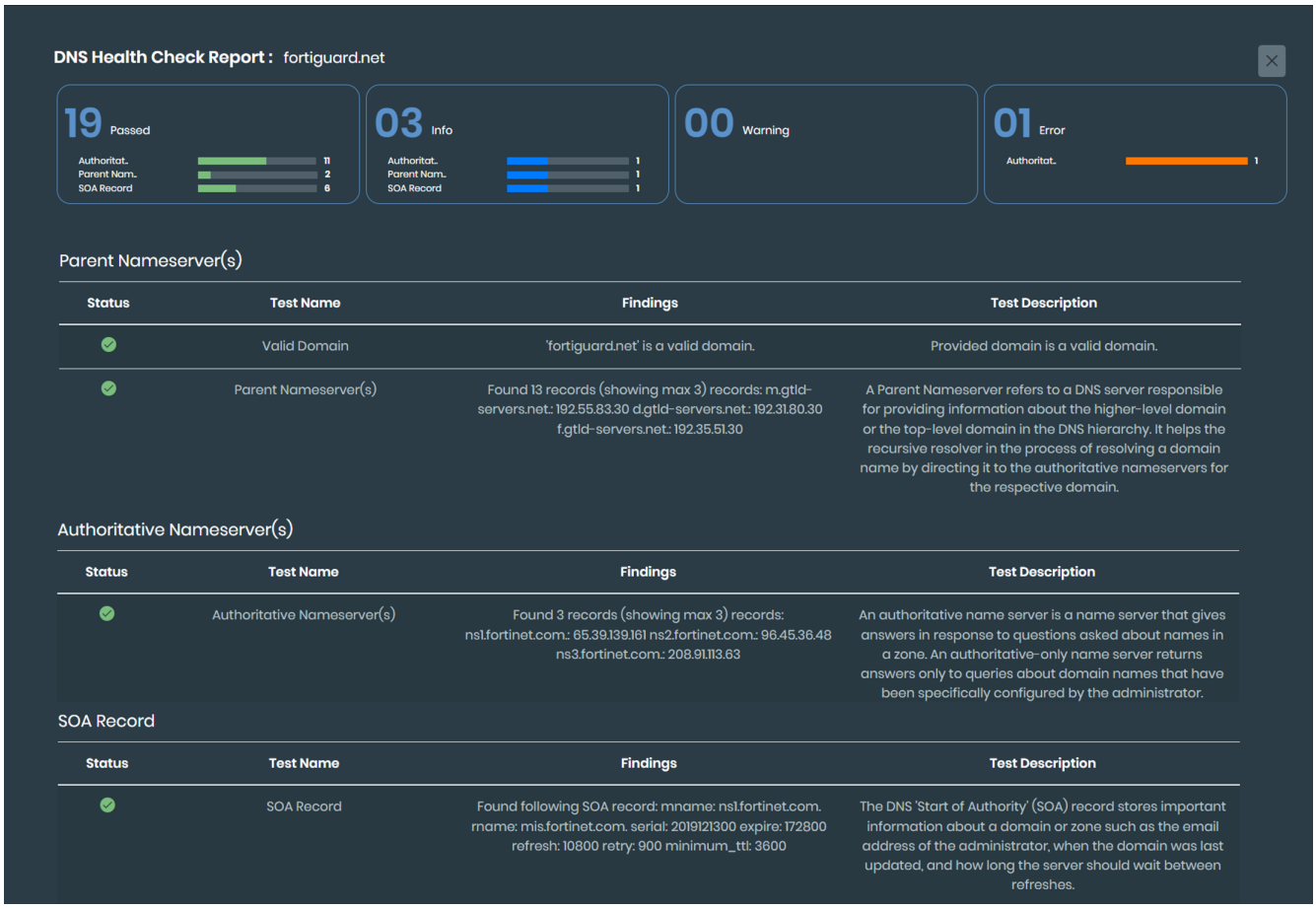
You can scan the same asset again by selecting *ReScan*.

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.

Web Application Assessment

The *Attack Surface Management* > *Web Application Assessment* page helps you identify vulnerabilities in your external-facing web applications. This lightweight, unauthenticated assessment uses an outside-in approach to efficiently discover risks visible to potential attackers.

The Web Application Assessment requires no user credentials or complex configuration, providing a fast and non-invasive way to continuously check your assets.

Key features

The Web Application Assessment provides the following core capabilities for assessing your application attack surface.

- *Unauthenticated Crawl* - The system performs an unauthenticated crawl of the target, automatically discovering exposed URLs, endpoints, and services, simulating an attacker's initial reconnaissance.
- *Frequency* - The assessment frequency follows your organization's EASM scan schedule.
- *Exploit Details* – Provides technical evidence, including full HTTP request and response data, for supported vulnerability categories.
- *WAF Detection* – Automatically identifies the presence of a Web Application Firewall (WAF) and its vendor.
- *Vulnerability Coverage* - The assessment identifies a wide range of security issues, including:
  - **Pervasive and High-Impact Injection Flaws**
    - SQL Injection (SQLi)
    - NoSQL Injection (NoSQLi)
    - Cross-Site Scripting (XSS)
    - Remote Command Execution (RCE)
    - Local File Inclusion (LFI)
    - Path Traversal
    - Server-Side Template Injection
    - Expression Language Injection
    - Code Injection
  - **Access Control & Authentication Flaws**
    - Broken Access Control
    - Indirect Object Reference
    - Forced Browsing
  - **Configuration & Design Flaws**
    - *Security Misconfiguration* - Header Misconfigurations, Missing Security Headers, Insecure Cookie Flags.
    - *Cryptographic Failures* - Deprecated SSL/TLS Versions, Expired or Improper TLS Certificates.
    - *Insecure Design* - Unrestricted File Upload, Web Cache Poisoning, HTTP Request Smuggling, Open Redirect, Clickjacking.
  - **Other High-Impact Vulnerabilities**
    - Malware Detection (identifying common malware signatures on public-facing assets)

> The assessment is strictly unauthenticated and limited to 50 URLs per application.

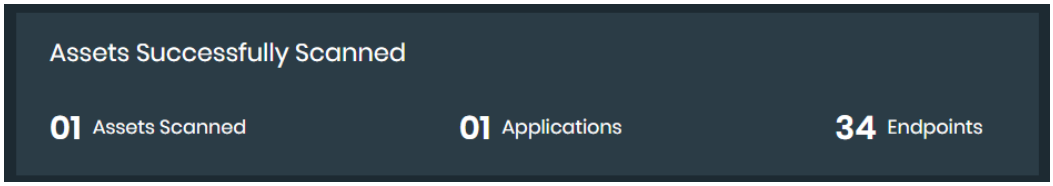
From the *Attack Surface Management* > *Web Application Assessment* page, you can.

- Review the assets discovered and summarized from the assessment for the successful scans. See Reviewing Assets.
- Filter the list of assets by IP, status, severity, and category. SeeFiltering Assets.
- Access the detailed page for each asset to review findings. See Reviewing Asset Details.
- Review exploit details, including request and response data, for supported vulnerability categories. See Reviewing Vulnerability Exploit Details.
- Manage the vulnerability lifecycle by updating statuses. See Modifying Vulnerability Status.
- Review the failed scans. See Reviewing Failed Application Scans.

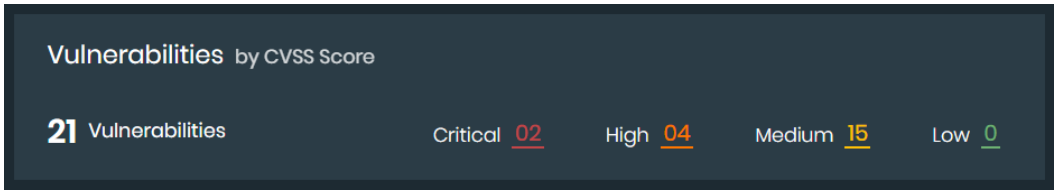
Reviewing Assets

The *Web Application Assessment* > *Assets Successfully Scanned* page provides a high-level summary of the assessment results for successful scans.

- At the top, you'll find a summary of the assessment run, including the *Total assets scanned*, as well as the *Scanned date*.
- The *Assets Successfully Scanned*widget shows a summary of your discovered web assets, including the total count of assets, applications, and endpoints.

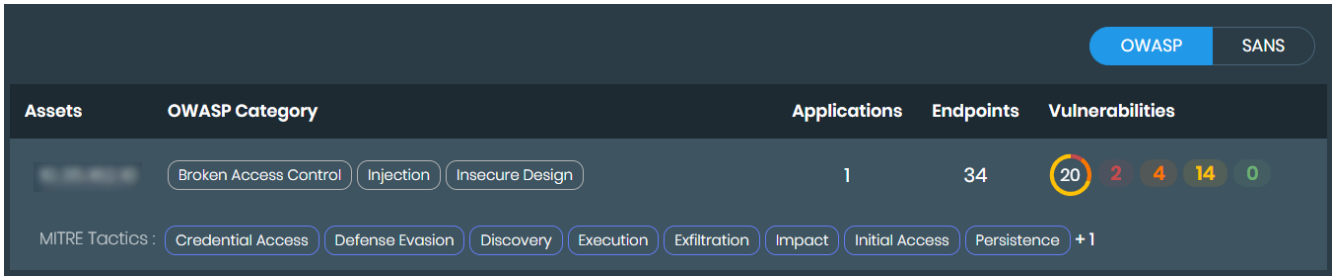


- The *Vulnerabilities* widget provides an overview of all vulnerabilities, displaying the total count and a breakdown by severity: *Critical*, *High*, *Medium*, and *Low*.



The *Assets* table lists all discovered IPs and domains. Each entry contains a *Assets*, *OWASP or SANS Category*, *MITRE Tactics*, and the count of *Applications*, *Endpoints*, and *Vulnerabilities* (total and for each severity). Use the *OWASP* and *SANS* toggle above the assets table to switch between and filter by the respective categories. The *Categories* and *MITRE Tactics* are clickable and automatically apply the corresponding filter when selected.

Click the domain name to view more detailed information about that asset. You can also use the filters to narrow the list of assets, see Filtering Assets.



Filtering Assets

Use the Filters sidebar on the left to narrow down the list of assets displayed in the main table.

- Select the *Show Non-WAF Assets* checkbox to view assets that do not have a Web Application Firewall (WAF) configured.
- Use the search bar to filter assets by IP address or domain name.
- Filter assets by the severity of their vulnerabilities: *High*, *Medium*, or *Low*.
- Use the *OWASP* and *SANS* toggle above the assets table to switch between and filter by the respective categories.
- Select one or more *MITRE Tactics* to filter the list.
- Click the *Clear* button to clear all applied filters.

Reviewing Asset Details

When you click an asset from the *Web Application Assessment* page, its detailed page opens. This page provides an overview of the asset's name and a badge indicating if it's *Public* or *Private*, as well as its authentication status. The following summary cards are displayed.

- The *Applications* card displays the total count of applications discovered and includes a drop down to select application. When you select a specific application, the vulnerability list updates to display only the security issues identified for that application. Applications with an active Web Application Firewall (WAF) display a WAF tag next to their name in the dropdown.
- The *URL* card displays the total URL count and the count of *Vulnerable* and *Safe URLs*.

The detailed findings for the asset are organized into two tabs.

- Vulnerabilities
- Endpoints

Reviewing Vulnerabilities

The *Vulnerabilities* tab provides a comprehensive view of all security issues identified for the selected asset .

At the top of the tab, a donut chart displays vulnerabilities categorized by their *CVSS Score*, showing a count for each severity. Next to it, a horizontal bar chart categorizes vulnerabilities by OWASP Category and displays the total count. Use the *OWASP* and *SANS* toggle to switch the category view and update the filters.

The vulnerability list displays each identified vulnerability. The following information is available for each entry:

- A clickable *Category* that updates the filter.
- Severity rating and threat level score.

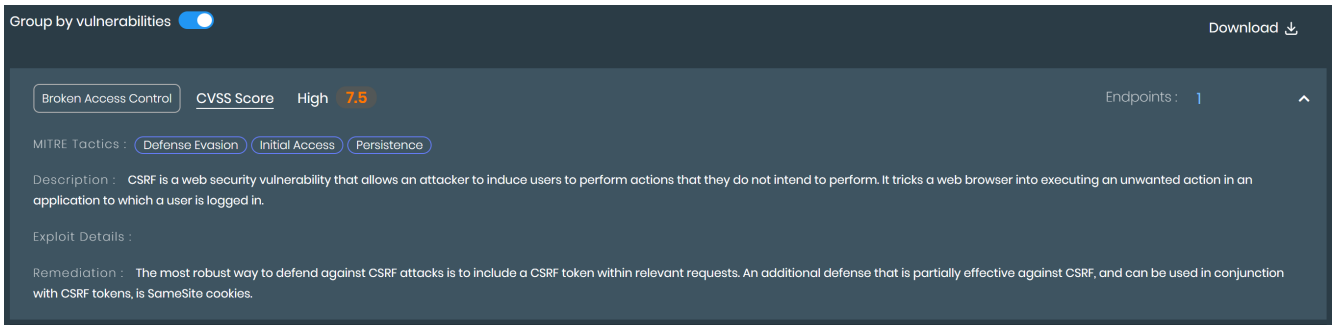
> The threat level score is derived from the CVSS score categories and is represented by values between 0 and 10. The threat level scores are categorized based on the following severities.
>
> - **Low** - 0.1 - 3.9
> - **Medium** - 4.0 - 6.9
> - **High** - 7.0 - 8.9
> - **Critical** - 9.0 - 10.0

- The *Endpoint* identified for the vulnerability.
- A *Description* of the vulnerability.

When you expand an entry, the following information is displayed.

- *MITRE Tactics* clickable tags that apply specific filters to the vulnerability list.
- *Endpoint* identified for the vulnerability. You can copy the endpoint URL to your clipboard by clicking the copy icon next to it.
- *Exploit Details* provides technical evidence and data for supported vulnerability categories. See Reviewing Vulnerability Exploit Details.
- *Remediation* provides recommended steps to fix or mitigate the identified security issue.
- *Status* dropdown allows you to manage the vulnerability lifecycle. You can update the status to *Active*, *Resolved*, *Risk Accepted*, or *False Positive*. See Modifying Vulnerability Status.

Use the *Group by vulnerabilities* option to group similar vulnerabilities by tag. When this is enabled, the *Endpoint* field changes to a count of affected endpoints. Click the count to view the full list. Click *Download* to export the vulnerability details list for the selected asset to *CSV*.



You can filter the vulnerability list by searching for a term, or by *Severity by CVSS score*.

Filtering WAF detected Applications

You can monitor the security posture and WAF status for specific applications.

When *All Applications* is selected in the *Applications* dropdown menu, the *Show Only WAF Detected Applications* toggle appears in the *Filters* panel if at least one application has an active WAF. Enabling this toggle filters the vulnerability list to display only WAF protected applications.

Upon enabling the filter, a summary message appears below the charts (for example, 4 Applications have WAF detections). Click the application count in the message to open a window displaying the following details:

- *Application*: The name of the protected application.
- *Vendor*: The provider of the detected WAF.
- *Message*: Status information regarding the WAF detection.

If no WAF is detected for a selected application or across the asset, the system displays the following security recommendation:

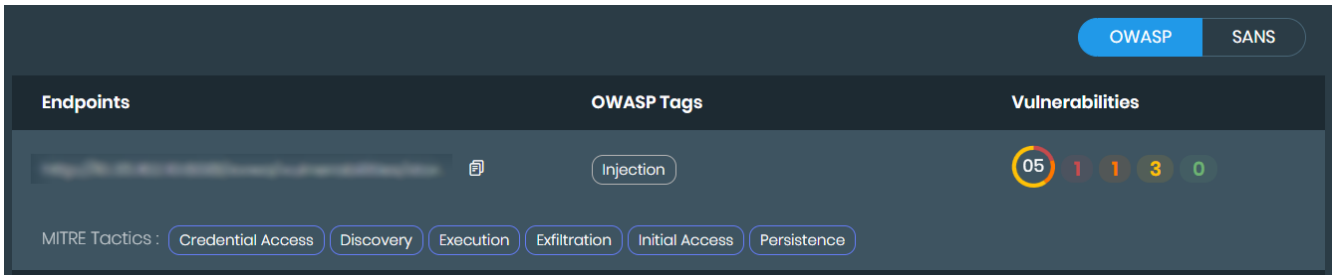
We strongly recommend configuring a WAF and implementing rules.

Reviewing Endpoints

The *Endpoints* tab provides a list of all endpoints discovered during the assessment. Use the OWASP and SANS toggle to switch the category view and update the filters.

Each list entry includes the following information:

- The *Endpoint URL*. Click *Copy* icon to copy the endpoint,
- Clickable *Categories* and *MITRE Tactics* that updates the filter.
- The endpoint type (*URL* or *API*).
- The total *Vulnerabilities* count and count by severity. Click the total count to view the complete list of vulnerabilities associated with that endpoint.



You can filter the endpoints by using the search bar, by *Severity by CVSS score*, by *OWASP* or *SANS* category, and by *MITRE Tactics*.

Reviewing Vulnerability Exploit Details

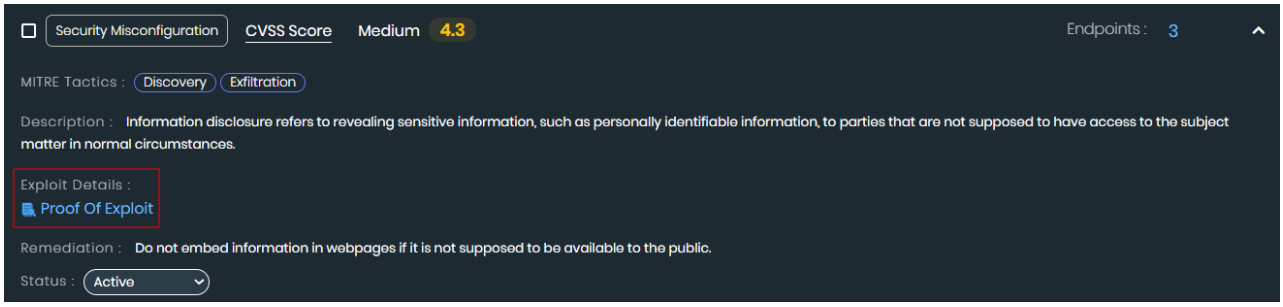
For supported vulnerability categories, FortiRecon provides technical evidence to verify the presence of a security issue. This evidence, known as *Exploit Details*, helps security analysts understand how a vulnerability was identified and its potential impact.

FortiRecon currently supports *Exploit Details* for the following categories:

- *SQL Injection (SQLi)*
- *Clickjacking*
- *Server-Side Template Injection (SSTI)*
- *Code Injection (CODEI): Including ASP and PHP environments.*
- *HTML Injection*
- *Path Traversal*
- *Information Disclosure*
- *Remote Code Execution (RCE)*

To View Exploit Details:

1. Navigate to the *Attack Surface Management* > *Web Application Assessment* page and select a required asset.
2. In the *Vulnerabilities* tab, locate a vulnerability and click the arrow to expand the entry.
3. Locate the *Exploit Details* field and click the *Proof of Exploit* button.

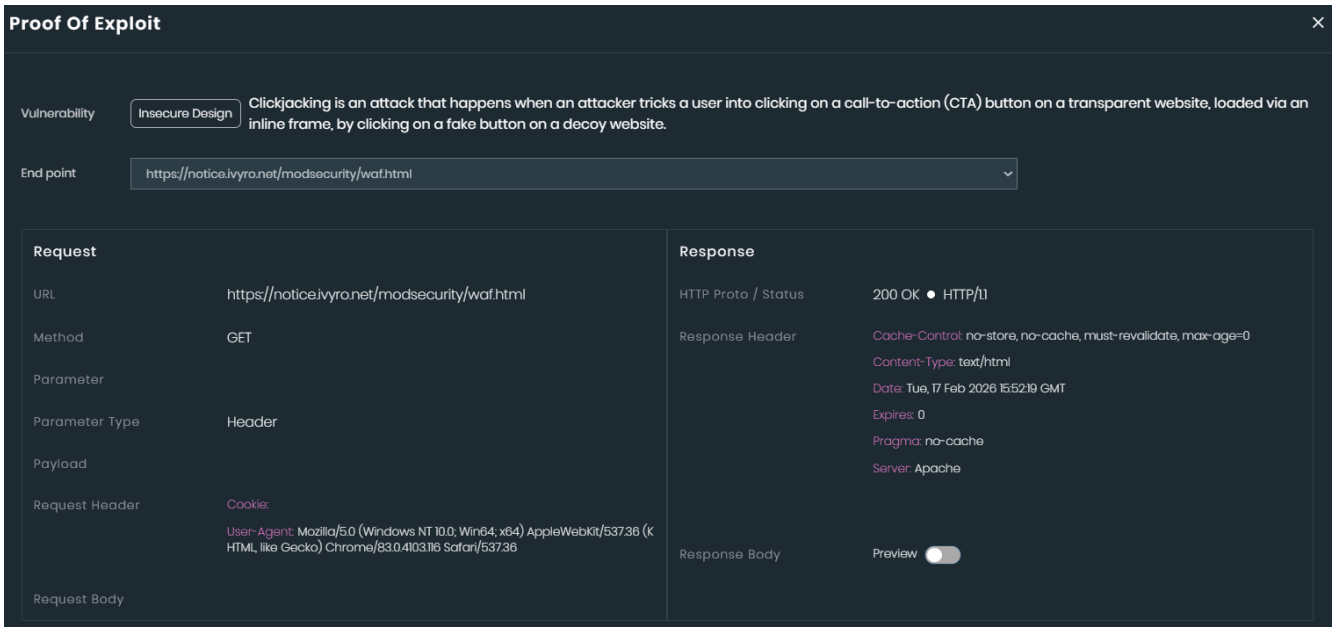


When you click *Proof of Exploit*, a window appears displaying the specific data captured during the scan. This information includes:

- *Vulnerability*: Displays the vulnerability category and a detailed definition of the attack vector.
- *End point*: The specific URL where the vulnerability was detected. Use the dropdown menu to select different endpoints if multiple locations are affected.
- **Request Section**
  - This section details the exact HTTP request sent to the endpoint:
  - *URL* and *Method*: The target URL and the HTTP method used.
  - *Parameter* and *Parameter Type*: Identifies the specific parameter and its location used in the exploit.
  - *Payload*: The specific malicious string or data sent to trigger the vulnerability.

  - *Request Header* and *Body*: The full headers and any data sent in the request body.
- **Response Section**
  - This section details how the server responded to the request:
  - *HTTP Protocol / Status*: The protocol version and server status code.
  - *Response Header:* The full headers returned by the server, including information like Server, Content-Type, and security headers.
  - *Response Body*: Toggle the *Preview* switch to view the raw response data.

> The Preview mode displays the raw HTML or text content. CSS is not rendered in this view.



Modifying Vulnerability Status

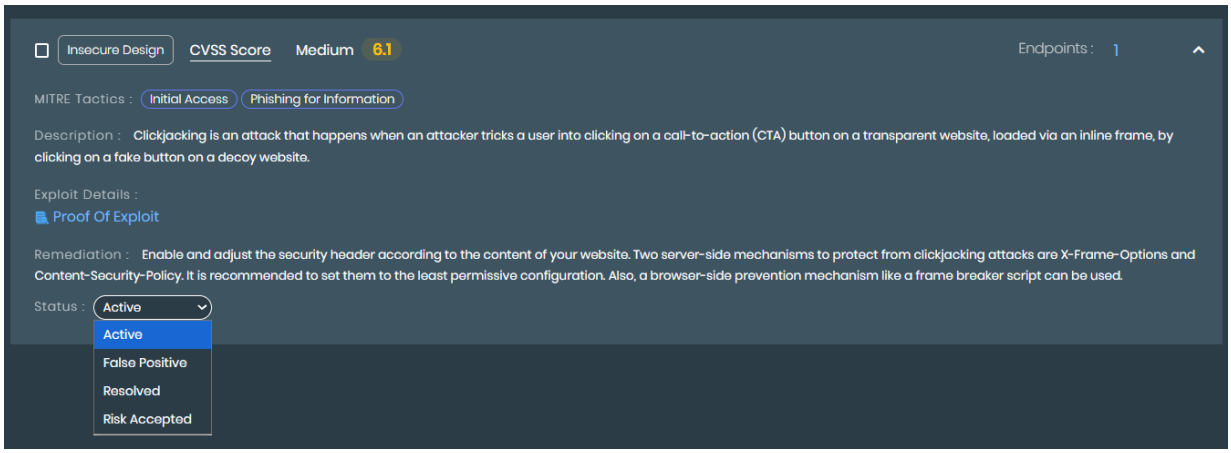
You can manage the lifecycle of identified vulnerabilities by updating their status in the *Vulnerabilities* or *Endpoints* views. Use the *Status* dropdown to categorize vulnerabilities based on their current remediation stage or validity.

Status	Description
Active	The default state for all newly discovered vulnerabilities. FortiRecon continues to monitor these issues.
Resolved	Select this status when the vulnerability has been successfully patched or mitigated and is no longer present on the asset. FortiRecon will attempt to verify the fix during the next scan.
Reopened	This state is automatically assigned by FortiRecon when a vulnerability previously marked as *Resolved* is detected again during a rescan.

Status	Description
Risk Accepted	Select this status for valid vulnerabilities that your organization has decided not to remediate at this time. The vulnerability will remain in this status during subsequent scans.
False Positive	Select this status if the identified vulnerability is an error and does not actually exist on the asset. The vulnerability will remain in this status during subsequent scans.

To Update an Individual Vulnerability

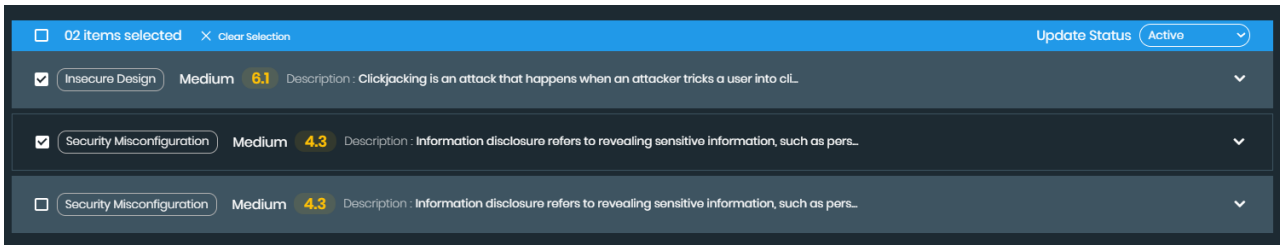
1. Navigate to the *Attack Surface Management* > *Web Application Assessment* page and select a required asset.
2. From the *Vulnerabilities* tab:
   a. Locate the vulnerability and click the arrow to expand the entry.
   b. Select a new status from the *Status* dropdown menu.
   c. Click *Yes* to confirm the status update.



3. Or, from the *Endpoints* tab:
   a. Locate the endpoint and click the *Vulnerabilities* count to view the associated vulnerability list.
   b. Expand the desired vulnerability and update the *Status* dropdown.
   c. Click *Yes* to confirm the status update.

To Perform Bulk Status Updates

1. Go to the *Vulnerabilities* pr *Endpoints* tab and select the checkboxes next to the vulnerabilities you wish to update.
2. Select the new status from the *Update Status* dropdown for all selected items.
3. Click *Yes* to confirm the status update.



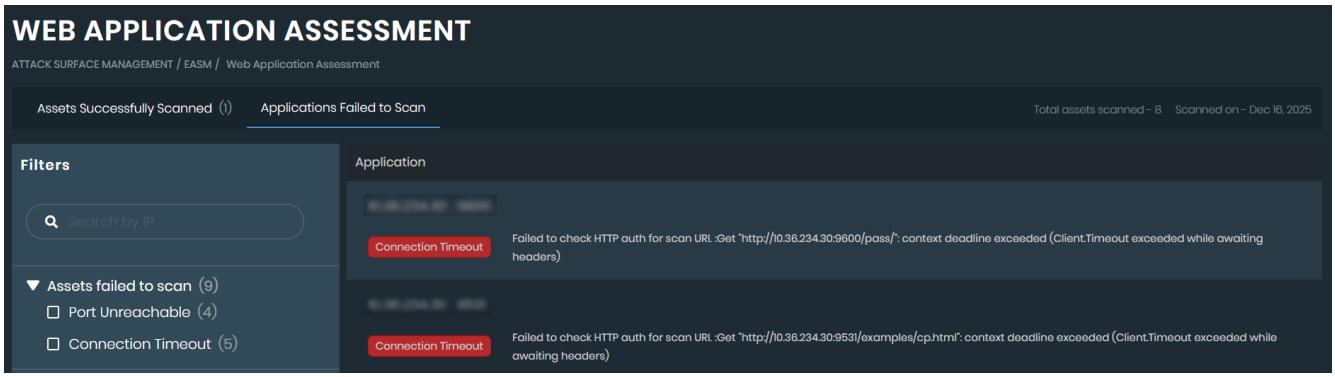
Reviewing Failed Application Scans

The *Web Application Assessment* > *Applications Failed to Scan* tab lists assets that FortiRecon was unable to scan. Each entry provides the application's IP address or domain and the specific reason for the failure such as:

- *Port Unreachable*
- *Connection Timeout*
- *Invalid Service*
- *SSL/TLS Handshake Failure*
- *TLS Connection Aborted*

You can filter the list in two ways.

- Use the search bar to filter by IP address or domain name.
- Use the filters in the *Assets failed to scan* section, which displays the failure reason and the corresponding count.



EASM 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 Management.
- 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 95.

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 68. Groups can be filtered in all *Attack Surface Management* pages.

Tag Management

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

- Create a new asset tag. See Creating a tag on page 86.
- Assign individual and bulk assets to an asset tag. See Adding assets to a tag on page 86.
- Manage, edit, and delete asset tags. See Managing tags on page 88.
- 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 *EASM* toggle.
3. Select the *Tag Management* tab.
4. Click *+Add* and select *Create Tags*. The *Create Tag* dialog is displayed.
5. Enter a *Tag Name*.
6. Enter a *Tag Description*.
7. Select the *Theme Color* icon to assign the tag color.
8. Click *Submit*. The new tag is added to the *Tag Management* > *Tags* tab.

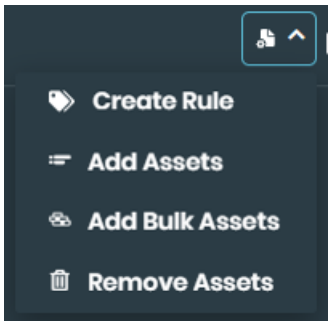
Adding assets to a tag

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 71.
- Tags can also be assigned to assets in *Attack Surface Management* > *Asset Discovery*. See Assigning tags on page 72.

To create a tagging rule

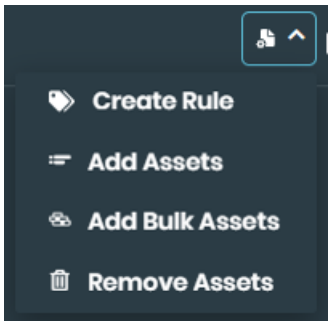
1. Go to *Attack Surface Management* > *Asset Management*.
2. Select *EASM* toggle.
3. Select the *Tag Management* > *Tags* tab.
4. For a single tag, locate the tag you want to create tagging rule and click *Settings* icon. A dropdown menu is displayed. Click *Create Rule*.



   For multiple tags, select the tags you want to create tagging rule for and click *+Add* > *Create Rules*.
5. 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 *EASM* toggle.
3. Select the *Tag Management* > *Tags* tab.
4. Locate the tag you want to add assets to and click *Settings* icon. A dropdown menu is displayed.

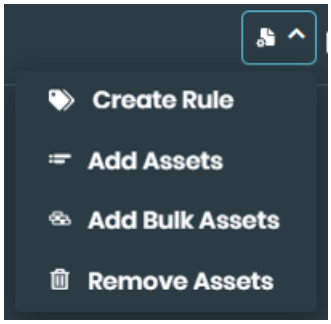


5. Select *Add Assets*.
6. Select the assets to add from the *Validated Assets list*.
7. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
8. Click the right arrow. The selected assets will be moved into the tag field.
9. Click *Save*.

To add bulk assets to a tag:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select *EASM* toggle.
3. Select the *Tag Management* > *Tags* tab.

4. Locate the tag you want to add assets to and click *Settings* icon. A dropdown menu is displayed.



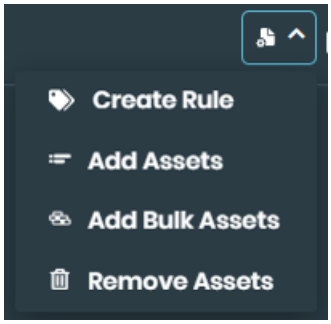
5. Select *Add Bulk Assets*.
6. Enter the asset information in the left field.
7. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
8. Click *Save*. FortiRecon validates the assets. If any invalid assets are found, a list appears in the left field. Correct or remove the invalid values from the list to assign assets to the tag.

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 *EASM* toggle.
3. Select the *Tag Management* > *Tags* tab.
4. Locate the tag you want to remove assets from and click *Settings* icon. A dropdown menu is displayed.



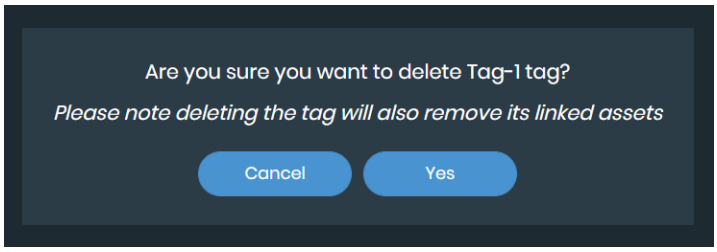
5. Select *Remove Assets*.
6. Select the assets you want to remove or click *Select All*.
7. Click *Remove Selected*.

To edit a tag:

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

To delete a tag:

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



5. Click *Yes*.

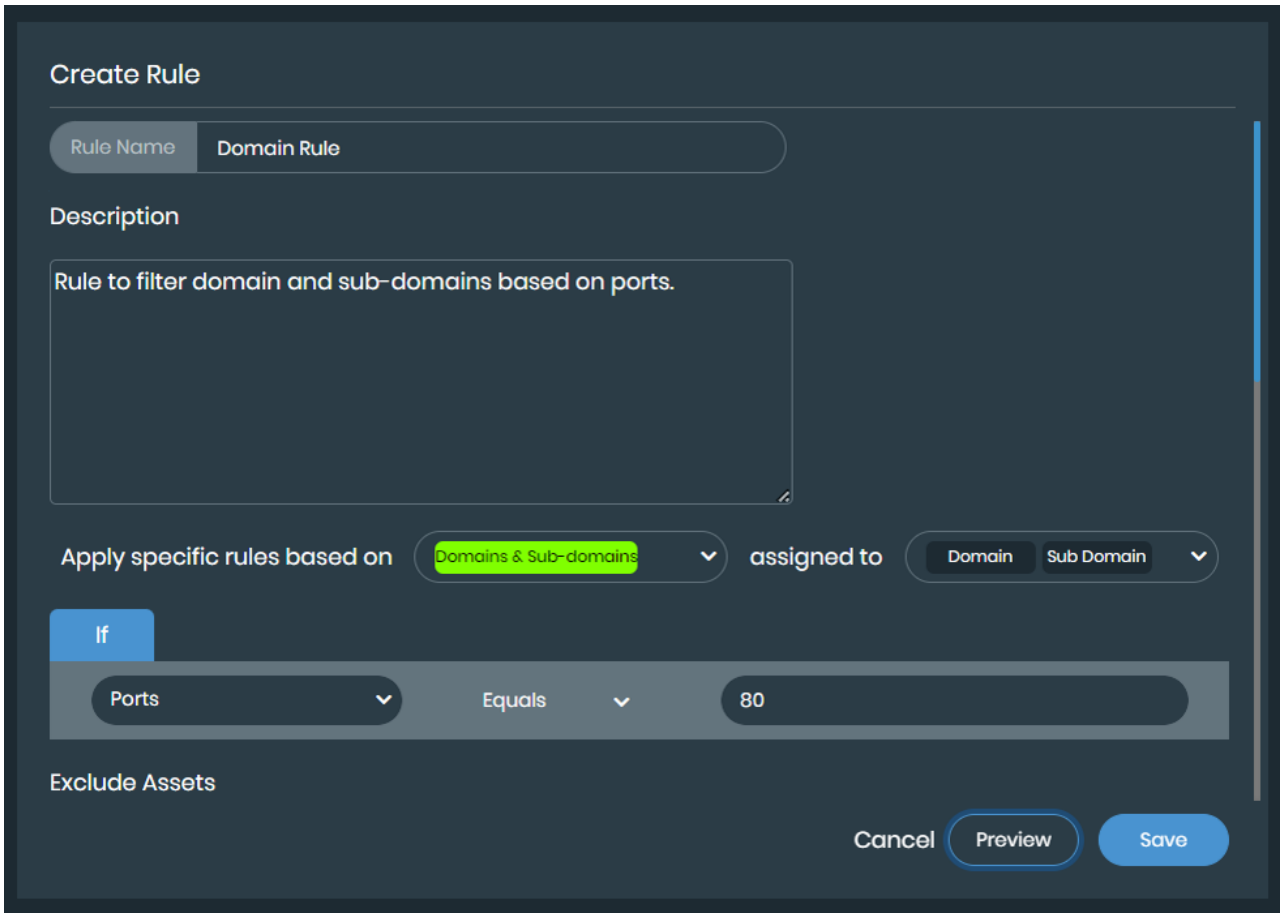
Creating a tagging rule

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 *EASM* toggle.
3. Select the *Tag Management* tab.
4. Click +*Add* and select *Create Rules*. The *Create Rule* dialog is displayed.
5. Enter a *Rule Name*.
6. (Optional) Enter a *Description*.
7. Select *Tags* and *Asset type*.
8. Define your rule using supported conditions.
9. (Optional) Specify the assets to exclude from the rule.
10. Click *Preview* to see a sample of assets the rule would affect displayed in the *Assets Tagged* section.
11. 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 Name (Starts with, Ends with, Wildcard)

Asset Type	Conditions
	• 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 *EASM* toggle.
3. Select the *Tag Management* > *Rules* tab.
4. 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 *EASM* toggle.
3. Select the *Tag Management* > *Rules* tab.
4. Locate the rule you want to clone and click the *Clone* icon.
5. Enter a name and description.
6. Click *Submit*.

To edit a rule:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select *EASM* toggle.
3. Select the *Tag Management* > *Rules* tab.
4. Locate the rule you want to edit and click the *Edit* icon.
5. Enter
6. Click *Submit*.

To delete a rule:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select *EASM* toggle.
3. Select the *Tag Management* > *Rules* tab.
4. Locate the rule you want to delete and click the *Delete* icon. A confirmation message is displayed.
5. 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 92.
- Assign individual and bulk assets to an asset group. See Adding assets to a group on page 93.
- Manage, edit, and delete asset groups. See Managing groups on page 93.
- Filter *Attack Surface Management* pages by group. See Filtering by group on page 94.

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 *EASM* toggle.
3. Select the *Group Management* tab.
4. Click *Create*. The *Create Group* dialog is displayed.
5. Enter a *Group Name*.
6. Enter a *Group Description*.
7. 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 93.

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 71.

To add assets to a group:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select *EASM* toggle.
3. Select the *Group Management* tab.
4. Locate the group you want to add assets to and click *Manage Assets* icon. A dropdown menu is displayed.
5. Select *Add Assets*.
6. Select the assets to add from the *Validated Assets list*.
7. Click the right arrow. The selected assets will be moved into the tag field.
8. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
9. Click *Save*.

To add bulk assets to a group:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select *EASM* toggle.
3. Select the *Group Management* tab.
4. Locate the group you want to add assets to and click *Manage Assets* icon. A dropdown menu is displayed.
5. Select *Add Bulk Assets*.
6. Enter the asset information in the left 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*. FortiRecon validates the assets. If any invalid assets are found, a list appears in the left field. Correct or remove the invalid values from the list to assign assets to the tag.

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 *EASM* toggle.

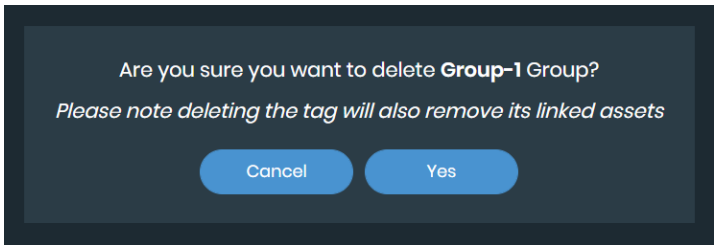
3. Select the *Group Management* tab.
4. Locate the group you want to remove assets from and click *Manage Assets* icon. A dropdown menu is displayed.
5. Select *Remove Assets*.
6. Select the assets you want to remove or click *Select All*.
7. Click *Remove Selected*.

To edit a group:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select *EASM* toggle.
3. Select the *Group Management* tab.
4. Locate the group you want to edit and click the *Edit* icon.
5. Edit the fields.
6. Select *Assign Group To All Users* to make the assets visible to all users. See Limiting access to assets and issues on page 95.
7. Click *Submit*.

To delete a group:

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



5. Click *Yes*.

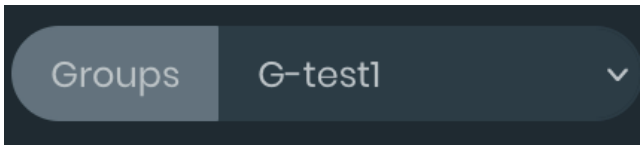
Filtering by group

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.

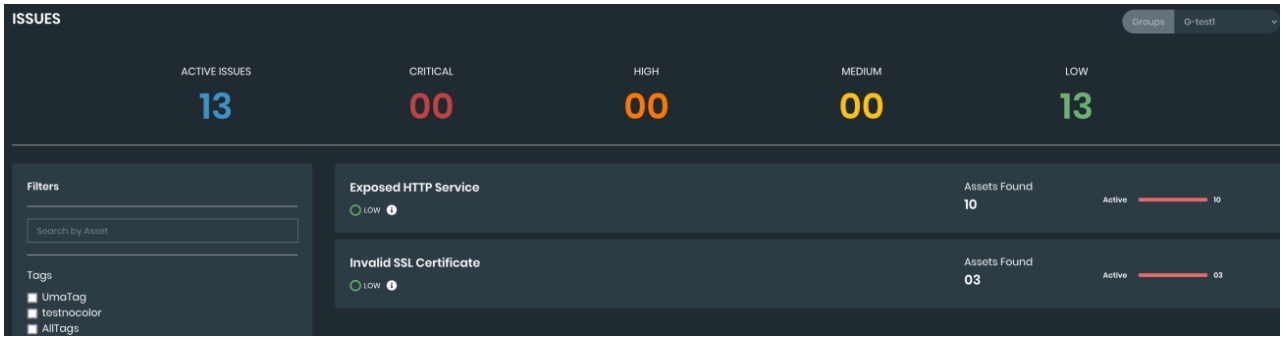
The following example demonstrates filtering by group in the *Attack Surface Management* > *Security Issues* page.

To filter by group:

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



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



Limiting access to assets and issues

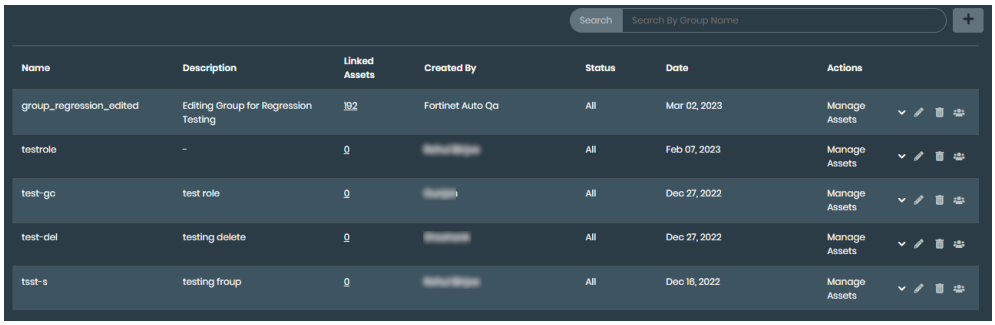
User access to specific assets and security issues can be limited through the use of groups and tags. User asset and security issue visibility is limited to the groups they are assigned to and any tags associated with these group assets.

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

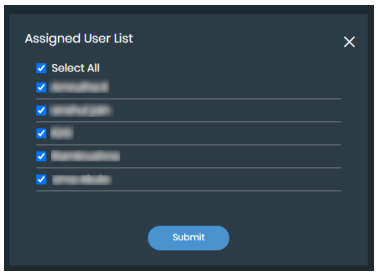
User assigned to	Visible assets	Hidden assets
A single group with no tags assigned	• All assets that have been added to the group	• Assets that have not been added to the group
A single group with tags assigned to the assets	• Assets that have been added to the group that also have the tags assigned	• 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 *EASM* toggle.
3. Select the *Group Management* tab.



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



5. 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.
6. Click *Submit*.

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.

Also, the IASM module actively identifies and profiles Operational Technology (OT) and Internet of Things (IoT) assets exposed across the attack surface and detects the vulnerabilities or security issues related to them. The following OT / IoT protocols are supported:

- *OT*: Siemens S7, Modbus, CIP (EtherNet/IP), DNP3, BACnet, and OPC-UA.
- *IoT*: CoAP, MQTT, and UPnP.

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.

- IASM Dashboard
- IASM Security Issues
- IASM Asset Discovery
- IASM Asset Management

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.

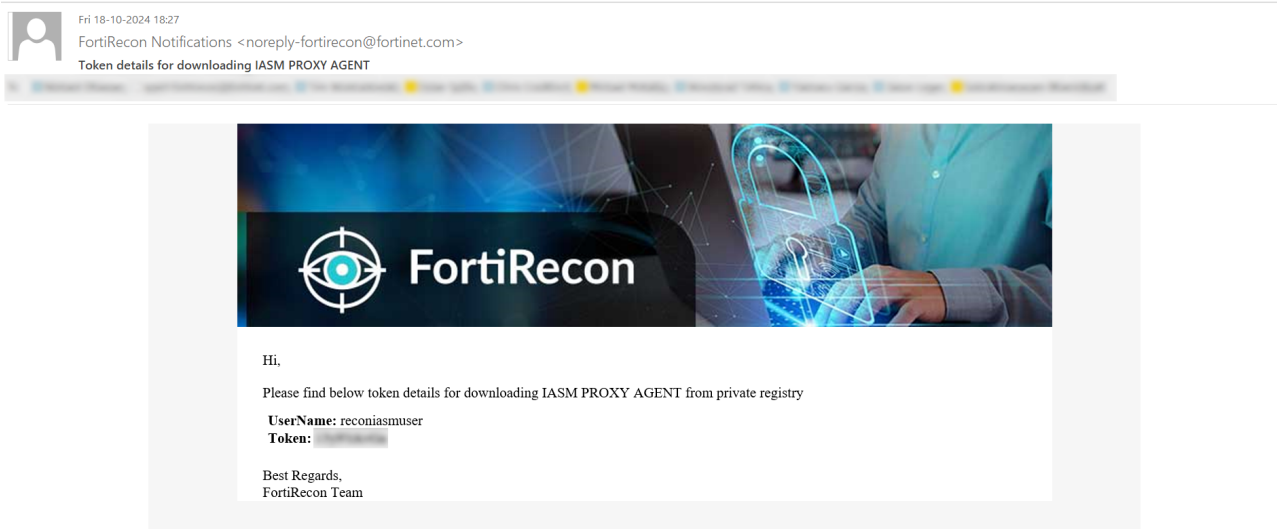
> Ensure that System Requirements and Prerequisites are met before deploying IASM Agent.

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.

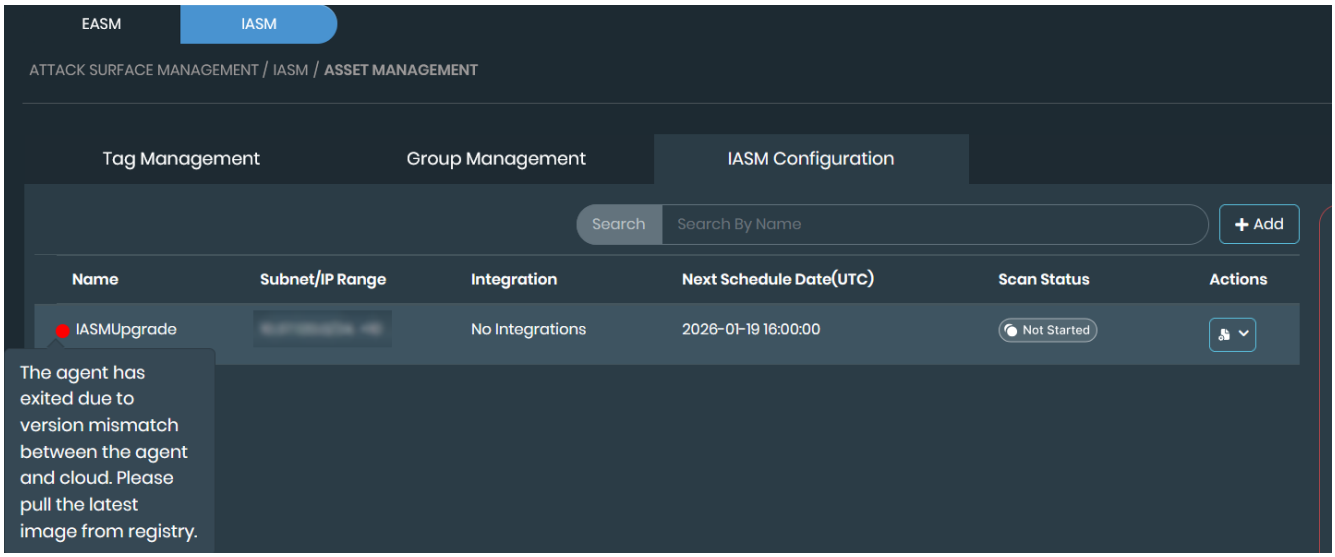
Upgrading IASM Agent

FortiRecon supports automatic upgrades for the Internal Attack Surface Management (IASM) Agent and Proxy binaries for all minor version updates. Once your environment is running the latest version, the system periodically checks for and automatically applies these updates. The system distinguishes between updates based on the scope of the changes:

- *Major Upgrades*: Occur when the major base or underlying framework becomes outdated or is replaced. These updates require a manual upgrade. You will receive a notification when a major update is available. See Upgrading IASM agent manually.
- *Minor Upgrades*: Occur when there is a change to the scan logic or security signatures. These are handled automatically by the system.

When a major framework change occurs, the agent will stop running to prevent compatibility issues. In the FortiRecon UI, the agent status will turn *Red*, and the following message will be displayed:

The agent has exited due to a MAJOR version mismatch between the agent and cloud. Please pull the latest image from the registry.



> If you are an existing customer, you must perform a one-time manual upgrade to enable the automatic update functionality for future minor versions.

To upgrade the agent manually:

Use the following steps for initial setup, major version updates, or if an automatic update fails:

1. Open a terminal on the host machine and navigate to the directory containing your existing *iasmproxy.yml* file.
2. Stop the currently running containers.
   ```
   sudo docker-compose -f <iasmproxy.yml> down
   ```
3. Log in to the FortiRecon Docker registry.
   ```
   sudo docker login demo.fortirecon.forticloud.com
   ```
   When prompted, enter the credentials provided to you in your email notification.
4. Pull the latest agent image from the registry.
   ```
   sudo docker pull demo.fortirecon.forticloud.com/iasmproxy:latest
   ```
5. Start the updated agent in detached mode:
   ```
   sudo docker-compose -f <iasmproxy.yml> up -d
   ```

> Replace <*iasmproxy.yml*> with the specific name of your configuration file. The agent will automatically reconnect and resume monitoring once the process is complete.

Troubleshooting the IASM Agent

Verify that you are using the correct *iasmproxy.yml* configuration file for your environment if the agent fails to start. Contact Fortinet Support for assistance if the agent fails to start after you have verified and corrected the *iasmproxy.yml* file.

IASM Dashboard

The *Attack Surface Management* > *Dashboard* > *IASM* 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.

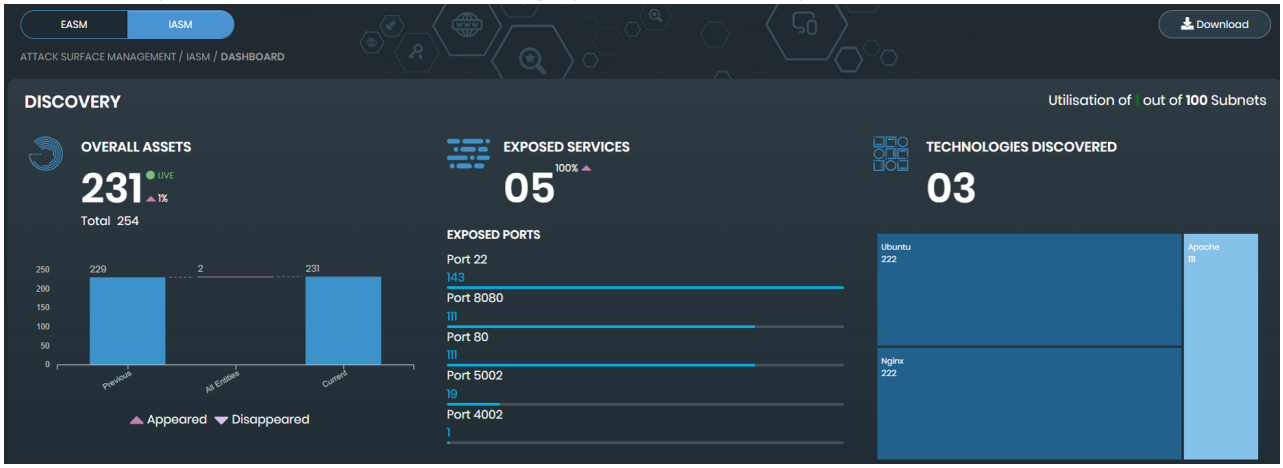
Viewing discovered assets summary

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 IASM 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.

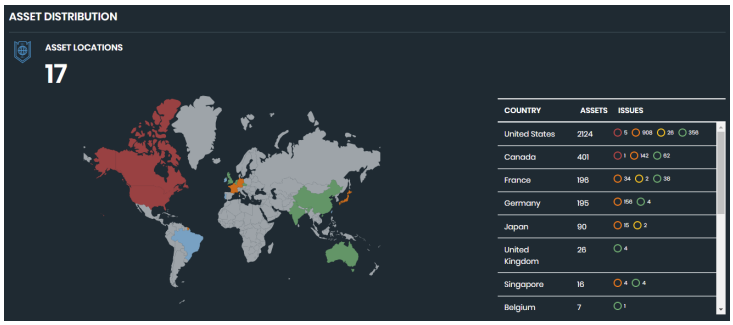
3. Click an issue or vulnerability to display more details on the *Security Issues* page. See IASM Security Issues.

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 IASM 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 271.

IASM Security Issues

The *Attack Surface Management* > *Security Issues* > *IASM* 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

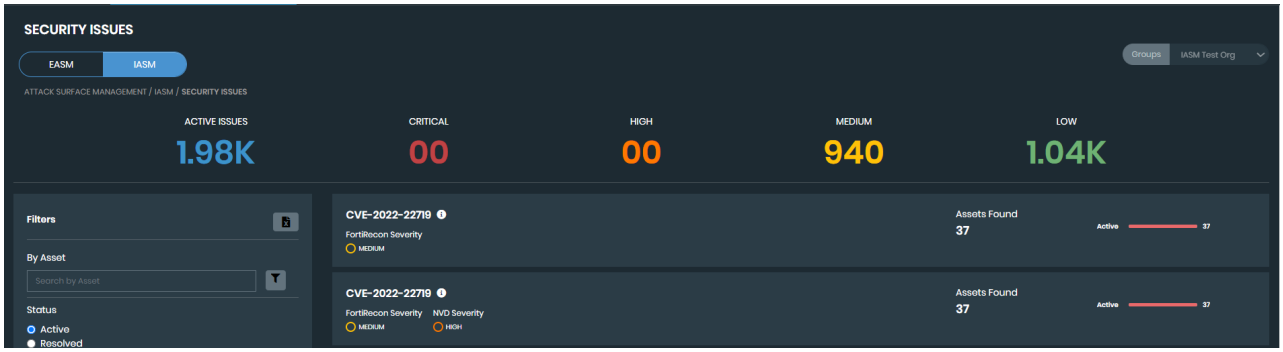
The *Attack Surface Management* > *Security Issues* page displays the number of active security issues and how many of the active security issues are rated critical, high, medium, and low. Color indicates the severity of a security issue:

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.

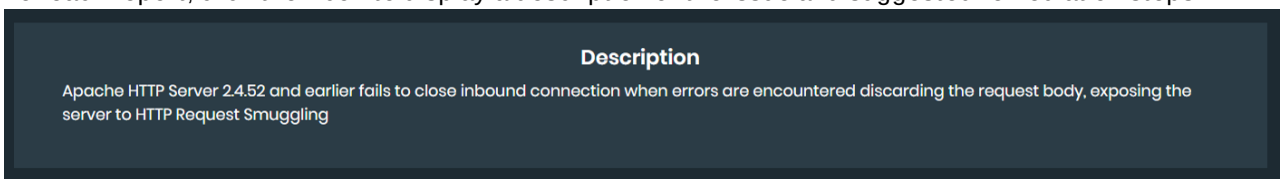
You can use search and filters to change the list of reports that are displayed, and then click each report to display its details.

To view security issues:

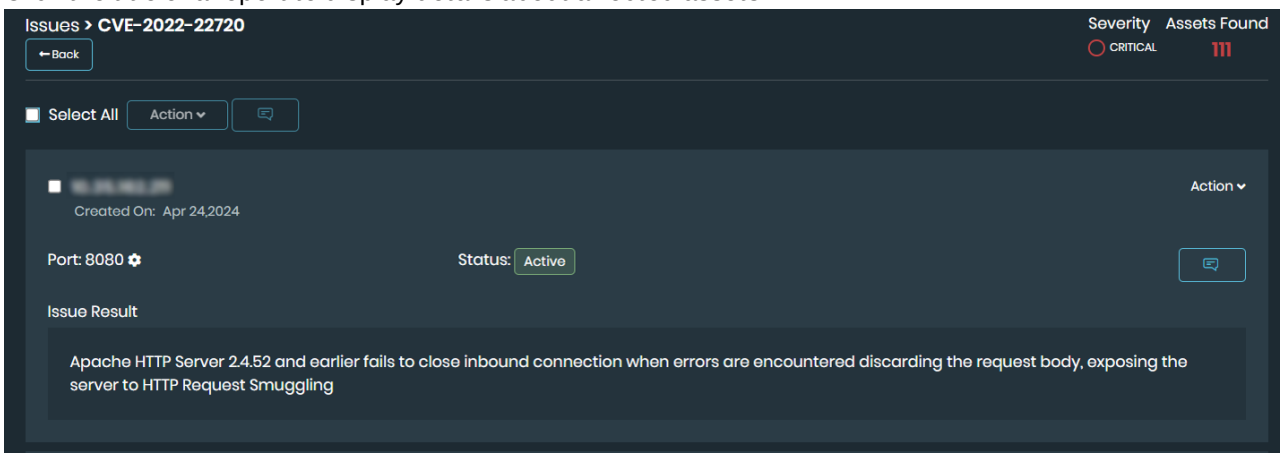
1. Go to *Attack Surface Management* > *Security Issues*. Choose *IASM* using toggle, the respective security issues are displayed.
   The *Issues* bar across the top displays the number of active security issues and the number of active security issues that are rated critical, high, medium, and low 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 identified CVEs, a brief description is displayed.
4. For each report, click the *i* icon to display a description of the issue and suggested remediation steps.



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

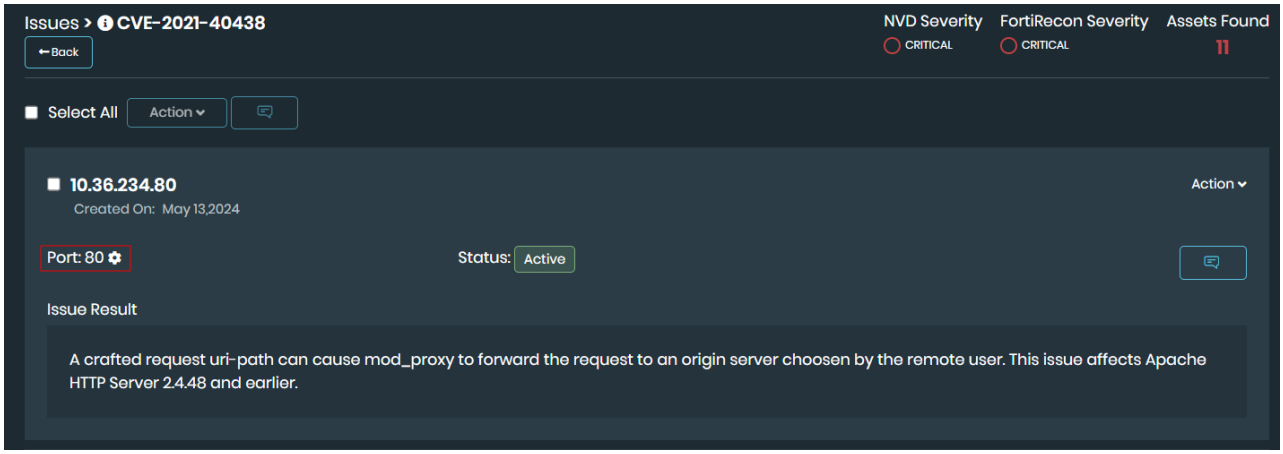


6. Click gear icon next to Port to view *Service Discovery* information. See Reviewing Service Discovery.

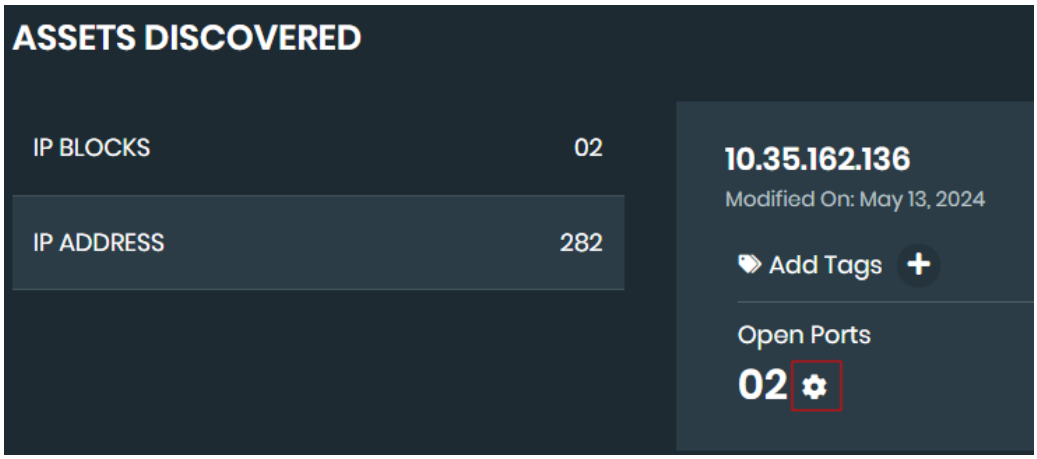
Reviewing Service Discovery

The *Service Discovery* view provides a technical breakdown of the services, protocols, and versions running on your internal assets. You can access the *Service Discovery* view through the following two methods:

1. *From Security Issues page*: Navigate to *Attack Surface Management* > *Security Issues* > *IASM*. Click an issue title to view the affected assets. If discovery data is available, click the gear icon next to the port number for a specific asset.



2. *From Asset Discovery page*: Navigate to *Attack Surface Management* > *Asset Discovery* > *IASM*. In the *IP Addresses* tab, locate the required asset and click the gear icon next to the *Open Ports* count. Use the *Search* bar at the top to filter results by port



The following information is displayed.

- *Discovered Date*: The date the service was identified.
- *Port*: The network port number.
- *Service*: The name of the identified service or protocol.
- *Version*: The version of the service, if detected.
- *CPE*: The Common Platform Enumeration (CPE) string identifying the hardware or software.

Click *View Full Detail* in the table to expand the metadata for a specific entry. This section provides granular discovery data, including:

- *CPE*: The full CPE identifier.
- *Created Date*: The precise system timestamp of the discovery.
- *IP Address*: The IP address of the target asset.
- *Port*: The specific port associated with the entry.
- *Product*: The identified product name (e.g., simatic_s7-1500_et_200pro). This is especially useful for identifying OT and IoT devices.
- *Service*: The protocol or service type identified.

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:

Filter	Options
Status	Select one of the following statuses: • *Active* • *Resolved* • *Risk accepted* • *False positive*
FortiRecon Severity	Select one or more of the following FortiRecon severity statuses: • *Critical* • *High* • *Medium* • *Low*
NVD Severity	Select one or more of the following NVD 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. • *OT/IoT* • *CORS Misconfiguration* • *Security HTTP Headers* • *Information Disclosure* • *Suspicious Domains* • *Web Filter Rating Lookup* • *SSL Tests* • *Weak Cipher* • *Vulnerable Web Technologies* • *Vulnerable Network Services* • *CMS Security*
Tags	Select one or more tags. Tags list includes system generated *OT* and *IOT* tags.

   The list of filtered security issues is displayed.
5. In the *Filters* list, click *Clear* to remove all filters.
6. The *Archived Results (All Time)* section displays all results previously marked as *False Positive* or *Risk Accepted*. To revert an archived action and return a result to an *Active* state, locate the result in the *False Positive* or *Risk Accepted* lists and change the status back to *Active*.

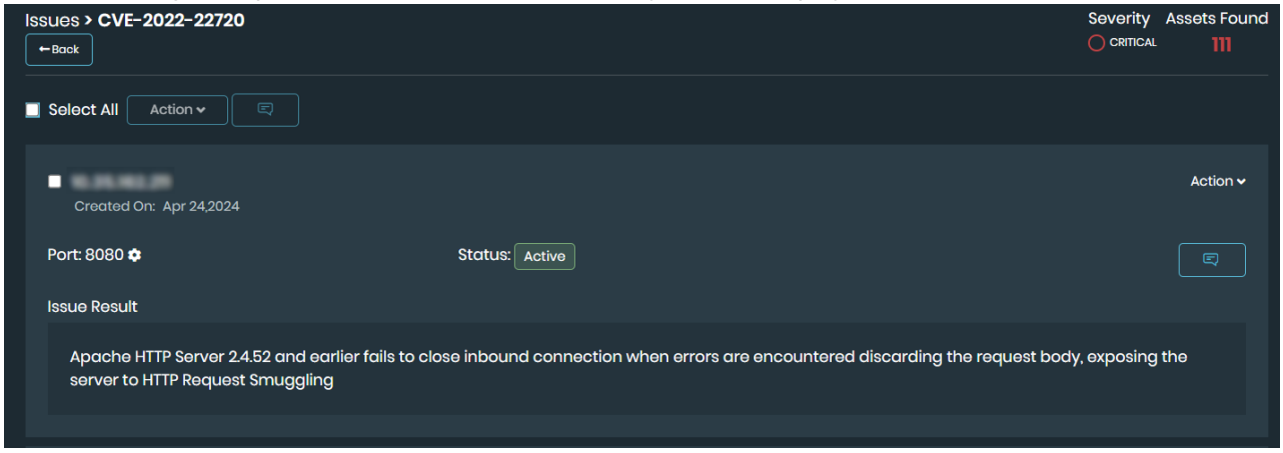
Changing the status of security issues

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.
   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*.

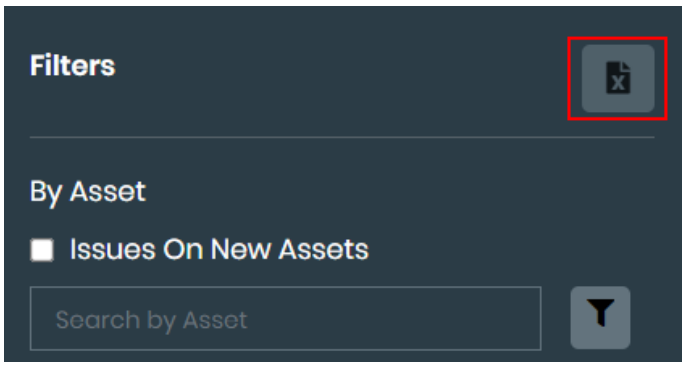
Exporting security issues

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.



IASM Asset Discovery

The *Attack Surface Management* > *Asset Discovery* > *IASM* 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.
- Filter the discovered assets. See Filtering IASM Assets.
- Assign tags to assets for focused filtering. See Assigning tags.

Viewing asset details

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

You can view details about an asset by clicking *IP Block* and *IP Address* count in the *Overview* section or by selecting a category in the *Assets Discovered* section.

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* section, click *IP Block* or *IP Address* count, or in the *Assets Discovered* list, click an asset category. Details about the selected item are displayed on the right side of the page. To filter discovered assets see Filtering IASM Assets.
   - **IP Block Details**

     Selecting an IP block displays network-level information, including:
     - *IP Block Range*: The CIDR notation for the discovered block (e.g., 10.36.239.0/24).
     - *Modified On*: The date the block information was last updated.
     - *Total IPs*: The total number of IP addresses contained within the block.
     - *Live IPs*: The number of IP addresses currently active and reachable.
   - **IP Address Details**

The following information is displayed for each IP address discovered.

- *IP Address*: The IP address of the asset.
- *Tags*: Existing tags (such as *OT* or *IOT*) and the *Add Tags* option to manually categorize the asset.
- *Open Ports*: The total count of open ports identified. Click the gear icon to open the *Service Discovery* view. See Reviewing Service Discovery
- *Issues*: The total count of identified security issues. Click the link icon to view vulnerability details.

Filtering IASM Assets

You can use the search and filter tools on the *IASM Asset Discovery* page to narrow down the list of discovered assets based on specific criteria, such as integration types, technologies, or tags.

- The primary search bar allows you to locate specific assets quickly. Type a value in the search bar to find a specific asset. Click Advance Search to refine your search by:
  - *Search Type*: Select *Exact*, *Starts With*, *Ends With*, or *Wildcard*.
  - *Asset Type*: Filter results by *IP Block* or *IP Address*.
- If you have configured third-party integrations, use the dropdown menu next to the search bar to filter assets by their source.
  - *All Assets*: Displays every asset discovered by IASM.
  - *FortiGate Integration*: Filters the list to show only assets discovered via integrated *FortiGate* devices.
- Click the Filter icon to expand granular filtering options. You can filter assets using the following categories:
  - *Ports*: Search for assets with specific open ports.
  - *Technology*: Filter by identified technology stacks.
  - *Tags*: Use the *Tags* section to filter by automated or manual tags.
    - Select the checkboxes for *IOT* or *OT* to view specific asset classes. FortiRecon automatically classifies and tags discovered *OT* and *IoT* assets during IASM scans.
    - Use the Search tag bar to find a specific tag quickly.
- Click *Clear All* to reset your tag selections.

Assigning tags

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

To assign a tag to an asset:

1. Go to *Attack Surface Management* > *Asset Discovery*.
2. Select *IASM* toggle.
3. 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 Adding assets to a tag.

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

IASM Asset Management

The *Attack Surface Management* > *Asset Management* > *IASM* 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. See Tag Management.
- 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.
- 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. Groups can be filtered in all *Attack Surface Management*pages.

Tag Management

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 86.
- Assign individual and bulk assets to an asset tag. See Adding assets to a tag.
- Manage, edit, and delete asset tags. See Managing tags.

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

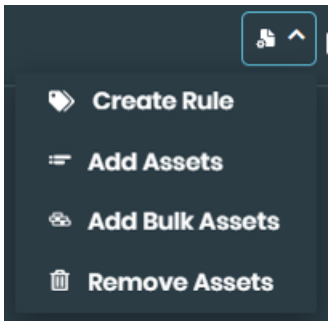
Adding assets to a tag

You can add individual or bulk assets to a tag from the *Tag Management* 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.
> - Tags can also be assigned to assets in *Attack Surface Management* > *Asset Discovery*. See Assigning tags.

To add assets to a tag:

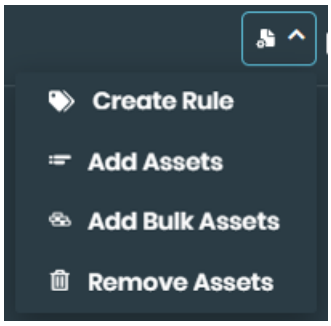
1. Go to *Attack Surface Management* > *Asset Management*.
2. Select *IASM* toggle.
3. Select the *Tag Management* tab.
4. Locate the tag you want to add assets to and click *Settings* icon. A dropdown menu is displayed.



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

To add bulk assets to a tag:

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



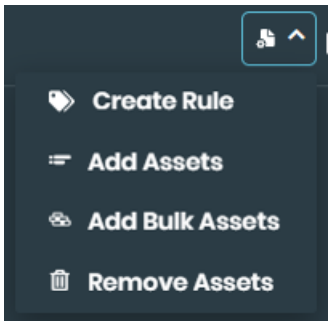
5. Select *Add Bulk Assets*.
6. Enter the asset information in the left field.
7. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
8. Click *Save*. FortiRecon validates the assets. If any invalid assets are found, a list appears in the left field. Correct or remove the invalid values from the list to assign assets to the tag.

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 *IASM* toggle.
3. Select the *Tag Management* tab.
4. Locate the tag you want to remove assets from and click *Settings* icon. A dropdown menu is displayed.



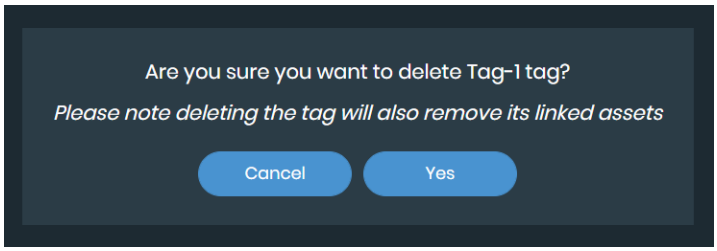
5. Select *Remove Assets*.
6. Select the assets you want to remove or click *Select All*.
7. Click *Remove Selected*.

To edit a tag:

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

To delete a tag:

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



5. 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.
- Assign individual and bulk assets to an asset group. See Adding assets to a group.
- Manage, edit, and delete asset groups. See Managing groups.
- Filter *Attack Surface Management* pages by group. See Filtering by group.

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 *IASM* toggle.
3. Select the *Group Management* tab.
4. Click *Create*. The *Create Group* dialog is displayed.
5. Enter a *Group Name*.
6. Enter a *Group Description*.
7. 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.

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.

To add assets to a group:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select *IASM* toggle.
3. Select the *Group Management* tab.
4. Locate the group you want to add assets to and click *Manage Assets* icon. A dropdown menu is displayed.
5. Select *Add Assets*.
6. Select the assets to add from the *Validated Assets list*.

7. Click the right arrow. The selected assets will be moved into the tag field.
8. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
9. Click *Save*.

To add bulk assets to a group:

1. Go to *Attack Surface Management* > *Asset Management*.
2. Select *IASM* toggle.
3. Select the *Group Management* tab.
4. Locate the group you want to add assets to and click *Manage Assets* icon. A dropdown menu is displayed.
5. Select *Add Bulk Assets*.
6. Enter the asset information in the left 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*. FortiRecon validates the assets. If any invalid assets are found, a list appears in the left field. Correct or remove the invalid values from the list to assign assets to the tag.

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:

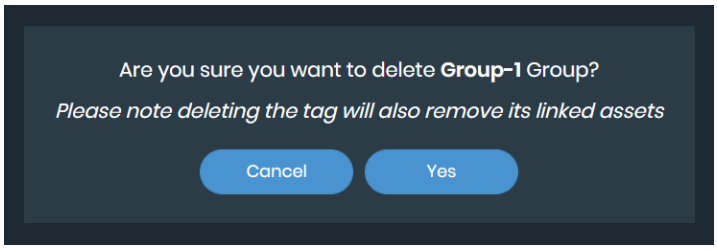
1. Go to *Attack Surface Management* > *Asset Management*.
2. Select *IASM* toggle.
3. Select the *Group Management* tab.
4. Locate the group you want to remove assets from and click *Manage Assets* icon. A dropdown menu is displayed.
5. Select *Remove Assets*.
6. Select the assets you want to remove or click *Select All*.
7. Click *Remove Selected*.

To edit a group:

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

To delete a group:

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



5. Click *Yes*.

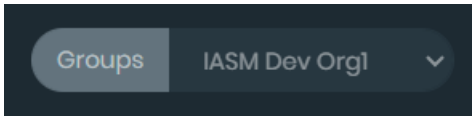
Filtering by group

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. Select *IASM* toggle.
3. Click the *Groups* dropdown menu.



4. 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.

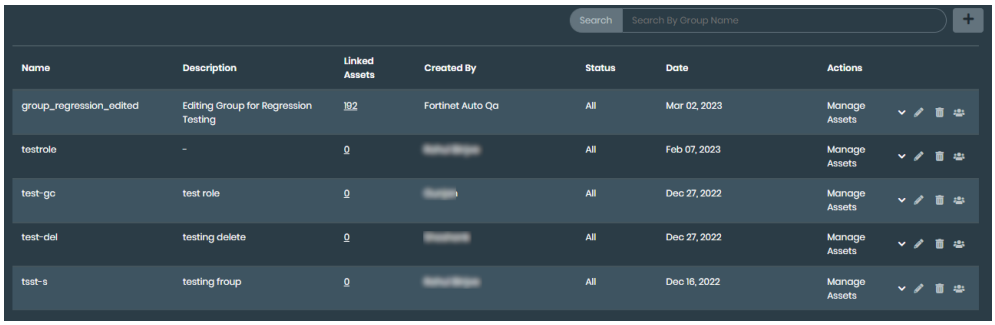
The following table presents examples of visible and hidden assets based on the groups that a user is assigned to:

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

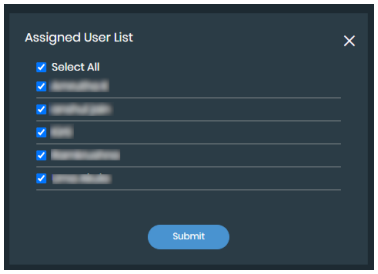
User assigned to	Visible assets	Hidden assets
A single group with tags assigned to the assets	• Assets that have been added to the group that also have the tags assigned	• Assets that have not been added to the group • Any assets included in the assigned group that do not have the tags assigned
Multiple 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 *IASM* toggle.
3. Select the *Group Management* tab.



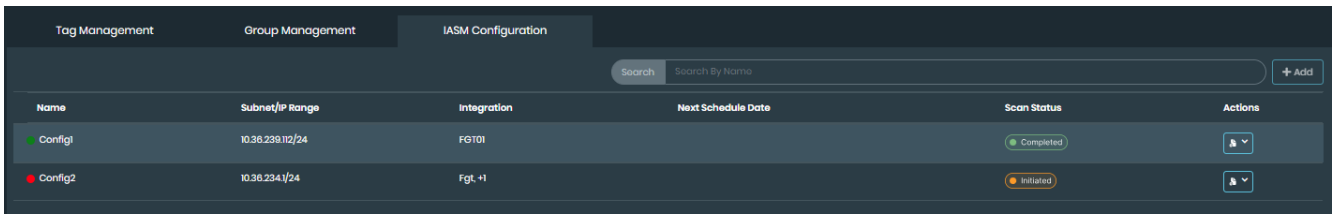
4. Select *Assign User*. The *Assigned User List* dialog is displayed.



5. 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.
6. Click *Submit*.

IASM Configuration

The *Asset Management* > *IASM* > *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.

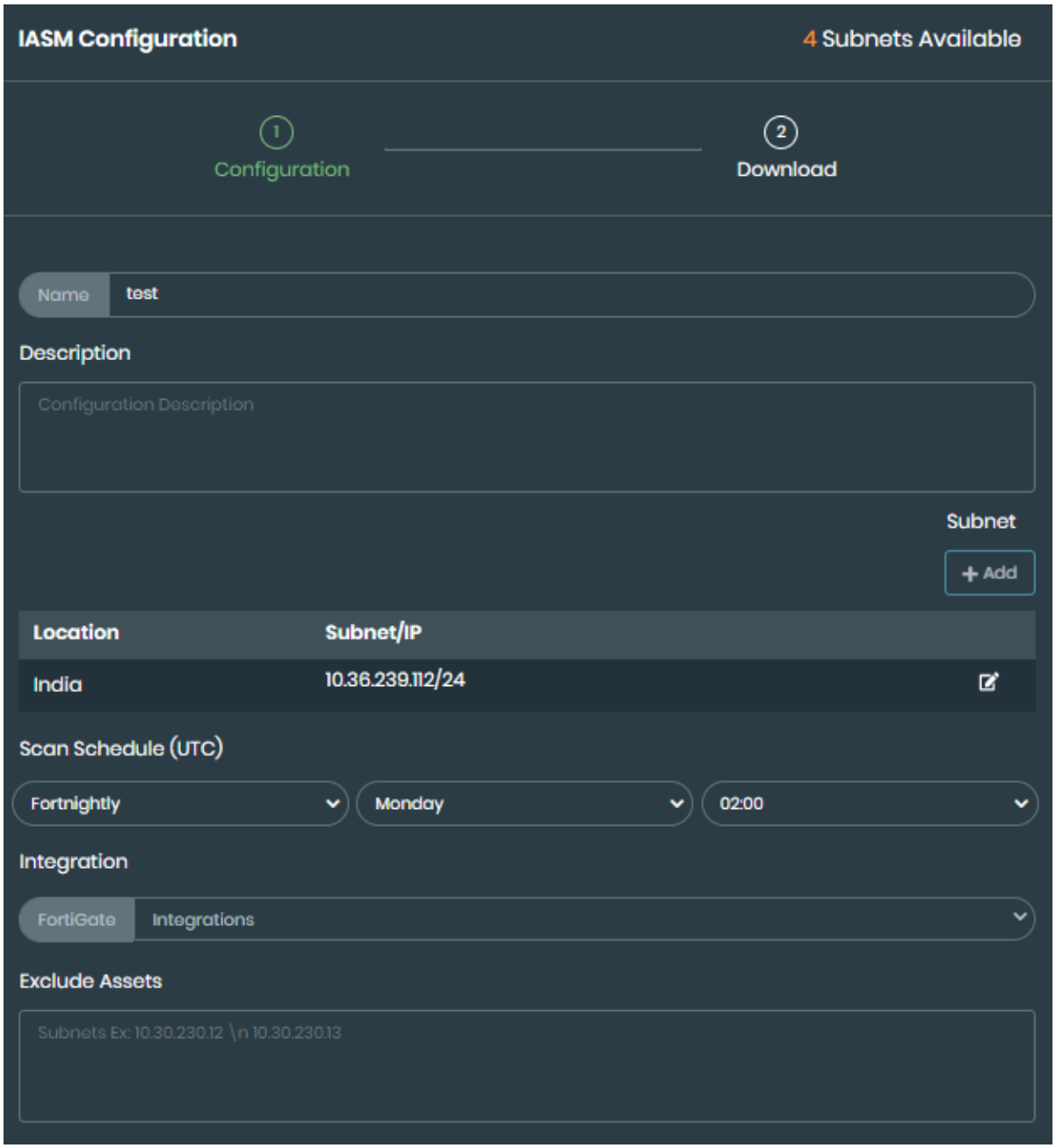
- *IASM Agent Status*: A green indicator signifies a connected IASM agent; red indicates a disconnected agent.
- *Name*: The identifying name assigned to the configuration.
- *Subnet/IP Range*: The subnet(s) specified in the scan configuration.

  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* .
2. Select *IASM* toggle.
3. Select *IASM Configuration* tab.
4. Click +*Add*.
5. Provide a name and description.
6. 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*.
7. Schedule your scans to run weekly or fortnightly, select the desired days of the week, and specify the start time in UTC.
8. (Optional) Select FortiGate integration. You can integrate FortiGate with IASM to discover the attack surface of the devices managed by FortiGate.
9. (Optional) In *Exclude Assets* section, enter IP addresses of any assets to be excluded from the scan.
10. Review the details and click *Next*.
11. 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.
12. Click *Save*.



To edit an existing configuration:

1. Navigate *Attack Surface Management* > *Asset Management* .
2. Select *IASM* toggle.
3. Select *IASM Configuration* tab.
4. Click *Actions* icon next to the configuration you want to modify and click *Edit*.
5. 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:

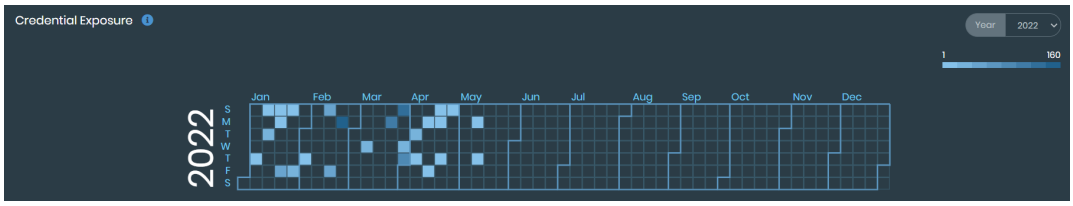
- View leaked credentials by year. See Viewing leaked credentials by year on page 122.
- View breached datasets. See Viewing breached datasets on page 123.
- View leaked credential details. See Viewing leaked credential details on page 123.
- Export a list of leaked accounts. See Exporting leaked accounts on page 125.

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 123.

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.
5. Click *Run Automation* in the *Actions* dropdown to run playbooks. See Security Orchestration.

- Only an administrator can view leaked passwords. Click the view icon to reveal the masked password.
- Records where the password field is marked *Unavailable* indicate older breaches (prior to November 27, 2025) for which FortiRecon did not index the passwords.

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. Filter records *With Password* or *Without Password* in the *Credentials Exposed* section.
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

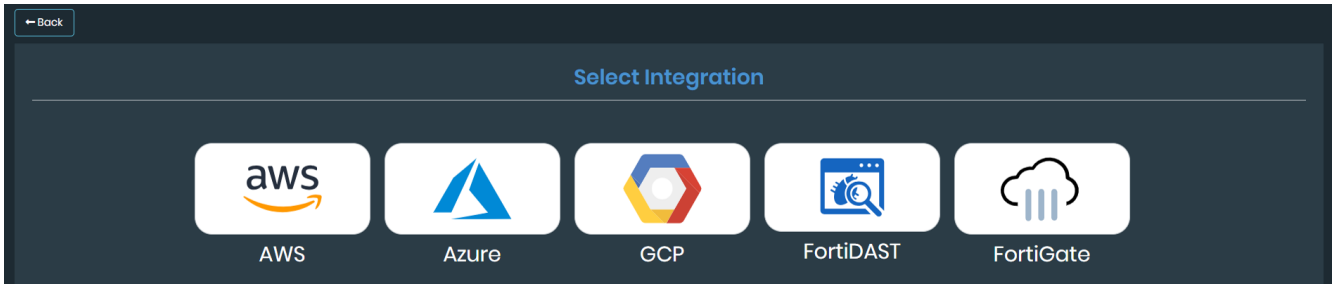
You can export a list of leaked accounts to Microsoft Excel format.

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 125.
- Edit and delete existing integrations. See Editing integrations on page 128.

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:

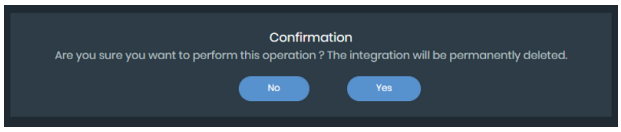
1. Go to *EASM* > *Integrations*.
2. Click *Edit*. The integration details are displayed.
3. Edit the fields you want to change.

   > 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 130.
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 133.
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 140.
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 144.
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 152.
Open Bucket Exposure	Displays a list of files exposed in open buckets. See Open Bucket Exposure on page 156.
Take Down	Displays a list of takedown request tickets and their current status. You can initiate a new takedown or revoke the existing takedown request. See Takedown on page 158.

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. The metrics and elements on the dashboard are clickable, which allows you to quickly drill down to view the corresponding detailed information.

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 130.
- View a summary of brand abuse, such as rogue apps or social media threats. See Viewing the brand abuse summary on page 131.
- View a summary of information exposure, including code and file exposure. See Viewing the information exposure summary on page 131.
- View trends and important alerts of threats to your brand. See Viewing the alert summary on page 132.
- View total credits used and available for domain takedown. See Viewing the takedown credit summary on page 133.

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.

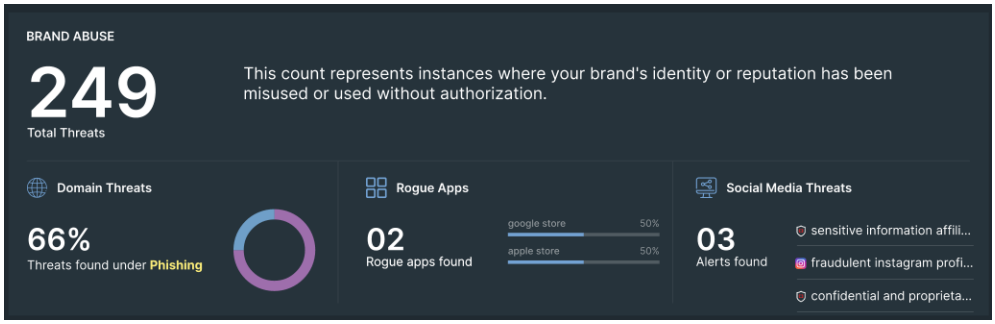
3. Hover over the threat type distribution bar to see the number of threats for each type.

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:

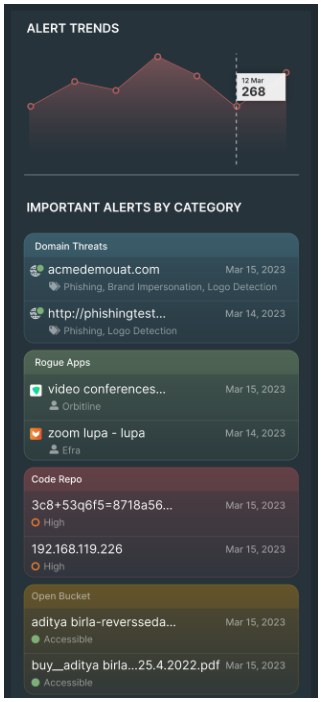
1. Go to *Brand Protection* > *Dashboard*.
2. Scroll to the *Information Exposure* widget. High level information about code and file exposure is displayed.

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.



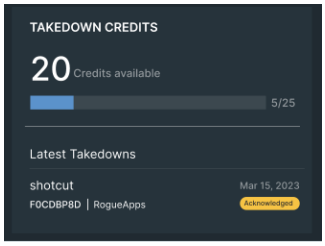
3. Hover over the graph for more information on daily alerts.

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 134.
- Take action against impersonating domains, such as requesting domain takedown. See Managing domain threats on page 135.
- Filter the list of domains. See Filtering domains on page 135.
- Create a digital watermark. See Digital watermark on page 136.
- Add a new domain or URL for monitoring or takedown. See Adding a new domain threat.
- Manage referrer logs. See Managing referrer logs.

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
- Other URLs

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.
   - To view the complete list of related URLs for a domain, click *Other URLs*.
   - To copy a domain to your clipboard, click the copy icon next to the domain name.

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 **Run Automation** in the *Actions* dropdown to run playbooks. See Security Orchestration.
5. 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. Select the original domain in the *By Original Domain* section.
8. Select the sources in the *By Source* section.
   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*.

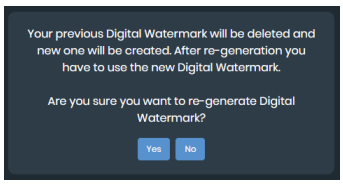
Editing watermarks

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.



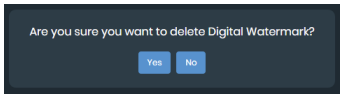
4. Click *Yes*.

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 threat

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 Domain Threats*.
3. Click *Add* icon.
4. Select the *Original Domain* from the dropdown.
5. Enter the *Domain* information.
6. Select the tags that you want to add to the domain threat.
7. Click *Select file* to browse and upload a screenshot of the domain threat. Single file uploads are supported. To upload additional files, click *Select files* next to *Add supporting documents (if any)*.

   Uploading a screenshot is mandatory to save the new domain threat.

8. Provide comments in the *Add comment* field, if any.
9. Click *Save*.

To add a new URL:

1. Go to *Brand Protection* > *Domain Threats*.
2. Click *Add Domain Threats*.
3. Click *Add* icon.
4. Select *URL* toggle.
5. Select the *Original Domain* from the dropdown.
6. Enter the *URL* information.
7. Select the tags that you want to add to the domain threat.
8. Click *Select file* to browse and upload a screenshot of the domain threat. Single file uploads are supported. To upload additional files, click *Select files* next to *Add supporting documents (if any)*.

   Uploading a screenshot is mandatory to save the new domain threat.

9. Provide comments in the *Add comment* field, if any.
10. Click *Save*.

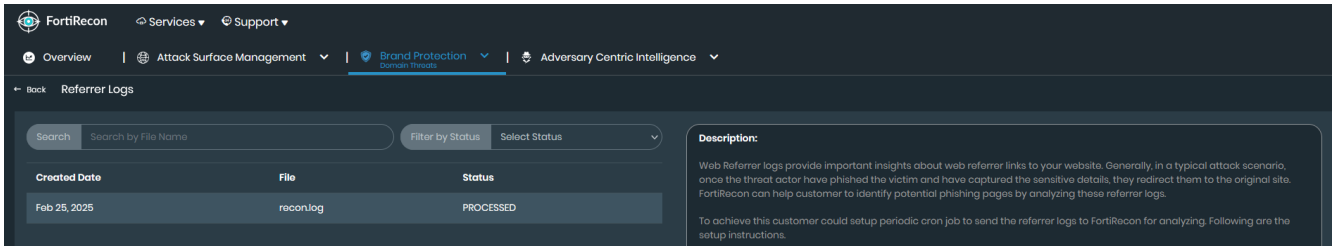
After you add a new domain or URL, the status field in the *Add Domains* page will indicate one of the following:

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

Managing referrer logs

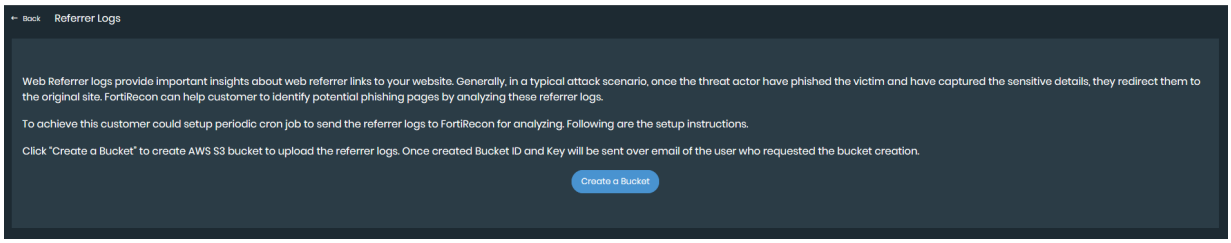
FortiRecon analyzes web referrer logs to identify potential phishing attacks. Web referrer logs provide valuable insights into the links that direct traffic to your website. In a typical phishing attack, threat actors redirect victims to the legitimate site after capturing sensitive information. By analyzing these logs, FortiRecon can detect suspicious referrer patterns indicative of phishing activity.

To enable this analysis, you must configure a periodic cron job to upload your web referrer logs to FortiRecon via Amazon Web Services Command Line Interface (AWS CLI).



Before uploading log files, ensure that AWS CLI is installed and configured on the server where the logs are stored. Perform the following steps to setup referrer logs.

1. *Create AWS Bucket*. You need to create a new S3 bucket once, for the initial setup.
   a. In FortiRecon, navigate to *Brand Protection* > *Domain Threats* > *Manage Referrer Logs*.
   b. Click *Create a Bucket*.
   c. Upon successful bucket creation, the necessary access information will be shared with you via email.



2. *Download and Install AWS CLI*. Install AWS CLI on your system using the appropriate commands for your operating system:
   - *Windows*: Download the installer from the AWS CLI Installation page.
   - *macOS*: Run the command `brew install awscli` in your terminal.
   - *Linux*: Run the following command in your terminal.
     - For Debian-based systems, run the command `sudo apt-get install awscli`.
     - For Red Hat-based systems, execute the command `sudo yum install aws-cli`.
3. *Configure AWS CLI*. After installing AWS CLI, configure it with your AWS access key and secret key shared via email.
   a. Open your terminal or command prompt.
   b. Run the command `aws configure`.
   c. Enter your credentials when prompted.
     - *AWS Access Key ID*: Enter your access key.
     - *AWS Secret Access Key*: Enter your secret key.
     - *Default region name*: Enter your preferred AWS region (e.g., us-east-1).
     - *Default output format*: Press Enter to accept the default (usually json).
4. *Upload Log Files*. Upload your log files to the designated S3 bucket using the following command.

   ```
   aws s3 cp /path/to/local/file s3://your-bucket-name/
   ```

   Replace /path/to/local/file with the actual path to your log file.

   Replace your-bucket-name with the name of your S3 bucket.

   Example: `aws s3 cp /home/user/documents/apache.log s3://cddf82s42-22sced-e6nws4c436-referal-logs-testing/Co531lMJyOQXBJI9741ifVwgNPSGaNCJ1F0qqGlUNECTHbfMHiBvbg5tnsoJRAw3/`

- Only valid log files in **.log** or **.zip** format will be processed.
- Uploaded files are processed within a few hours.
- Files are automatically deleted after 7 days.
- FortiRecon currently supports **Apache** and **Nginx** web server logs. If you use a different web server, open a support ticket to request support.

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 **X (formerly known as 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 140.
- Take action against impersonating profiles, such as requesting profile takedown. See Managing social media threats on page 141.
- Filter the list of profiles. See Filtering social media threats on page 141.
- Add official social media profiles. See Adding official profiles on page 142.
- Add a new social media profile for monitoring. See Adding a new social media threat.
- Export information on discovered profiles. See Exporting impersonating profiles.
- View archived alerts. See Alerts.

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:

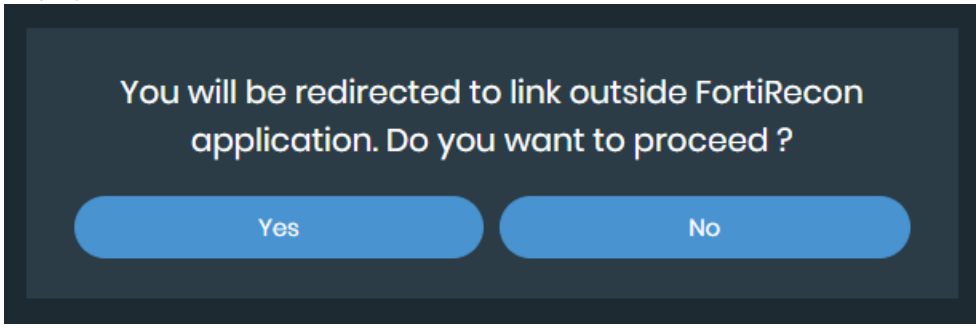
- Profile name
- Handle name
- Location
- Friends count
- Followers count
- Posts count

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 **Run Automation** in the *Actions* dropdown to run playbooks. See Security Orchestration.
5. 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.

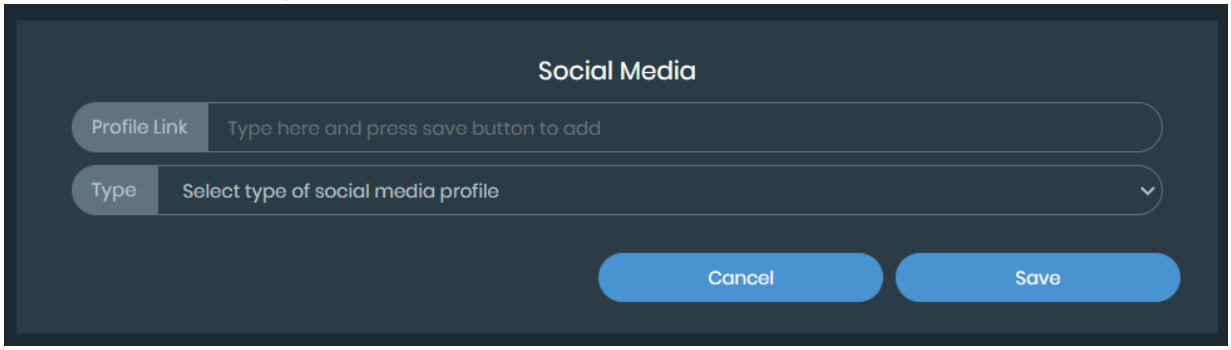
   c. Select a month, year, and day to specify the end date of the range.
   Only threats from the date range are displayed.
   d. Click the *Filter By Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, 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 Actions* 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.

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.

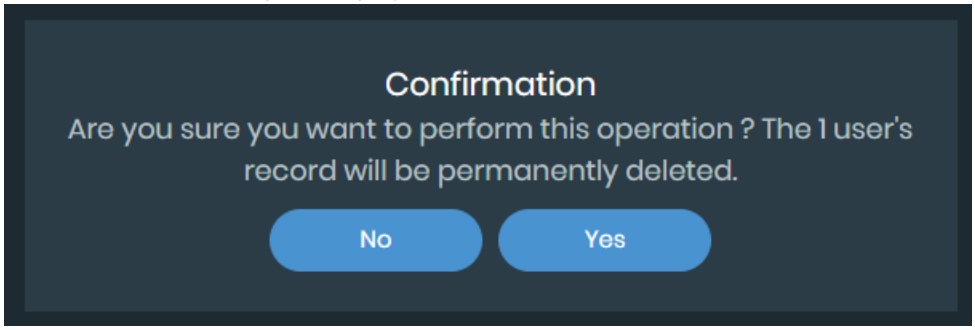


5. You can also add official social media profiles in bulk by uploading excel (XLS) file containing profile information including profile URL and type.
   a. Click Upload XLS icon.
   b. Browse and select the file. Click *Open*.
   Note: Ensure that the format in which the profiles data is stored matches 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 threat

You can add social media profiles for monitoring.

To add a new social media threat:

1. Go to *Brand Protection* > *Social Media Threats*.
2. Click *Add Social Media Threat*.
3. Click *Add* icon.
4. Select the *Type* of social media from the dropdown.
5. Enter the profile URL in *Link* field.
6. Enter the *Profile Name*.
7. Enter the *Handle Name*.
8. Click *Select file* to browse and upload a screenshot of the social media threat. Single file uploads are supported. To upload additional files, click *Select files* next to *Add supporting documents (if any)*.

   Uploading a screenshot is mandatory to save the new social media threat.

9. Provide comments in the *Add comment* field, if any.
10. 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.
- **Approved**: The profile has been validated and approved.
- **Rejected**: The profile was deemed invalid. A comment will explain the reason for rejection.

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:

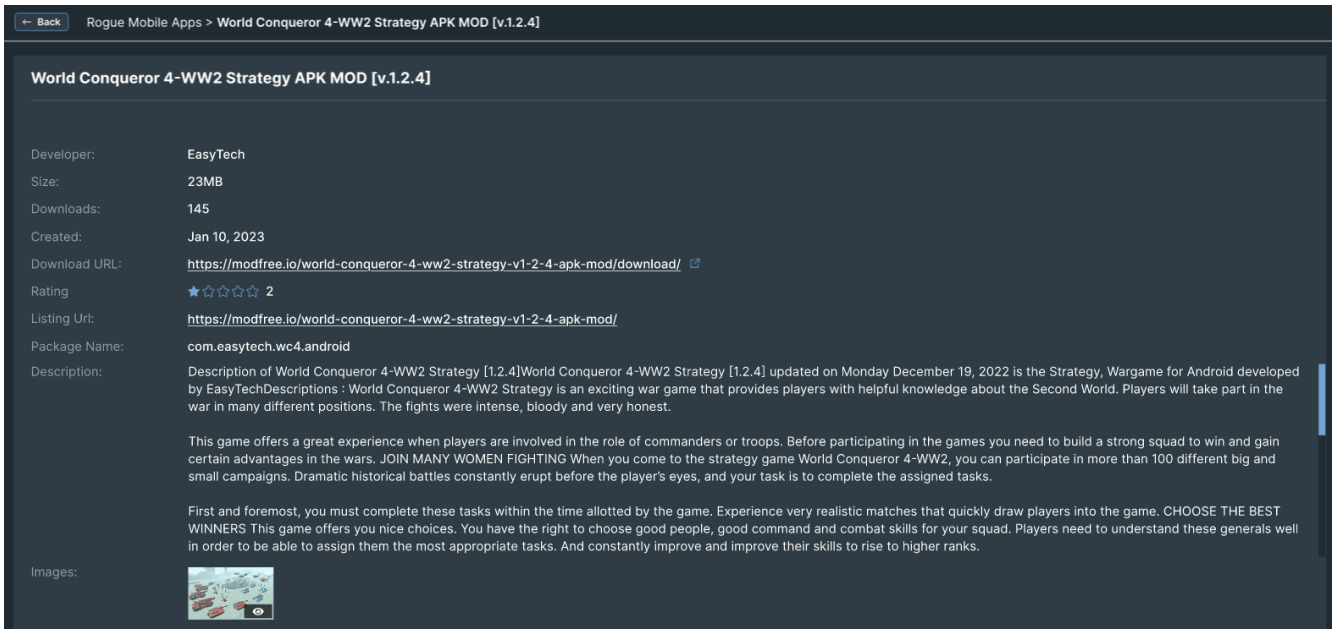
- View information on monitored applications. See Reviewing rogue applications on page 144.
- Filter for specific mobile applications. See Filtering rogue applications on page 145.
- Add official applications. See Adding official applications on page 146.
- Assign an app status. See Assigning application status on page 147.
- Initiate takedown of a rogue application. See Taking down rogue apps on page 147.
- Export information on applications. See Exporting rogue applications on page 148.

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 145.
4. Select the application you want to review. The app information is displayed in a new tab.
5. Click **Run Automation** in the *Actions* dropdown to run playbooks. See Security Orchestration.



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:

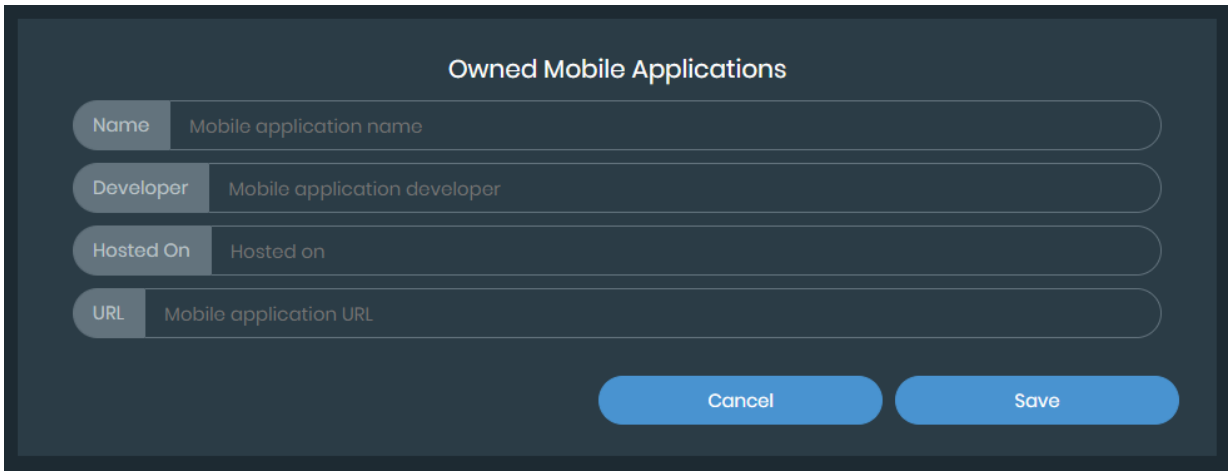
1. Go to *Brand Protection* > *Rogue Mobile Apps*.
2. Filter reports by a date range:
   a. Click *Filter By Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and 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 *Actions*, either *Unofficial*, *Takedown*, or *Rogue*.
5. Select the *App Stores*.
   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



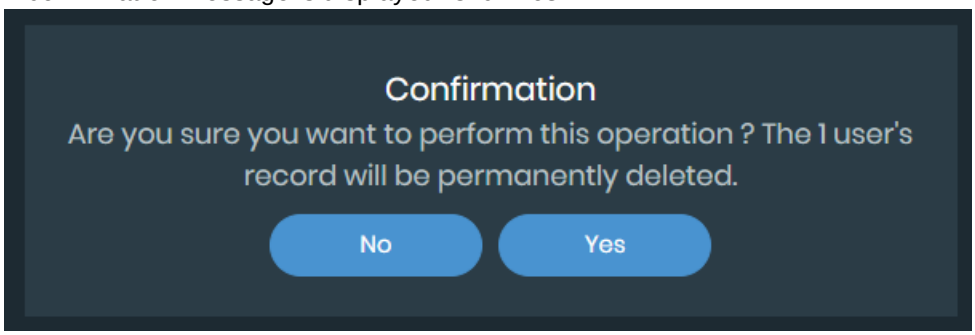
5. You can also add official applications in bulk by uploading excel (XLS) file containing application information including application name, mobile app developer, hosted on and app URL.
   a. Click Upload XLS icon.
   b. Browse and select the file. Click *Open*.

   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*.



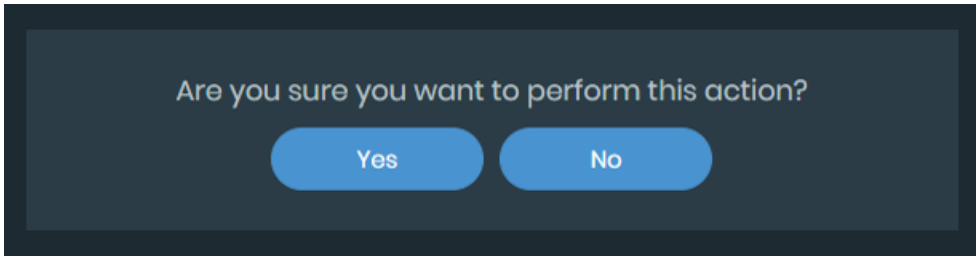
Assigning application status

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.



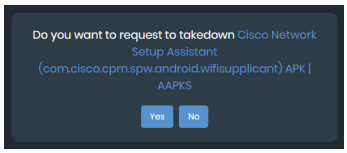
3. Click *Yes*.

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 147.
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.

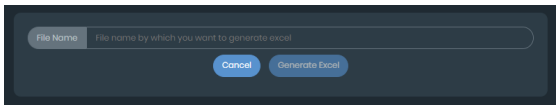
Exporting rogue applications

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

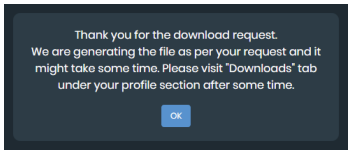
- App name and size
- Description
- Developer name and URL
- Download count and URL
- Date the app was discovered
- Listing URL
- Package name
- Source name
- Status

To export rogue application details:

1. Go to *Brand Protection* > *Rogue Mobile Apps*.
2. Set the desired filters. See Filtering rogue applications on page 145
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.

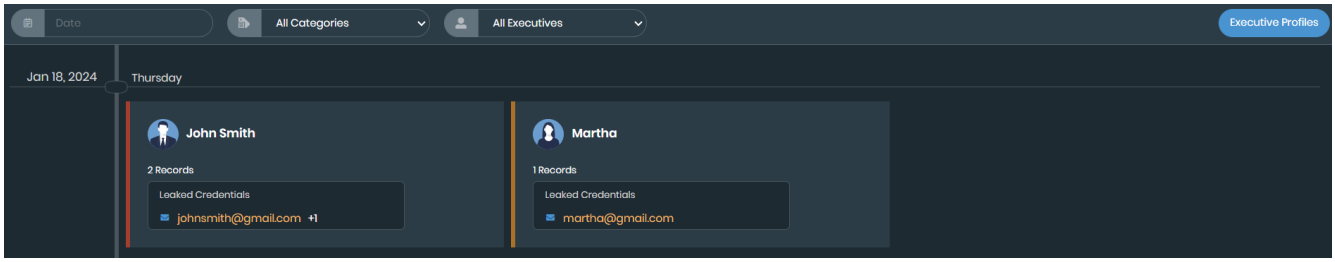
Executive Monitoring

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 149.
- Filter the list of executive profile threats. See Filtering executive profile threats on page 150.
- Add official executive profiles. See Adding executive profiles on page 150.

> 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 posed to the executive's security or reputation on social media platforms (*LinkedIn,*

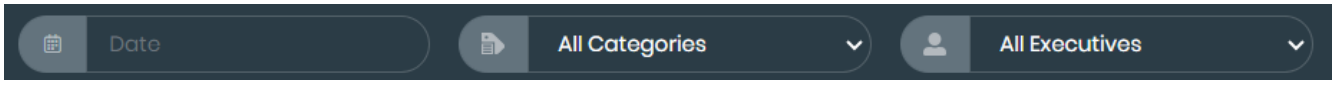
Threat Category	Description
Threats	*Facebook, Instagram* and *Twitter*).
Stealer Infections	Indications of malware or malicious software infecting the executive's devices with the intent of stealing sensitive information.
Leaked Documents	Instances where documents or files associated with the executive 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:

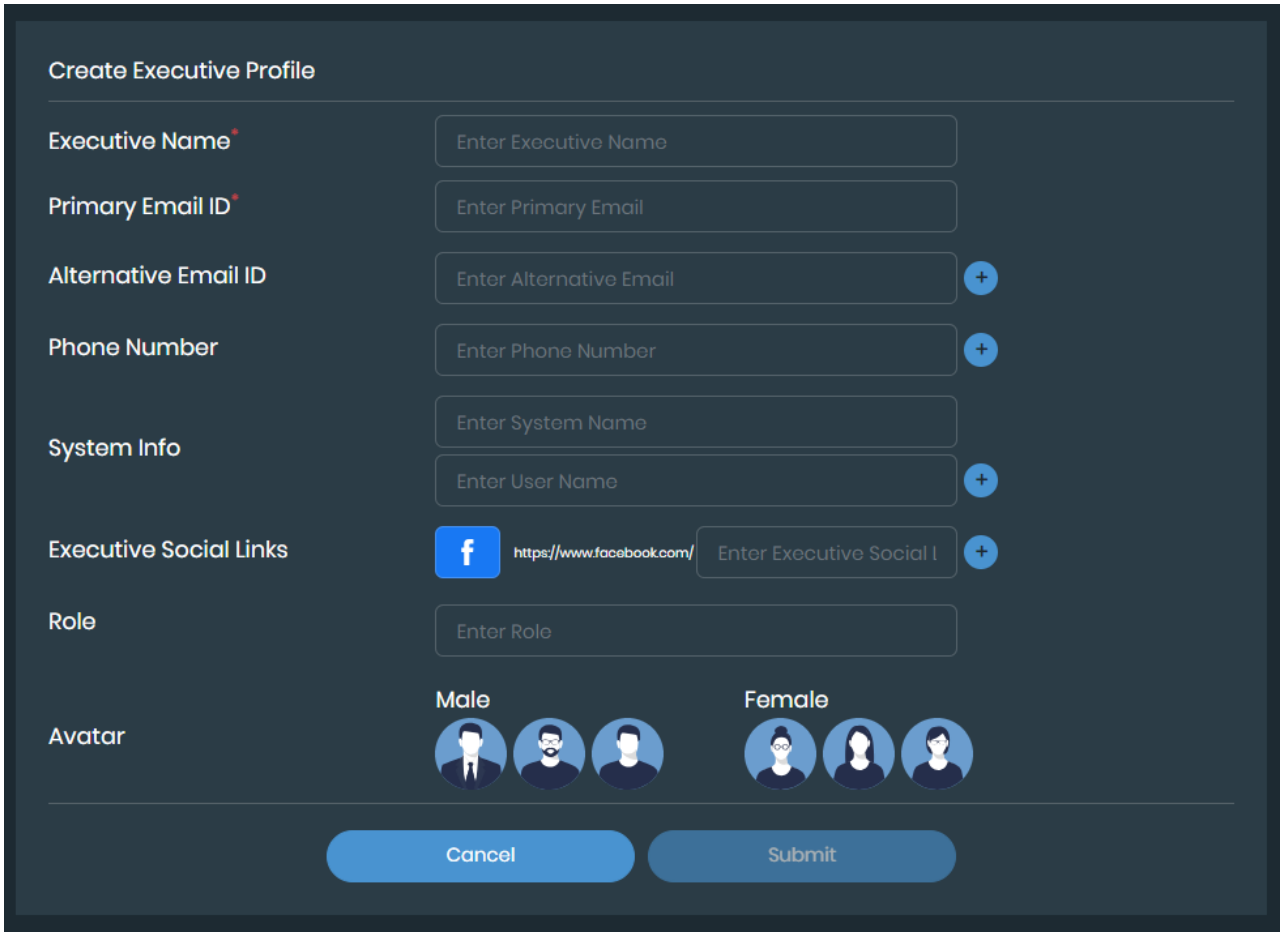
1. Go to *Brand Protection* > *Executive Monitoring*
2. Filter threats by a date range:
   a. Click *Date* . Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. Select a month, year, and day to specify the end date of the 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*.

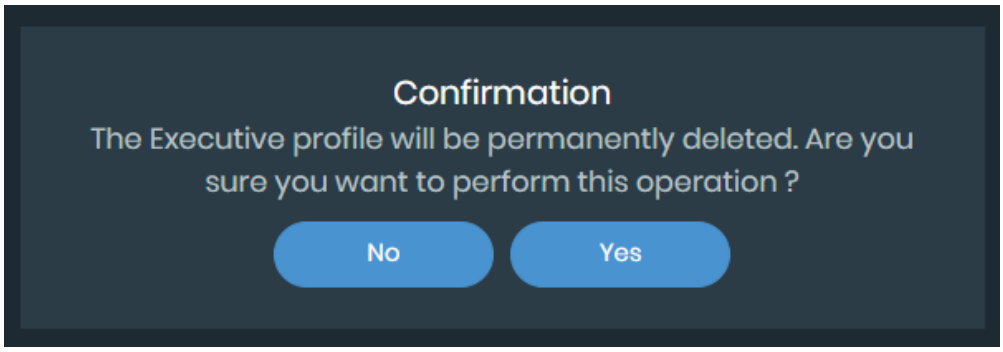


To edit a executive profile:

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 154.
- Take action against the discovered attributes. See Managing attributes on page 155.
- Filter attributes. See Filtering attributes on page 155.

Managing keywords

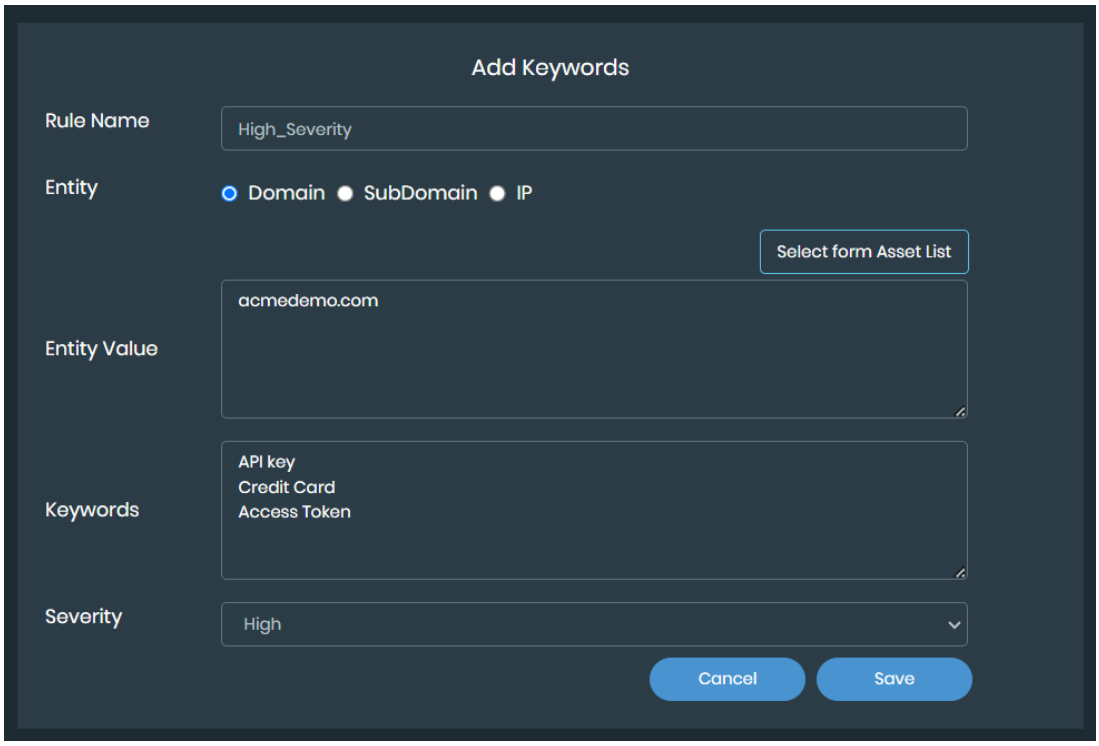
You can add a custom rule to match keywords against the discovered domains, sub domains and IPs.

To add a keyword rule:

1. Go to *Brand Protection* > *Code Repo Exposure*.
2. Click *Keyword Watchlist*.

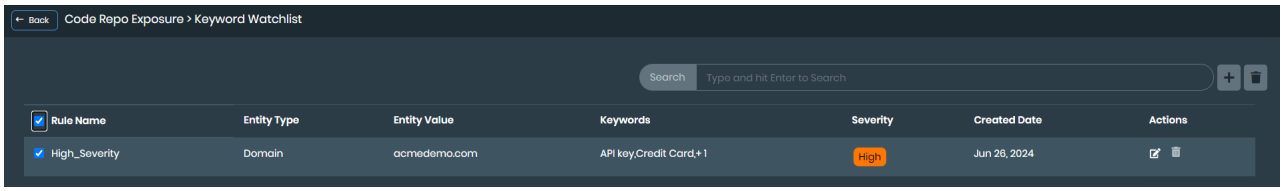
3. Click **+** icon.
4. In the *Add Keywords* pop-up, enter the following information and click *Add*.
   a. *Rule Name*: Enter a name for the rule.
   b. *Entity*: Select the type of entity.
   c. *Entity Value*: Based on the entity type selected, you can either enter entity values or select the required 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.

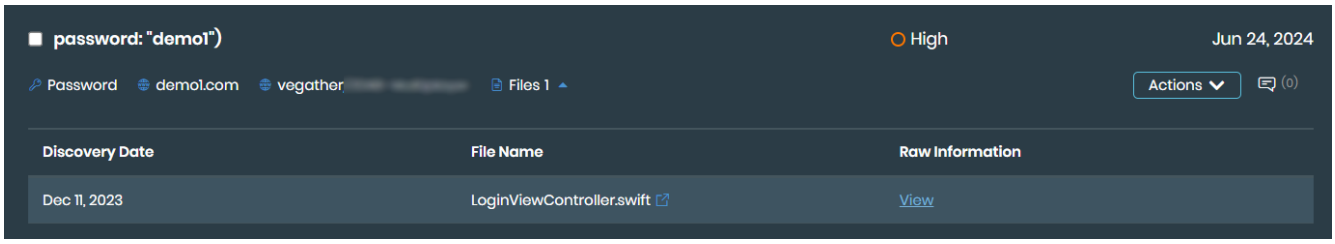
Reviewing attributes

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 **Run Automation** in the *Actions* dropdown to run playbooks. See Security Orchestration.
5. 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 Actions* 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.

   The attributes with the matching filters are displayed.

Open Bucket Exposure

The *Open Bucket Exposure* page provides details of files and data potentially exposed to the public internet through misconfigured cloud storage containers. FortiRecon currently monitors and reports open bucket exposures for the following public cloud platforms:

- *Amazon Web Services (AWS)*
- *Google Cloud Platform (GCP)*
- *Microsoft Azure*

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

- Review files exposed on open buckets. See Reviewing files on page 156.
- Take action against discovered files. See Managing files on page 157.
- Filter files. See Filtering files on page 157.

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 **Run Automation** in the *Actions* dropdown to run playbooks. See Security Orchestration.
5. 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 Actions* 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 File Type* section.
   The files with the matching filters are displayed.

Takedown

FortiRecon's takedown service is an on-demand solution designed to mitigate threats to your brand. This service actively takes down entities that impersonate your brand, including phishing websites, fraudulent social media accounts, and unauthorized mobile applications.

The FortiRecon team employs various avenues to initiate a takedown. We contact the following parties, as applicable, and leverage local and international copyright, trademark infringement, and intellectual property laws to facilitate takedowns:

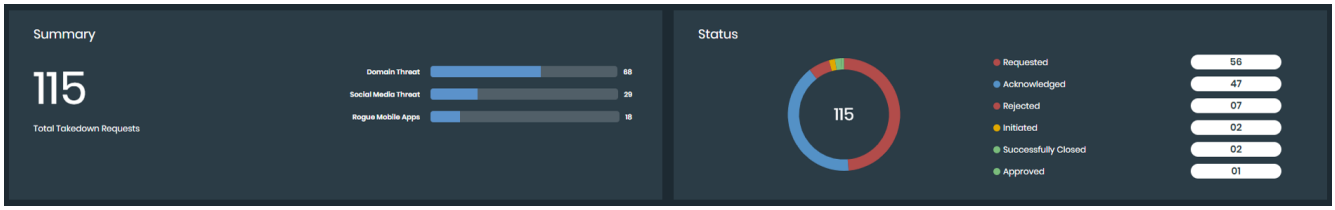
- Offending parties
- Hosting providers
- Reverse-Proxy Providers
- Blocklists
- Social Media Platforms
- App Stores
- Domain Registrars
- Government Authorities

The FortiRecon team validates each takedown request. If the entity requested for takedown does not genuinely impersonate or phish against the brand, FortiRecon rejects the request. Content that is critical of a brand but does not involve impersonation, such as website or social media commentary, does not qualify for takedown. Similarly, generic applications not presented as official publications are not considered valid candidates for takedown.

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.

FortiRecon team strives to action takedowns as quickly as possible. However, successful takedowns depend on the response and action from the relevant parties.

- For domain threats and rouge apps, the team will continuously follow up with relevant parties for 7 working days. If there is no response or action, the takedown request will be closed as unsuccessful, and takedown credits will be reversed.
- For social media takedowns, the team will continuously follow up with social media platforms for 15 working days. If there is no response or action, the takedown request will be closed as unsuccessful, and takedown credits will be reversed.
- If relevant parties raise a concern or request additional information from FortiRecon, the takedown timeline extends.



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

- Create and manage Authority Letters. See Authority Letters.
- Initiate takedown requests for impersonating profiles or groups found on instant messaging platforms, including *WhatsApp* and *Telegram*. See Initiating Takedowns for IMs.
- View the current status of the takedown requests and provide additional information if required. See Reviewing takedown requests.
- Filter for specific takedown requests by date, category, status, and ticket number. See Filtering takedown requests on page 165.
- Revoke active takedown requests that meet specific status criteria. See Revoking Takedown Requests.

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

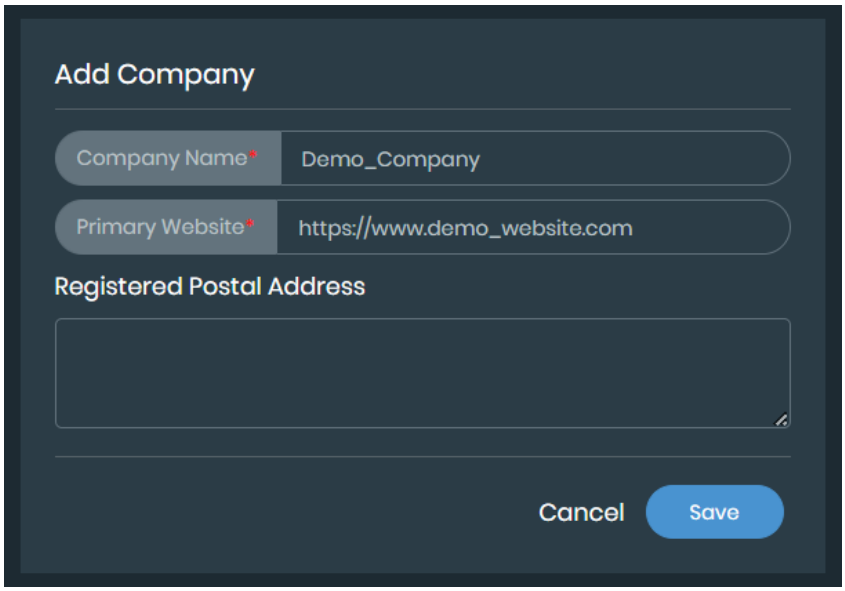
Creating Authoring Letters

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.

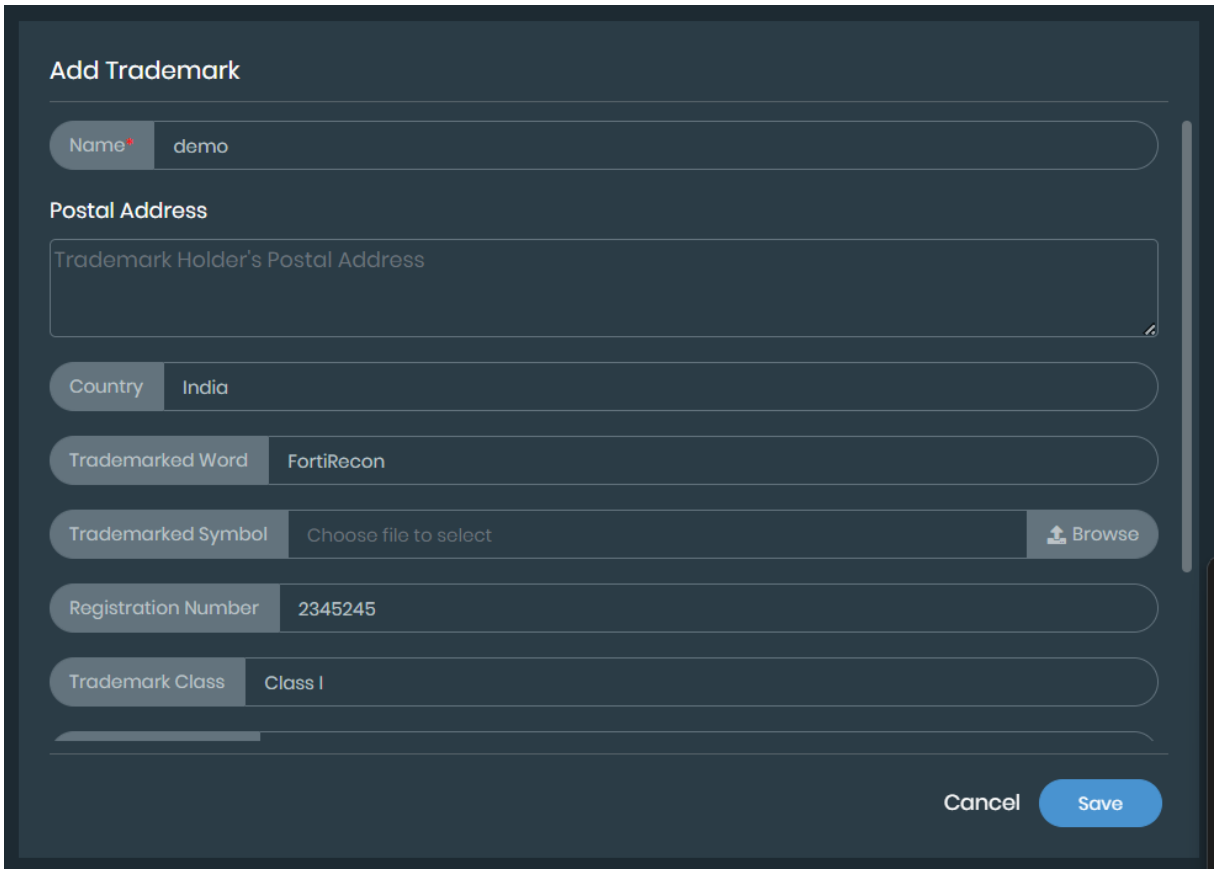
1. Navigate to *Brand Protection* > *Take Down*.
2. Click *Authority Letters*.
3. In the *Authority Letters* page, click + *Add*.

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.

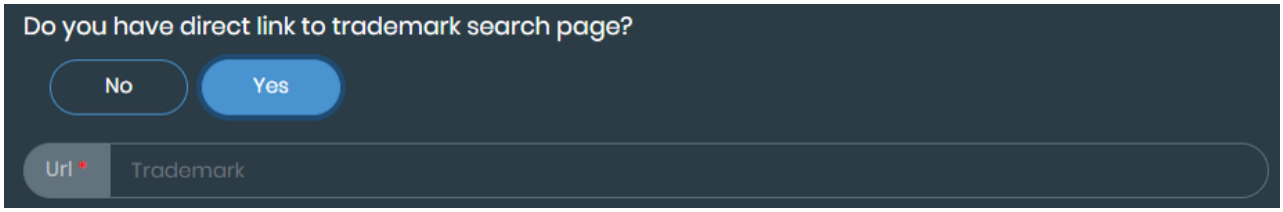
5. In the *Company Details Overview* page, click + *Add Company* to add a new company and enter the following details. .
   - Company Name
   - Primary Website
   - (Optional) Registered Postal Address



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*.

> If you do not have actively registered trademarks, you can skip the Trademark Portfolio Management page. However, be aware that the absence of actively registered trademarks may affect FortiRecon's ability to initiate takedowns.

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.

Initiating Takedowns for IMs

The *Brand Protection*> *Takedown* page allows you to initiate takedown requests for impersonating profiles and groups on instant messaging (IM) platforms including *WhatsApp* and *Telegram*.

Perform the following steps to initiate a new takedown for an instant messaging profile or group.

1. Navigate to *Brand Protection* > *Takedown*.
2. Click *Initiate Takedown for IM*.
3. Select *WhatsApp* or *Telegram*.
4. Enter the profile or group URL in the URL field. Ensure that the URL uses one of the supported formats.
5. Click *Save*.

Supported URLs

When you initiate a takedown, you must use a supported URL format for the profile or group you want to report. The system only processes requests that use the following URL structures

- **WhatsApp**
  - https://wa.me/
  - https://api.whatsapp.com/
  - https://chat.whatsapp.com/
  - https://www.whatsapp.com/
- **Telegram**

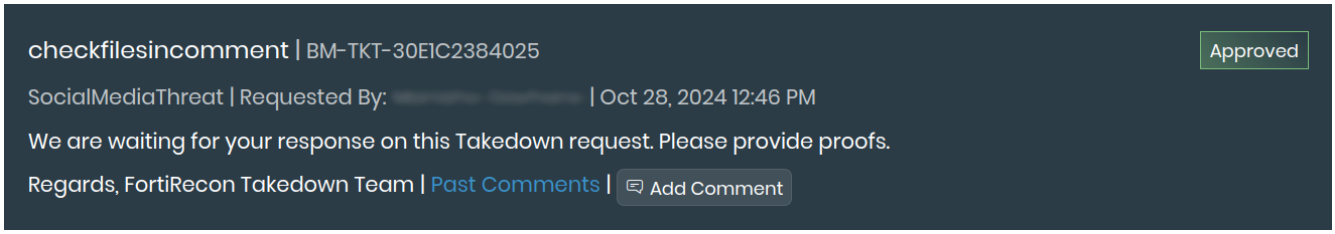
- https://t.me/

Reviewing takedown requests

You can review information about takedown requests in the *Brand Protection* > *Takedowns* page. Each request includes the following information.

- Entity to be taken down
- Takedown Ticket ID
- Entity Type
- Requested By
- Request Date
- Latest Comment
- Current Status

Click *Past Comments* to view all previous comments. Click *Add Comments* (if available) to add comments and upload supporting documents when requested by the FortiRecon team.



Understanding Takedown Request Statuses

You can track a takedown's lifecycle by observing its status. The following stages define a takedown's lifecycle:

1. *Requested*: Indicates you requested the takedown, and it is awaiting initial action.
2. *Acknowledged*: Indicates FortiRecon received the takedown request and is analyzing if the entity is a valid takedown candidate.
3. *Rejected*: Indicates FortiRecon rejected the takedown request because the entity is not a valid candidate. FortiRecon does not use takedown credits for rejected requests.
4. *Awaiting Customer Response*: Indicates FortiRecon requires additional information from you to determine if the entity is a valid takedown candidate.
5. *Approved*: Indicates FortiRecon approved the takedown request because the entity is a valid candidate. FortiRecon uses a takedown credit at this stage.
6. *Cancelled*: Indicates that the takedown request was canceled before FortiRecon took action.
7. *Initiated*: Indicates FortiRecon has begun efforts to complete the requested takedown.
8. *Revoked*: Indicates that the takedown was stopped after FortiRecon had already taken action; credits will not be reverted in this instance.
9. *Successfully Closed*: Indicates FortiRecon successfully took down the entity.
10. *Unsuccessfully Closed*: Indicates FortiRecon could not take down the entity within the stipulated time. FortiRecon returns the takedown credit used during approval at this stage. You can request another takedown in these cases.

11. *Delayed Success*: Indicates FortiRecon took down the entity after the stipulated time. FortiRecon does not deduct a takedown credit at this stage.

- If you mistakenly request and then revoke a takedown after FortiRecon has already initiated it, FortiRecon can only stop any further efforts to complete the takedown. Actions already taken cannot be reversed. This means previous efforts by FortiRecon may still lead to a takedown, even if you cancel the request. In such situations, FortiRecon cannot reverse the effects of the takedown; the responsibility for reversal falls on the party who requested the takedown.
- If FortiRecon successfully closes a takedown and the threat actor rehosts the entity, you must submit a new takedown request for this rehosted entity.

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*, *Successfully Closed*, or *Unsuccessfully Closed* to filter takedown requests by their assigned status.
5. Filet by category in the By Category section:
   - Select *Domain Threat*, *Social Media Threat*, *IM*, *Log Purchase*, or *Rogue Mobile Apps* to filter takedown request by threat category.

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

Revoking Takedown Requests

You can revoke a takedown request directly from the *Brand Protection* > *Takedown* page, provided the request has not yet reached a final processing status. Revoking a request cancels the process and prevents further action.

The Revoke button is only visible for requests in the following statuses:

- *Requested*
- *Acknowledged*
- *Approved*
- *Awaiting response*
- *Initiated*

Perform the following steps to revoke an eligible takedown request.

1. Navigate to *Brand Protection* > *Takedown*.
2. Locate the request you want to cancel and click *Revoke*.
3. Confirm that you want to cancel the request.

Revocation Outcomes

After you revoke a request, the final status and credit refund depend on the request's prior status. If the request was in *Requested*, *Acknowledged*, *Approved*, or *Awaiting response* status, the system marks the request as *Cancele*d, and you receive a credit refund. If the request was already in the *Initiated* status, the system marks it as *Revoked*, and no credit refund is provided.

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 167.
Reports	Displays the threat intelligence analyst reports and FortiAI Insights available to you. See Reports on page 171.
Card Fraud	Displays information about credit or debit cards that are for sale on darknet marketplaces. See Card Fraud on page 176.
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 179.
OSINT - Cyber Threats	Displays OSINT-based intelligence reports about threat events. See OSINT Cyber Threats on page 185.
Vulnerability Intelligence	Displays information on monitored CVEs. See Vulnerability Intelligence on page 189.
Ransomware Intelligence	Displays information on total and potential ransomware incidents. See Ransomware Intelligence on page 196.
Vendor Risk Assessment	Displays information on a vendor watchlist and the vendor's security hygiene. See Vendor Risk Assessment on page 207.
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 218.

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 168.
- View your organization's risk exposure. See Viewing risk exposure summary on page 168.

- View global threat reports. See Viewing global threat report summary on page 170.

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	Displays statistics related to credit or debit cards that are listed for sale on darknet marketplaces.

This widget is only displayed for banking organizations that issue credit or debit cards.	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

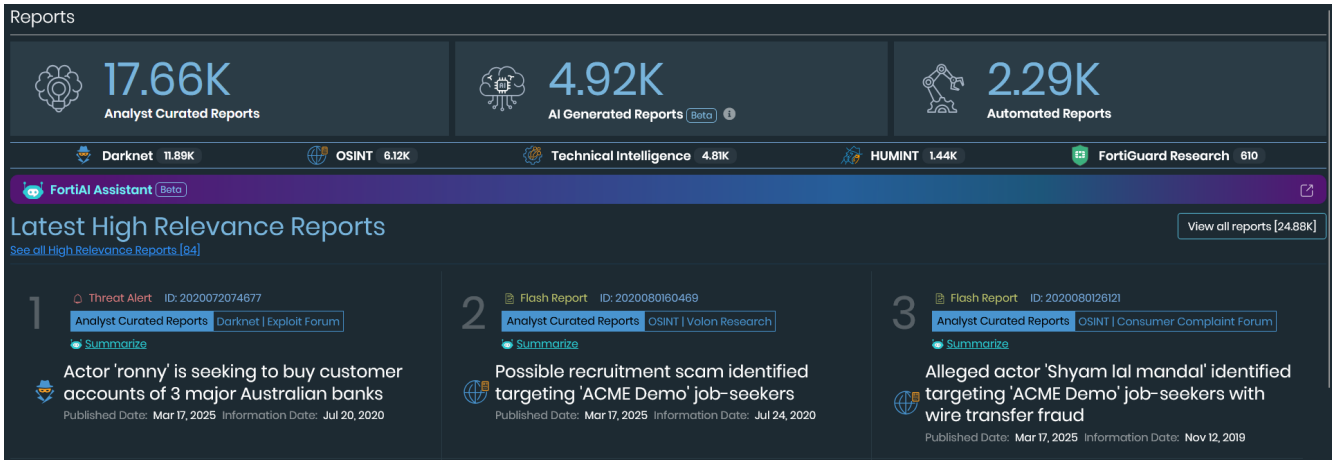
The *Adversary Centric Intelligence* > *Reports* page provides a centralized location to access and analyze various threat intelligence reports. These reports, categorized as Curated Analyst, FortiAI Insights, and Automated, offer valuable insights into emerging threats and trends. *Analyst Curated Reports* are reports by our expert threat analysts, while *Automated Reports* are sourced from external feeds. *FortiAI Insights*, powered by Fortinet's AI technology, provide advanced threat intelligence and analysis capabilities.

Additionally, the integrated *FortiAI Assistant* enables you to ask questions about cybersecurity trends and get AI-powered summaries of reports.

From the *Adversary Centric Intelligence* > *Reports* page, you can:

- Use FortiAI Assistant to query cybersecurity trends and insights, and to summarize reports. See Using FortiAI Assistant
- View the details of each report. See Viewing reports on page 173.
- Apply filters to the list of reports to hone in on specific reports. See Filtering reports on page 175.

- Share reports. See Sharing reports on page 176.



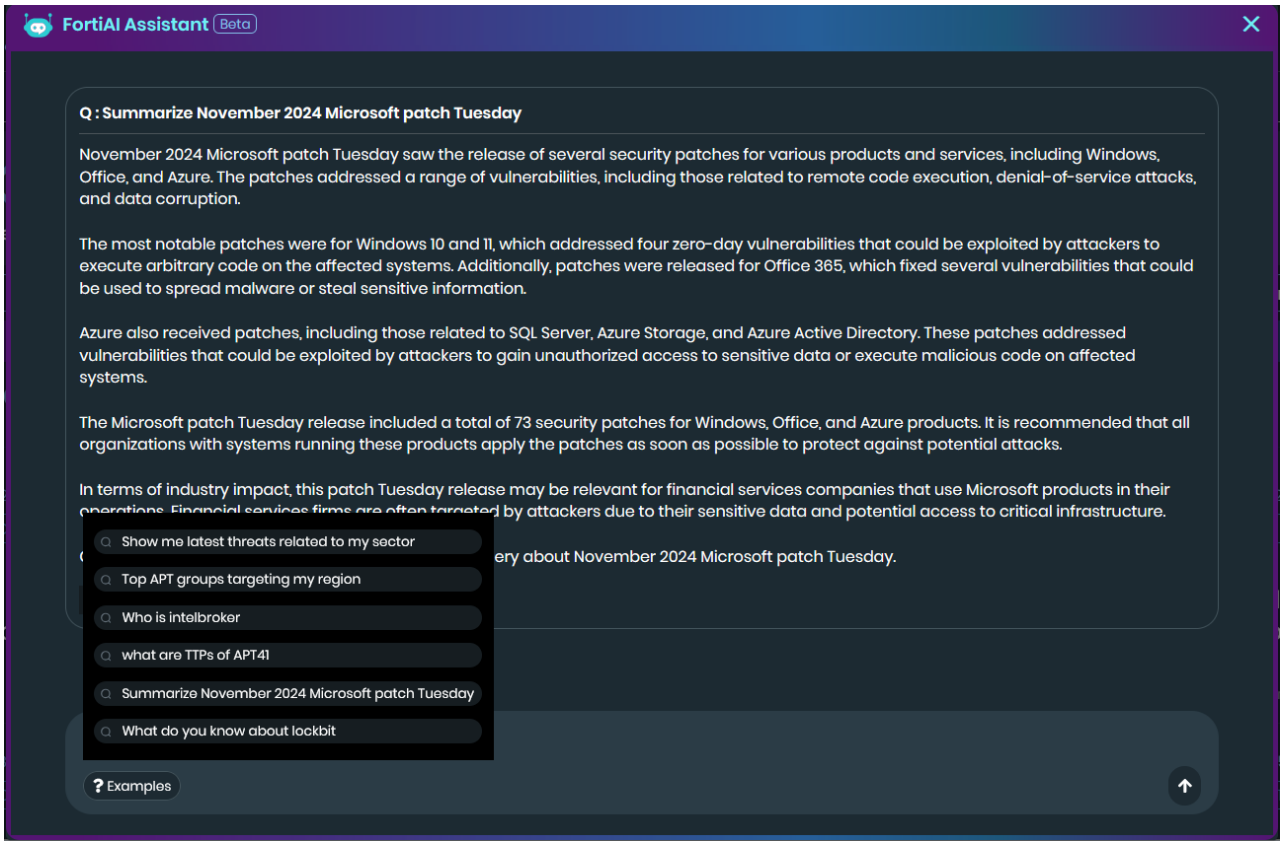
Using FortiAI Assistant

FortiAI Assistant is an Artificial Intelligence(AI) powered tool that provides valuable insights into cybersecurity trends and threats. It can also summarize complex reports, making key information more easily understandable.

FortiAI Assistant analyzes reports published within the last year (or a custom date range) and provides a concise summary. You can interact with the assistant by submitting custom queries. The assistant processes these queries and presents a summarized response. Due to the dynamic nature of AI-generated content, the structure of these responses may vary. To get started, several pre-built sample queries are provided. You can also view the cited reports used to generate each summary for deeper analysis.

To use FortiAI Assistant:

1. Go to *Adversary Centric Intelligence* > *Reports* .
2. In the *FortiAI Assistant* text box, type your query. Following are examples of queries.
   - *AI-driven phishing attack trends in the financial sector 2024*
   - *AI applications in detecting supply chain cyber threats across industries 2024*
   - *Impact of machine learning on email fraud prevention in the banking sector 2024*
   - *AI advancements in cybersecurity for protecting financial institutions from phishing*



3. *Additionally, you can leverage FortiAI Assistant to summarize reports:*
   - *Click Summarize on High Relevance reports to view the summary.*
   - *The report page contains the FortiAI Summary in the Full Report section.*

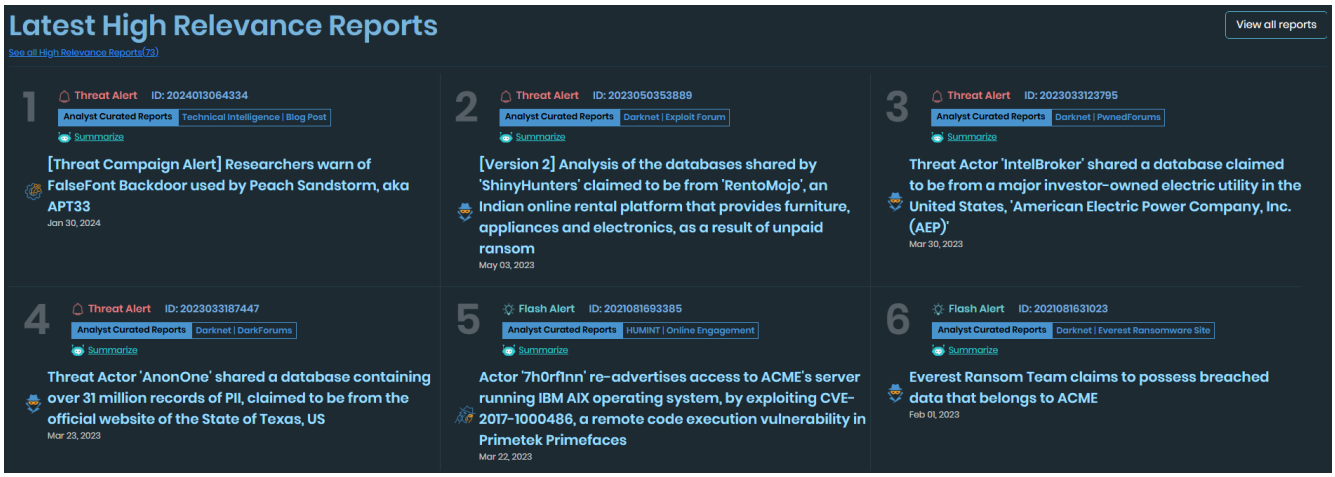
Viewing reports

The *Adversary Centric Intelligence* > *Reports* page displays a list of threat intelligence reports. By default, the top six high-relevance reports are shown.

You can filter the list of reports, and search the list of reports using a keyword. See Filtering reports on page 175.

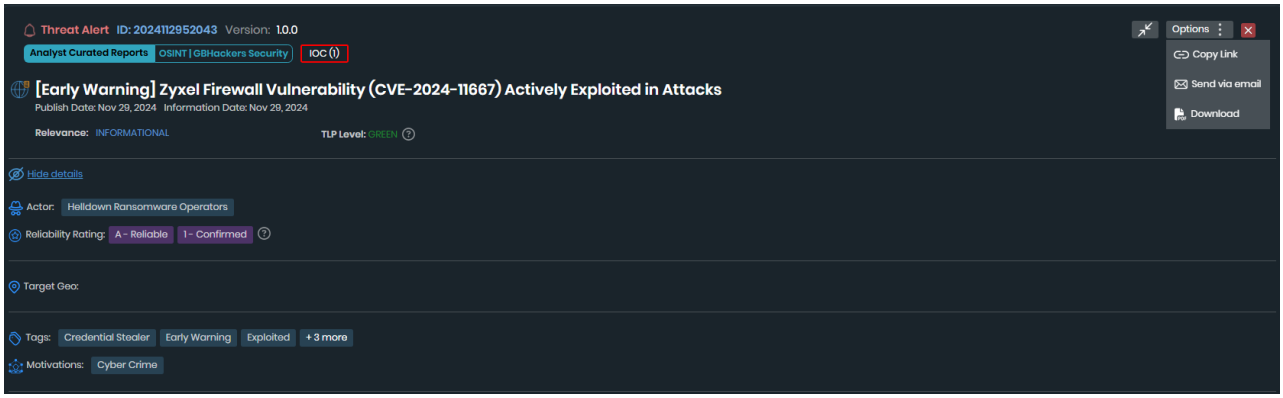
To view high relevance reports:

1. Go to *Adversary Centric Intelligence* > *Reports* .
2. The top six high-relevance reports are displayed, if available.
3. Click a report title to view its details in the right pane.
4. Click *See all High Relevance Reports*. All high-relevance reports will be displayed.



To view all reports:

1. Go to *Adversary Centric Intelligence* > *Reports.*
2. Click *View All Reports*. All available reports will be displayed.
3. Click a report title to display the report details in right pane.
   Once you open a report, its details are displayed in the right pane. From here, you can:
   - Click the help icon next to the *TLP Level* to view definitions of the different TLPs and rules around sharing the information.
   - Click the help icon next to the *Reliability Rating* to view how ratings are assigned.
   - Click the *Options* menu and select *Download* to download a PDF of the report.
   - Click the *Options* menu and select *Copy Link* to copy a link to the report. You can then share this link with another user who has a FortiRecon account. Alternatively, you can select *Send via Email* to share the link directly via email.



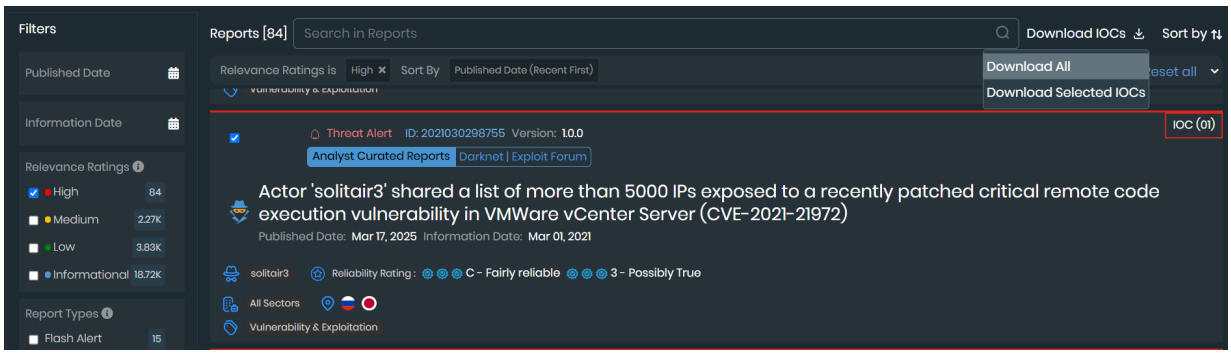
The following information is displayed for each report.

- *Full Report*: The detailed report, including a FortiAI summary.
- *Data Attributes*: Identified data attributes, such as CVEs and URLs.
- *Observables*: A list of indicators of compromise (IOCs). Click **Download** to download the IOCs in Microsoft Excel format.
- *Victims*: Details about the entities that the threat actors targeted in the report.

When the report includes indicators of compromise (IOCs), you can download the IOCs in Microsoft Excel format.

To bulk download IOCs:

a. Select the reports containing the IOCs you want to download.
b. Locate the **Download IOCs** button, which appears next to the search bar.
c. Click the **Download IOCs** button.
   - If the total number of IOCs from your selected reports is less than 200, a menu appears. Choose either **Download All** to get all IOCs from the selected reports or **Download Selected IOCs** if you've specifically chosen individual IOCs within those reports. The file will download directly to your computer.
   - If the total number of IOCs is greater than 10,000, FortiRecon initiates the download process in the background. You can monitor the progress and download the completed file from the **Profile Settings > Downloads** page.



Filtering 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*.
2. Filter reports by a date range:
   a. Click *Published Date* or *Information Date*.
   b. Select quick filters or click *Custom range*.
   c. In the left calendar, select a month, year, and day to specify the start date of the range.
   d. 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.
   e. Click *X* to remove the date range filter.
3. Filter using quick filters. Click the *Analyst Curated Reports*, *Automated Reports*, or *AI Insight* widget to filter the data. You can combine multiple filters. Additionally, you can quickly filter the data using category filters.
4. 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.
5. In *Filters* section on the left pane, select one or more filters. The following filters are available:

- *Relevance Ratings*
- *Report Origin*
- *Report Types*
- *Categories*
- *Source Reliability*
- *Information Reliability*
- *Industries*
- *Geographies*
- *Threat Types*
- *Threat Actors*
- *Motivation*
- *Tags*

6. To clear all the selected filters click *Reset all*.
7. Under *Report Type* > *Relevance*, click *High*, *Medium*, and/or *Low* to enable the filters, and clear the filters to disable them.

Sharing reports

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

To share a report:

1. Go to *Adversary Centric Intelligence* > *Reports*.
2. Click a report to display its details.
3. **a.** Click *Options* and select how you would like to share the link:
   - **i.** 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.
   - **ii.** Click *Send via Email* to email the link.
     Your personal email opens with a draft that includes the report link.

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 177.

- Filter the information. See Filtering leaked card information on page 177.
- Download the list of leaked cards to Microsoft Excel format. See Exporting a list of leaked cards on page 178.

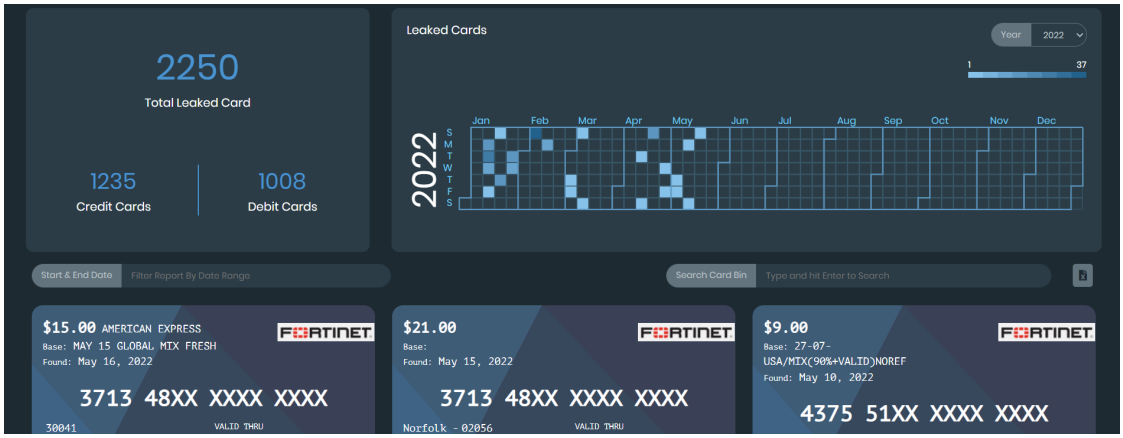
Viewing leaked card information

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.



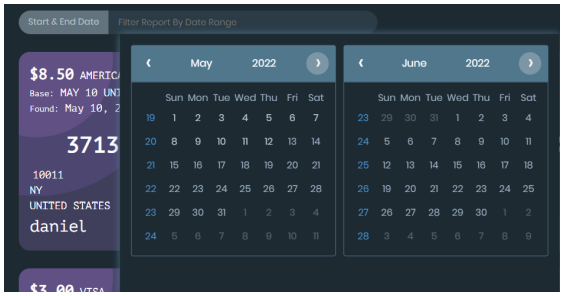
2. You can filter the displayed information. See Filtering leaked card information on page 177.

Filtering leaked card information

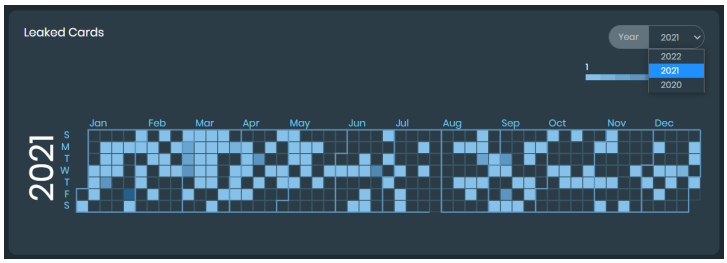
You can filter information about leaked cards by year, date range, and bank identification number (BIN).

To filter leaked card information:

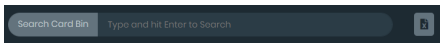
1. Go to *Adversary Centric Intelligence* > *Card Fraud*.
2. Filter reports by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.



   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*.

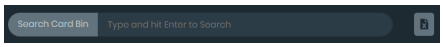


Exporting a list of leaked cards

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 181.
- Export market place data. See Exporting stealer infections data on page 184.

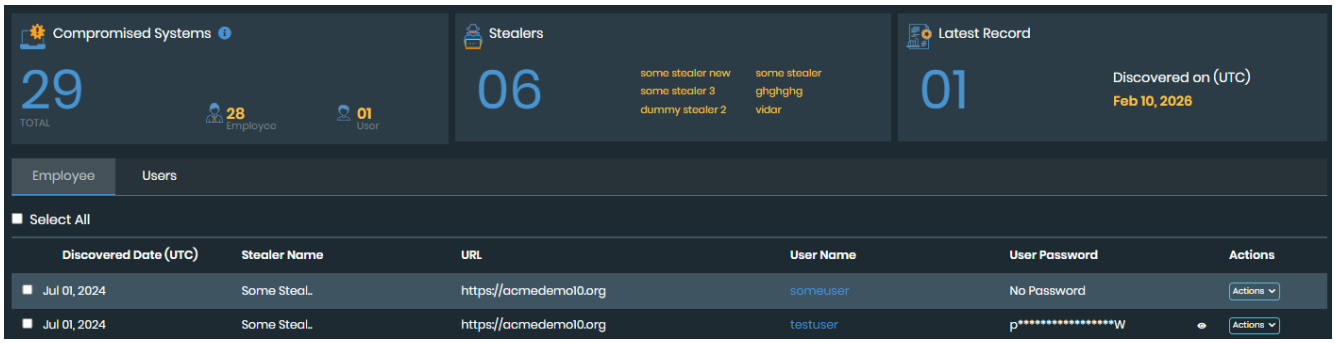
Viewing leaked compromised systems

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.



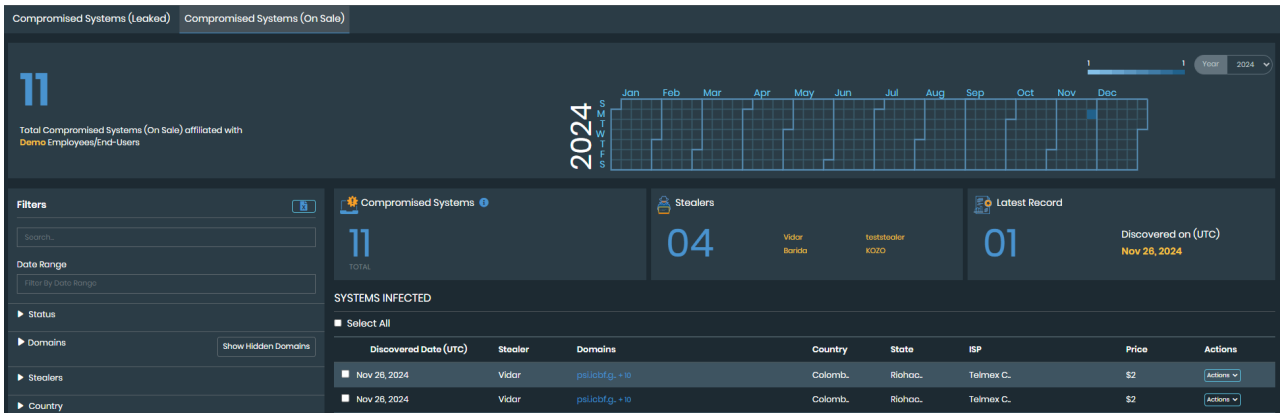
- The values in all widgets are updated based on the filters applied, except for *Total Compromised Systems(Leaked) affiliated with <organization name>* value.
- Only an administrator can view leaked passwords. Click the view icon to reveal the masked password.
- Click *Run Automation* in the *Actions* dropdown to run playbooks. See Security Orchestration.
- The *Discovered Date* is displayed in *Coordinated Universal Time (UTC)*.

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.
- Click *Run Automation* in the *Actions* dropdown to run playbooks. See Security Orchestration.
- The *Discovered Date* is displayed in *Coordinated Universal Time (UTC)*.

Filtering stealer infection information

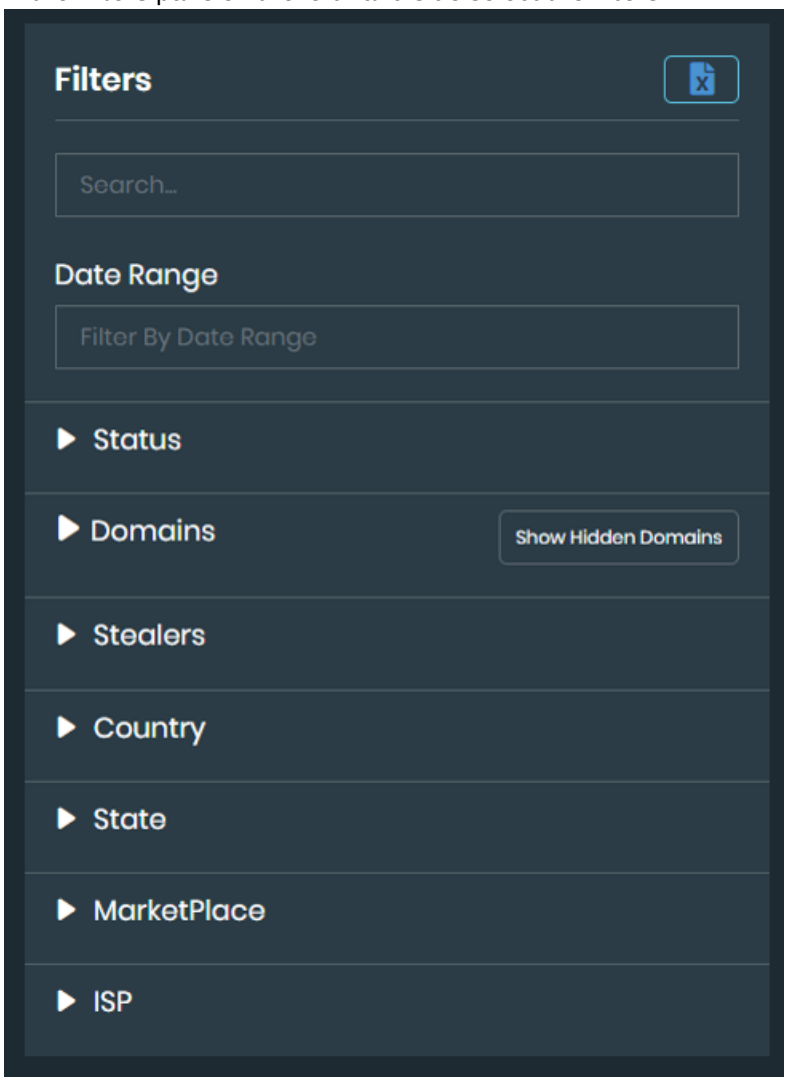
You can use several methods to filter information in the *Stealer Infections* .

All date and time data is displayed in *Coordinated Universal Time (UTC)*. Any filters applied will process results using the UTC date only.

To filter stealer infection information:

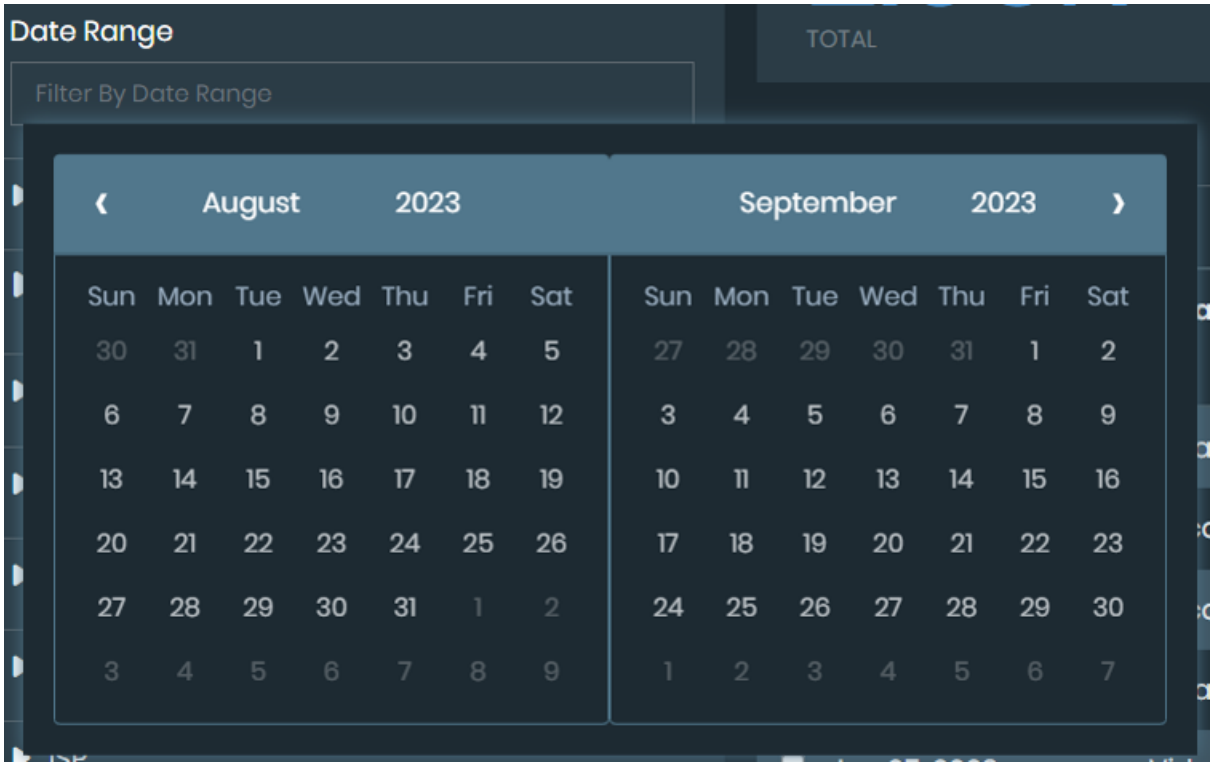
1. Go to *Adversary Centric Intelligence* > *Stealer Infections*.
2. Select the desired tab *Compromised Systems(Leaked)* or *Compromised Systems(On Sale)*.

3. In the *Filters* pane on the left hand side select the filters.

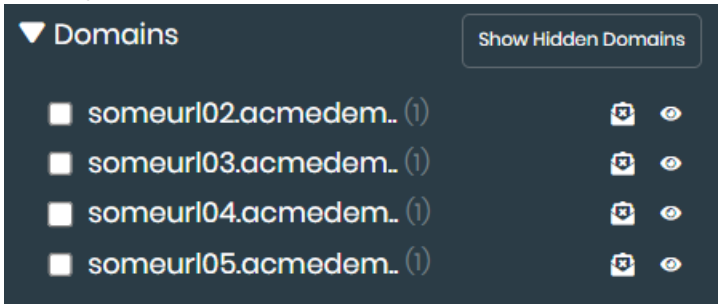


4. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
      The information is filtered.
   b. Clear the keyword and press *Enter* to remove the filter.

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

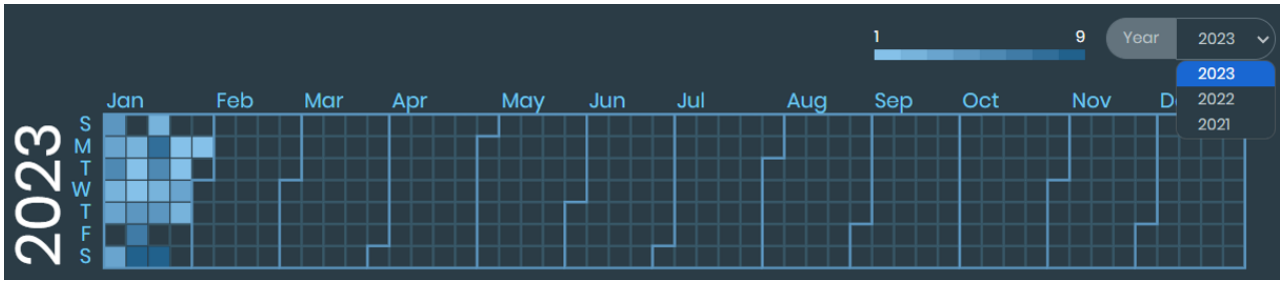


   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range.
      Only information from the date range is displayed.
   d. Click the *X* in the *Start & End Date* box to 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:

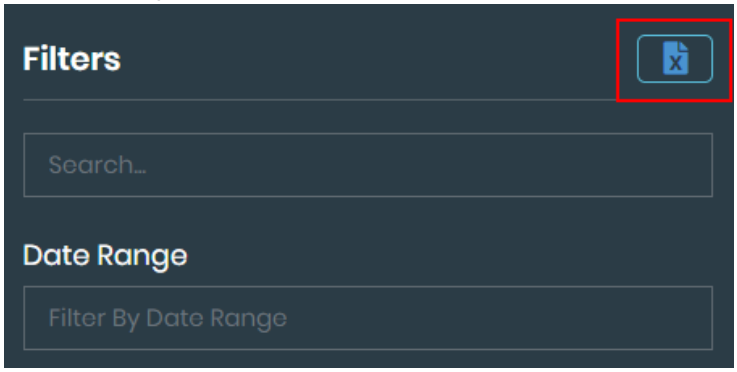


Exporting stealer infections data

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 181.
4. In the Filters pane on the left hand side, click the *Download* icon.



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

> When exporting Compromised Systems(Leaked) data, only an administrator has the option to download stealer information that includes passwords.

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:

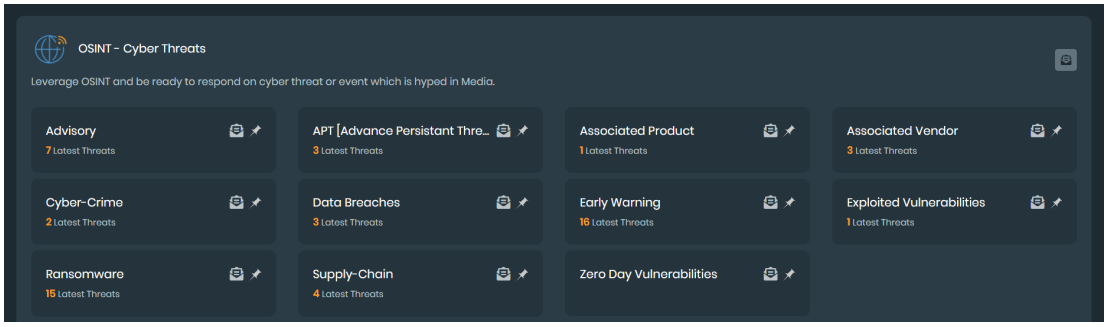
- Review threat events. See Reviewing threats on page 185.
- Pin threat events to the top of the list. See Pinning events on page 186.
- Subscribe to threat event notifications. See Subscribing to event notifications on page 187.
- Subscribe other FortiRecon users to event notifications. See Adding subscriptions on page 188.

Reviewing threats

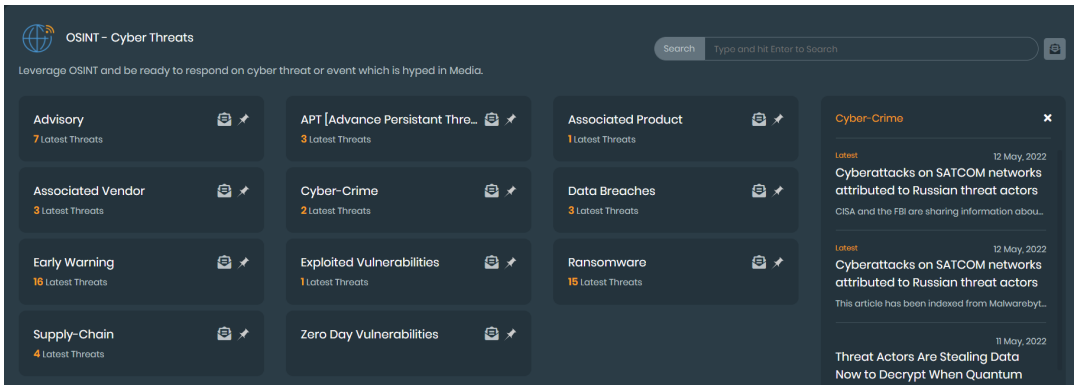
You can view more information about each threat.

To review threats:

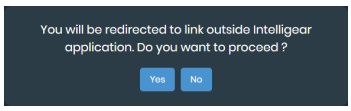
1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*. The list of events is displayed.



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.



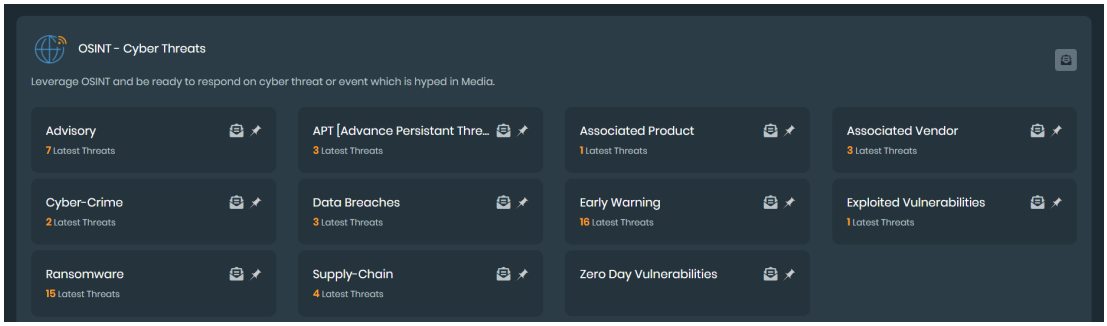
4. Click *Yes* to open the link in a new tab in your browser.

Pinning events

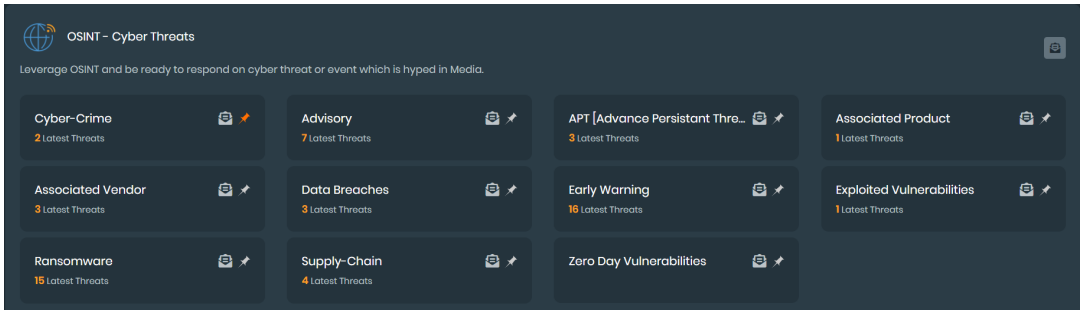
You can pin events to the top of the list. Pinned events have an orange *Pin* icon. Unpinned events have a white *Pin* icon.

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.



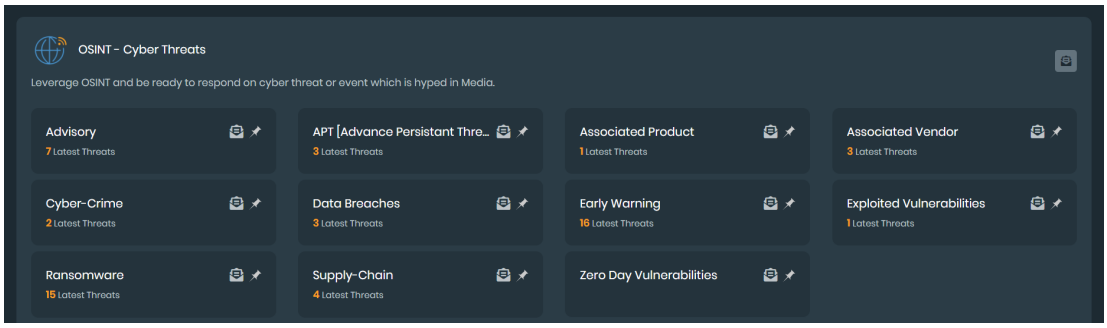
Click the *Pin* icon again to turn the pin white and unpin the event from the top of the list.

Subscribing to event notifications

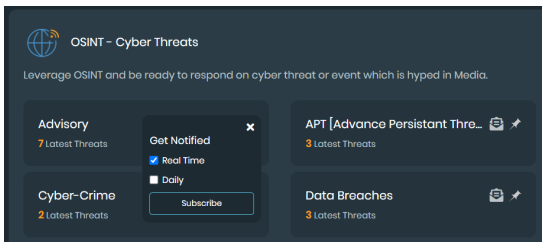
You can enable subscriptions to receive notifications for one or more threat events. You can also change subscriptions and unsubscribe.

To subscribe to event notifications:

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



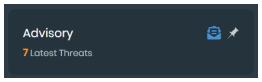
2. For an event, click the *Subscribe* icon. The subscription options are displayed for the event.
   In the following example, subscription options are displayed for the *Advisory* event:



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

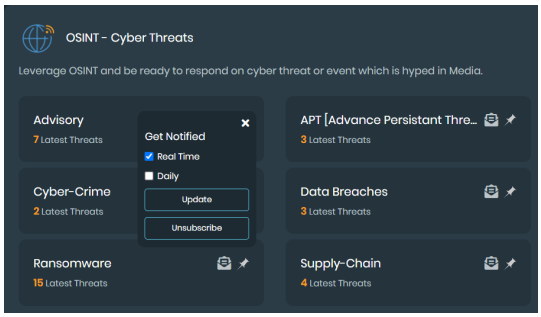
Real time	Select to receive a notification when a new threat event is published.
Daily	Select to specify the time each day to receive a notification about new threat events.

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:

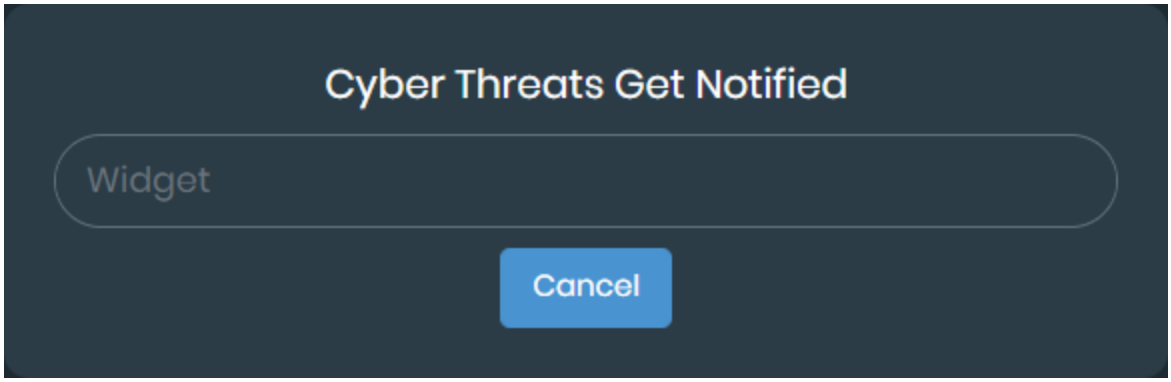
1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*. The list of events is displayed.
2. Click a blue *Subscribe* icon. The subscription options are displayed.
3. Click *Unsubscribe*.
   The *Subscribe* icon turns white, and notifications are turned off.

Adding subscriptions

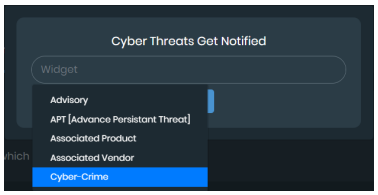
FortiRecon users with Admin privilege can set up subscriptions for other FortiRecon users to receive notifications about events.

To add subscriptions:

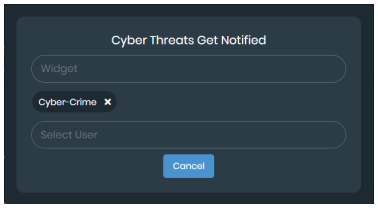
1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*, and click the *Add Subscription* button. The *Cyber Threats Get Notified* dialog is displayed.



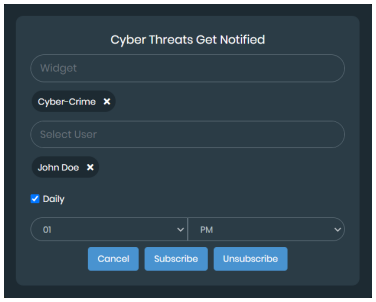
2. Click the *Widget* box, and select the threat events.
   In the following example, *Cyber-Crime* is selected.



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:

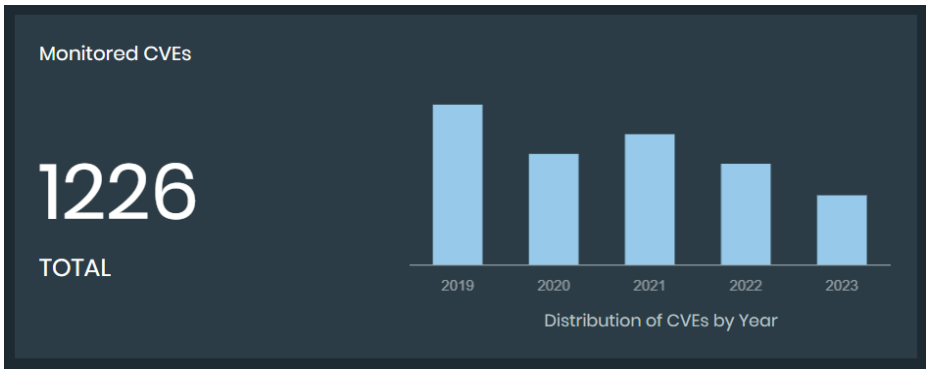
- Review known CVEs. See Vulnerability exposure on page 189.
- Review the notable global CVEs. See Global notable vulnerabilities on page 192.
- View specific CVE reports. See Viewing and filtering CVE reports on page 193.
- Export a list of CVEs. See Exporting CVEs on page 195.
- Bulk add CVEs to monitor. See Manually adding CVEs on page 195.

Vulnerability exposure

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

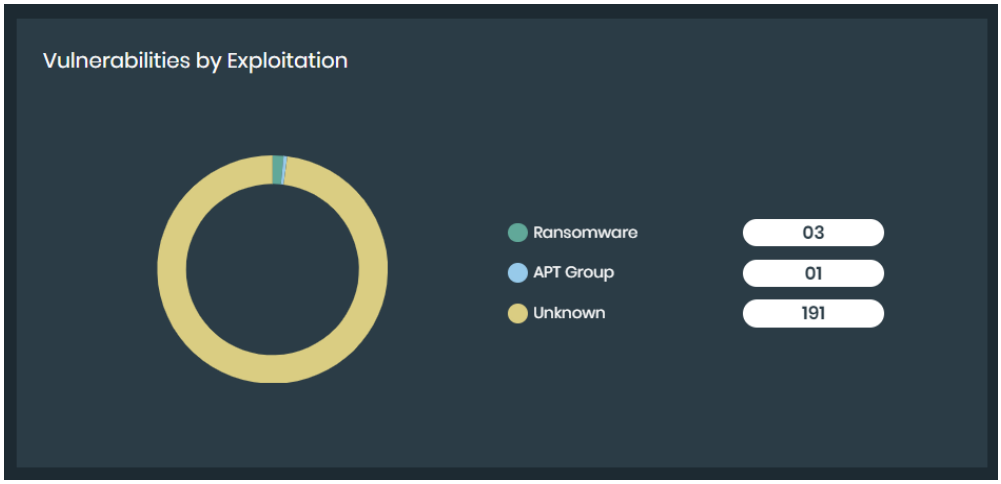
> Clicking on any chart element or legend item will filter the view and navigate you to a CVE details page pre-populated with the chosen filter.

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

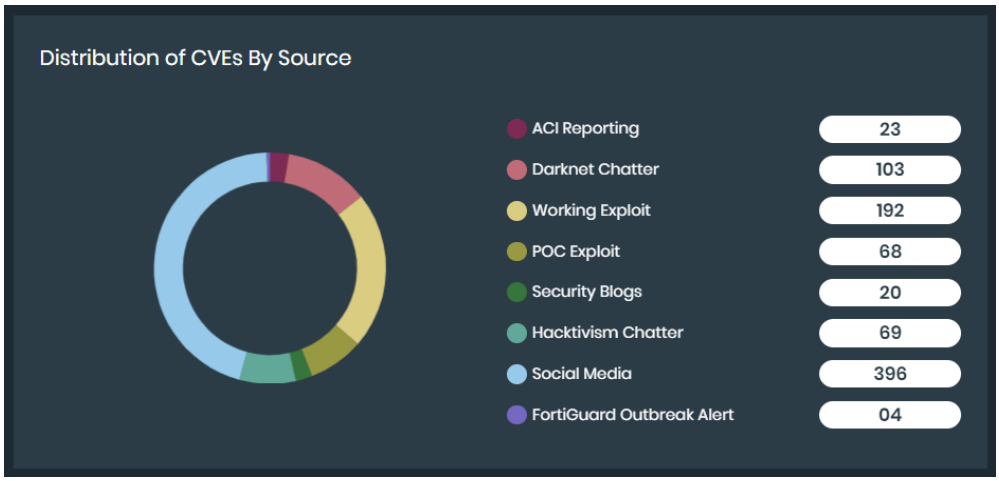


- *Severity Wise Disribution*: This tile displays a graph of CVEs to show the total count of CVEs per rating, from *Low* to *Critical* using both NVD and FortiRecon severity classifications.

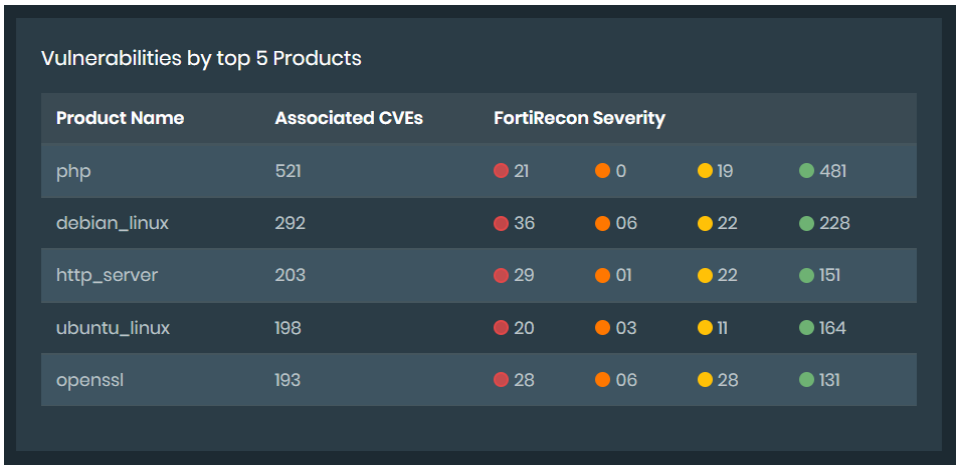
- *Vulnerabilities by Exploitation*: This tile displays the distribution of vulnerabilities based on the availability of known exploits.



- *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 Products

Product Name	Associated CVEs	FortiRecon Severity			
php	521	21	0	19	481
debian_linux	292	36	06	22	228
http_server	203	29	01	22	151
ubuntu_linux	198	20	03	11	164
openssl	193	28	06	28	131

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

Vulnerabilities by top 5 Vendors

Vendor Name	Associated CVEs	FortiRecon Severity			
php	524	23	01	19	481
debian	293	36	06	22	229
apache	203	28	02	24	149
canonical	196	20	03	11	162
openssl	193	28	06	28	131

- *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.

CVE ID	Vendor	NVD Severity	FortiRecon Severity	Addition Date
CVE-2020-0796	microsoft	Critical	Critical	Jan 12,2024
CVE-2013-4547	f5, suse, opensuse	High	Critical	Jan 12,2024
CVE-2011-3368	apache	Medium	Critical	Jan 11,2024
CVE-2011-3192	canonical, suse, opensuse, apache	High	Critical	Feb 29,2024
CVE-2011-4885	php	Medium	Critical	Feb 29,2024
CVE-2012-1823	php	High	Critical	Jan 12,2024
CVE-2010-1899	microsoft	Medium	Critical	Feb 29,2024
CVE-2014-0160	redhat, debian, mitel, openssl, ricon, o..	High	Critical	Jan 12,2024
CVE-2013-6955	synology	Critical	Critical	Feb 29,2024
CVE-2010-3972	microsoft	Critical	Critical	Feb 29,2024

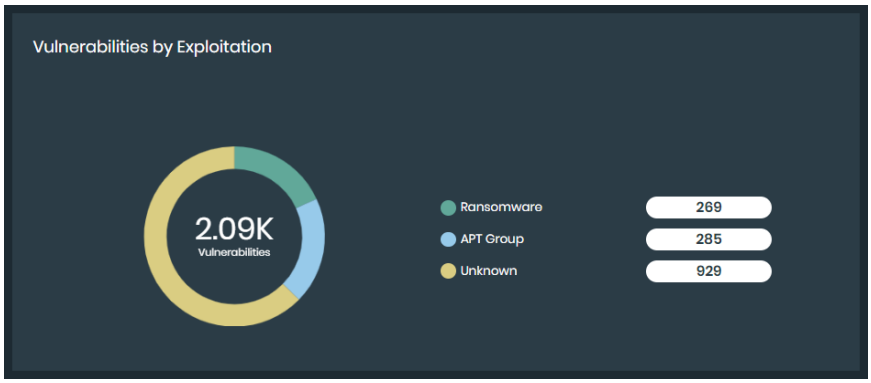
- *CVEs added Manually*: Displays a list of CVEs added by the user.

Global notable vulnerabilities

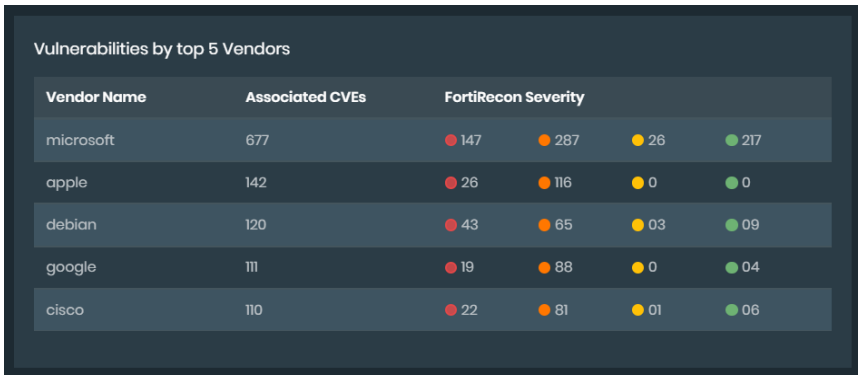
Monitored CVEs can be reviewed at a high level from the *Adversary Centric Intelligence* > *Vulnerability Intelligence* page in the *Global notable vulnerabilities* section:

> 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*.



Vulnerabilities by top 5 Vendors

Vendor Name	Associated CVEs	FortiRecon Severity			
microsoft	677	147	287	26	217
apple	142	26	116	0	0
debian	120	43	65	03	09
google	111	19	88	0	04
cisco	110	22	81	01	06

- *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.

Latest 10 Notable CVEs

Date

CVE ID	Vendor	NVD Severity	FortiRecon Severity	Addition Date
CVE-2021-28482	microsoft	High	High	Mar 22,2024
CVE-2022-1386	fusion_builder_project, theme-fusion	Critical	High	Mar 22,2024
CVE-2022-10270	-	-	High	Mar 22,2024
CVE-2019-1096	microsoft	Medium	Low	Mar 22,2024
CVE-2020-3956	linux, vmware	High	Critical	Mar 22,2024
CVE-2020-17127	microsoft	High	Low	Mar 22,2024
CVE-2019-9081	-	-	Low	Mar 22,2024
CVE-2021-29484	ghost	Medium	Low	Mar 22,2024
CVE-2023-28231	microsoft	High	High	Mar 22,2024
CVE-2022-22583	apple	Medium	High	Mar 22,2024

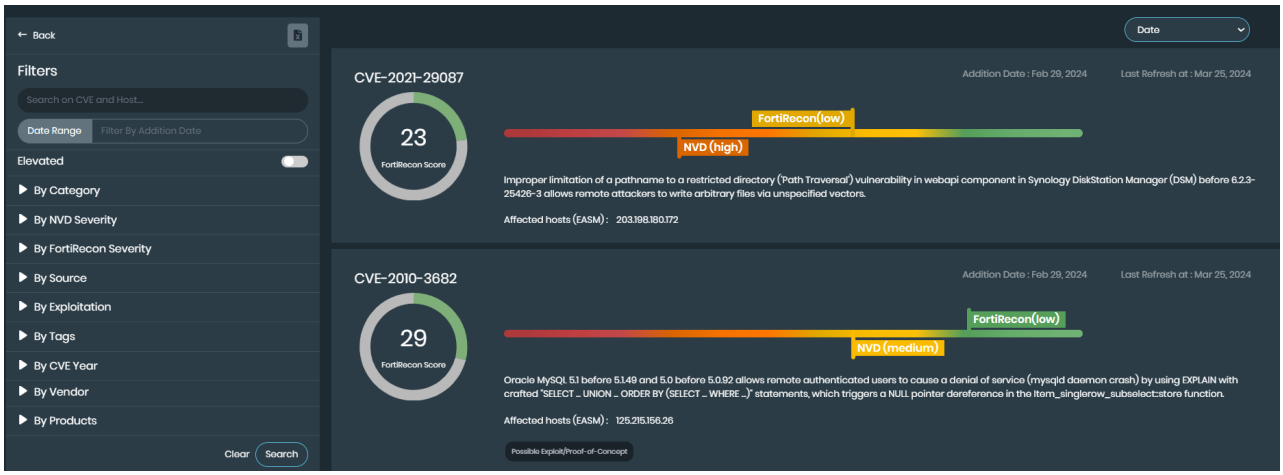
Showing latest 10 records View All

Viewing and filtering CVE reports

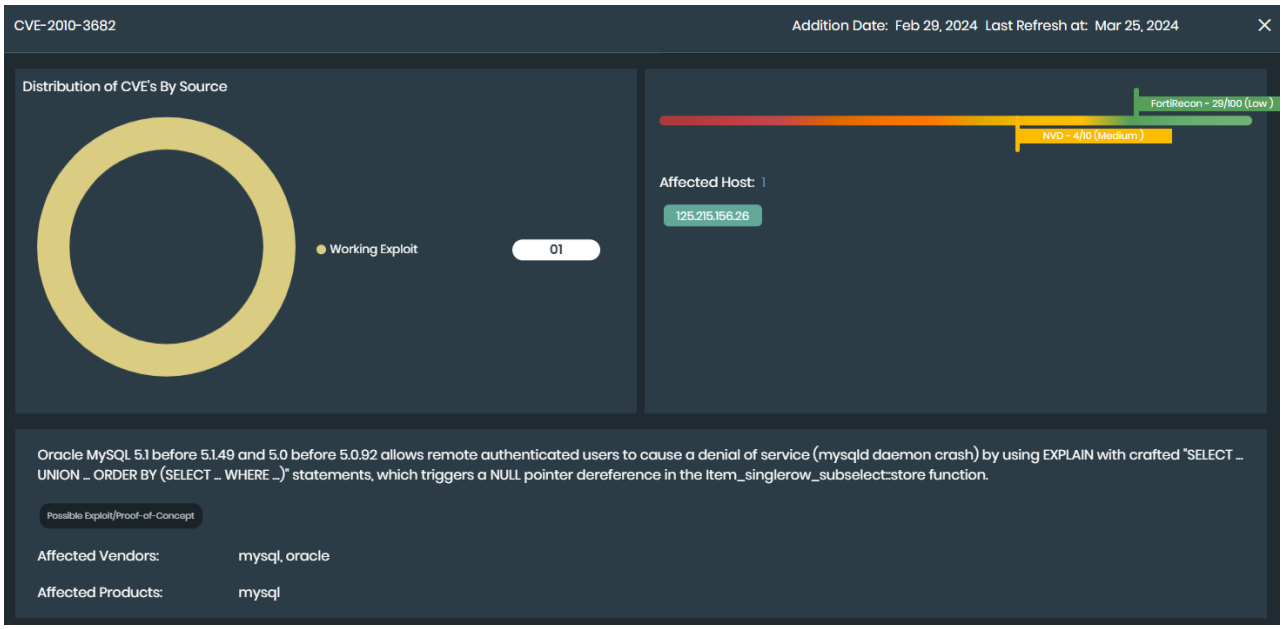
You can review detailed CVE reports in the *Adversary Centric Intelligence* > *Vulnerability Intelligence* page by selecting the *View All* button from the *Vulnerability exposure* > *CVEs from EASM Module*, *Vulnerability exposure* > *CVEs added Manually*, or *Global notable vulnerabilities* > *Latest 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. The CVE reports that match the filters are displayed.
7. 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 193.
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 196.
- Filter ransomware incident information. See Filtering ransomware intelligence on page 203.
- Export information on ransomware incidents to an Excel file. See Exporting ransomware information on page 205.
- Create, edit, and monitor a ransomware watchlist. See Managing My Watchlist on page 205.

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

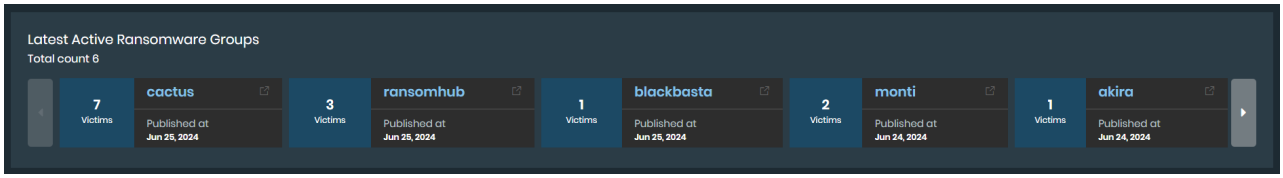
Ransomware Trends

This section provides a high-level view of global ransomware activity.

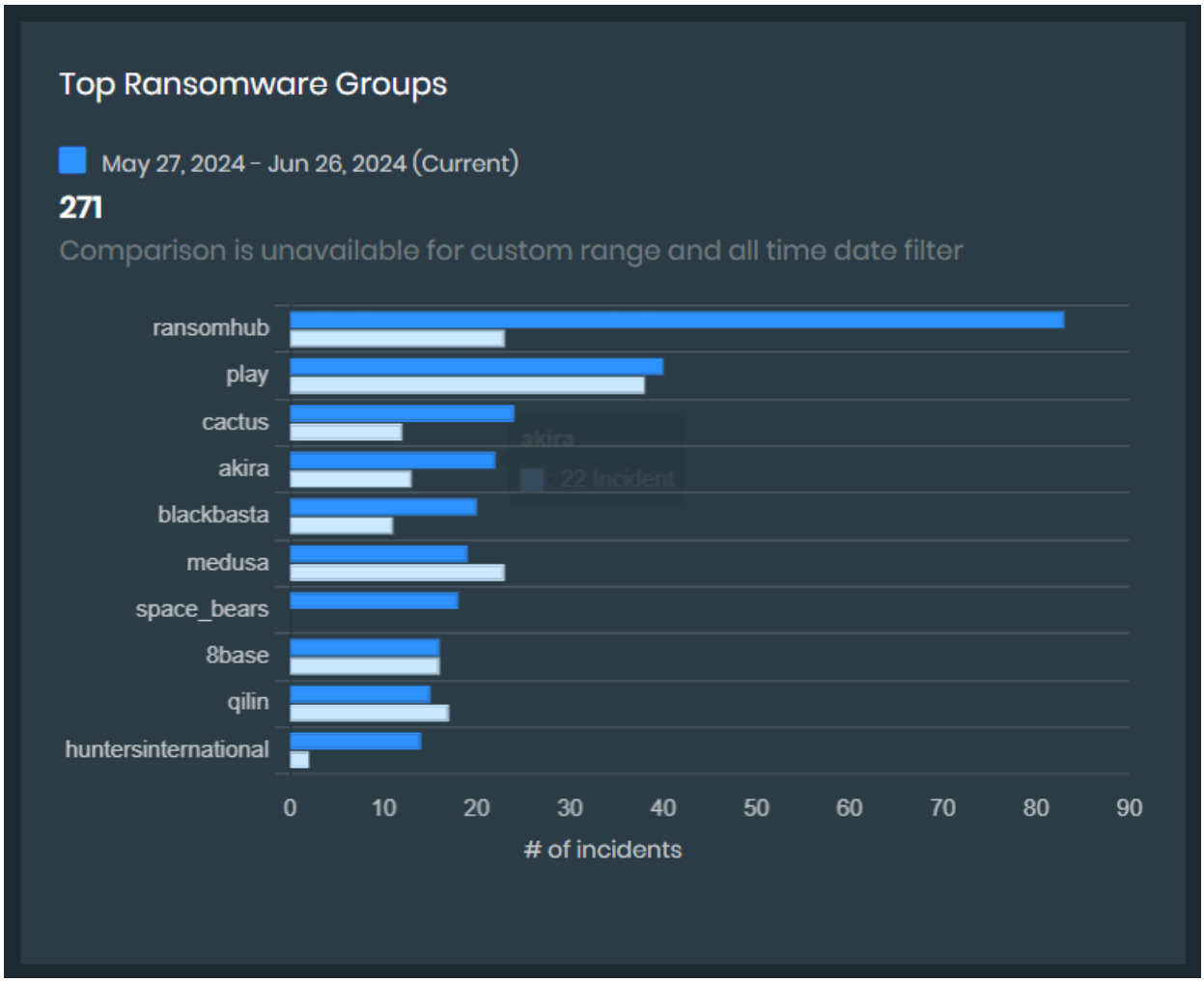
You can filter the data displayed in *Ransomware Trends* using the *Ransomware Group* and *Date* filters.

- *Summary*: A summary of total number of ransomware groups tracked, ransomware victims, most active ransomware groups, top targeted sector, and top victimized countries.

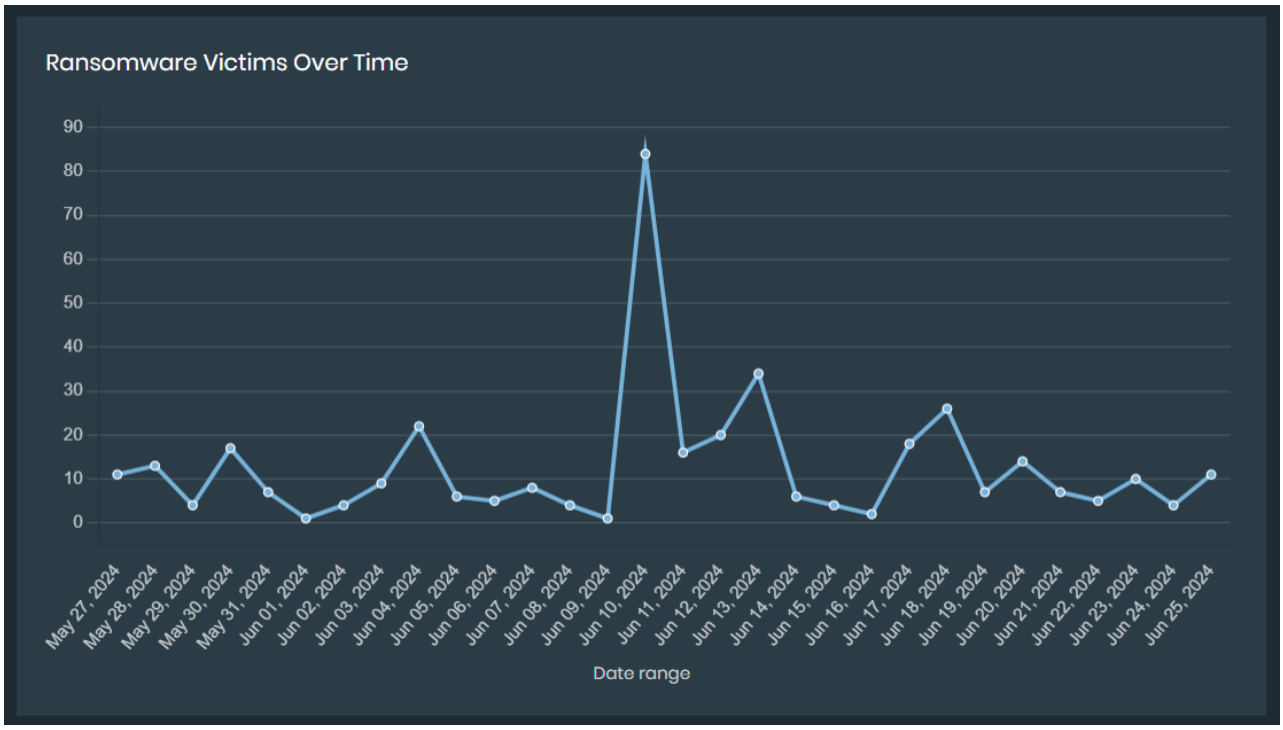
- *Latest Active Ransomware Groups*: A list of known, active ransomware groups, including victim count, group name, and published date. Click link icon to view ransomware victims affected.



- *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.



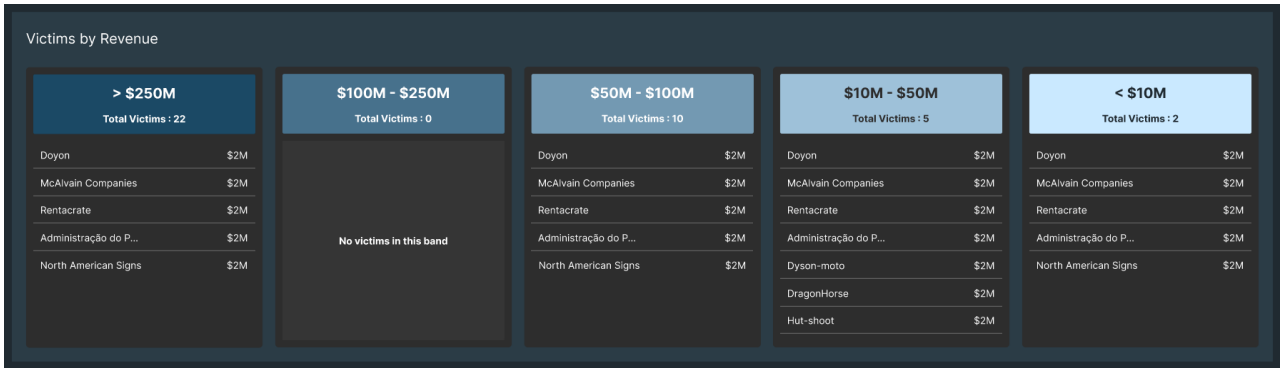
- *Ransomware Victims Over Time*: A line graph that tracks the number of ransomware victims identified over time.



- *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.

	United states	United Kingdom	Canada	Germany	France	Italy	Australia	Brazil	Spain	
Education	75	70	50	2	75	75	75	75	75	75
Business Services	35	75	35	75	75	35	75	75	4	4
Retail	35	35	75	75	75	35		75	75	75
Construction	35	75	75	4	75	75	75	75	75	75
Commercial & Resident...	75			4	75	75	75	4	35	35
Finance	75	66	68	4	75	75	75	4	75	35
Industrial machine...	4	62	67	75	75	35	75	4	75	75
Hospitality	75	4	70	70	35	75	35	75	72	75
Transportation	75	4	75	75	75	75	75	75	56	75
Agricultural	75	75	75	75	75	75	75	75	71	70

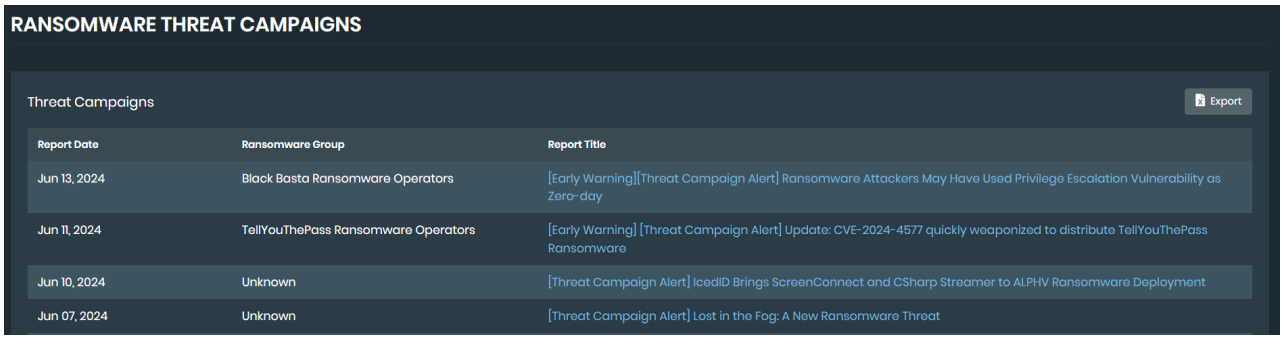
- *Victims by Revenue*: A list of organizations impacted by ransomware attacks, along with their estimated revenue.



Ransomware Threat Campaigns

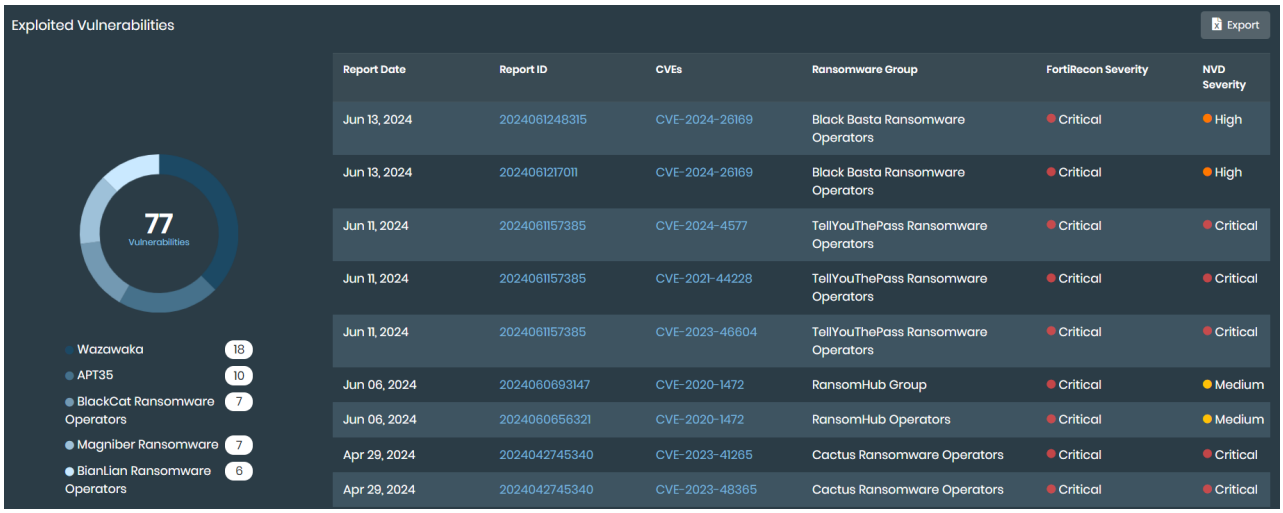
This section provides information on specific ransomware attacks.

- *Threat Campaigns*: A list of ransomware campaigns including report date, ransomware group and link to the report. Click *Export* to export the data.



Report Date	Ransomware Group	Report Title
Jun 13, 2024	Black Basta Ransomware Operators	[Early Warning][Threat Campaign Alert] Ransomware Attackers May Have Used Privilege Escalation Vulnerability as Zero-day
Jun 11, 2024	TellYouThePass Ransomware Operators	[Early Warning] [Threat Campaign Alert] Update: CVE-2024-4577 quickly weaponized to distribute TellYouThePass Ransomware
Jun 10, 2024	Unknown	[Threat Campaign Alert] IcedID Brings ScreenConnect and CSharp Streamer to ALPHV Ransomware Deployment
Jun 07, 2024	Unknown	[Threat Campaign Alert] Lost in the Fog: A New Ransomware Threat

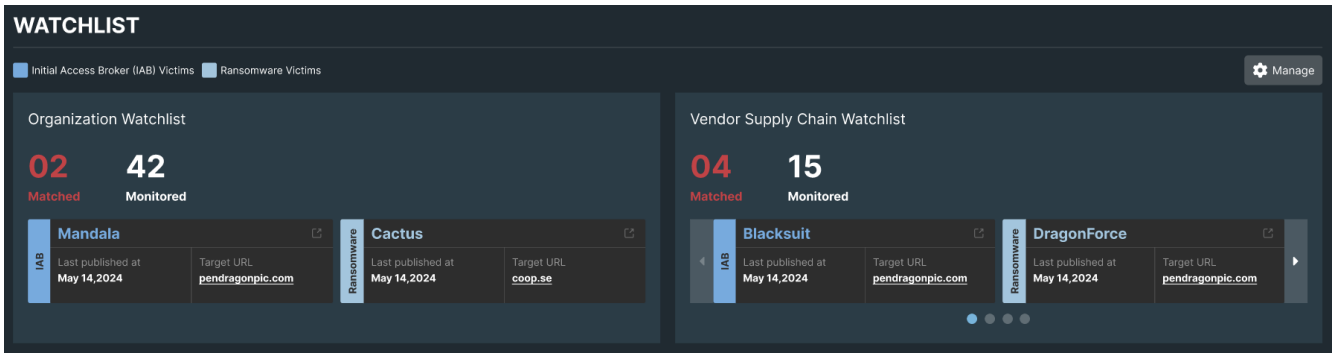
- *Exploited Vulnerabilities*: A list of exploited vulnerabilities including CVE, ransomware group, FortiRecon and NVD severity information.
  - Click *Report ID* to view the report
  - Click *CVE* to view the detailed information on *Vulnerability Intelligence* page with selected CVE as filter.
  - Click *Export* to export the data.



Report Date	Report ID	CVEs	Ransomware Group	FortiRecon Severity	NVD Severity
Jun 13, 2024	2024061248315	CVE-2024-26169	Black Basta Ransomware Operators	Critical	High
Jun 13, 2024	2024061217011	CVE-2024-26169	Black Basta Ransomware Operators	Critical	High
Jun 11, 2024	2024061157385	CVE-2024-4577	TellYouThePass Ransomware Operators	Critical	Critical
Jun 11, 2024	2024061157385	CVE-2021-44228	TellYouThePass Ransomware Operators	Critical	Critical
Jun 11, 2024	2024061157385	CVE-2023-46604	TellYouThePass Ransomware Operators	Critical	Critical
Jun 06, 2024	2024060693147	CVE-2020-1472	RansomHub Group	Critical	Medium
Jun 06, 2024	2024060656321	CVE-2020-1472	RansomHub Operators	Critical	Medium
Apr 29, 2024	2024042745340	CVE-2023-41265	Cactus Ransomware Operators	Critical	Critical
Apr 29, 2024	2024042745340	CVE-2023-48365	Cactus Ransomware Operators	Critical	Critical

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.

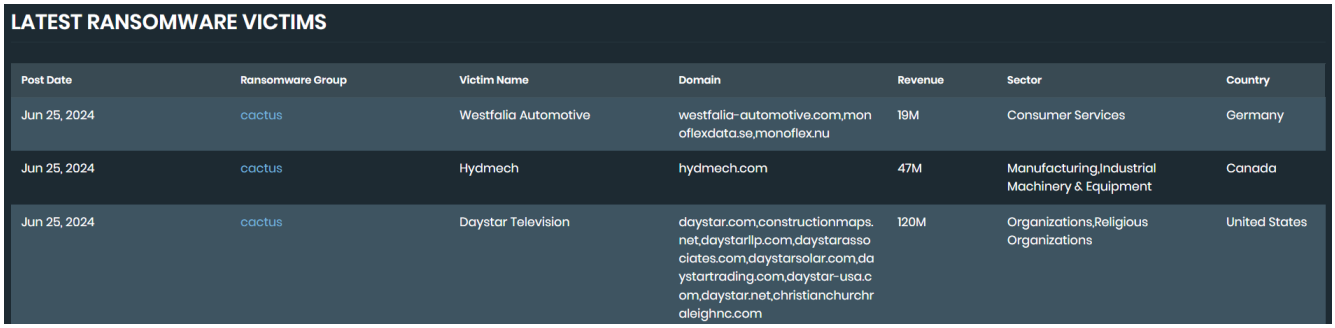


Latest Ransomware Victims

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.



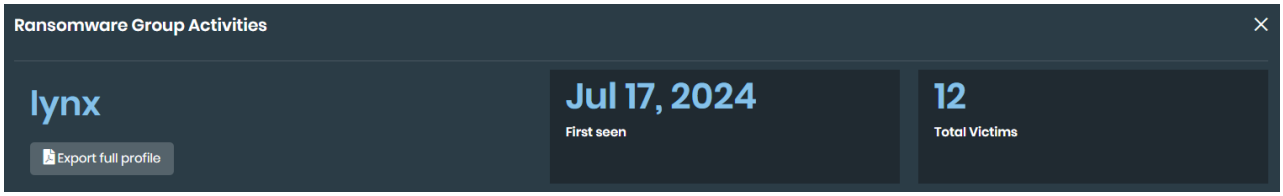
LATEST RANSOMWARE VICTIMS

Post Date	Ransomware Group	Victim Name	Domain	Revenue	Sector	Country
Jun 25, 2024	cactus	Westfalia Automotive	westfalia-automotive.com,monoflexdata.se,monoflex.nu	19M	Consumer Services	Germany
Jun 25, 2024	cactus	Hydmech	hydmech.com	47M	Manufacturing,Industrial Machinery & Equipment	Canada
Jun 25, 2024	cactus	Daystar Television	daystar.com,constructionmaps.net,daystarllp.com,daystarassociates.com,daystarsolar.com,daystartrading.com,daystar-usa.com,daystar.net,christianchurchraleighnc.com	120M	Organizations,Religious Organizations	United States

Ransomware Group Activities

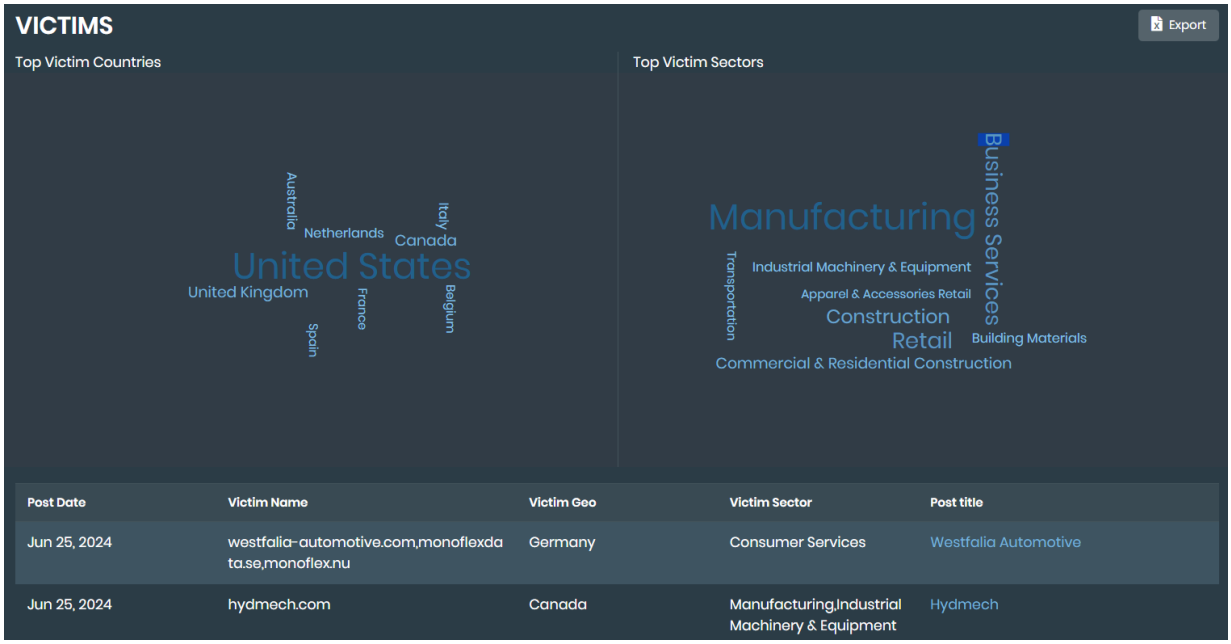
This page provides detailed information about a specific ransomware group, including its activity, victims, exploited vulnerabilities, and technical indicators. It includes following sections.

- 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.



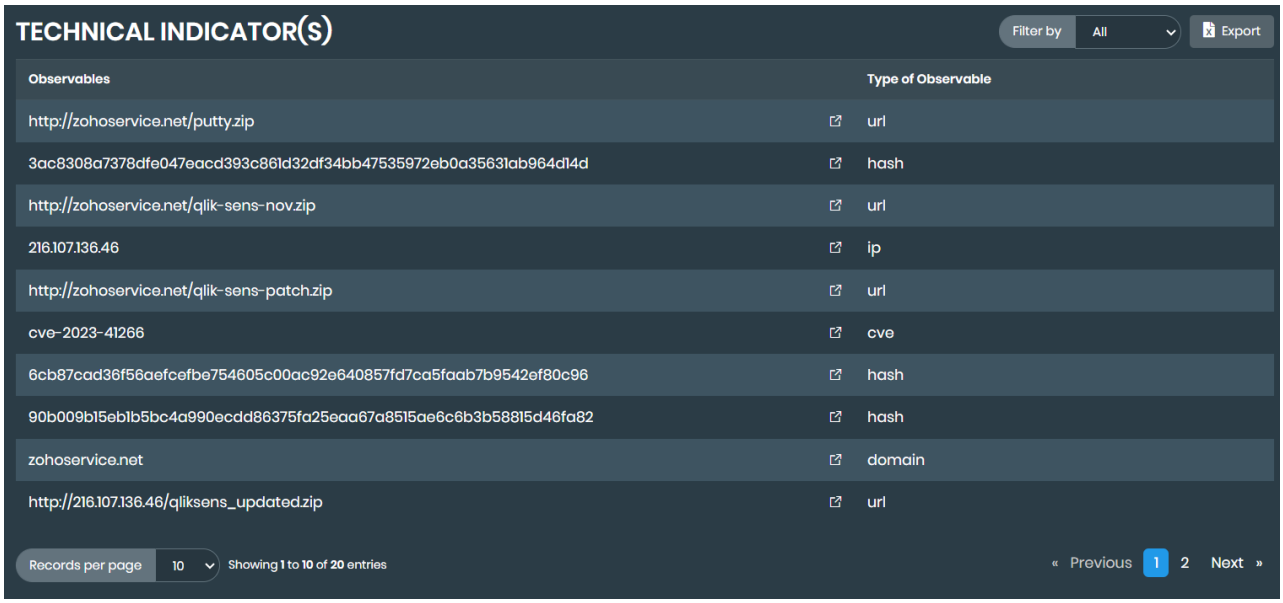
- The *Victims* section includes the following information.
  - *Top Victim Countries*: This word cloud displays the most frequently targeted countries by the group. The size of a country name corresponds to the number of victims in that location.

- *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.



TECHNICAL INDICATOR(S)

Filter by All | Export

Observables	Type of Observable
http://zohoservice.net/putty.zip	url
3ac8308a7378dfe047eacd393c861d32df34bb47535972eb0a35631ab964d14d	hash
http://zohoservice.net/qlik-sens-nov.zip	url
216.107.136.46	ip
http://zohoservice.net/qlik-sens-patch.zip	url
cve-2023-41266	cve
6cb87cad36f56aefcefbe754605c00ac92e640857fd7ca5faab7b9542ef80c96	hash
90b009b15eb1b5bc4a990ecdd86375fa25eaa67a8515ae6c6b3b58815d46fa82	hash
zohoservice.net	domain
http://216.107.136.46/qliksens_updated.zip	url

Records per page 10 Showing 1 to 10 of 20 entries « Previous 1 2 Next »

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.

LATEST INITIAL ACCESS BROKER (IAB) VICTIMS

Report Date	Actor	Source	Victim Name	Target Domain	Revenue	Sector	Country
Jun 25, 2024	Xaos, Shop	HUMINT	W Hydrocolloids	www.whydrocolloids.com	0	-	
Jun 24, 2024	GirlBF	Darknet	University of Central Lancashire	www.uclan.ac.uk	8M	Education,Colleges & Universities	United Kingdom
Jun 24, 2024	violets	Darknet	LSPR ID Communication and Business Institute	www.lspr.ac.id	0	-	
Jun 24, 2024	togi	Darknet	SiS Distribution Public Company Limited	www.sisthai.com	775M	Retail,Consumer Electronics & Computers Retail	Thailand
Jun 22, 2024	ctf	Darknet	Cineplex Bistro Bar	www.cineplex.com.ec	1M	Hospitality,Movie Theaters	Ecuador

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 country from *Country* dropdown.
   - Select a sector from *Sector* dropdown.
   - 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.

   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.

   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 203.
5. Click the *Export List* icon. The file is downloaded to your computer.

Managing My Watchlist

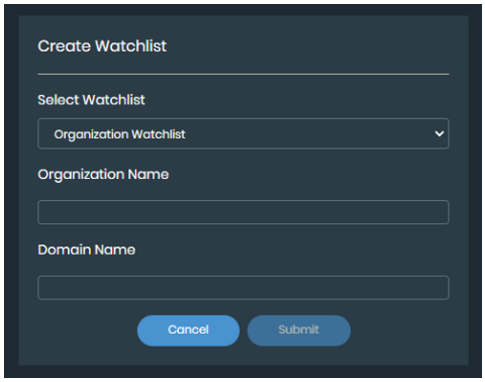
Users can monitor certain vendor and organization names in the *My Watchlist* page in the *Vendor Watchlist* and *Organization Watchlist*, respectively. If a match for a monitored asset appears, it triggers an alert. Vendors and organizations can be added to the watchlist manually by users or automatically by EASM.

To filter the monitored assets, see Filtering ransomware intelligence on page 203.

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.

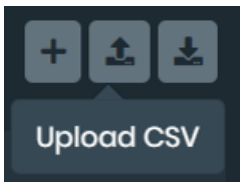
3. Click + icon. The *Create Watchlist* dialog is displayed.



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:

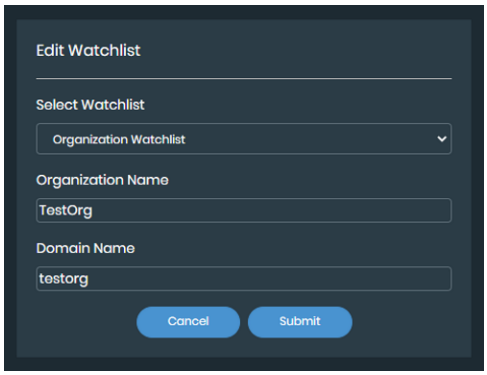
1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Watchlist* section, click *Manage*. The *My Watchlist* page is displayed.
3. Click *Upload CSV* icon to upload the .csv files containing the vendors list. Browse and select the file. Click **Open**.



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:

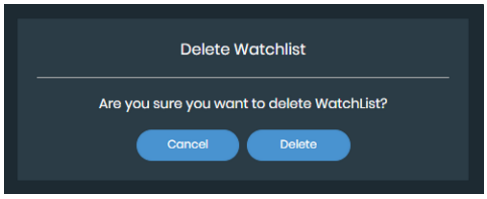
1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Watchlist* section, click *Manage*. The *My Watchlist* page is displayed.
3. Search the asset you want to edit and click *Edit icon*. The *Edit Watchlist* dialog is displayed.



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 207.
- View the security hygiene assessment of a vendor. See Viewing the vendor risk assessment on page 208.

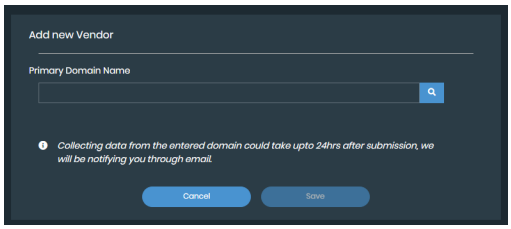
Adding a new vendor to the watchlist

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.

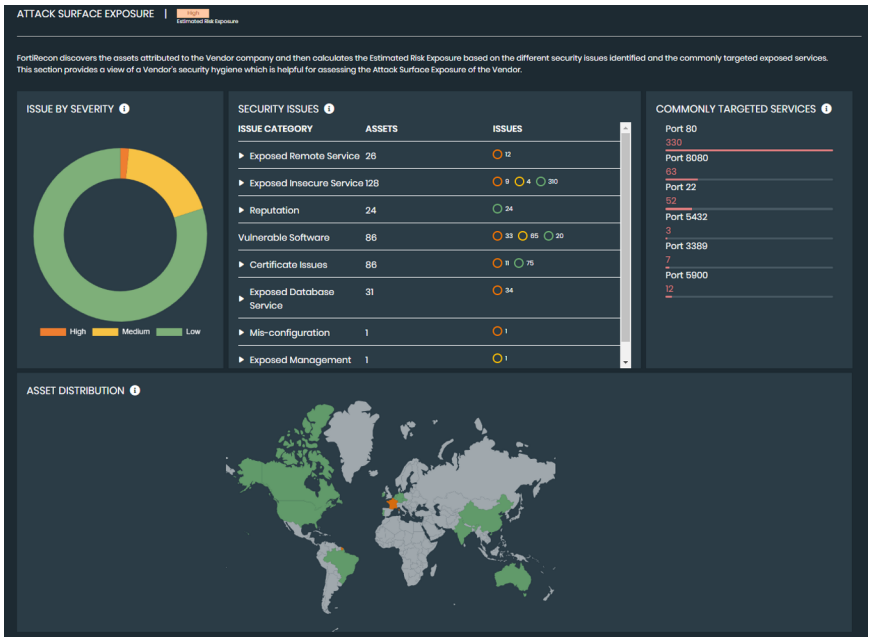
Removing a vendor from the watchlist

To remove a vendor from the watchlist, click *Remove* on its watchlist card.

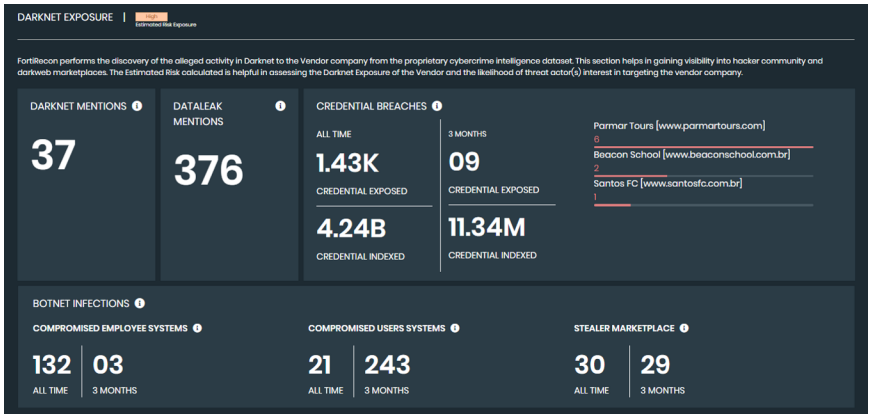
Viewing the vendor risk assessment

The vendor risk assessment organizes the generated vendors data into:

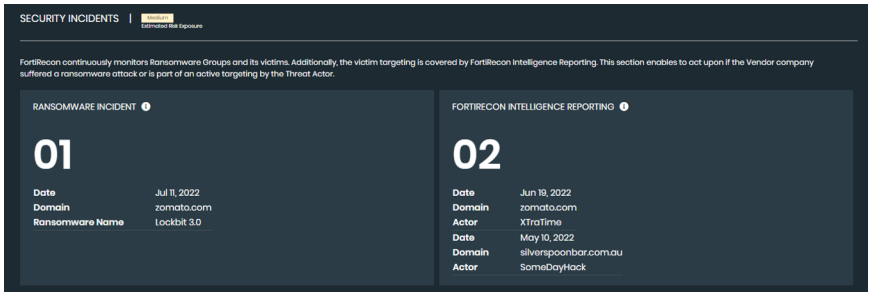
- *Attack Surface Exposure*: Provides an overview of the vendor company's assets and current security hygiene to assess the estimated risk exposure.



- *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.



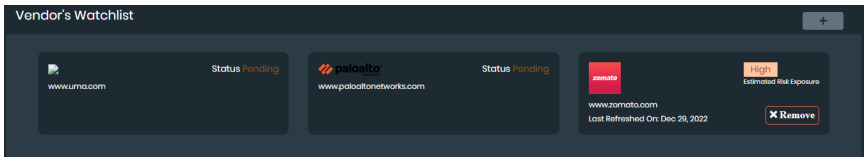
- *Security Incidents*: Provides an overview of ransomware incidences and intelligence reporting so that action can be taken if the vendor company suffers a ransomware attack or is targeted by a threat actor.



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*:

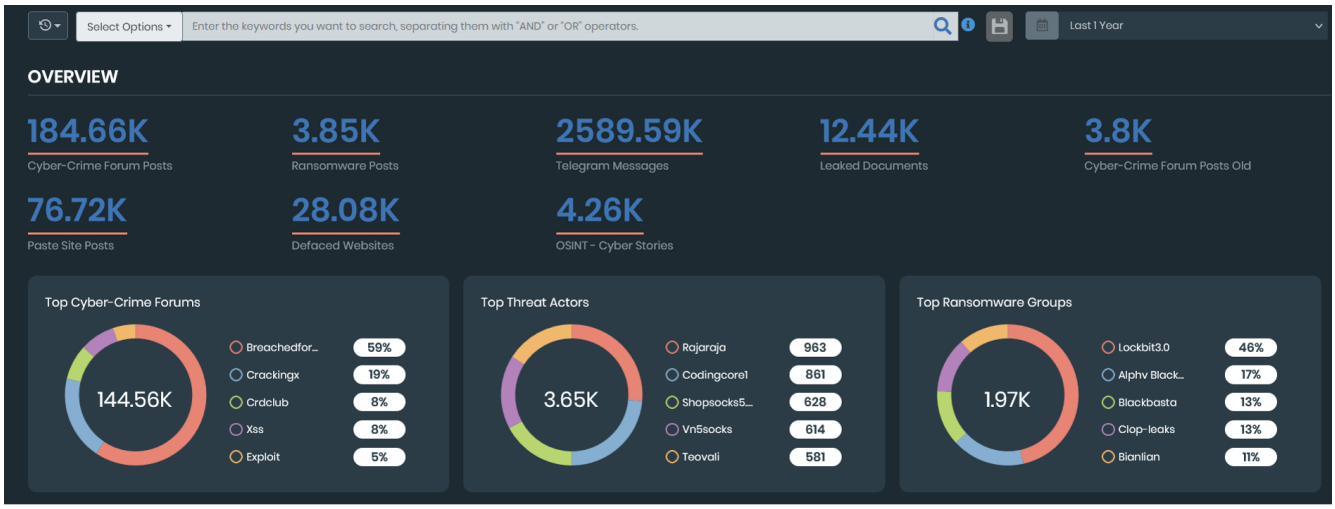
Ransomware Incident	The vendor name or domain appeared on the victim list by a ransomware group.
FortiRecon Intelligence Reporting	FortiRecon ACI reporting contains mention of the vendor's name or domain.

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.



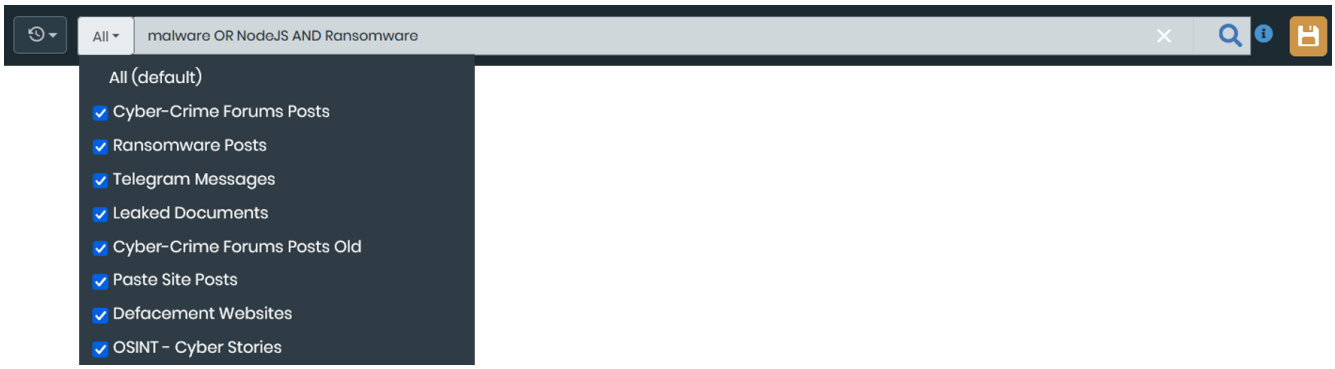
Search Query

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.



> The *Cyber-Crime Forum Posts* tab includes content from various threat marketplaces. To filter this data, use the query `source: marketplaces`. English translation is available for the marketplace content.

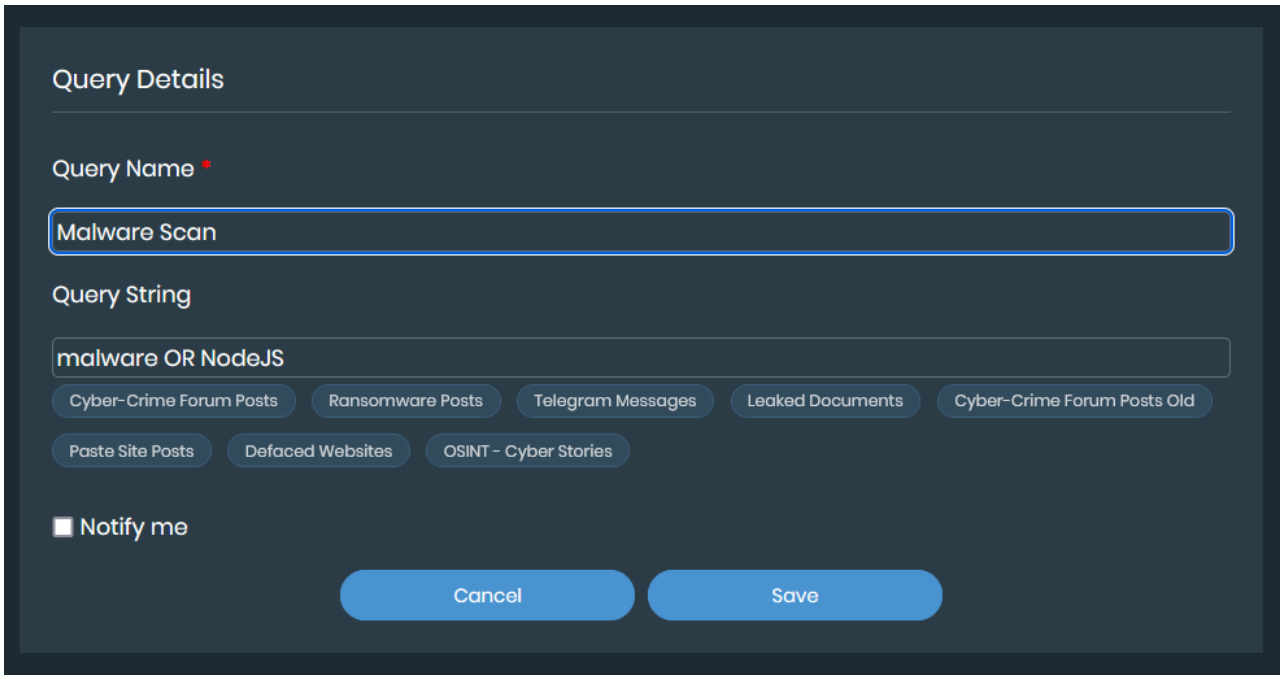
Saving a search query

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.

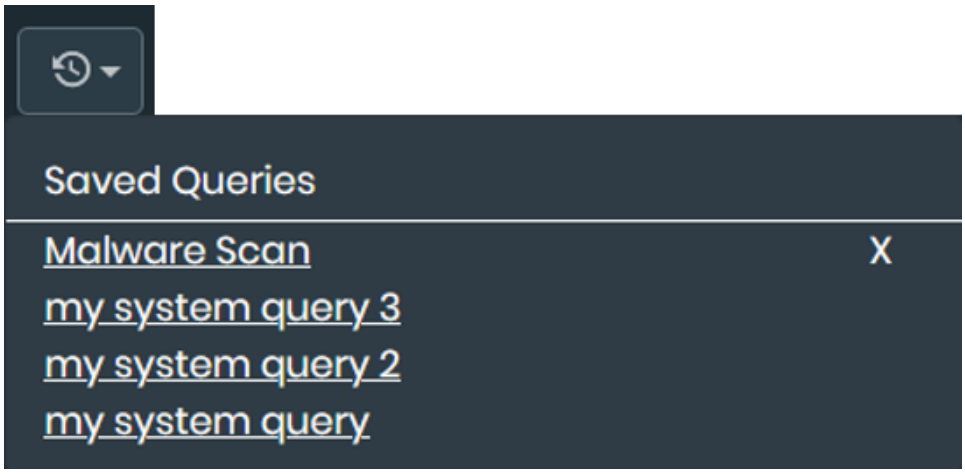
To save a user search query:

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.



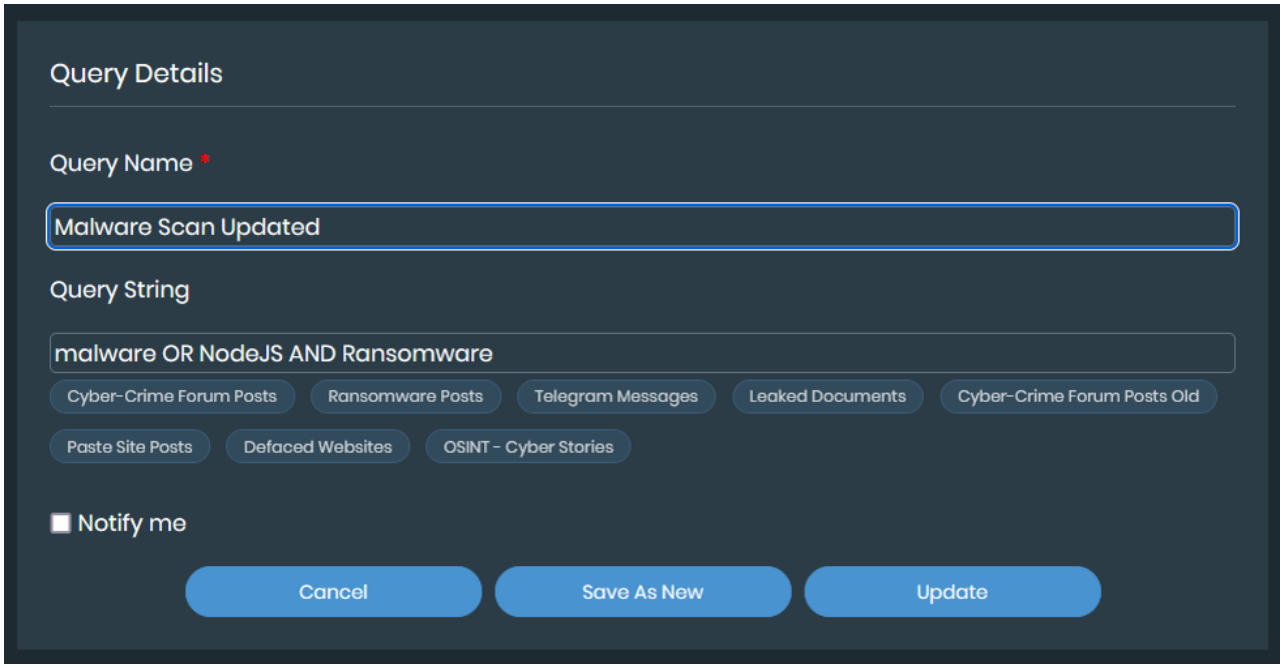
To delete a saved search query:

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.

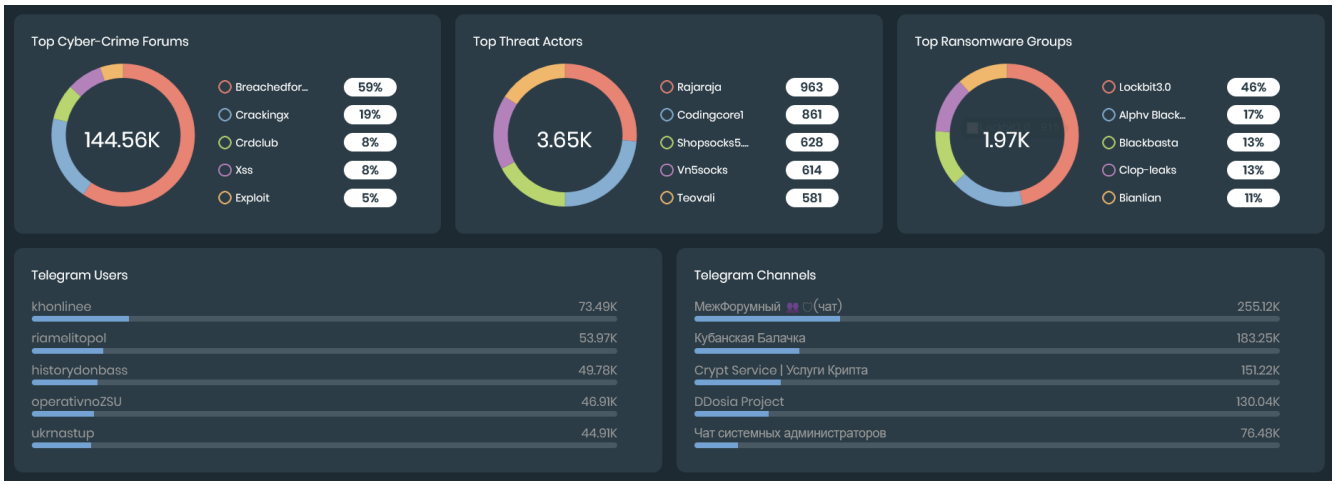
- Overview
- Detailed Results

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.

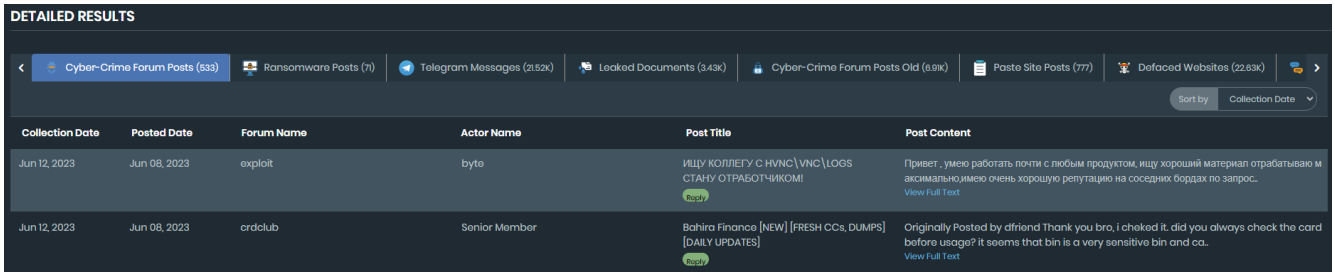
- *Cyber-Crime Forums Posts*
- *Ransomware Posts*
- *Telegram Messages*
- *Leaked Documents*
- *Cyber-Crime Forums Posts Old*
- *Paste Site Posts*
- *Defacement Websites*
- *OSINT- Cyber Stores*



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. Use *Sort by* dropdown to sort data based on *Collection Date*, *Posted Date*, or *Updated Date*.

Intelligence Source	Fields Displayed
Cyber-Crime Forum Posts	• Collection Date • Posted 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	• Posted Date Updated 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	• Collection Date • Posted Date • Username • Channel • Message
Leaked Documents	• Collection Date • Posted Date • Leak Name • File Name • File Data Click *View Full Text* to view the full content.
Cyber-Crime Forum Posts Old	• Collection Date • Posted Date • Forum • Name • Actor Name • Posts Title • Posts Content

Intelligence Source	Fields Displayed
	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	• Collection Date • Posted Date • Author Name • Title • Content Click *View Full Text* to view the full content. Click link icon to view the site posts in detail.
Defaced Websites	• Collection Date • Posted Date • Source • Notifier • Domain Click link icon to view the website.
OSINT - Cyber Stories	• Collection Date • Posted 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 219.
- Review the reputation of a domain. See Reviewing domain reputation on page 219.
- Review a file hash. See Reviewing a file hash on page 219.
- Review a CVE. See Reviewing a CVE on page 219.

Fair usage policy restrictions apply.

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.

Security Orchestration

The Security Orchestration module helps you investigate and respond to security threat findings from FortiRecon's *Attack Surface Management*, *Brand Protection*, and *Adversary Centric Intelligence* modules. This solution reduces the time responders require to prioritize and take appropriate actions by automating and streamlining security workflows.

Every FortiRecon core subscription includes a standard entitlement of *100 playbook executions per month*. You can increase your monthly limit by purchasing *Security Orchestration Playbook* add-on packs. Each pack adds *2000* executions to your monthly capacity. These licenses are stackable. See Standard FortiRecon Licensing.

Example: If you purchase any one of the core solution bundles—*EASM*, *EASM and BP*, or *EASM, BP, and ACI*, you receive a default entitlement of *100* playbook executions per month.

If you then purchase a *Security Orchestration Playbook* add-on, your total capacity increases to *2100* executions per month (*100* from the core bundle + *2000* from the add-on). Each additional add-on pack stacks an extra *2000* executions onto your monthly limit.

For steps to begin using the pre-defined playbooks, see Getting Started on page 222

If you are an existing user of Security Orchestration, you must manually upgrade the FortiRecon Automation Service solution pack. This step is not necessary for new installations or for existing users who have not yet accessed *Security Orchestration*.

1. To uninstall the older version of solution pack, navigate to *Content Hub* > *Installed* tab, apply the *Solution Packs* filter, select the *FortiRecon Automation Service 1.0.0* entry, and then click *Delete Template* in the dialog box.
2. To install the new version, navigate to *Content Hub* > *Discover* tab, apply the *Solution Packs* filter, search for and select *FortiRecon Automation Service 1.0.1*, and then click *Install* in the dialog box.

For more information on managing Solution Packs, see Solution Packs .

The Security Orchestration module contains the following tabs.

Home	The *Home* tab provides a quick overview of your Security Orchestration usage and available playbook collections. See Home on page 229.
Playbooks	The *Playbooks* tab allows you to create and manage your playbook collections and individual playbooks. See Playbooks Overview on page 230.
Playbook Assets	The *Playbook Assets* tab enables you to create and manage global variables and event templates for your playbooks. See Playbook Assets on page 245.
Content Hub	The *Content Hub* tab provides Discover and Installed tabs to help you install and manage connectors, widgets, and solution packs. See Content Hub on page 247.

Agents	The *Agents* tab allows you to create and manage agents. See Agents on page 252.
Execution Logs	The *Execution Logs* tab allows you view results and debug executed playbooks. See Execution Logs on page 252.
Tasks	The *Tasks* tab displays a list of automations that are awaiting your input before they can continue their execution. See Tasks.

Getting Started

The Security Orchestration module comes pre-installed with the *FortiRecon Automation Service Solution Pack*. This pack includes pre-defined playbooks for various security use cases, helping you get started quickly.

If you are an existing user of Security Orchestration, you must manually upgrade the FortiRecon Automation Service solution pack. This step is not necessary for new installations or for existing users who have not yet accessed *Security Orchestration*.

1. To uninstall the older version of solution pack, navigate to *Content Hub* > *Installed* tab, apply the *Solution Packs* filter, select the *FortiRecon Automation Service 1.0.0* entry, and then click *Delete Template* in the dialog box.
2. To install the new version, navigate to *Content Hub* > *Discover* tab, apply the *Solution Packs* filter, search for and select *FortiRecon Automation Service 1.0.1*, and then click *Install* in the dialog box.

For more information on managing *Solution Packs*, see Solution Packs .

Running Playbooks

You can run playbooks from various locations within FortiRecon, including the Home tab, the Playbooks tab, or directly from supported FortiRecon pages.

The **Action** button in the following FortiRecon modules contains the **Run Automation** option, allowing you to execute compatible playbooks:

- **Attack Surface Management**: Security Issues (EASM), and Leaked Credentials.
- **Brand Protection**: Domain Threats, Social Media Threats, Rogue Mobile Apps, Code Repo Exposure, and Open Bucket Exposure.
- **Adversary Centric Intelligence**: Stealer Infections.

On FortiRecon pages, the system initially displays contextual playbooks. Remove any applied filters to view all available playbooks.

Playbook Types

Security Orchestration features two types of playbooks, each designed for different execution methods:

- **Standalone Playbooks**: You configure and run these playbooks directly from the Security Orchestration module by clicking Run Automation or from action menus on specific pages within other FortiRecon modules. They contain end-to-end steps for complete automation. See Configuring and Running a Standalone Playbook.
- **Contextual Playbooks**: You configure these playbooks within the Security Orchestration module, but you execute them from action menus on specific pages within other FortiRecon modules. These playbooks require input data directly from those FortiRecon modules. For instance, you configure the *Create Ticket for Typosquat Domain Threat Alerts* playbook in Security Orchestration, but you execute it from the *Brand Protection > Domain Threats* page. See Configuring and Running Contextual Playbooks.

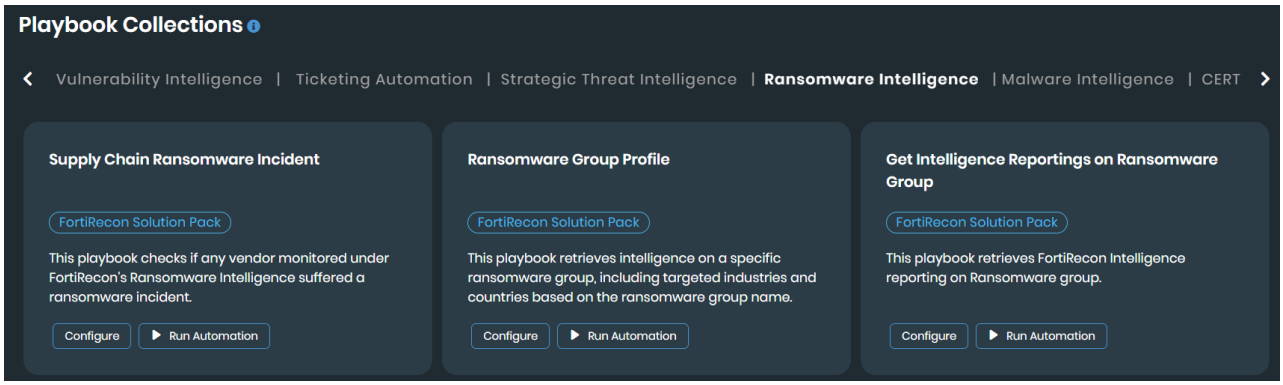
Only users with the FortiRecon Admin role can configure connectors.

Configuring and Running a Standalone Playbook

Follow these steps to configure and run a standalone playbook:

1. Navigate to **Security Orchestration > Home** tab. You can also run predefined playbooks or create and run new playbooks from **Security Orchestration > Playbooks**. See Playbooks.
2. Select a desired collection in the **Playbook Collections** section.

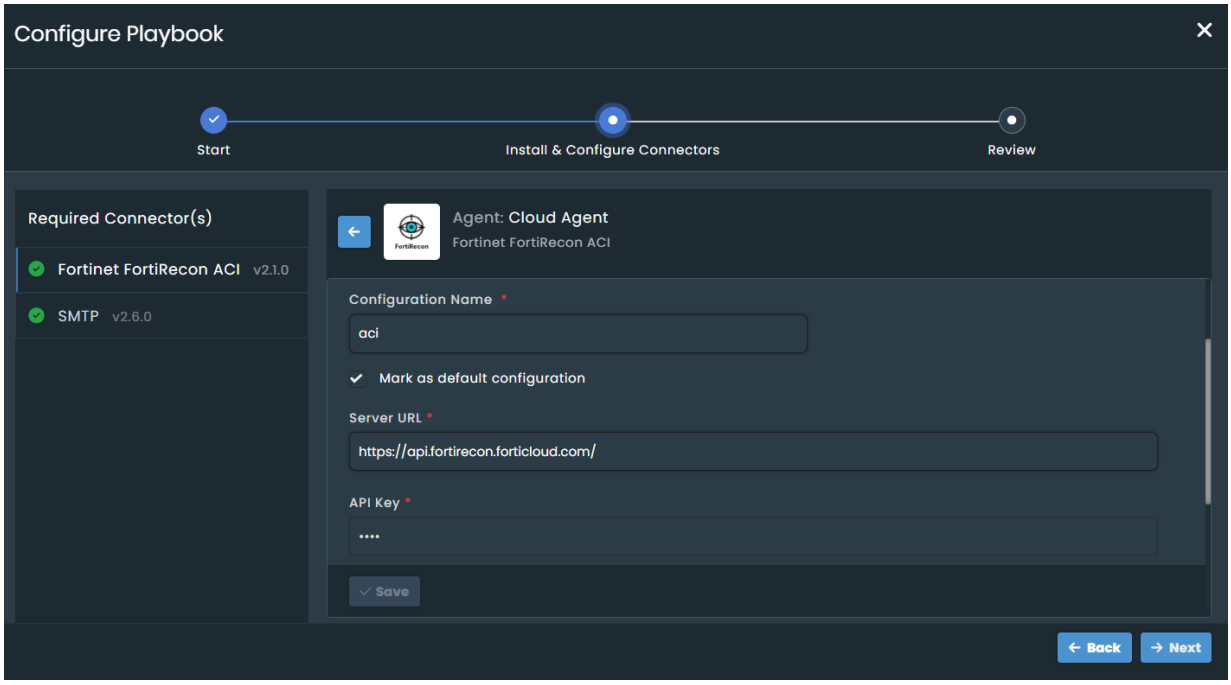
   For example, select the **Ransomware Group Profile** playbook under the **Ransomware Intelligence** collection.
3. Click **Configure**.



4. In the Configure Playbook window, perform the following steps.
   a. Click **Start**.
   b. Configure the required connectors. For example, the **Ransomware Group Profile** playbook requires **Fortinet FortiRecon ACI** and **SMTP** connectors.
      i. The SMTP connector comes preconfigured. If you require a different server, update its configuration.
      ii. For the Fortinet FortiRecon ACI connector, provide the following details:
         - **Configuration Name**: Enter a descriptive name.
         - **Server URL**: The URL `https://api.fortirecon.forticloud.com/`.
         - **API Key** and **Organization ID**: Fetch both details from **Profile Settings > Profile** page.
         - **Verify SSL**: Enable this toggle if required.

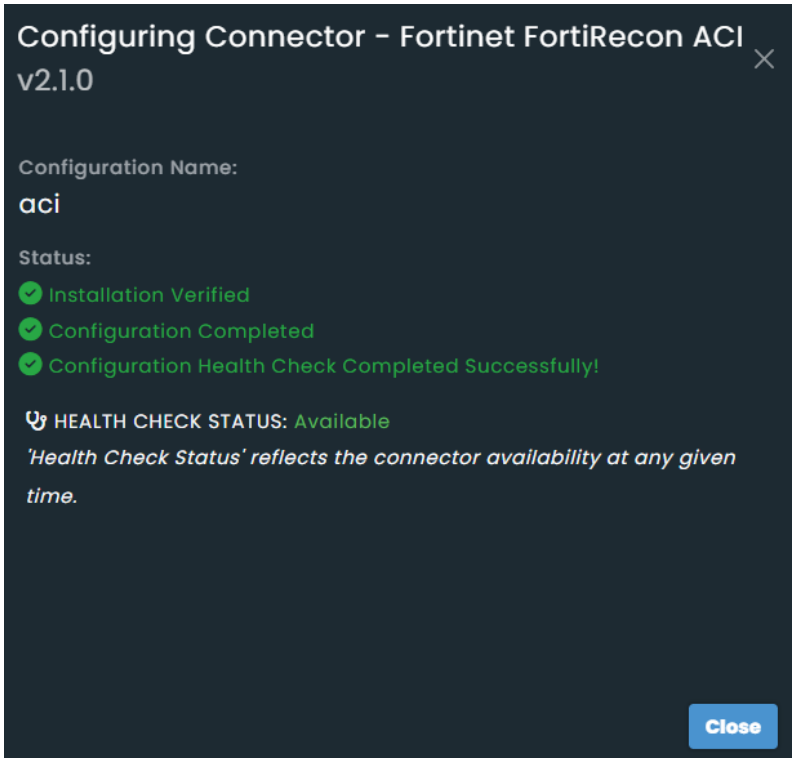
- **Tags**: Add tags if required.

iii. Click **Save**.



For detailed information on configuring connectors, see Connectors.

5. The Configuring Connector status dialog displays information about the configuration process. Ensure the Health Check Status is **Available** to confirm the connector is configured properly. If the status shows **Disconnected**, reconfigure the connector.



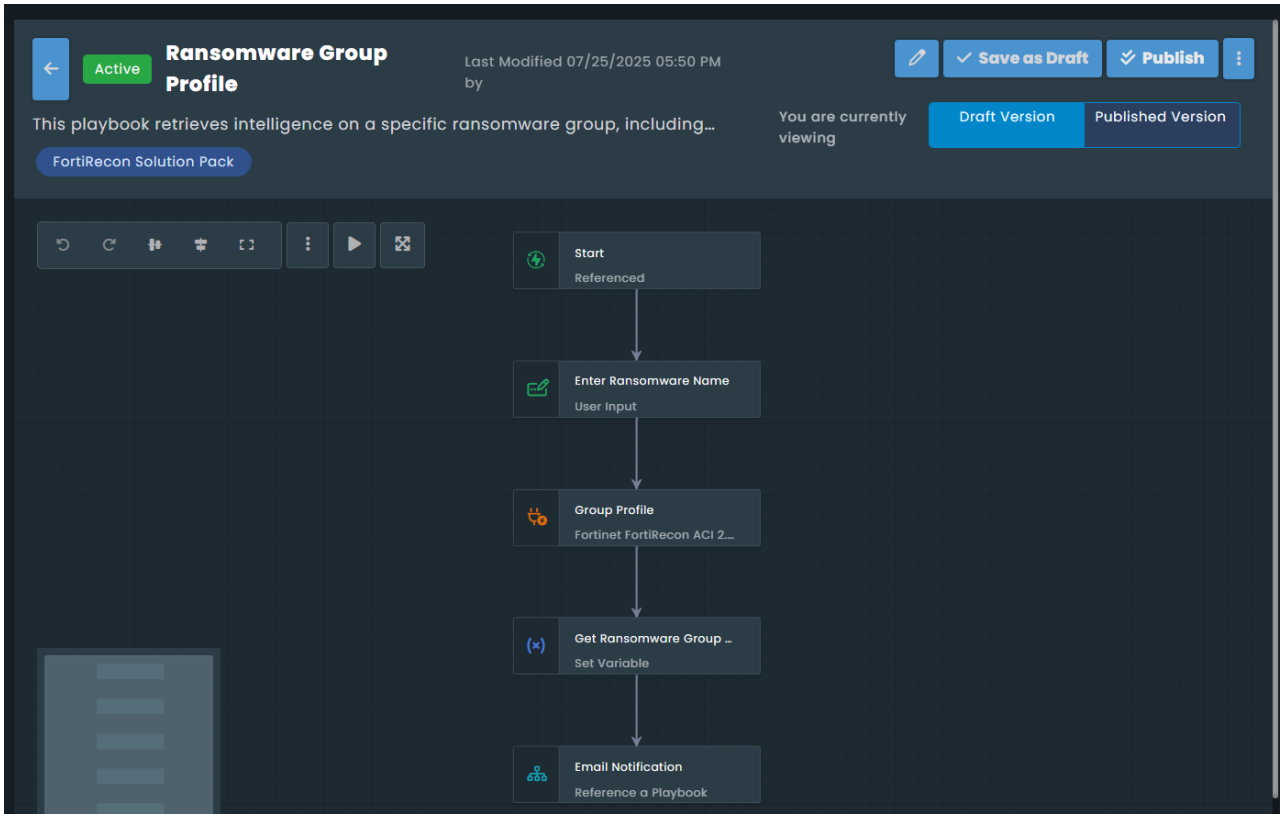
6. Click **Close**.
7. Click **Next** and then **Close**.

> If you configure a connector in one playbook, its configuration becomes available in all other playbooks that use the same connector. You can also configure connectors directly from **Security Orchestration > Content Hub > Installed** tab.

8. Once successfully configured, you can run the automation. Click **Run Automation**.

   The playbook designer window opens, displaying the configured steps. For this example, the playbook begins by prompting you to enter a ransomware group name, then uses the Fortinet FortiRecon ACI connector to fetch relevant data. It then sets a variable with this data and proceeds to send an email notification.

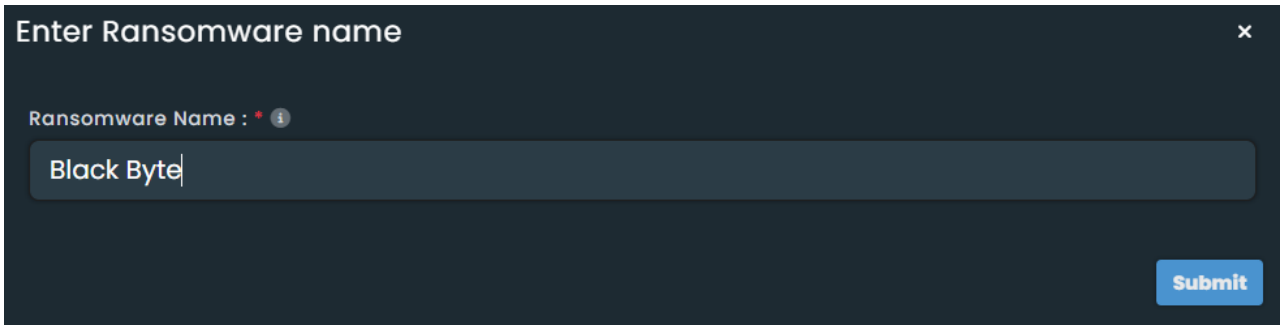
   The Email Notification is a referenced playbook. This referenced playbook starts by using a Utilities connector to convert JSON data to CSV format, then prompts you to enter an email ID, and finally uses an SMTP connector to send the email.



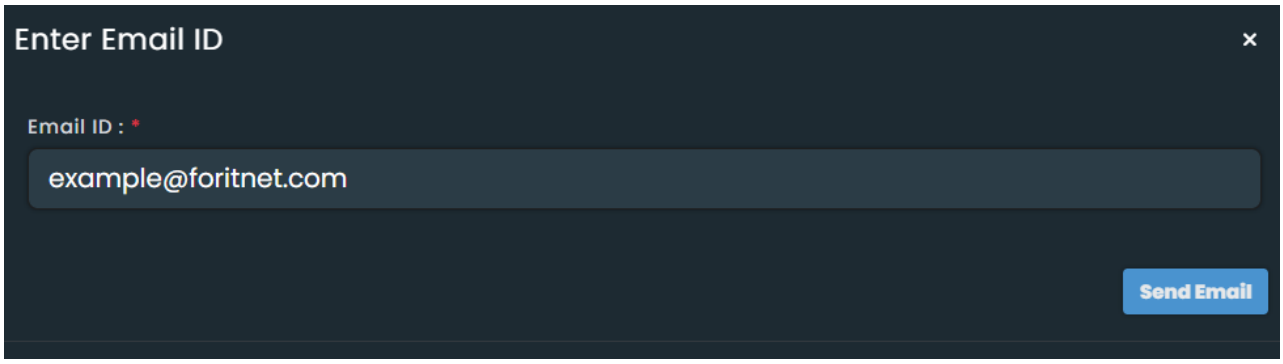
9. Click **Run**.
10. Select **Provide sample input**, leave it blank, and click **Trigger Playbook**. See Playbook Designer.

> You can also execute standalone playbooks from the **Action** menu in supported FortiRecon pages. Remove any applied filters to view all available playbooks.

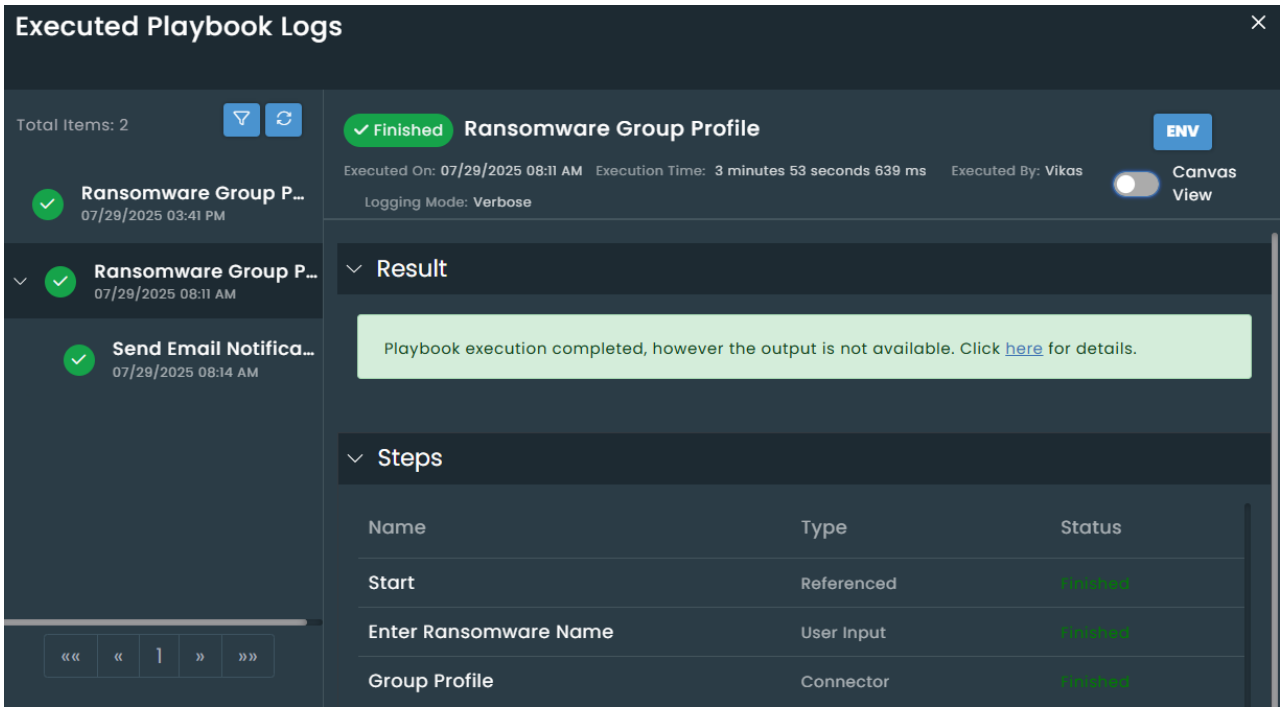
11. For the example, after you click **Trigger Playbook**, an **Enter Ransomware Name** dialog opens. This is a step in the playbook. Enter a ransomware group name (e.g., "Black Byte").



12. A success message displays if the step executes completely. Next, provide an email address in the subsequent step, which is part of the referenced playbook. This step takes your email ID as input, converts the output JSON to CSV, and then sends an email with the CSV attachment to the provided email ID.



13. You can view the details of each step in the execution history, including environment data in the **INPUT** and **OUTPUT** sections. Toggle to the canvas view for a visual representation. See Execution Logs.



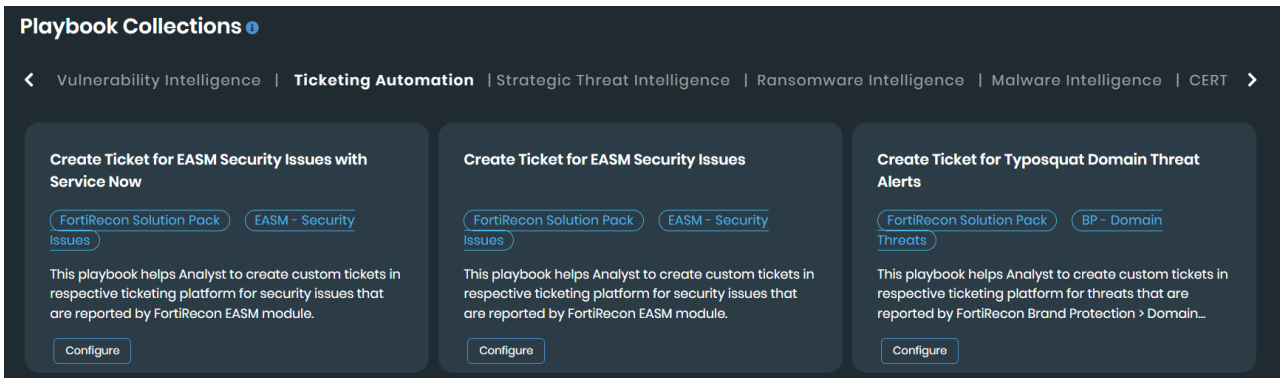
Configuring and Running Contextual Playbooks

Contextual playbooks display only the **Configure** option in the Security Orchestration module. The Run Automation option for these playbooks is available only on specific FortiRecon pages.

You can also run predefined playbooks or create and run new contextual playbooks from **Security Orchestration > Playbooks**. See Playbooks.

For example, to configure and run the **Create Ticket for EASM Security Issues** playbook:

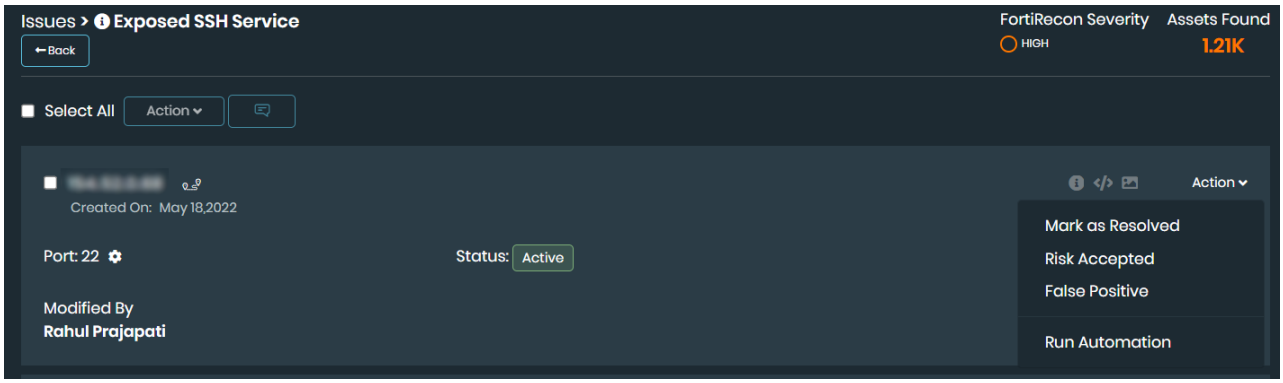
1. Go to the **Ticketing Automation** collection in **Security Orchestration > Home > Playbook Collections** section.



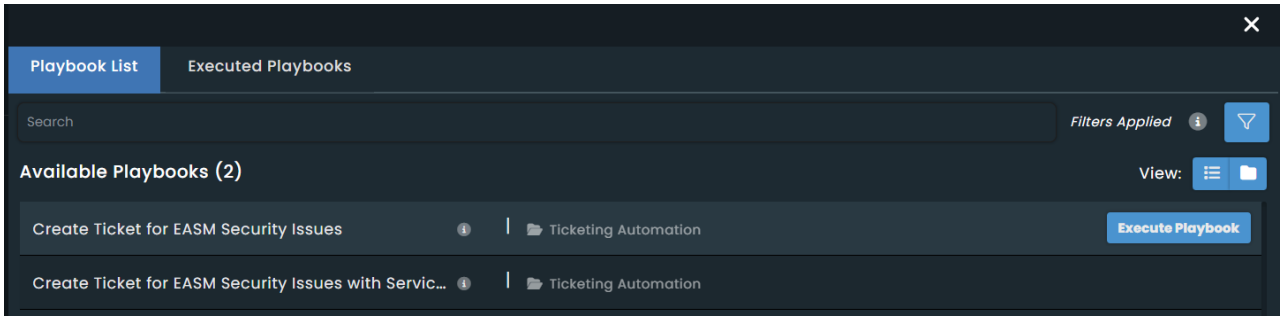
2. Select **Create Ticket for EASM Security Issues**. Click **Configure** and then click **Start**.
3. Configure the Jira connector by providing the necessary information:
   - **Configuration Name**: Provide a name for configuration.
   - **Server URL**: (e.g., https://api.test.atlassian.com/)
   - **Username**: Enter a username with access to the desired project for creating tickets in Jira.
   - **API Token**: Provide the API token for the configured user.
   - **Verify SSL**: Enable this toggle if required.
   - **Tags**: Add tags if required.
4. Click **Save**.
5. Click **Next** after successful configuration, then click **Close**. The playbook is now configured.

> By default, the solution pack includes a Jira connector. However, you can replace this with any other ticketing platform. To check the availability of other ticketing platform connectors, visit **Security Orchestration > Content Hub > Discover**.

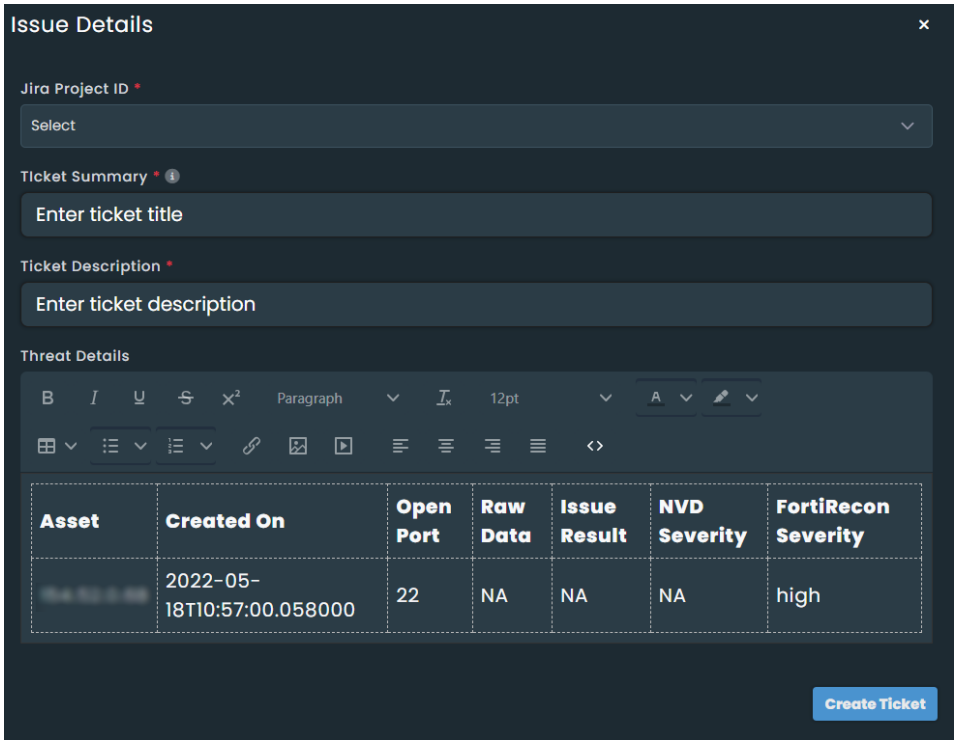
6. To run the playbook, navigate to **Attack Surface Management > Security Issues (EASM)**.
7. Select any issue.
8. Under the **Action** menu, click **Run Automation**. You will see the configured playbook listed.



9. Click **Execute Playbook**.



10. The **Issue Details** input dialog opens. This is a step within the playbook. Provide the required information, select the project ID, enter the ticket summary and description, and then click **Create Ticket**.

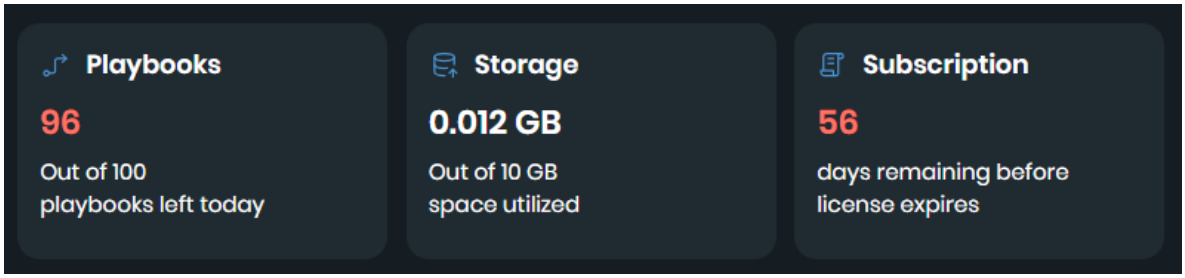


To view the playbook steps, navigate to **Playbooks**, click **Ticketing Automation**, and then click **Create Ticket for EASM Security Issues**.

Home

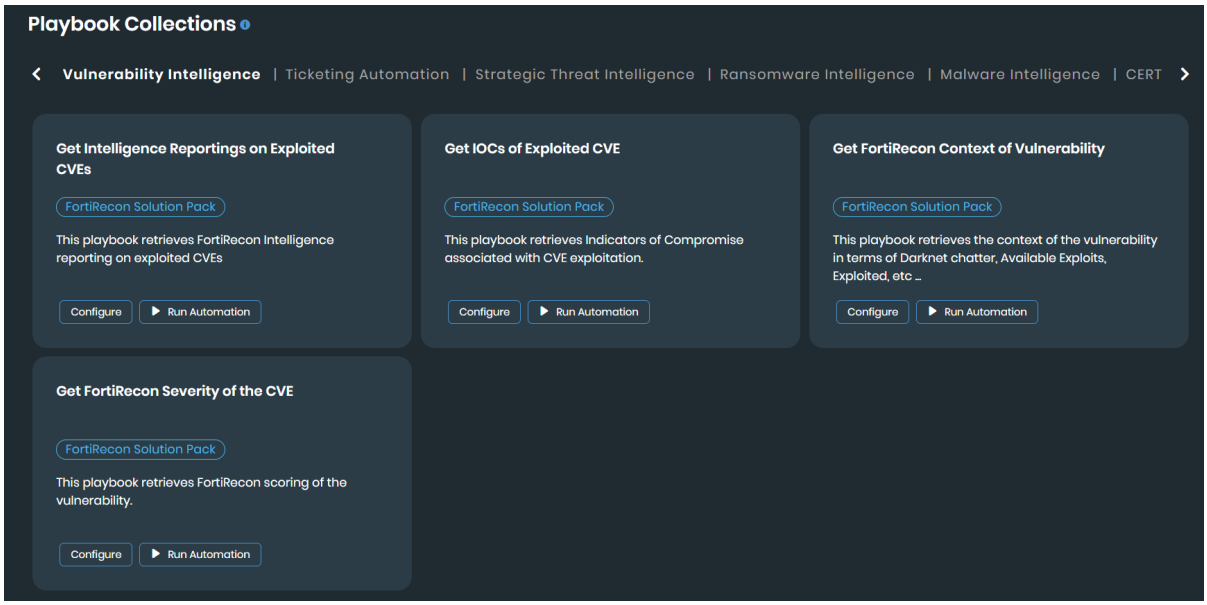
The *Security Orchestration* > *Home* tab provides a quick overview of your usage and available pre-defined playbook collections. The following information cards are displayed.

- **Playbooks**: Displays the number of playbooks you can run in a day and the remaining count. You can execute up to 100 playbooks daily.
- **Storage**: Displays the amount of storage space currently utilized.
- **Subscription**: Displays the number of days remaining before your license expires.



FortiRecon provides the following pre-defined playbook collections that are part of *FortiRecon Automation Service Solution Pack* to help you quickly get started with common security use cases. To use a playbook from these collections, you must first configure the necessary connectors. The following playbook collections are available.

- Vulnerability Intelligence
- Ticketing Automation
- Strategic Threat Intelligence
- Ransomware Intelligence
- Malware Intelligence
- CERT Advisories
- APT Intelligence



Playbooks Overview

The *Security Orchestration* > *Playbooks* tab allows you to create and manage playbooks collections and playbooks. Playbooks automate tasks within the FortiRecon, such as inserting data records, sending email notifications, and determining execution paths based on specified conditions. They are highly configurable, providing consistent and efficient execution of incident response (IR) plans.

- Playbooks Collections
- Playbooks Overview
- Playbook Designer
- Playbook Steps

Playbooks Collections

Playbook Collections help you organize your playbooks. A playbook collection where you group playbooks based on specific strategies in your environment.

You can create new playbook collections or import them in JSON format.

To create a new playbook collection:

1. Click the *Create Collection* + icon.
2. In the *Create Playbook Collection* dialog specify the name of the playbook collection.

   Optionally, you can specify the description for the playbook collection and add keywords in the Tags field. Tags can be used to reference the playbook collections.

   Note: Tags can include special characters and spaces; but the following are not supported: ', , , ", #, ?, and /.
3. Click *Save* to create the playbook collection.

You can perform the following actions on selected playbook collections.

- *Edit* : Update the collection's name, description, or tags.
- *Clone*: Clone the collection, which is saved with the name *%Playbook Collection Name%(1)*.
- *Export*: Export all playbooks in the collections in JSON format.
- *Delete*: Delete the selected playbook collection.

Additionally, to include saved versions of the playbooks by selecting *Yes, include versions* in the *Export with Versions* dialog. Selecting *No, only playbooks* exports only the current version of the playbooks.

Playbooks

Playbooks are sequences of steps designed to automate tasks and achieve specific goals. Playbooks steps are the building block of playbooks that follow a predefined flow to improve investigation and response efficiency.

While designing playbooks, consider:

- What actions are required?
- What conditions need to be addressed (manual vs. automatic)?

- Is looping needed?
- Are there time-senstive requirements?
- What remediation actions can be added?

Common entities in a playbook:

- Triggers
- Actions
- Conditions
- Loops
- Inputs and Output

Playbooks start with a trigger step, followed by various playbook steps to achieve the desired result.

To create a new playbook.

1. Click the Add a new playbook + icon.
2. In the *Create Playbook* dialog, specify the name of the playbook and select the collection in which you want to create the playbook.

   Optionally, provide the description for the playbook and add keywords in the *Tags* field. *Tags* are used reference the playbooks and playbook collections, making it easier to search and filter them.

   Note: Tags can include special characters and spaces in tags; but the following are not supported: ', , , ", #, ?, and /.

   To create a Contextual Playbook, add a tag using the format `Module Name - Page Name`. For example, **EASM - Security Issues**. Suggestions appear as you type the tags. Based on the tag you add, the playbook displays on that specific FortiRecon page.

   You can also add these tags to a playbook collection, which then applies them to all playbooks within that collection.

   The following tags are supported for contextual playbooks:

   Attack Surface Management

   - EASM - Security Issues
   - EASM - Leaked Credentials

   Brand Protection (BP)

   - BP - Domain Threats
   - BP - Social Media Threats
   - BP - Rogue Mobile Apps
   - BP - Code Repo Exposure
   - BP - Open Bucket Exposure

   Adversary Centric Intelligence (ACI)

   - ACI - Stealer Infections

3. If you want to create the playbook in the *Inactive* state, toggle the *Active* option. By default, playbooks are created in the Active state.
4. Click *Save* to create the playbook and open it in the Playbook Designer.

Playbook Actions

The *Security Orchestration* > *Playbooks* page allows you to sort and filter playbooks based on defined criteria. You can also use menu in column headers to autosize columns, clear sort orders, or pin columns.

You can perform the following actions on selected playbooks.

- *Activate/Deactivate*: Set the playbook's status as *Active* or *Inactive*.
- *Clone*: Clone playbooks, which are saved with the name *%Playbook Name%(1)*. You might need to clone a playbook if you want to reuse the playbook as a starting point for a new playbook. Cloning the playbook clones every step within the playbook. You can select more than one playbook to clone at a time.

  Note: If you have cloned a playbook that contains a reference to other playbooks, either within the same collection or in different collections, then the references do not get automatically updated.

  However, if you **simultaneously clone playbooks in the same collection** where either one references the other or they both reference each other, then the references get automatically updated.

  For example, consider a playbook named 'Extract and Enrich Indicators' playbook that references the 'Enrich Indicators' playbook. Now, if you simultaneously clone both the 'Extract and Enrich Indicators' and 'Enrich Indicators' playbooks to create the 'Extract and Enrich Indicators (1)' and 'Enrich Indicators (1)' playbooks, all references in the 'Extract and Enrich Indicators (1)' playbook are updated to 'Enrich Indicators (1)' playbook.
- *Move*: Move playbooks to another existing collection. Clicking *Move* displays the *Move Playbook* dialog. In this dialog, in the Move to collection field, click the *Select Collection* option to display a list of existing collections, from which select the collection to which you want to move the playbooks and click *Submit*.
- *Delete*: Delete the playbooks.
- *Export*: Export playbooks in JSON format, including any associated tags.

  Additionally, to include saved versions of the playbooks by selecting *Yes, include versions* in the *Export with Versions* dialog. Selecting *No, only playbooks* exports only the current version of the playbooks.
- *Change Logging Levels*: Change the logging level for playbooks. Clicking *Change Logging Levels* displays the *Playbook Execution Log Level* dialog. From the *Select Execution Log Level* field, select *VERBOSE* or *MINIMAL* as the logging levels for the playbooks, and click Apply.

> It is recommended to set the playbook logging level to *MINIMAL* for production instances and in scenarios where you want to use storage space efficiently; whereas set the logging level to *VERBOSE* while designing or debugging playbooks since this option can quickly fill up the storage space.

Playbook Designer

The *Playbook Designer* is a visual canvas that allows you to design and edit your playbooks. To open a playbook in the designer, double-click it from the *Security Orchestration* > *Playbooks*page.

Top-bar actions

The Playbook Designer top-bar provides the following options:

- **Edit**: Modify the playbook's details, including:
  - Update its name, description, or tags.
  - Toggle its state between **Active** and **Inactive**.
  - Change the logging level to either **Minimal** or **Verbose**.
- **Save as Draft**: Save a draft version of the playbook without publishing.
- **Publish**: Save and publish the playbook, making the current version available in the system.
- **More Options**: Contains the following additional options:
  - **Save Version**: Save multiple versions of a playbook while creating or updating it. This allows you to revert to a specific version, making the design process more efficient. Clicking **Save Version** opens the `Add Playbook Version` dialog containing a **Note** field where you can add descriptive notes to help identify each version. After adding notes, click **Save** to save the version.

    > A maximum of 10 versions can be saved. If this limit is exceeded, older versions (beginning with the first version) will be overwritten.

  - **View Saved Versions**: View the saved versions. Clicking this option opens the `View Saved Versions` dialog. Click the version name or click **More Options** and choose **Open** to display a `Confirmation` dialog. Clicking **Yes, Confirm** loads the selected version. You can then either click playbook, you can click **Save as Draft** or **Publish** to use this version, or click the version number in the Playbook Designer to select a different version.
  - **Delete Playbook**: Delete the playbook. Clicking this option opens a `Confirmation` dialog on which clicking **Yes, Confirm** deletes the playbook.
  - **Execution History**: View the `Execution Logs` for previous executions of the playbook.

Playbook Designer Canvas actions

Within the Playbook Designer canvas, you can use the following features to design your playbook:

- **Pan and Zoom**: Navigate large playbooks using Pan to scroll and Zoom to adjust the view.
- **Undo** and **Redo** buttons: The **Undo** (`Ctrl+z` on Windows / `Cmd+z` on Mac) and **Redo** (`Ctrl+y`on Windows / `Cmd+shift+z`on Mac) functions are helpful when making frequent changes during playbook creation. Use **Undo** to reverse changes and **Redo** to restore undone actions. Note that **Redo** can only be used after performing an **Undo**.
- **Align Horizontal** and **Align Vertical** buttons: Align the playbook's elements horizontally or vertically using these buttons.
- **Zoom To Fit**: Resize the playbook to fit the browser window.
- **More Options**: Contains the following additional options:
  - **Jinja Playground**: Apply a Jinja template/expression to a JSON input and then render the output. You can check the validity of the Jinja and the output before adding the Jinja to the Playbook.
    The Jinja Playground consists of the following areas:
    - **Jinja Expression**: Define dynamic values within *curly* brackets or click **More Options** to open the `Input/Output` dialog to access variables, inputs, or step results.
    - **Test Data**: Provide JSON inputs in `"Key":"Value"` pairs. Syntax errors will be indicated by a `"Bad String"` prompt. You can define nested key-value pairs.
      After entering the Jinja expression and JSON, click **Execute** to view the result in the `Test Output` dialog. If the result is an object, it will be displayed in the object format instead of a text area.
      The '**Code**' view in the JSON area includes options to:

- **Format JSON Data**: Formats data with proper indentation and breaks.
- **Compact JSON Data**: Compacts data to remove unnecessary whitespaces.
- **Sort Contents**: Sorts contents based on fields in the ascending or descending order.
- **Repair JSON**: Fixes common issues such as incorrect escape characters, quotes, removing comments, etc.
- **Undo**: Reverts the last action.
- **Redo**: Redoes the last action.

- **Input Parameters**: Define input variables to receive data from "Reference Playbook" steps. Use `vars.input.param` to access these within the playbook. Click **Add New** to add a new input variable and then click **Save** to save the parameter.

- **Run Playbook**: Trigger the playbook directly from the designer in '**Verbose**' mode for testing and debugging. This eliminates the need to navigate between the designer and other modules. For details, see Playbook Debugging - Triggering and testing playbooks from the Designer.

Playbook Debugging - Triggering and testing playbooks from the Designer

You can trigger playbooks directly from the Playbook Designer, in the 'Verbose' mode, simplifying the process of testing and debugging while building. This allows developers to edit and run the playbook without needing to navigate to the module, select a record, choose the playbook, trigger it, and then return to the designer for further changes.

> ⚠ Triggering a playbook from the designer starts the execution of the playbook, which can result in changes to your data. Therefore, it is important to review the playbook thoroughly before execution to avoid unintended modifications or data loss.

To trigger the playbook in the Playbook Designer, click **Run Playbook** and then specify the following:

1. Select the reference data source:
   - **Select data from a previous execution**: If you have run the playbook earlier in the 'Verbose' mode, you can choose this option. From the drop-down list, choose a previous playbook run to use its environment to trigger the playbook.
   - **Provide custom JSON as Input**: Provide record data as input using `vars.input.record` or provide custom JSON to trigger the playbook.
2. Select the **Use Step Mock Output** option to execute the playbook with the mock output data that has been added in the steps.
   Only steps such as create record, ingest bulk feed, reference playbook, etc, where 'Mock Output' can be enabled at the step level are supported for enabling mock output at the playbook level. Steps like manual task, wait, approval, and so forth do not support mock output.
3. Click **Trigger Playbook** to run the playbook and review the corresponding *Executed Playbook Logs* for detailed output.

For details about Playbook Steps, which are the building blocks of a playbook, see Playbook Steps.

Playbook Steps

Playbook steps are the foundational elements of playbooks, designed to follow a predefined sequence that enhances investigation and response efficiency. A playbook is built using triggers, actions, and flows.

At the core of playbooks are *steps*, which represent distinct actions or data processing tasks during the playbook's execution. Steps are linked in sequences to define the flow of the playbook, starting with the *Trigger* step. For more information, see Trigger Steps.

Working with Playbooks

Creating a Workflow

To create a workflow in the Playbook Designer, begin by adding a Trigger step, which is saved with connection points. Drag-and-drop a connection point to create a placeholder step and open the `Select Step` dialog, which displays all the available playbook steps. Select a step, configure it according to your requirements, and save it. This step is now connected to the Trigger step. Continue adding and configuring steps based on your use case to complete the workflow. A playbook ends when no further steps remain.

Editing or Removing a Playbook Step

To edit or remove an existing playbook step, double-click the step to reopen it. From there, you can edit the step or delete it by clicking **Delete Step**.

Connecting steps and removing step connections

To connect a playbook step, hover over the step to reveal connection points. Select a connection point and drag the arrow connector to the step you want to link.

To remove a connection between steps, hover over the arrow connector between the steps until a red "X" appears. Click the "**X**" to remove the link.

Actions available within playbook steps

Each Playbook step includes icons for **Info**, **Reference Playbook** (only for the Reference A Playbook step), **Edit**, **Clone**, and **Delete** actions, allowing you to perform various actions directly within the step:

- **Info**: Displays additional information about the step (if available).
- **Reference Playbook** (applicable only to the Reference A Playbook step): Opens the 'Referenced' playbook in a new window. This allows users to view the referenced playbook's contents without losing context of the current playbook's flow.
  NOTE: The **Reference Playbook** will open in a new window only when users select the reference playbook from the **Playbook Reference** drop-down list in the 'References' step and not when user refers to a playbook using Dynamic Values (jinja).
- **Clone**: Creates a copy of the current step and opens this step with the name as `Copy of %Step Name%`. All properties of the original step are copied to the cloned version, which you can edit and save.
- **Edit**: Reopens the step for editing its properties. After making changes, save the step.
- **Delete**: Deletes the step entirely from the playbook.

Playbook actions used for extending playbook steps

Variables

To add a variable to a step, click **Variables** in the footer of the step or use the **Variables** section within the step. Variables allow you to store and access custom expressions within the playbook, for example store the output of the step directly in the step itself, providing flexibility in your playbook design. Therefore, instead of frequently using the `Set Variable` step to o capture specific response data, you can directly use variables within the step itself.

> ⚠ Do not use reserved words, which are listed in the List of reserved keywords section, as variable names.

To insert dynamic values:

- Type `$` and select from the list of suggested variables.
- Select **Input/Output** to search for variables, inputs, and step results
- Select **Functions** to search for and add 'Utility' functions.
- Click **More Options** and choose from the following options:
  - Select **Switch to Advanced Editor** to add jinja for advanced expressions and create complex conditions.
  - Select **Test** to check the validity of the Jinja and the output before adding the Jinja to the Playbook.

Loop

To iterate the playbook step, click the **Loop** link in the footer of the playbook step. There are two types of loops: 'for each' loop and 'do until'.

for each loop

The input for the `for each` loop is an array of objects and the `for each` loop iterates over an array of objects. Use the reserved keyword `item` to access each object in the array. For example, to iterate over indicator objects:
`[{"name":"Indicator Name1"},{"name":"Indicator Name2"},{"name":"Indicator Name3"}]`
Access each object using `vars.item.name`. You can optionally add a '**condition**' to the `for each` loop, based on which the loop to determine when the loop executes.

The 'for each' loop can run in **Sequential** or **Parallel** execution mode. Sequential execution processes one item at a time in a serial manner, while parallel execution uses multiple independent paths to processes items in parallel threads for improved performance.

do until loop

The **do until** loop executes the step at least once and continues to executes the step until the specified condition is met or the retry limit is reached. You can configure the number of retries the playbook step will execute to meet the condition and also the delay in seconds before the step gets re-executed in a loop. By default, the number of retries is set to `3` and delay is set to `5` seconds.
In a do until loop, you can access the current step's result using `vars.steps.<step_name>.keyname` notation. For example, use `vars.steps.<step_name>.message == 'Success'` to retry a connector action until it succeeds.

> Do not use `do until` with `when` or `for_each`.

Condition

To add a condition to a step, click the **Condition** link in the footer of the playbook step. This adds the **When** field where you can define an expression (condition) that determines whether the step executes. If the condition is met, then the playbook step is executed. If the condition is not met, then the playbook step is skipped.

To insert dynamic values, click **More Options**, then choose **Input/Output** to search variables, inputs, and step results, or choose **Functions** to search for and add 'Utility' functions. Choose **Test** to check the validity of the Jinja and the output before adding the Jinja to the Playbook.

> If you use `when` without a `for each` loop, the condition applies to the entire step and it is the first thing that is evaluated for the step. If you use `when` with the `for each` loop, then the condition applies to each item in the loop.

Mock Output

You can use mock output (in JSON format) for a step to simulate real outputs for debugging purposes. Mock output will override the actual step output when the playbook is run.

> To enable mock output, either trigger the playbook with the **Use Step Mock Output** option or add a variable named `useMockOutput` and set its value to '*true*' in the trigger step. If this variable is set to false or not declared, the playbook will use actual step outputs. Also, ensure that you write `useMockOutput` as is since this variable name is case-sensitive.

Ignore Error

You can configure a step to continue executing even if it fails by clicking the **Yes**/**No** button next to **Ignore Error**. If this option is enabled, the status of this step will be `Finished with Error` in the playbook log. To view the log, click the **Executed Playbook Logs** icon at the top-right of the FortiRecon screen. Click the step whose log you want to view, and in the `Step View` section, the status of the playbook is displayed in the `status` item, and the error is described in the `result` item.

List of reserved keywords

Following is the list of reserved words that must not be used as 'Variable' names:

- 'items'
- 'result'
- 'input'
- 'request
- 'values'
- 'keys'
- 'files'
- 'env'

- 'message'
- 'resources'
- 'step_variables'
- 'do_until'
- 'ignore_errors'
- 'when'
- 'for_each'
- 'cyops_playbook_iri'
- 'cyops_playbook_name'
- 'collaborationNote'
- 'inputVariables'
- 'displayConditions'

Trigger Steps

A **Trigger** step defines the starting point of a playbook's execution and is always the first step in a playbook. After the playbook is triggered, it follows the defined steps based on the routes set on the canvas, using the trigger as the starting point.

When you create a playbook, it is initially generated with a placeholder **Trigger** step. Depending on your requirements, you can choose between two trigger methods: Application Event or Referenced .

Application Event

The **Application Event** trigger starts a playbook from either an application event or a scheduled event. Playbooks are triggered when an event, to which they are subscribed, is received. For details on events, see Playbook Assets.

To add a playbook with an Application Event trigger:

1. In the `Playbook Designer`, click **Application Event**.
2. In the `Application Event` dialog search for the event triggers you want to listen to for initiating the playbook.
   Application events are grouped by connector (integration) names. Expand the relevant integration and select the desired application event.
3. In the selected application event dialog, provide the following details:
   a. The **Step Name** field contains the name of the application event. You can optionally click **Add Description** to add a description for the step..
   b. (Optional) To add additional filter criteria to trigger the playbook, such as triggering the playbook only when the event is of a specific type, define the filter conditions in the **Configure Filter Criteria** section.
   c. Toggle the **Enable to configure periodic event polling** option to configure periodic event polling, which pulls content from the third-party integration into FortiRecon at defined intervals:
      i. From the **Target** field, select whether you want to run the action on the **Self Agent** node that is configured by default on FortiRecon or another configured custom agent.
      ii. From the **Configuration** field, select the configuration name to be used for running the action. You can add multiple configurations while configuring the connector.

d. Click the **Edit** icon in the `Configure Connector Action: <Name of the action>` section to view the action parameters used to pull content from the third-party integration. Update the values of parameters as per your requirements.
e. Use the `Schedule` section to adjust the frequency of pulling content from the third-party integration. By default, events are configured with a periodic pull of 5 minutes.
f. Use the `Batch Processing (Looping)` section to select your playbook execution preferences. You can choose between:
   - **Single Execution for Entire Dataset**: Choose this option to run the playbook once for the entire dataset.
   - **Execute in Batches**: For large datasets, this option is recommended for better performance. If selected, then you must specify the batch **Size** for processing.

4. Click **Save** to save the trigger.

Referenced

The **Referenced** trigger is used for playbooks triggered from another playbook using the `Reference a Playbook` step or from a specific schedule. Keep in mind that any dynamic data required for a child playbook during execution must be provided by the parent(s) playbooks.

To add a playbook with a Referenced trigger:

1. In the `Playbook Designer`, click **Referenced**.
2. In the `Referenced` dialog enter the following details:
   a. In the **Step Name** field, type the name of the step.
   b. (Optional) Click **Add Description** to add a description for the step.
   c. (Optional) Add playbook actions, such as Variables Loops, etc., to this step by clicking **Variables** in the playbook step footer. For more information on playbook actions that extend playbook steps, see Playbook Steps.
   d. Click **Save** to save the trigger.

Core Steps

Core steps represent steps that allow you to create and store contextual information relevant to the current playbook.

Set Variable

The **Set Variable** step allows you to create and save variables for use in later steps within the same playbook or across referenced playbooks.

To create a `Set Variable` step:

1. In the Playbook Designer, from the `Select Step` dialog, choose **Set Variable**.
2. In the **Step Name** field, type the name of the step.
3. (Optional) Click **Add Description** to add a description for the step.
4. In the `Variables` section, define the `Name` and `Value` for the variable. Click **Add More** to define multiple variables within the step. For more information on **Variables**, see Playbook Steps.

5. (Optional) Add playbook actions such as Loop (which iterates over the step) by clicking **Loop** in the playbook step footer. For more information on playbook actions that extend playbook steps, see Playbook Steps.
6. Click **Save** to save the step.

Evaluate Steps

Evaluate steps represent steps that facilitate decision-making by allowing users to assess scenarios and provide inputs based on specific conditions.

Decision step

The **Decision** step allows conditional validation within the playbook. You can specify "if this, then that" criteria to direct the flow of the playbook based on the results of a condition. Many organizational processes differ depending on particular criteria, and to accomplish this; you can use the Decision step.

Use the Decision step to enable the playbook to execute a particular path based on defined conditions; "If criteria = x, then do this next step." You can configure the Decision step with a variety of operators (equals, does not equal, <, >, etc.) and chain logical conditions with AND/OR logic to create granular decision-making criteria.

To add a `Decision` step:

1. In the Playbook Designer, from the `Select Step` dialog, choose **Decision**.
2. In the **Step Name** field, type the name of the step.
3. (Optional) Click **Add Description** to add a description for the step.
4. To define a decision step click **Add Condition** or **Add Default Condition**, and then specify the conditions for the decision:
   - Add the Step Name and save the step. Then at a later time add the conditions and corresponding execution steps.
     OR
     Define entire step setting, or workflow, for the decision step, even if the corresponding execution steps are unavailable. This allows you to write the complete logic of the decision and plug in the execution steps later.
     The decision step functions in such a way that it evaluates multiple (alternative) conditions until any of them is fulfilled. This means that when the **Decision** step finds one condition that is fulfilled, then it skips the other conditions.
     Note: The Decision step evaluates conditions sequentially and executes the first condition that is true, skipping the others.
   - **Add Default Condition**: Define default condition or route when no other condition is met. You must select the default step to execute.
5. Click **Save** to save the Decision step.

Wait

The **Wait** step allows you to define a specific delay before the playbook resumes executing its remaining steps. This is useful for time-based escalations, such as missed SLAs.

To add a `Wait` step:

1. In the Playbook Designer, from the `Select Step` dialog, choose **Wait**.
2. In the **Step Name** field, type the name of the step.
3. (Optional) Click **Add Description** to add a description for the step.
4. In the `Playbook will resume after` section, specify the time the playbook waits before executing the remaining steps.
   Enter values in the **Weeks**, **Days**, **Hours**, **Minutes**, and **Seconds** fields based on your requirements.
   To insert dynamic values, type `$` and choose from the list of suggested variables, Input/Output parameters or Functions.
5. Click **Save** to save the Wait step.

User Input

The User Input step displays a custom form to users, allowing them to provide data or provide contextual confirmation to the playbook.

To add a `User Input` step:

1. In the Playbook Designer, from the `Select Step` dialog, choose **User Input**.
2. In the **Step Name** field, type the name of the step.
3. (Optional) Click **Add Description** to add a description for the step.
4. In the `User Input Design` section, click **Edit** to design the form:
   a. In the **Title** field, enter the title for the user prompt.
      To insert dynamic values, type `$` and choose from the list of suggested variables, Input/Output parameters or Functions.
   b. (Optional) In the **Description** field, enter additional information to guide users in providing inputs.
   c. Select form fields to include in the input form. Drag and drop them into the **Drop Buttons Here** area, which displays the properties that are used to configure the form field.
   d. In the `Properties` pane for each form field, enter the field label. Optionally, you can set the default value for the field, and provide more information about the field in the **Tooltip** field. To mark this field as mandatory in the user prompt, select the **Mark this field as required** checkbox.
      After designing the input form, click **Save**.
5. In the `User Input Design` section, click **Medium**to choose the medium for delivering the user input prompt. Also, choose whether the input prompt will be limited to users within FortiRecon or also be accessible to non-FortiRecon users to provide inputs.
   - Select the **Collect input from Internal users** option if you want the user input to be accessible to only FortiRecon users, where they contextually provide inputs based on record information. Then, choose one of the following options to determine who is responsible for responding to the input prompt:
     - **Specific Users**: The user input is visible and actionable by users other than the user who is assigned to the record. When selecting this option, **Select** multi-select list appears allowing you to choose users responsible for making decisions. You can also add custom expressions in this field. You can also select the **Customize email template** checkbox to create a custom email body using a rich text field, instead of using the default template. This allows you to provide context for the input prompt and personalize notifications for each record. You can also include playbook variables using custom Jinja input in the email body.
       Additionally, in the **Attachment IRI List** field, enter an array or a comma-separated list of record IRIs (file IRI or attachment IRI) for attachments you want included in the email.
     - **No specific assignee**: The input prompt is visible and actionable by all users in the FortiRecon system.

- Select the **Collect input from external users** option, if you want to non-FortiRecon users to provide decisions or inputs. In this case, an email with a link to a page containing the input form will be sent to external users. Clicking the link opens the form in a new page, where users can submit their responses. In the **Provide Email Address (es)** field, add email addresses as a JSON list or comma-separated values list, of non-FortiRecon users, who should provide responses. You can also add custom expressions in this field. You can also select the **Customize email template** checkbox to define a custom email body using a rich text field, instead of sending the default template. This allows you to provide context for the input prompt.
  Once you have specified the users who need to provide inputs, click **Save**.

6. Expand the **Escalation** section to define actions for cases where input is not provided within the specified time frame. From the `Do you wish to configure e-based escalation?` section, choose **No** or **Yes**.
   If you choose **No**, then there is no time-based escalation.
   If you choose **Yes**, then:
   - In the **If the decision is not provided within** field, specify the time window within which the input must be provided must be specified. You can specify the time in Days, Hours, or Minutes.
   - From the **The following step will be executed** field, select the escalation step if the time frame is exceeded.
     For example, if you want to send an email notification to the managers, then you can define that step as `Escalation Email` and connect it to the User Input step and select this option in **The following step will be executed** field.
     Once you have defined the escalation steps, click **Save**.
7. (Optional) Add playbook actions, such as Variables Loops, etc., to this step by clicking **Variables** in the playbook step footer. For more information on playbook actions that extend playbook steps, see the Playbook Steps chapter.
8. Click **Save** to save the User Input step.

Execute Steps

Execute steps represent steps that allow playbooks to perform automated operations.

Connector

Use the **Connector** step to add connectors,or third-party integrations, to your playbook. Connectors, such as Fortinet EDR and Fortinet FortiSIEM, enable retrieval of data from custom sources and perform automated operations. FortiRecon includes built-in connectors, such as SMTP, which are pre-installed and used to perform actions such as sending emails.

> To add a 'Connector' step, that connector must be configured in the FortiRecon system.

To add a `Connector` step:

1. In the Playbook Designer, from the `Select Step` dialog, choose **Connector**.
2. On the Connector dialog, enter the name of the connector in the **Search Connectors** field, then select the connector.
3. In the selected connector dialog, provide the following details to configure the connector:
   a. In the **Step Name** field, type the name of the step.
   b. (Optional) Click **Add Description** to add a description for the step.

   c. From the **Target** field, select whether you want to run the action on the **Self Agent** node that is configured by default on FortiRecon or another configured custom agent.
   d. From the **Configuration** field, select the configuration name to be used for running the action. You can add multiple configurations while configuring the connector.
   e. From the **Action** field, select the action you want to perform using the connector.
4. (Optional) Add playbook actions, such as Variables Loops, etc., to this step by clicking **Variables** in the playbook step footer. For more information on playbook actions that extend playbook steps, see the Playbook Steps chapter.
5. Once you have completed configuring the connector, click **Save** to save the step.

Utilities

Use the **Utilities** step to run various utility functions and scripts that come built-in. You can add the Utilities step to your playbook in the same way as the Connector step.

Utilities include functions such as:

- **Utils: Make REST API Call**: Makes a RESTful API call to a valid URL endpoint.
- **Utils: Convert JSON into an HTML table**: Converts input JSON into an HTML-formatted string . You can also select the layout of the converted HTML table to be either Vertical or Horizontal (default).
- **FSR: Extract Artifacts from String**: Extracts artifacts (indicators) from the provided string.

References

References represent steps that help create a chain of playbooks.

Reference a Playbook

Use the **Reference a Playbook** step to trigger another playbook within the current playbook, creating a chain of multiple playbooks. This step allows you to call any playbook in the system, whether active or inactive, by name.

To add a `Reference a Playbook` step:

1. In the Playbook Designer, from the `Select Step` dialog, choose **Reference a Playbook**.
2. In the **Step Name** field, type the name of the step.
3. (Optional) Click **Add Description** to add a description for the step.
4. From the **Playbook Reference** field, choose the playbook you want to reference from the list of available playbooks across all playbook collections in the system.
5. From the **Parent Data Reference** field, choose what data the parent playbook will pass to the referenced playbook:
   - **Full ENV**: Pass the complete environment data from the parent playbook to the reference playbook. This allows the referenced playbook to access any dynamic variable from the parent playbook and use it just as it is being used in the parent playbook.
   - **Pass Input Record Only**: Pass only the record inputs available under `vars.input.records` from the parent playbook to the reference playbook.
   - **Not Required** (default): Prevents any data of the parent playbook from being passed to the reference playbook. This is useful when you want to avoid unnecessary data passing, such as when the

referenced step loops on lot of items or when the playbook is run in the debug mode, consuming memory and database space.

6. (Optional) Add playbook actions, such as Variables Loops, etc., to this step by clicking **Variables** in the playbook step footer. For more information on playbook actions that extend playbook steps, see the Playbook Steps chapter.
7. Click **Save** to save the step.

Send Email

Use the **Send Email** step to automatically send an email to the user(s) identified in the step. The email can include either static criteria or dynamic data relevant to the record that triggered the playbook. If the email needs to reflect entity-specific data, use *dynamic values* in the fields.

To add a `Send Email` step:

1. In the Playbook Designer, from the `Select Step` dialog, choose **Send Email**.
2. In the **Step Name** field, type the name of the step.
3. (Optional) Click **Add Description** to add a description for the step.
4. From the **Select Target** field, select whether you want to run the action on the **Self Agent** node that is configured by default on FortiRecon or some other custom agent that you have configured.
5. From the **Configuration** field, select the configuration name using which you want to run the action.
   You can create multiple configurations while configuring the connector.
6. From the **Action** field, select the action that you want to perform:
   - **Send Email (Advanced)**: Choose this option to send an email with Jinja and email template support. This allows you to customize the email body type, content, and other input parameters. You can send the email in one of the following formats:
     Plain Text: A simple, unformatted email.
     Rich Text: An email with formatted content, images, and custom Jinja expressions using dynamic values.
     Email Template: Choose an existing email template to build upon, ensuring consistency and avoiding unnecessary rework.
     Recipients can be specified as:
     - A comma-separated list of email addresses, including those of non-FortiRecon users.
     - The IRI values for users and/or teams, which allows reuse of user/team information from previous playbook steps as Jinja statements.
     - Select FortiRecon users/teams by choosing from a pre-populated drop-down list containing 30 most recently created users/teams in the To, CC, and BCC fields. This allows users to dynamically utilize the email IDs already provided in user or team records.
   - **Send Email**: Choose this option to send a **Rich Text** email, which can include formatted content, images, and even custom jinja expressions using Dynamic Values.
     In this option, specify email addresses in a list or CSV format in the recipient fields.
     For details, see the SMTP Connector document.
7. (Optional) Add playbook actions, such as Variables Loops, etc., to this step by clicking **Variables** in the playbook step footer. For more information on playbook actions that extend playbook steps, see the Playbook Steps chapter.
8. Click **Save** to save the step.

Playbook Assets

The *Security Orchestration* > *Playbook Assets* page allows you to create and manage *Global Variables* and *Event Templates*.

Global Variables

Global Variables are variables that can be used across multiple playbooks. Once declared, a global variable can be referenced in any playbook, eliminating the need to redefine it each time.

To create a global variable:

1. Navigate to **Security Orchestration > Playbook Assets** > **Global Variables**.
2. Click **Create New**.
3. In the `Create Global Variable` dialog, enter the following details:
   a. In the `Variable Name`, enter the name of the variable.
   b. In the `Field Value` field, enter the value for the variable.
   c. (Optional) In the `Default Value` field, enter a default value to be used if no value is provided by the user.
   d. Click **Save** to create the global variable.

> Variable Names must start with a letter and can only contain letters and numbers. Special characters and spaces are not allowed.

To ensure the correct hostname appears in email links sent by System Playbooks, update the `server_fqhn` global variable. To update its value:

1. In the `Global Variables` list, click the **Edit** icon in the **Actions** column in the `server_fqhn` global variable row.
2. In the `Field Value` field, enter the appropriate hostname value. Optionally, add a default value,
3. Click **Save**.

If the hostname is not specified in the global variables, the default hostname used during FortiRecon installation will be included in the email. Ensure the `server_fqhn` global variable is used in the **Send Email** step of your playbook.

Event Templates

An event template defines events that trigger playbooks. By default, event templates are **event-driven** and use the provided Web Hook API to trigger playbooks when an event, to which the playbook is subscribed, is received. You can also modify event templates to fetch content periodically according to a set schedule.

In the FortiRecon UI, events are created using installed connectors, which typically include pre-built event templates. For example, the FortiSIEM connector provides an event template, "When an incident is created",

which triggers playbooks when a FortiSIEM incident is created. You can further edit this template to configure periodic polling. You can also Creating Custom Event Templates.

Event templates also provide a simulation feature, allowing you to test the event template and associated playbook using sample data provided with the event template.

Web Hook API

Events can be posted by calling the following API endpoint:

```
METHOD: POST
URL: https://{HOSTNAME}/api/workflow/trigger/events
BODY:
{
"eventId":"fortinet-fortisiem.get_incidents_created",
"data": [
  {
    "eventType":{},
    "incidentID:{},
    "eventSeverityCat":HIGH
  }
]
```

Users can add a filter criteria as:

```
# Condition attribute from UI
filters:
  {
    eventSeverityCat:HIGH
  }
}
```

The `eventId` must match the identifier defined in the event template. It is used to correlate with playbooks and filters.

Creating Custom Event Templates

To create a custom event template, follow these steps:

1. Navigate to **Security Orchestration > Playbook Assets** > **Global Variables**.
2. Click **Create New Event Template**.
3. In the `Create Event Template` dialog:
   a. In the **Event Template Name** field, enter a descriptive name that reflects the event triggering the playbook.
   For example, if the playbook should be triggered when a ticket is created, then the event template name can be added as "**Get Created Tickets**".
   b. The **Event Identifier**: Gets auto-populated based on the event template name.
   For example, if the event template name is added as "Get Created Tickets, the identifier will be set as "`Get.Created.Tickets`
   An event identifier provides the correlation with the playbooks and filters.
   c. (Optional) Click **Add Event Description** to provide additional details about the event.

4. (Optional) In the **Configure Filter Criteria** section, set conditions to trigger the playbook based on specific criteria. You can also define conditions when the event is used in a playbook.
   For example, triggering the playbook only when the event is of a specific type.
   To view sample events in JSON format click **View Sample Events**, which displays the **Sample Events** panel.
5. To ensure the event template is set up correctly and can process events, create a playbook that uses the template and click the **Simulate** button on the **Sample Events** panel.
6. **Configure Periodic Event Polling**:
   a. Toggle the **Enable to configure periodic event polling** option to fetch content from third-party integrations at defined intervals.
   b. In the **Connector** field, select the connector to use for triggering the playbook. For example, *Fortinet FortiSIEM*.
      Note: The connector must be installed for it to be listed in the **Connector** field.
   c. Configure the connector/connector parameters:
      - If using an included event template, such as from FortiSIEM, then the action based on which events would be fetched would already be selected and you need only configure the parameters as per your requirements.
        For example, for the *List Incidents* action of the Fortinet FortiSIEM connector, click the **Edit** icon in the `Configure Connector Action: List Incidents` section and configure the required parameters, such as, From Date, To Date, Incident Status, etc. These parameters will determine which incidents are fetched from Fortinet FortiSIEM.
        For custom templates, you must specify both the action, and the parameters used to fetch the events. In this case, click the **Edit** icon in the `Configure Connector Action` section, and from the **Select action** list. Based on the action selected, the input parameters will be populated. Configure these parameters to fetch content as per your requirements.
   d. Use the `Schedule` section to adjust the frequency of fetching content from the third-party integration.
7. (Optional) Use the `Batch Processing (Looping)` section to select your playbook execution preferences. Choose one of the following playbook execution options:
   a. **Single Execution for Entire Dataset**: Run the playbook once for the entire dataset.
   b. **Execute in Batches**: Recommended for large datasets to optimize performance. If selected, specify the **Batch Size** for processing.
8. Click **Save** to save the event template.

The **Application Events** trigger playbooks from either application events scheduled events. For details, see the Trigger Steps chapter.

Content Hub

The *Security Orchestration* > *Content Hub* tab allows you to access, install, and manage out-of-the-box reference material and product add-ons such as connectors, widgets, and solution packs, to help you effectively use FortiRecon Security Orchestration.

Viewing Content Hub

To access the `Content Hub` page, navigate to Security *Orchestration* > *Content Hub*. The `Content Hub` page consists of the **Filters** panel on the left and the **Discover** and **Installed** tabs.

You can perform the following actions on the `Content Hub` page:

- **Search**: Search across all the tabs.
- **Sort**: Sort the content alphabetically (A-Z) or by release date.
- **Filter**: Filter the content by type: All, Certified, or Featured.
- **Show All**: Display all content in specific categories: Solution Packs, Widgets, and Connectors.

Using the **Filters** panel, you can filter content across tabs. To clear all filters, click **Clear All**, or clear individual filters by clicking the **Clear** button next to each category. You can use the **Search** box within each filter criterion to search for specific content. The Filters panel can be collapsed or expanded by clicking the **<<** arrows. If multiple filters are applied, the **Filtered By** list will display all active criteria.

Use the **Filter** panel narrow down the displayed content. You can filter by:

- **Content Type**: Filter by the content type. Currently, Connectors, Solution Packs, and Widgets are the add-on content types present in FortiRecon.
- **Category**: Filter by the content's functional category. Examples of categories are Breach and Attack Simulation, Content Management, Data Enrichment & Threat Intelligence, Endpoint Security, Malware Analysis, etc.
- **Publisher**: Filter by the publisher of the add-on. The add-ons can be developed and published by Fortinet or Community (anonymous) or by various contributors such as Bay Dynamic, EclecticIQ, etc.

The `Content Hub` page contains the following tabs:

- **Discover**: Displays all available add-ons.
- **Installed**: Displays all add-ons that you have installed.

Discover Tab

The **Discover** tab displays all the content that are available in the Content Hub. Click a tile to open the content's dialog and view detailed information about the add-on, including summaries for solution packs and widgets, or installation instructions for connectors.

Installed Tab

The **Installed** tab displays all of your content, i.e., all the content that you have installed on the FortiRecon instance. You can search for an add-on by its name in the **Search** box and sort the content either alphabetically or by release date. If any add-on has an available update, an orange **Update Available** bar will appear on its tile. To filter installed content by updates, select **Filter By: Updates Available** from the drop-down list.

Connectors

Connectors allow you to send and retrieve data from various third-party sources, enabling you to integrate with external cybersecurity tools and automate interactions using playbooks. FortiRecon provides several pre-installed connectors, such as the Utilities and SMTP connectors, which can be added in FortiRecon playbooks, as a connector step, to perform automated operations.

Each connector includes documentation that covers installation, configuration, and usage. See FortiSOAR Connectors.

Viewing Connectors

To view connectors, go to **Security Orchestration > Content Hub** tab. On the `Content Hub` page, select **Connectors** from the **Filter** panel to see all currently available connectors.

You can search for a connector using the **Search** field and sort the results alphabetically (A-Z) or by release date. Installed connectors are marked with a green check and the word 'Installed' on their card.

Working with Connectors

On the `Content Hub` page, from the **Filters** panel, select the **Content Type** as **Connectors** to view the list of available connectors. Click a connector 's tile to open its details, which include the **Summary**, **Actions**, and **Installation** tabs:

- **Summary Tab**: This tab provides information about the SP publisher, its certification and featured status, a brief description, and its category.
- **Actions Tab**: This tab lists the actions the connector can perform.
- **Installation Tab**: This tab displays the **Agents** where the connector can be installed. By default, a **Self Agent** node is configured on FortiRecon in which connectors are installed. You can also configure another custom agent.
  Choose an **Agent** and click **Install** to install the connector and its dependencies. This action opens the connector's dialog on the **Configuration(s)** tab, where you can Configuring a connector for use in FortiRecon.

Managing Connectors

The **Installed** tab displays the installed connectors and allows you to manage them. Select a connector in the **Installed** tab to opens the connector's dialog on the **Agents** tab. Here, you can add a configuration by clicking **Add Configuration**, which will open the **Configuration (s)** tab. On the **Configuration (s)** tab you can:

- Configuring a connector.
- Click **Uninstall** to uninstall the connector.

Configuring a connector

> Only users with the FortiRecon Admin role can configure connectors.

To configure a connector, either:

- Configure it immediately after installation by selecting the **Configuration(s)** tab in the connector's dialog.
- On the **Installed tab**, select the connector you want to configure, to open the connector's dialog on the **Agents** tab. Here, you can add a configuration by clicking **Add Configuration**, which will open the **Configuration (s)** tab.

> If a connector, such as the SMTP connector, is pre-configured, it will display a button showing the number of configurations available (e.g., 1 Configuration(s) Available). Clicking this button opens the Configuration(s) tab with the current configuration details and the **Add New Configuration** button which you can use to add a new configuration of a connector.

On the **Configuration (s)** tab, configure the connector as follows:

1. In the **Configuration Name** field, enter a unique name for the configuration. You can add multiple configurations, but each must have a unique name.
2. Check the **Mark As Default Configuration** option to set the selected configuration as the default for the connector on the FortiRecon instance. At least one configuration must be marked as default for the connector to function.
3. Each connector contains different fields for configuration. For detailed information, to the connector's specific documentation.
   Note: The `password` type fields such as password, client ID, etc. will be masked for security purposes.
4. Once you have completed adding all the details, click **Save** to save the connector configuration.

Additionally, on the **Configuration (s)** tab, you can perform the following operations:

- **Update Available**: If a newer version of the connector is available, click **Update Available** to upgrade the connector.
- **Active**: Toggle **Active** to activate or deactivate the connector.
- **Uninstall**: Click **Uninstall** to uninstall the connector.

Widgets

Widgets are simple, easy-to-use software applications designed to perform specific tasks. These independent applications can be embedded into websites and include examples such as event countdowns, visitor counters, and clocks.

Viewing Widgets

To view widgets, go to **Security Orchestration > Content Hub** tab. On the `Content Hub` page, select **Widgets** from the **Filter** panel to see all currently available widgets.

You can search for a widget using the **Search** field and sort the results alphabetically (A-Z) or by release date.

Working with widgets

On the `Content Hub` page, from the **Filters** panel, select the **Content Type** as **Widgets** to view the list of available widgets. Click a widget's tile to open its details, which include the **Summary** and a **Contents** tab.

- **Summary Tab**: This tab provides details about the widget's publisher, its certification and featured status, and a brief description. Additionally, it contains a **Install** button using which you can install the widget.
- **Contents Tab**: This tab contains more information about the widget including its feature list.

Managing Widgets

The **Installed Tab** displays all installed widgets and allows you to manage them. Selecting a widget in the **Installed** tab opens the widget's dialog; click **Uninstall** to uninstall the widget.

Solution Packs

FortiRecon uses modular architecture, and solution packs implement best practices for configuring and optimizing its use. These packs also include sample, simulation, and training data, allowing you to experience FortiRecon without needing all the physical devices. The *FortiRecon Automation Service* solution pack provides essential components like use case playbooks, connectors, and widgets to help users get started quickly and effectively.

Accessing Solution Packs

To access solution packs, go to **Security Orchestration > Content Hub** tab. The `Content Hub` page will open, where you can select **Solution Packs** from the **Filter** panel to view all available solution packs.

You can search for a solution pack using the **Search** field and sort the results alphabetically (A-Z) or by release date. The **Filters** panel allows you to filter packs by various criteria. Installed solution packs (SPs)are marked with a green check and the word *Installed* on their card. Some SPs feature a green medal icon, indicating they are essential for the seamless operation of FortiRecon. These are highlighted as Featured SPs.

Working with Solution Packs

On the `Content Hub` page, from the **Filters** panel, select the **Content Type** as **Solution Packs** to view the list of available SPs on the **Discover** tab. Click a solution pack's tile to open its details, including the **Summary** and **Contents** tabs.

- **Summary Tab**: This tab provides information about the SP publisher, its certification and featured status, a brief description, and its category. It also contains a prerequisites section that lists any other solution packs that must be installed and dependencies that are fulfilled during installation. Additionally, it contains a **Install** button using which you can install the solution pack.
- **Contents Tab**: This tab lists the roles, rules, playbook collections, widgets, connectors, and other components included in the solution pack.

Managing Solution Packs

The **Installed Tab** tab displays the installed solution packs and allows you to manage your installed content. Selecting an SP in the **Installed** tab opens the SP's dialog; click **Delete Template** to uninstall the solution pack.

Agents

FortiRecon's Security Orchestration module supports segmented networks, enabling the secure remote execution of connector actions across multiple network segments. This functionality is essential for investigating within multi-segmented networks. Use an Agent when you need to run connector actions remotely.

The **Security Orchestration > Agents** tab allows you to create and manage Agents.

Recommended Resource Requirements for Agents:

Ensure your system meets the following minimum resource requirements for Agents:

- 1 GB RAM
- 1 vCPU
- 16 GB of available disk space
- Rocky Linux 9.3/9.4/9.5 or Red Hat Enterprise Linux (RHEL) Server 9.3/9.4/9.5.

Prerequisites for installing an Agent

Before installing an Agent, ensure the following:

- The VM where you plan to install the Agent can reach or resolve `repo.fortisoar.fortinet.com`.
- The VM has outbound access to FCP on ports 443 and 5671.

High-level steps to install the Agent

1. Navigate to **Security Orchestration > Agents** tab.
2. Click the **+** icon to add a new Agent.
3. In the **Create Agent** window, provide a **Name** and **Description**. Click **Create**.
4. Click **Download Installer** to download the Docker Compose file.
2. Add the `extra_hosts` entry.
3. `SCP` the docker compose file to the collector.
4. SSH to the collector and run the following commands:
   a. `docker-compose -f docker-compose-agent.yaml build --no-cache`
   b. `docker-compose --project-name xf-agent -f docker-compose-agent.yaml up --detach`

Execution Logs

As you develop more advanced Playbooks, the ability to easily debug them becomes essential. The *Security Orchestration* > *Execution Logs* tab allows you view results and debug executed playbooks with ease.

The Execution Logs display the executed playbooks in the flowchart format, similar to the playbook designer. This layout makes it easier to follow playbook execution, especially for viewing the parallel execution paths.

Using Execution Logs

Accessing Execution Logs

To view the logs and results of executed playbooks:

- Navigate to **Security Orchestration** > **Execution Logs** tab to view the logs for all executed playbooks.
- In the Playbook Designer, click **More Options** > **Execution History** in the playbook designer to view the execution history of a specific playbook.

Navigating Logs

- Playbooks are listed in the Executed Playbook Logs left pane, sorted chronologically, with the most recent playbook execution displayed first.
- Pagination allows easy navigation through the logs. By default, **10** playbooks are shown per page.
- Select a playbook in the list to view it in the flowchart format.
- Playbooks are organized by parent-child relationships. You can click on a parent playbook to view its child playbooks.

Playbook Log Features

- **Filtering**: You can filter logs by Playbook Name or Record IRI, user, date range, status, or tags. For more information, see Filtering Playbook Execution Logs.
- **Refreshing**: Click the **Refresh** icon to update the playbook logs.
- **Execution History**: The Execution History section shows
  - Total number of executed playbooks.
  - Playbook execution details, including date, time, duration, mode (Minimal or Verbose), and execution status.
  - The user who triggered the playbook (under "Executed by").
  - Playbook step details, including completed, pending, failed, and skipped steps.
  - Status icons indicating the current playbook state. For example, a green checkmark for completion, orange pause for awaiting action, red cross for failure, etc.

Viewing Playbook Details

To open a playbook from the logs, click **Edit Playbook**. To view the complete environmental context in which the playbook was executed, click the **ENV** button. In *Verbose* mode, this will display input-output and computed variables across all playbook steps. In *Minimal* mode, only the status is shown.

Filtering Execution Logs

Click the **Filter** icon to a Filter options dialog where you can add the following filter criteria for filtering playbook logs and then click the **Apply Filter** button:

- **Playbook Name**: Filter by Playbook Name or Record IRI. In the **Search by Name or Record IRI** field, filter the log associated with a particular playbook, based on the playbook name or the record IRI associated with the playbook.
  Example of filtering logs using the Record IRI: `/indicators/bd4bf0a6-b023-4bd7-a182-f6938fa37ada`.
- **From Date**: Filter by the execution date from which the playbooks were executed.
- **To Date**: Filter by the execution date till which the playbooks were executed.
  Using the **From Date** and **To Date** fields, you can create a data range for retrieving the logs of playbook executed during that time period.
- **Run By**: Filter by the user who triggered the playbook. Select a user from the **Run By** drop-down list.
- **Status**: Filter by execution status. Select from the following statuses: Incipient, Active, Awaiting, Paused, Failed, Finished, Skipped, Terminated or Finished with error.
- **Filter By Tags**: Filter by tags or keywords associated with the playbook.

Click **Clear Filters** to remove any applied filters.

Terminating playbooks

Playbooks that are in the **Active**, **Incipient**, or **Awaiting** state can be terminated. You might want to terminate playbooks if there have configuration errors, or were triggered incorrectly, etc.

To terminate a running playbook instance:

1. Click **Automation** > **Playbook Execution Logs**.
2. In the `Executed Playbook Logs`, from the playbook listing, select the playbook to terminate and click **Terminate**
3. In the `Terminate Execution` dialog choose:
   - **Terminate Current**: Terminate only this particular running instance of the playbook.
   - **Terminate All**: Terminate all running instances of the playbook.
     Clicking the appropriate terminate option, changes the state of the playbook to '`Terminated`'

If needed, you can rerun the playbook from the point where it was terminated by clicking the **Rerun Pending Steps** button.

Execution Logs - Step Details

To view details for a specific playbook step in the Playbook Execution Logs, Select the playbook and then the specific step. You will see tabs associated with the playbook step: **Input**, **Pending Inputs** (if the playbook is in the awaiting state), **Output** (if the playbook finishes) or **Error** (if the playbook fails), and **Config**.

Input Tab

The input tab displays data for the first step of the playbook, such as the `Start` step. It shows input arguments and evaluated arguments. The `data` section displays the trigger information for the playbook. The `input_args`

section isplays the user-entered input in Jinja format, while the `evaluated_args` section shows how the user input was evaluated by the playbook once the step is executed.

Pending Inputs Tab

If a playbook is in an "Awaiting" state, meaning it requires user input or a decision to continue its workflow, the **Pending Inputs** tab is displayed. Once the user provides the necessary input and submits their action, the playbook resumes execution according to the defined workflow.

Output or Error Tab

If a playbook step completes, the **Output** tab displays the result/output of that step. For user input steps, it also shows the `username` of the user who provided the input, which led to the resumption of the playbook.

If a playbook step fails, the **Error** tab displays the **Error message** for that step. To view the error, click the step with the red cross icon. This helps you quickly identify the cause of the failure and debug the playbook.

FortiRecon also allows you to resume the same running instance of a failed playbook from the last failed step by clicking the **Rerun From Last Failed Step** button. This is useful if issues like an unconfigured connector or network problems caused the failure. Once resolved, you can continue from the failure point. However, if you modify the playbook steps, the playbook will be rerun from the beginning, not resumed from the failed step.

Resuming a Failed Playbook

If a playbook fails, you can resume it from the last failed step:

1. Open the `Executed Playbook Logs`.
2. Click the failed playbook, and then click the **Rerun From Last Failed Step** button.
   FortiRecon displays the `Playbook retriggered from last failed step` message and the playbook resumes from the point where it failed.
   A playbook that has been rerun will display the **Retriggered** text.

Config Tab

The **Config** tab displays the step variables entered by the user for the specific step, along with information on whether other variables, such as `ignore_errors`, `MockOutputUsed`, or the `when` condition are used (`true`/`false`) in the playbook step.

Instances Tab

The **Instances** tab is displayed for playbooks containing reference playbook steps. The "Instances" tab allows users to see details about child instances, such as their name and status in a single view.

Viewing Child Playbooks

Playbooks are organized hierarchically by parent-child relationships. The parent playbook includes a link to its child playbooks and also displays the number of child playbook(s) associated with the parent playbook. Click the link to view the execution history of the child playbooks. You can also view the children of child playbooks without losing context.

Tasks

The *Security Orchestration* > *Tasks* tab lists all automations that require manual input from a user before they can proceed. This ensures that playbooks pause when necessary, allowing you to review information or provide a required value.

Managing Tasks

Each entry in the task list represents a specific instance of an automation awaiting input.

- *Task ID* - A unique identifier assigned to the specific task instance.
- *Request*- The name of the automation or playbook step that generated the task.
- *Requester* - The user who initiated the automation.
- *Date* - The date the task was created.
- *Status* - The current state of the task, which can be *Pending*, *Complete*, or *Failed*.
- *Action* - Click *Provide Input* to open a dialog box where you enter the required data for the automation to continue.

Filtering the Task List

To quickly find a specific task, use the following filtering options at the top of the page:

- *Search* - Search for a task by entering the *Task ID* or the *Request* name.
- *Date Range* - Filter the list to display tasks created within a specific date range.
- *Status* - Select one or more task statuses (*Pending*, *Complete*, or *Failed*) to narrow the list.

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 257.

The *Profile Settings* module contains the following pages:

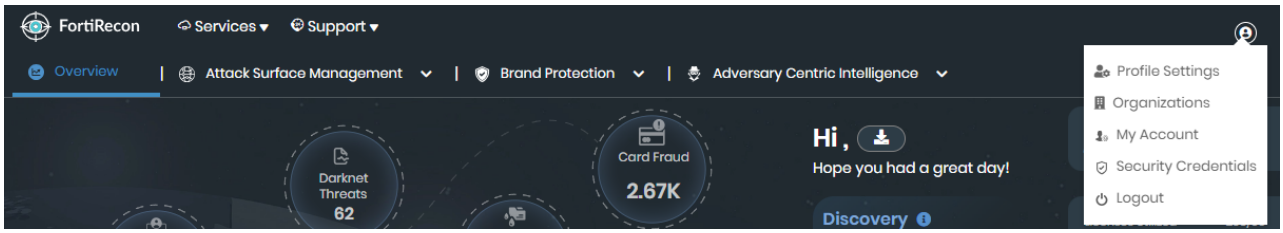
Profile	Displays information about your personal FortiRecon account. You can edit user idle timeout setting, view account details, upload your organization logo, and copy your API key for sharing. See Profile on page 258.
Users	Displays account information for members of your organization. Administrators can add, edit, and delete user accounts. See Users on page 261
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 267.
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 270.
Integrations	Displays the webhook integrations with Slack. You can create, edit, disable, and delete integrations. See Integrations on page 272.
Seeds	Displays the business names, domains, card BINs, social media profiles, and mobile applications of your organization that are being monitored by FortiRecon. See Seeds on page 274.
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 279.

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 258.
- View information about your subscription, such as registered domains, target industries and geography, keywords, and your API key. See Subscription Details on page 259.
- Modify your organization logo. See Uploading Organization Logo.
- Copy your API key for sharing. See Sharing the API key on page 261.

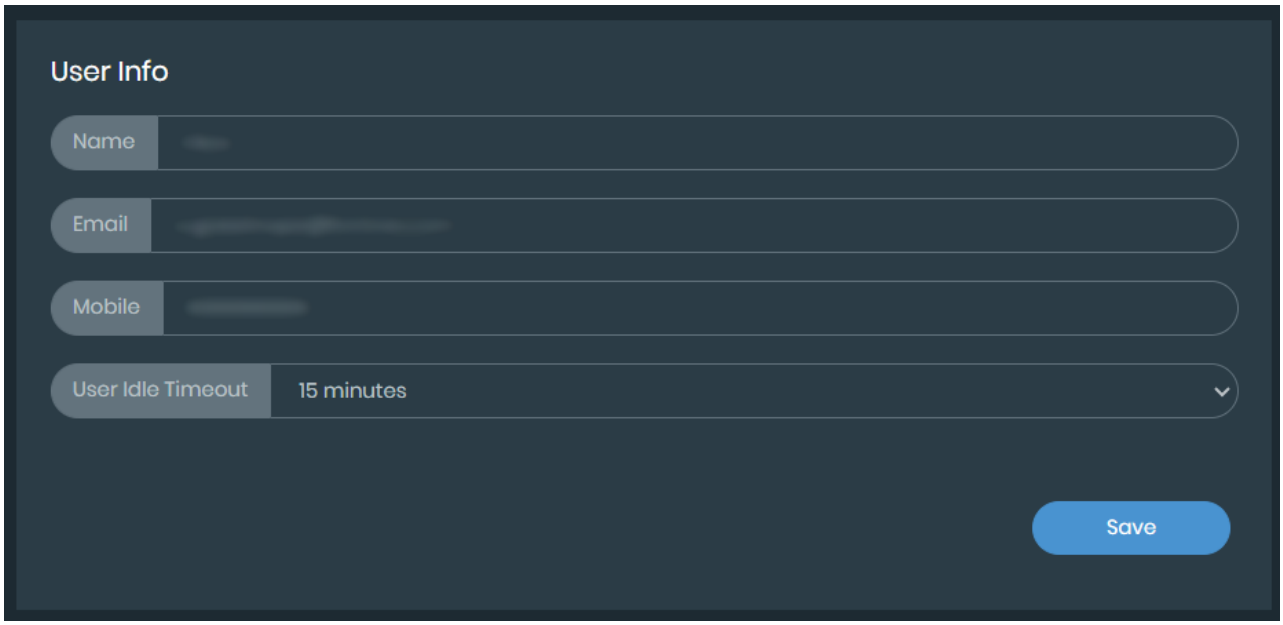
Editing user idle timeout

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 264.

To edit personal user information:

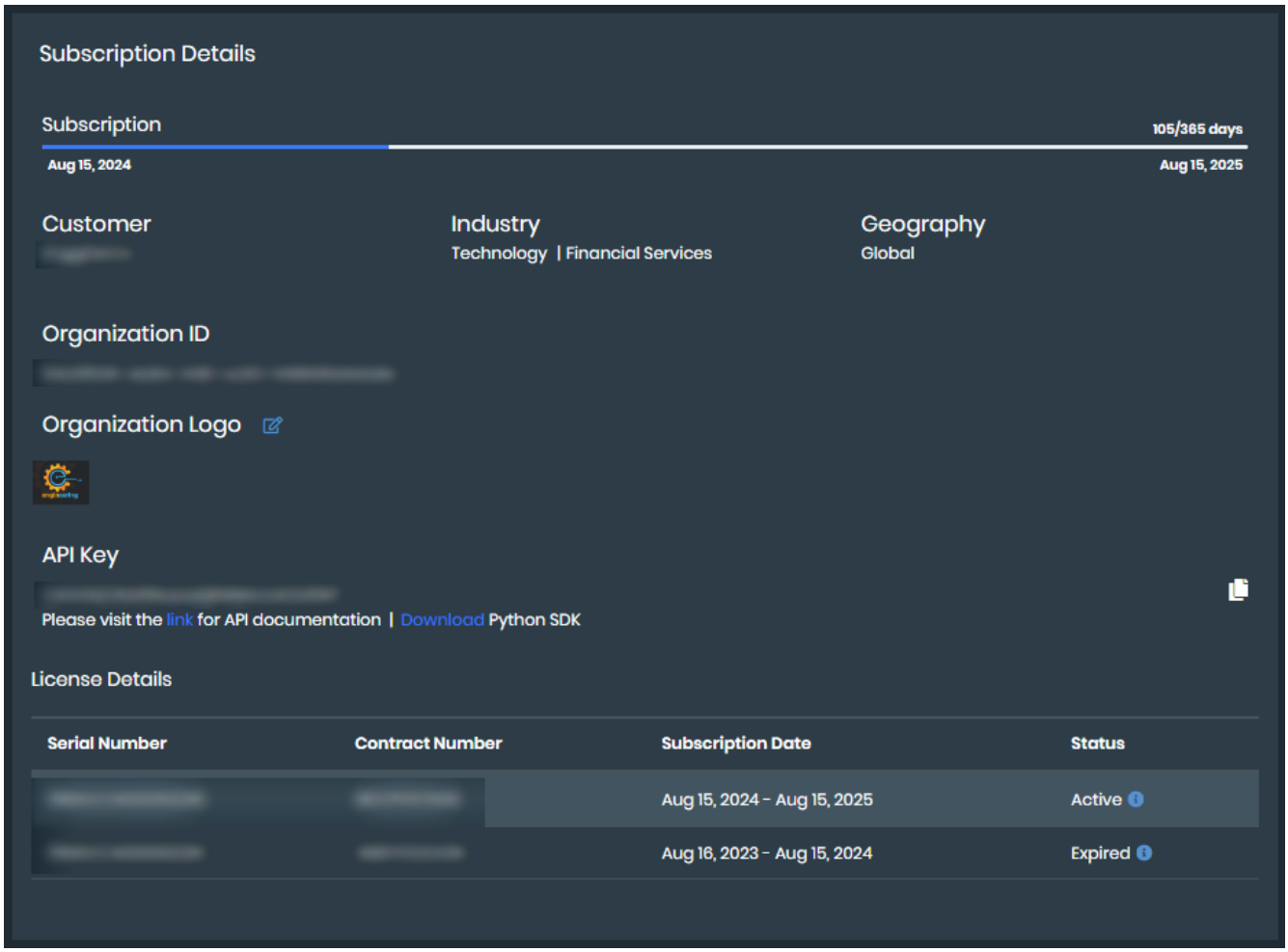
1. Go to *Profile Settings* > *Profile*.
2. Select the timeout period you want from the *User Idle Timeout* dropdown.
3. Click *Save*.

> By default, user idle timeout is set to *15 minutes*.



Subscription Details

Subscription Details provides information on your subscription, including organization ID, organization logo, 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
   - Organization Logo
   - API Key

     To access the API documentation or download the Python SDK package, click on the links below the API key.

   - License Details

Uploading Organization Logo

You can upload your organization logo in *Profile* tab.

To upload a logo:

1. Go to *Profile Settings* > *Profile*.
2. Click edit icon next to *Organization Logo* section in *Subscription Details*.
3. Browse and select the logo.
4. Click *Save*.

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.
- *Guest*: Has read-only access 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 262.
- Add new users. See Adding users on page 262.
- Edit existing users. See Editing users on page 264.
- Delete users. See Deleting users on page 265.

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 267.

You can add new user accounts using either email addresses, Identity and Access Management (IAM), or identity provider (IdP) details.

- Adding user account using email
- Adding an IAM user
- Adding an IdP user

To add a user account using email:

1. Access *Profile Settings*, and click the *Users* page. The users are displayed.
2. Click the *Add User* button. The *User Info* page is displayed.
3. Enable *Email* toggle and 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. • *Guest*: gives the user read-only 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.

To add an IAM user:

1. Access *Profile Settings*, and click the *Users* page. The users are displayed.
2. Click the *Add User* button. The *User Info* page is displayed.
3. Select *IAM* and complete the following options, and click *Next*. IAM user must be created in *support.forticloud.com*. See Adding IAM Users.

IAM User Name	Enter the configured IAM user name.
IAM Accountid	Enter IAM account id.
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. • *Guest*: gives the user read-only 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.

4. The *Permissions* page is displayed
5. Select a *User Template* from the dropdown. The *Main Modules*, *Sub Modules*, and *Access* are adjusted to the template's settings.
6. Click *Save*. The user is created.

To add an IdP user:

1. Access *Profile Settings*, and click the *Users* page. The users are displayed.
2. Click the *Add User* button. The *User Info* page is displayed.
3. Select *IDP* and enter the following details, and click *Next*. External IdP must be configured and IdP user must be created in *support.forticloud.com*. See Configuring External IdP.

IDP User Name	Enter the configured IDP user name.
IDP Accountid	Enter IDP account id.
IDP Name	Enter the configured identity provider name.
IDP User Role	Enter the configured IdP user role.

4.

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.

The *Permissions* page is displayed

5. Select a *User Template* from the dropdown. The *Main Modules*, *Sub Modules*, and *Access* are adjusted to the template's settings.
6. Click *Save*. The user is created.

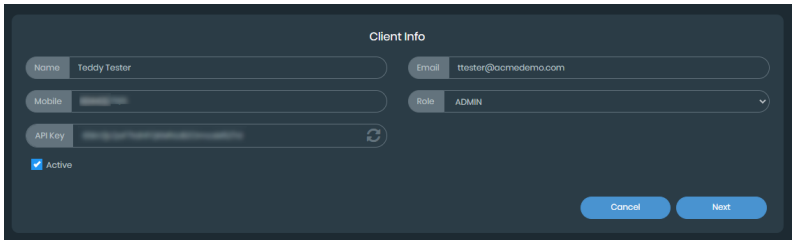
Editing users

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.

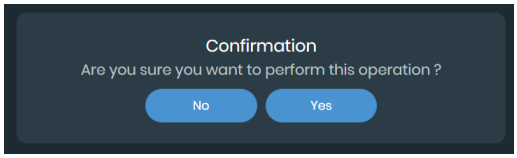
4. Select a new *User Template* from the dropdown, if needed. The *Main Modules*, *Sub Modules*, and *Access* are adjusted to the template's settings.
5. Click *Save*. The user information and access permissions are updated.

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.

Configuring External IdP

FortiRecon leverages the FortiCloud External Identity Provider (IdP) feature to support SAML 2.0 with IdP-initiated authentication. This integration allows users to authenticate through their organization's provider (such as Okta or Microsoft Entra ID) and access FortiRecon based on roles defined by the administrator.

For detailed information, see External IdP in *FortiCloud Identity & Access Management (IAM) Guide*.

- Enrolling for external IdP
- Adding external IdP roles in IAM
- Migrating from existing IAM and sub-users to external IdP
- Managing IdP users

Enrolling for external IdP

Before using the service, you must enroll your account with Fortinet. For detailed information, see Enrolling for external IdP.

1. Contact your *Fortinet Sales Representative* or *Fortinet Support* to initiate the enrollment process.
2. Next, configure your IdP application. In your IdP (e.g., Okta or Entra ID), create a *SAML 2.0* integration. Use a temporary URL (e.g., *https://customersso1.fortinet.com/*) for the *Single Sign-on URL* and *Audience URI* during initial setup.
3. Fill out the enrollment form with information about your IdP application and FortiCloud account. The following information must be included in the enrollment form:
   - *Company name*
   - *SAML 2.0 IdP name (Okta)*
   - *Account ID and the Master user email*
   - *Company administrator and Fortinet Inc. contact*
   - *IdP Metadata file*

> The account ID and email can be found in your FortiCloud account dropdown menu. To find the information, log into the Master account. In the top, right corner, select the account. A dropdown menu is displayed that lists the account ID and email information on the left side.

4. Share the with enrollment form the Fortinet team.
5. Once approved, replace the temporary URLs in your IdP application with the specific *SP Login* and *SP Entity ID URLs* provided by Fortinet. See Configuring external IdP.

Adding external IdP roles in IAM

After the IdP application is configured, you must map it to FortiCloud roles by configuring external IdP roles with which to access FortiRecon.

- In your IdP, set the *Group Attribute* name to *Role* (case-sensitive). See Adding external IdP roles to the application.
- In the *FortiCloud IAM portal*, create a new *External IdP Role*. The *Role Name* in the IAM portal must exactly match the *Group Name (Okta)* or *Object ID (Entra ID)* from your IdP. Select a permission profile that includes FortiRecon access. See Adding external IdP roles.

> For a user to successfully access the FortiRecon portal, the assigned Permission Profile must explicitly include FortiRecon with the appropriate access level. See Creating a permission profile.

Migrating from existing IAM and sub-users to external IdP

If your organization currently uses IAM users or sub-users and wishes to migrate to an External IdP, follow these steps.

- Set a *User Co-exist End Date* in the *Account Settings* of the IAM portal to allow both legacy and IdP users access during your transition. See Setting a co-exist end date.
- Audit your current permission profiles to ensure the new IdP roles grant the same level of access to FortiRecon.
- Communicate the new login procedure to users before the co-exist date expires, at which point all legacy IAM and sub-users will be disabled.

Managing IdP users

Once the external IdP configuration is complete, user accounts are managed through both the IAM portal and the FortiRecon interface. When a user logs in for the first time using the External IdP, their profile is automatically added to the user list in *FortiRecon* > *Profile Settings* > *Users*.

Administrators can also manually add an IdP user directly within *FortiRecon* > *Profile Settings* > *Users* once the initial IdP configuration steps are finished. See Adding users

Users must use the *Custom Login URL* provided during the enrollment process to authenticate via your organization's IdP

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 262

From the *Profile Settings* > *Access Template* page, you can:

- View available access templates. See Viewing access templates on page 267.
- Add a new access template. See Adding a template on page 267.
- Edit an existing access template. See Editing a template on page 268.

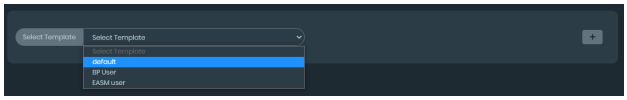
Viewing access templates

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

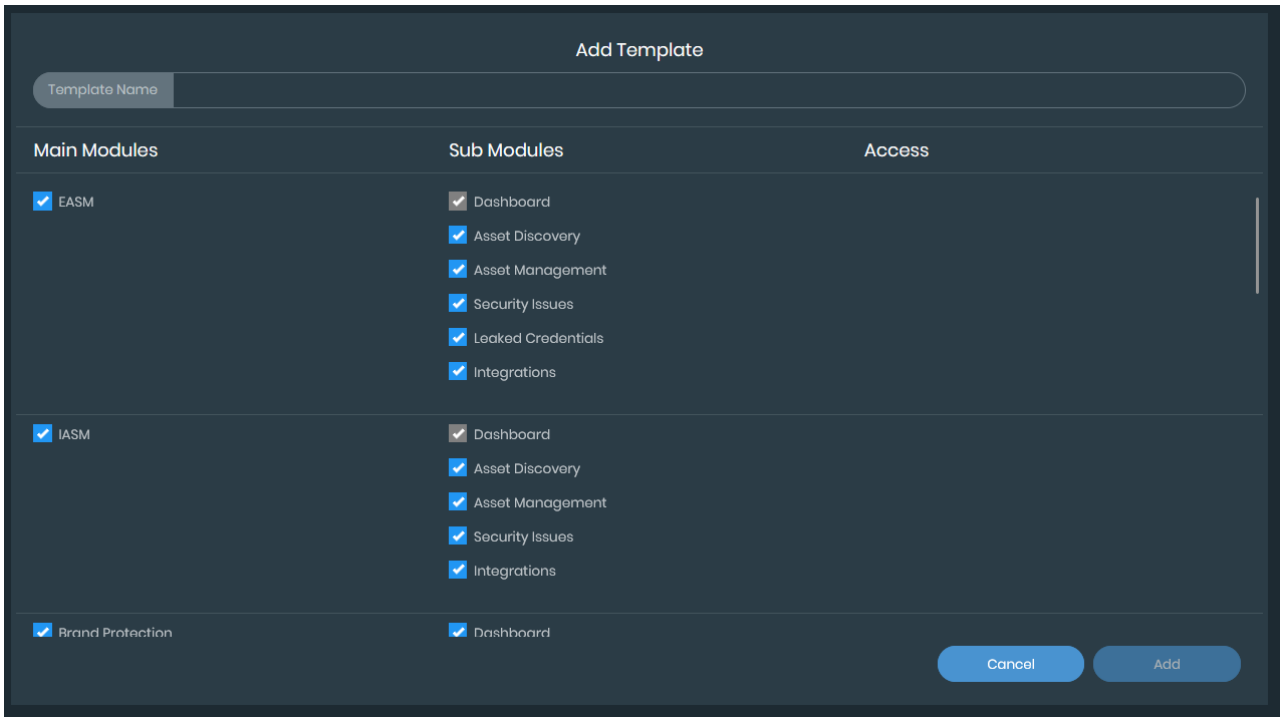
You can create new templates in the *Access Templates* page, and they can include any of the *Main Modules*, specific *Sub Modules*, and *Access* settings.

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
IASM	Dashboard
Brand Protection	Dashboard
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*
- *Entities*
- *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.

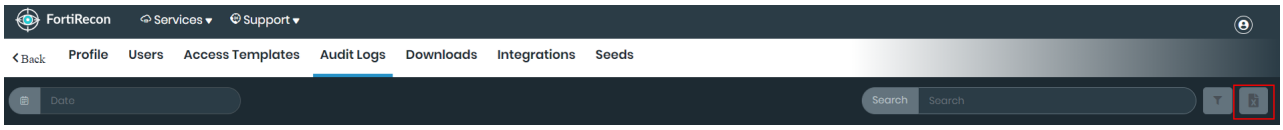
Exporting audit logs

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:

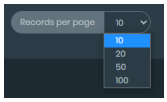
- View all downloads from the past 30 days. See Viewing downloads on page 271.
- Retrieve downloads from the past 30 days. See Retrieving downloads on page 271.
- Delete downloads. See Deleting downloads on page 271.

Viewing downloads

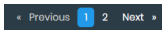
You can view all of your downloads from the past 30 days.

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.

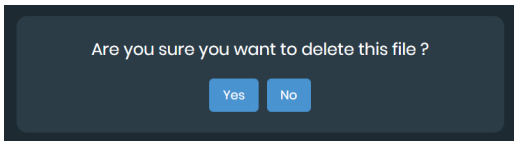
> If a file is not finished downloading, an update message is displayed when you hover your mouse over the file. You cannot click the file until it is finished downloading.

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 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 272.
- Create new integrations. See Adding integrations on page 272.
- Edit existing integrations. See Editing integrations on page 273.
- Disable integrations. See Disabling integrations on page 273.
- Delete integrations. See Deleting and disabling integrations on page 273.

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.
3. Click the name or icon of the integration. The *Update Integration* page displays the integration details.

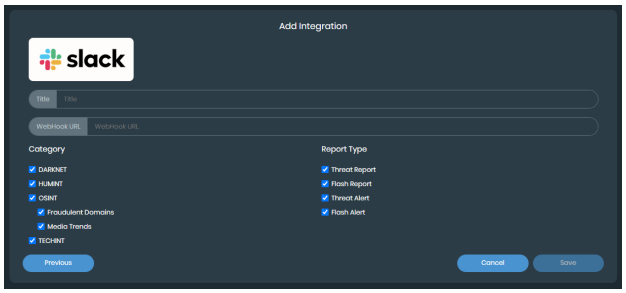
Adding integrations

You can add multiple webhook integrations to your account in FortiRecon.

> You must retrieve the webhook URL from Slack before adding an integration to FortiRecon. See 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:

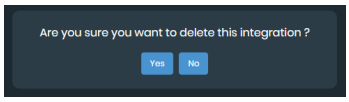
1. Go to *Profile Settings* > *Integrations* and find the integration.
2. Select the toggle to disable the integration. The notifications are no longer sent to the software.
3. Select the toggle again to enable the integration.

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 *Attack Surface Management* > *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.
- Add, edit, and delete business names. See Business Names.
- Add, edit, and delete all BIN numbers used by your organization to issue credit, debit, and gift cards. See Card BIN.

Viewing your assets

On the *Seeds* page, you can view the business names, 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:

- Business Names
- 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.

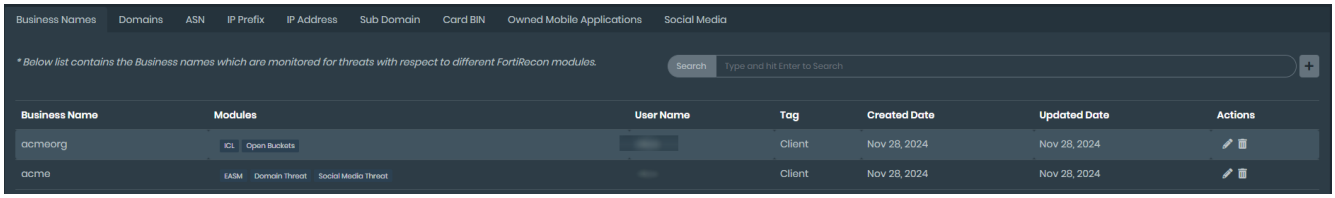
Business Names

You can add and manage business names that FortiRecon monitors for threats across various modules. Based on the selected module, FortiRecon uses the business name in the following ways:

- *EASM*: Identifies assets with matching certificate names or IP address ranges.
- *Domain Threats*: Detects domains that impersonate the brand.
- *Social Media Threats*: Identifies social media accounts that impersonate the brand.
- *Open Buckets*: Finds sensitive files exposed on the internet.
- *Intelligence Collection Lookup (ICL)*: Enhances threat intelligence gathering by adding the business name to the default ICL query.

From the *Profile Settings* > *Seeds* > *Business Names*, you can:

- Add business names. See Adding business names.
- Edit or delete existing business names. See Modifying business names.



Adding business names

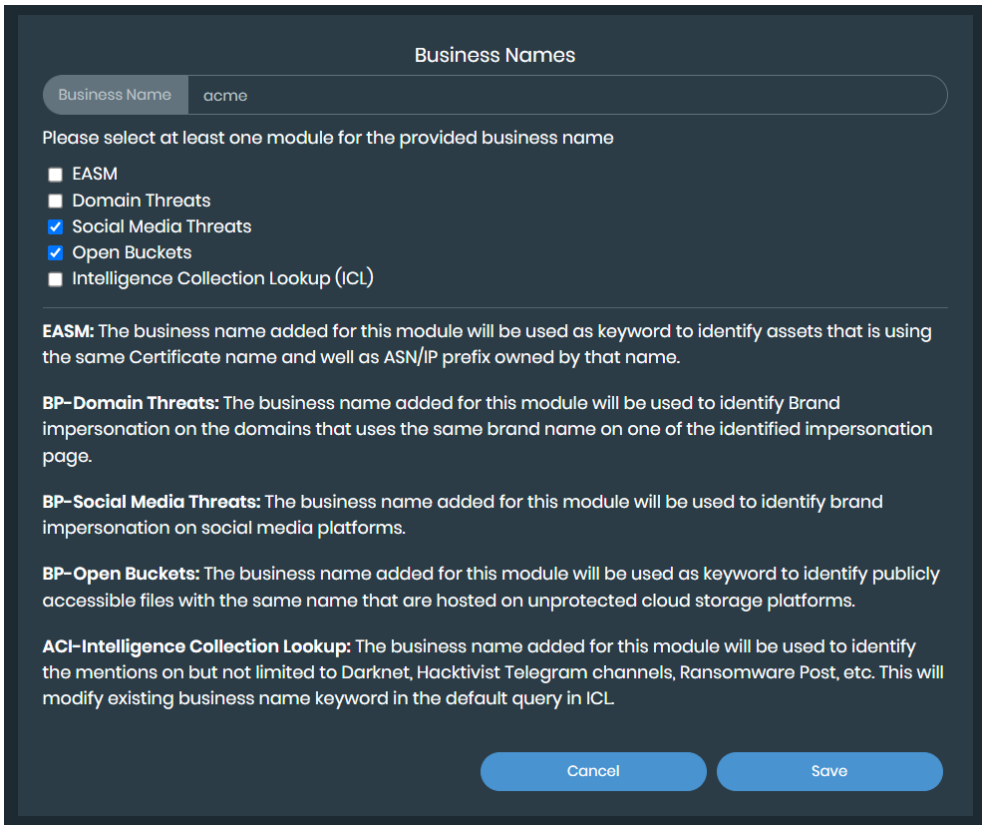
You can add business names as needed. You must select at least one module for each business name.

To add a new business name:

1. Go to *Profile Settings* > *Seeds* > *Business Names*.
2. Click + add icon.
3. Enter a business name.
4. Select at least one module for the provided business name.

- *EASM*: The business name added for this module will be used as keyword to identify assets that is using the same Certificate name and well as ASN/IP prefix owned by that name.
- *Domain Threats*: The business name added for this module will be used to identify Brand impersonation on the domains that uses the same brand name on one of the identified impersonation page.
- *Social Media Threats*: The business name added for this module will be used to identify brand impersonation on social media platforms.
- *Open Buckets*: The business name added for this module will be used as keyword to identify publicly accessible files with the same name that are hosted on unprotected cloud storage platforms.
- *Intelligence Collection Lookup (ICL)*: The business name added for this module will be used to identify the mentions on but not limited to *Darknet*, *Hacktivist Telegram channels*, *Ransomware Post*, etc. This will modify existing business name keyword in the default query in ICL.

5. Click *Save*.



Modifying business names

You can edit or delete previously added business names.

To edit a business name:

1. Go to *Profile Settings* > *Seeds* > *Business Names*.
2. Click edit icon next to the desired business name.
3. Select or deselect the modules.

4. Click *Save*.

To delete a business name:

1. Go to *Profile Settings* > *Seeds* > *Business Names*.
2. Click delete icon next to the desired business name.
3. Click *Yes* in the confirmation dialog.

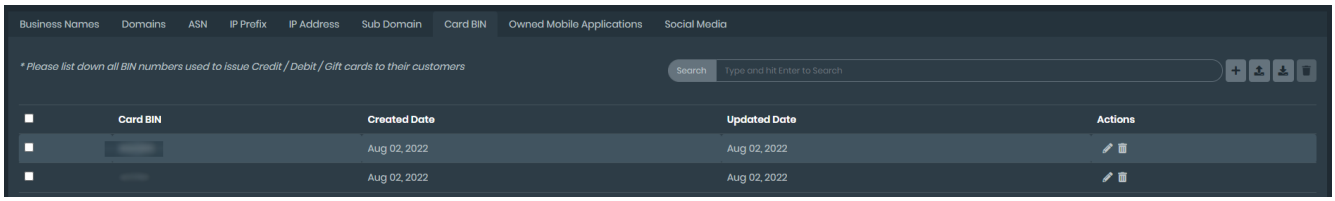
Card BIN

Providing your organization's card bank identification numbers (BINs) allows FortiRecon to monitor for card fraud by actors that may be trying to steal credit, debit, or gift card information. See Card Fraud on page 176.

> Card BIN information is needed only when your organization issues credit, debit, or gift cards.

From the *Profile Settings* > *Seeds* > *Card BIN* tab, you can:

- Add new card BINs. See Adding a card BIN on page 277.
- Edit existing card BINs. See Editing a card BIN on page 278.
- Delete existing card BINs. See Deleting a card BIN on page 278.

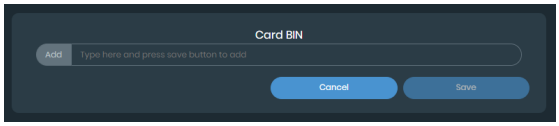


Adding a card BIN

You can add new BINs in the *Card BIN* tab, as needed. BINs must be six to eight characters long.

To add a new card BIN:

1. Go to *Profile Settings* > *Seeds* > *Card BIN*.
2. Click *Add*. The *Card BIN* window is displayed.



3. Enter the BIN in the *Add* text box.
4. Click *Save*. The card BIN is added.

To bulk upload card BIN:

1. Go to *Profile Settings* > *Seeds* > *Card BIN*.
2. You can use a Microsoft Excel file to upload bulk information to the *Seeds* page. The Microsoft Excel file requires a specific format, and you can download a sample file to review the needed format. Select *Download Sample XLS* in the tab.
3. Select *Upload XLS* in the tab.

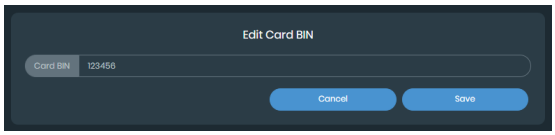
   Your computer file explorer is displayed.
4. Select the file and click *Open*. The data entries are displayed in the selected *Seeds* tab.

Editing a card BIN

You can edit a pre-existing card BIN in the *Card BIN* tab.

To edit a card BIN:

1. Go to *Profile Settings* > *Seeds* > *Card BIN* and find the card BIN.
2. Click the edit icon in the *Actions* column. The *Edit Card BIN* window is displayed.



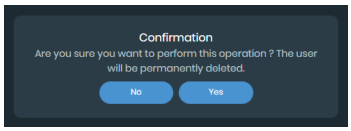
3. Edit the text in the *Card BIN* text box.
4. Click *Save*. The card BIN is edited.

Deleting a card BIN

You can delete BINs from the *Card BIN* tab. You can delete a single BIN or groups of BINs.

To delete a single card BIN:

1. Go to *Profile Settings* > *Seeds* > *Card BIN* and find the BIN.
2. Click the delete icon in the *Actions* column. A confirmation message is displayed.



3. Click *Yes*. The BIN is deleted from the list.

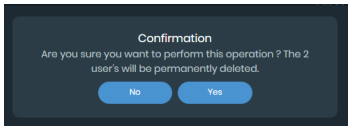
To delete multiple card BINs:

1. Go to *Profile Settings* > *Seeds* > *Card BIN*.
2. Select the BINs by using one of the following methods:

- Select the checkbox in the first row to select all BINs, and clear the checkbox beside any BINs that you want to keep.
- Select the checkbox next to specific BINs to mark them for deletion.

The *Delete Rows* icon becomes available.

3. Click *Delete Rows*. A confirmation message is displayed and lists the number of selected BINs.



4. Click *Yes*. The BINs are deleted from the list.

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:

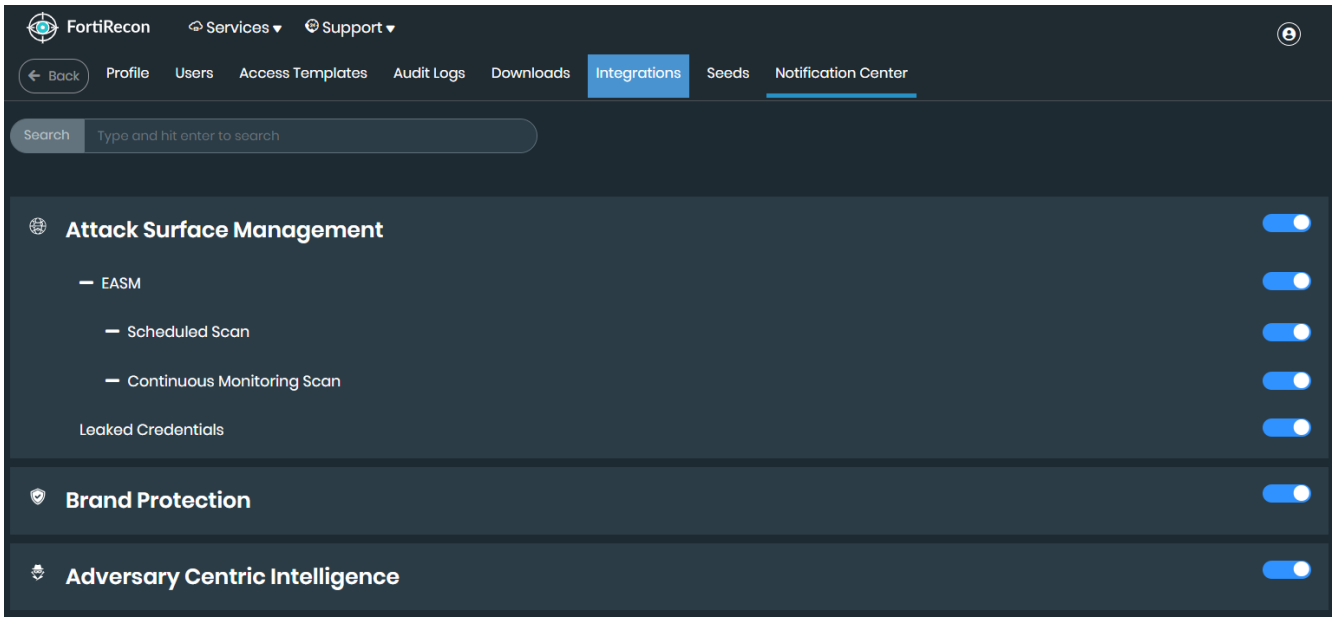
- View and edit your current notification settings. See Viewing and managing notification settings.
- Customize notifications in Adversary Centric Intelligence module. See Customizing notifications.
- Modify notification settings for other users as an Administrator. See Managing notifications as an administrator.

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*, *Time* and *Time Zone*.
	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.
	Intelligence Collection Lookup > List of Queries	Select from the list of available queries.

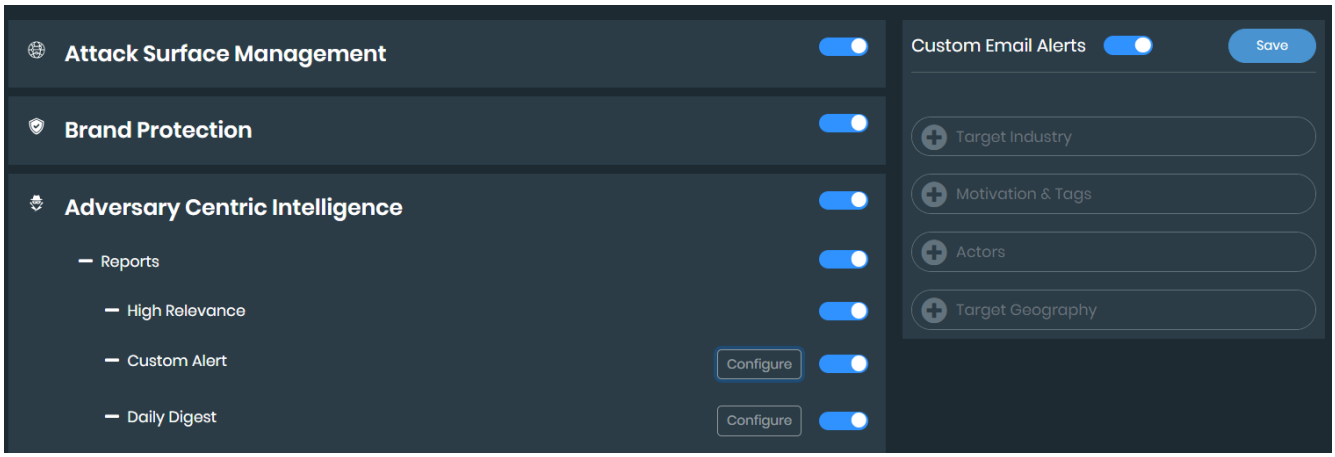
To customize notifications:

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.

> For *Stealer Infections* you can use the search bar to find specific domains, and then manage your subscription status. The default view displays the list of subscribed domains, showing both selected and unselected domains.
>
> *Unsubscribe* - Select all domains or select a few specific domains from the list, and then click *Unsubscribe* to stop receiving notifications for the selected domains.
>
> *View Unsubscribed* - Click the *Unsubscribed* button to view the list of domains for which you previously disabled notifications.
>
> *Subscribe*: From the unsubscribed list, select the domains you want to reactivate, and then click Subscribe to resume notifications.

5. Click *Save*.

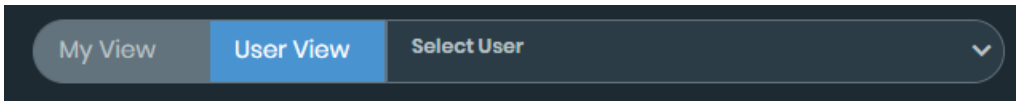


Managing notifications as an administrator

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.

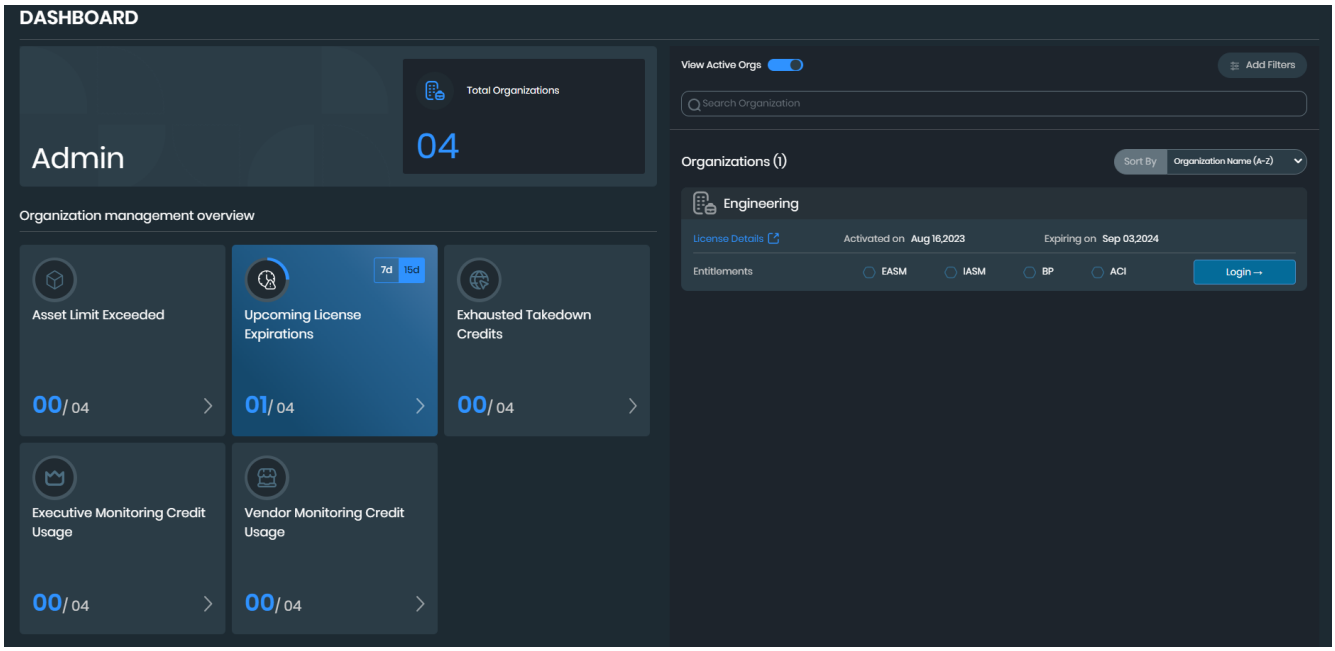
Any notification setting modified by an administrator can also be modified by the user.

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:

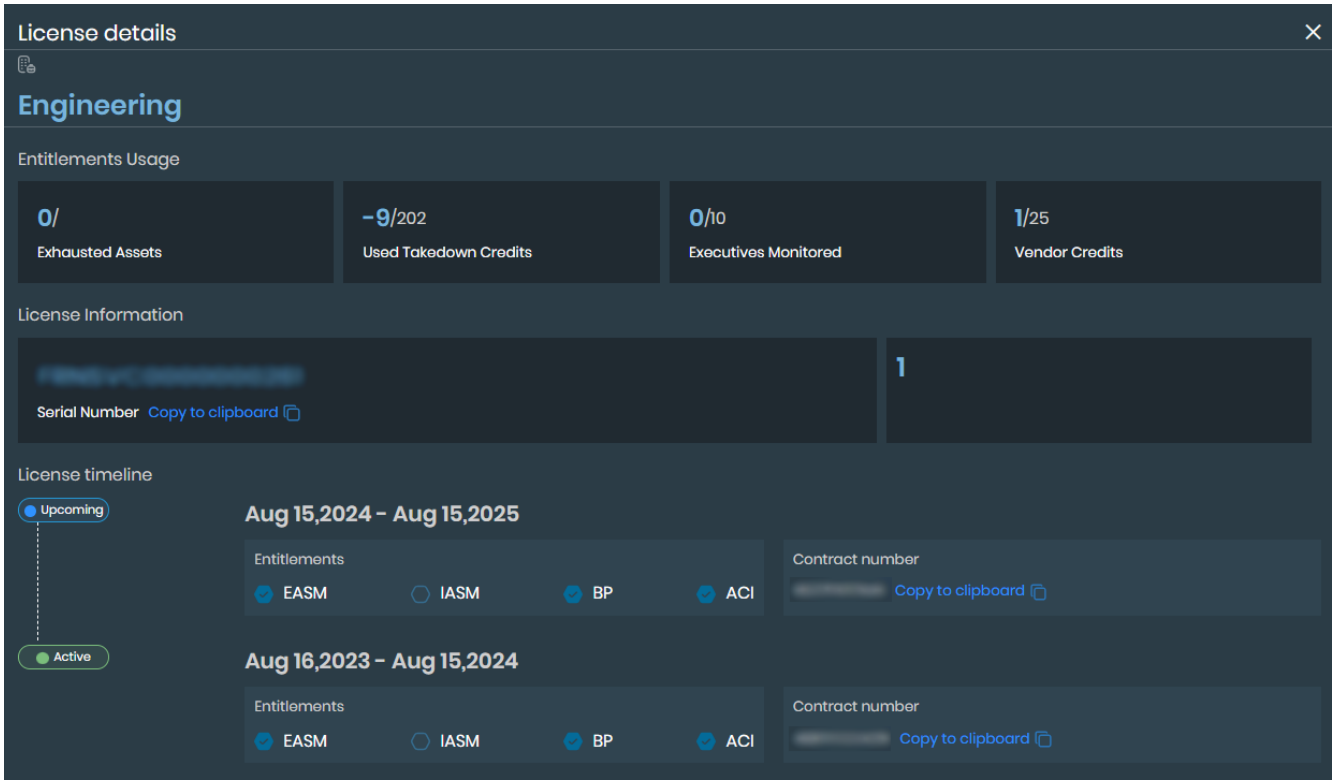
1. Toggle *View Active Orgs* to show or hide all active organizations.
2. Use search bar to search for a specific organization by name.
3. Click *Add Filters* to apply filters based on *Region*, *Country*, *Subscription Status*, and *Entitlements*.
4. Select predefined filters in *Organization management 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.
- Takedown license timeline displays a detailed history of your takedown credits, including those added by default and those you purchased.



www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.