Administration Guide

FortiDeceptor 5.2.2

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

October 06, 2025
FortiDeceptor 5.2.2 Administration Guide
50-520-933274-20251006

TABLE OF CONTENTS

Change Log **9**
Introduction **10**
Set up FortiDeceptor **11**
Connect to the GUI 11
Connect to the CLI 12
Change the system hostname 12
Change the administrator password 12
Configure the system time 13
Upload license file to FortiDeceptor 14
Default port information 14
DMZ Mode 15
Limitations of the DMZ Mode 15
JSON API 16
Deploy Decoy VM **17**
Dashboard **18**
System Resources 19
Reboot or shut down the unit 20
System Information 21
Update FortiDeceptor firmware 22
Back up or restore the system configuration 23
License Information 24
Disk Monitor 24
Incidents & Events Distribution 25
Incidents and Events Count 25
Decoy Distribution by OS 26
Lure Distribution 27
Incidents Distribution by Service 27
Top 10 Attackers by Incidents 28
Top 10 Attackers by Events 29
Global Incidents Distribution 29
Top 10 IPS Attacks 29
Customizing the dashboard 30
Central Management **32**
Remote Client 33
Configuring Central Management 33
Deception **36**
Custom Decoy Image 36
Customize the deception base OS image 37
Deception OS 66
Deployment Network 67
Setting up the deployment network 68

Lure Resources ... 69
Uploading lure resources ... 69
Importing users from LDAP ... 71
Examples: Import Users from LDAP ... 71
Deployment Wizard ... 72
Available Deception OSes, Decoys and Selected Services ... 74
Lure Settings ... 78
Decoy Status ... 86
Deception Token ... 88
Deployment Map ... 90
Discover & Deploy ... 92
Asset Discovery ... 92
Safe List ... 94
Incident ... 95
Analysis ... 95
Campaign ... 97
Attack Map ... 99
MITRE ICS ... 100
Viewing the MITRE ICS matrix ... 100
Fabric ... 103
Detection Devices ... 103
FortiSandbox ... 103
Cuckoo Sandbox ... 104
Virus Total ... 104
Quarantine Integration ... 105
FortiDeceptor on FortiGate Security Fabric topology map ... 105
FortiDeceptor integration for threat response mitigation ... 109
Integrate Method settings ... 112
Quarantine Status ... 117
IOC Export ... 118
Network ... 120
Interfaces ... 120
System DNS ... 121
System Routing ... 122
System ... 124
Administrators ... 124
Admin Profiles ... 127
Certificates ... 129
LDAP Servers ... 131
RADIUS Servers ... 132
Single Sign-On ... 133
Configuring SSO with Azure ... 134
Mail Server ... 137
Creating incident alerts ... 137
Creating alert delivery rules ... 138

SNMP 139
FortiGuard 143
FDC License 145
Settings 146
Login Disclaimer 146
Table Customization 146
Raw logs 148
Log 150
Log Servers 150
Log Categories 151
Logging Levels 151
Appendix A - Deploying FortiDeceptor in offline or air-gapped networks 153
Deception VM security 153
Applying the license in an offline or air-gapped network 153
Importing deception VMs in an offline or air-gapped network 155
Importing firmware in an offline or air-gapped network 157
Importing an FDS package via FDC GUI in an offline or air-gapped network 157
Importing FDS package and license file via FortiManager in an offline or air-gapped network 158
Appendix B - Deception deployment best practices 161
Deception strategy 161
Deception strategy components 162
Deception strategy goals 162
Deception philosophy 162
Deception light stack vs full stack 163
Deception for FortiGuard Outbreak Alerts 163
FortiDeceptor platform 167
FortiDeceptor components 167
FortiDeceptor Token Package 167
FortiDeceptor decoys 168
Decoy services details 169
Deploying deception 180
Deception decoy best practices 180
Deception token best practices 184
AD integration best practices 185
Deployment best practices checklist 186
Network topology best practices 187
Attack vectors vs deception 191
Compromised internal endpoint using lateral movement 191
Lateral movement based on AD mapping 193
Lateral movement based on Mimikatz / PTH 194
Deploying tokens using AD GPO logon script 195
Configuring the GPO logon script 197
Deploying AWS deception keys 200
Deploying Azure deception keys 210
Configuring trunk ports on FortiDeceptor VM 216

Configuring FortiDeceptor 219
Configuring the vSwitch 222
How to setup and use LDAP/RADIUS servers 226
Appendix C - Hardening 230
Building security into FDC-OS 230
Boot device security 230
FDC-OS kernel and user processes 230
Physical security 230
Vulnerability - monitoring PSIRT 231
Firmware 231
Encrypted protocols 231
Strong ciphers 231
FortiGuard databases 231
Trusted Hosts 231
Limit login user's access right 232
Administration access security 232
Admin administrator account 232
Maintainer account 232
Non-factory SSL certificates 233
Other recommended actions user can take 233
Appendix D - Configuration examples 234
Configure FortiDeceptor for admin access authentication from Active Directory 234
FortiDeceptor admin access authentication from FortiAuthenticator 234
Configure a Active Directory (AD) user as FortiDeceptor administrator 239
1. Configure the LDAP Server in FortiDeceptor 239
2. Set the Active Directory user to be an administrator 240
Import network users from the Active Director server for Decoy lure configuration 242
MFA (RADIUS) configuration 243
1. Configure FortiAuthenticator on the RADIUS server side 243
2. Configure the RADIUS user on FortiDeceptor 245
Integrate with Checkpoint Firewall 246
1. Configure the REST API permissions. 247
2. Configure FortiDeceptor 247
Integration with Crowdstrike 248
1 Configure CrowdStrike 248
Integrate with Cuckoo Sandbox 251
1. Configure Cuckoo Sandbox 251
1.1 Start Cuckoo Sandbox 251
2. Configure FortiDeceptor to integrate with Cuckoo Sandbox 252
3. Verify the detection result from Cuckoo Sandbox 253
Integration with FortiSIEM 254
1. Configure FortiSIEM as a remote log server in FortiDeceptor 254
2. Change the discovered FortiDeceptor status from Pending to Approved 255
3. Check the logs and generate reports in FortiSIEM 255
FortiSIEM Watch List 258
1. Configure FortiSIEM 258

2. Configure the Watch List in FortiDeceptor 259
3. Test the integration 260
4. Check the incidents on FortiSIEM 260
5. View the incidents on FortiDeceptor 261
Mitigation using windows Remote Command 262
1. Configure the endpoint 262
2. Configure FortiDeceptor 264
Integration with PAN devices 264
1. Configure PAN 265
2. Configure the PAN device on FortiDeceptor 265
3. Check the PAN status on FortiDeceptor 266
5. Attack a decoy and check the quarantine status in FortiDeceptor 267
Integration with Microsoft ATP 267
1. Configure Azure 267
2. Onboard devices on Microsoft 365 Defender 268
3. Configure FortiDeceptor 269
Integration with FortiSandbox 269
1. Create a new user role in FortiSandbox 270
2. Integrate FortiDeceptor with FortiSandbox 271
3. Verify the scanning results in FortiDeceptor and FortiSandbox 272
Integration with FortiNAC 272
1. Configure the attack host on FortiNAC 273
2. Convert the pingable device to a host 273
3. Verify the host was added successfully 274
4. Generate an API token on FortiNAC 275
5. Configure the integration with FortiNAC (Gen-Webhook) 275
6. Configure the integration with FortiNAC (FNAC-WEBHOOK) 276
Integration with FortiEDR 277
1. Configure FortiEDR 277
2. Configuration on FortiDeceptor 278
Integration with FortiAnalyzer 279
1. Configure the Log Servers in FortiDeceptor 280
2. Authorize FortiDeceptor in FortiAnalyzer 280
3. Create the FortiDeceptor security report in FortiAnalyzer 282
Integration with FortiGate over Webhook 284
1. Configure the API key on FortiGate 284
2. Configure Webhook on FortiGate 6.4.x 284
3. Configure Webhook on FortiGate 7.0.x 287
4. Configure FortiDeceptor to integrate with FortiGate over Webhook 294
Integrate with FortiGate 6.0.3 to 7.2.3 over REST-API 295
1. Configure FortiGate 296
2. Configure FortiDeceptor to integrate with FortiGate 298
3. Test the integration 299
Integrate FortiDeceptor with FortiGate over Fabric v7.2.4 299
1. Configure the Fabric Connector on FortiGate 300
2. Configure the upstream FortiDeceptor 303
3. Authorize FortiDeceptor on FortiGate 304
4. Configure the automation on FortiGate 306

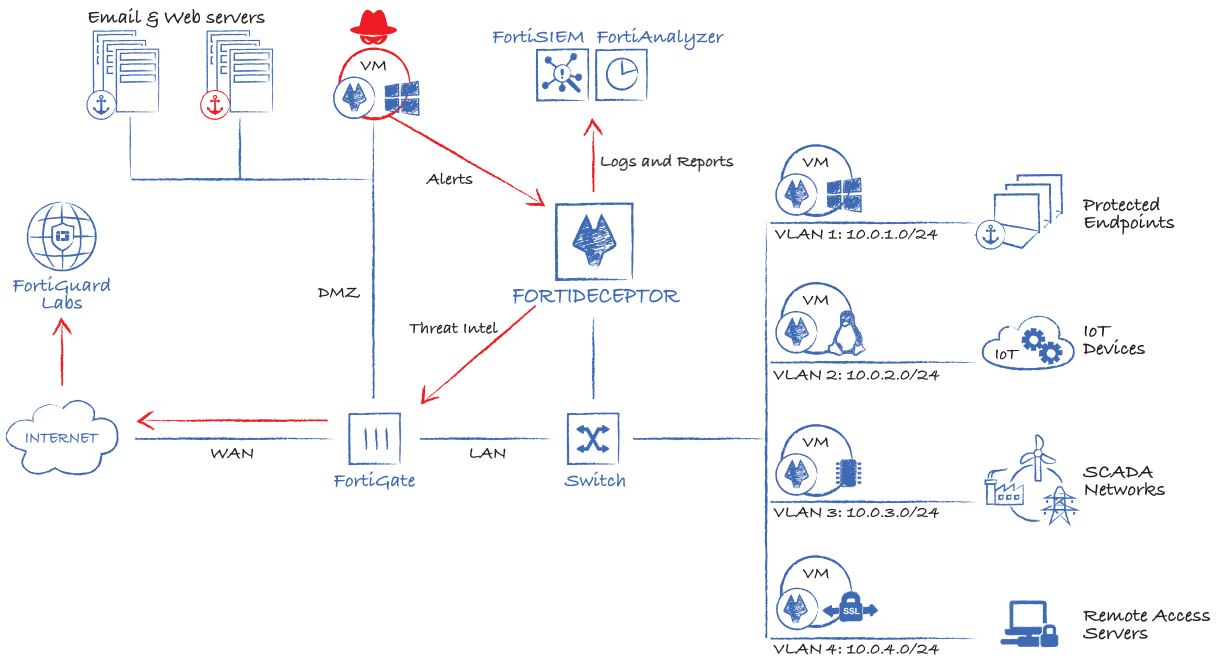
5. Create a stitch for manual block on FortiGate 309
6. Create a stitch for manual unblock 311
7. Check the quarantine status in FortiDeceptor 312
8. Check quarantine status on FortiGate 312
Integrate with Cisco ISE 312
Topology 312
1. Configure Cisco ISE 313
2. Configure the Authorization Policy 315
3 Check the configuration 316
4. Configure FortiDeceptor 317
5. Quarantine the endpoint 317
6. Un-quarantine the endpoint 318
Integrate Windows IR collector 318
Artifacts list 320

Change Log

Date	Change Description
2025-10-06	Initial release.

Introduction

FortiDeceptor creates a network of Decoy VMs to lure attackers and monitor their activities on the network. When attackers attack Decoy VMs, their actions are analyzed to protect the network.



Key features of FortiDeceptor include:

- **Deception OS**: Windows, Linux, SCADA OS, IoT OS, VoIP OS, ERP OS, Medical OS, SSL-VPN OS, or POS OS images are available to create Decoy VMs.
- **Decoy VMs**: Decoy VMs that behave like real network assets can be deployed via FortiDeceptor.
- **Deception Lures**: Deception Lures are services, applications, or users added to a Decoy VM to simulate a real user environment.
- **FortiDeceptor token package**: Install a FortiDeceptor token package to add breadcrumbs on real endpoints and lure an attacker to a Decoy VM. Tokens are normally distributed within the real endpoints and other IT assets on the network to maximize the deception surface. Use tokens to influence attackers' lateral movements and activities. Examples of what you can use in a token include: cached credentials, database connections, network share, data files, and configuration files.
- **Monitor the hacker's actions**: Monitor *Incidents*, *Events*, and *Campaign*.
  - An *Event* represents a single action. For example, a login-logout event on a victim host.
  - An *Incident* represents all actions on all actions taken by a hacker on a single decoy/victim host. Examples include, a login-logout, file system change, a registry modification, and a website visit on a single victim host.
  - A *Campaign* represents the hacker's lateral movement. All related *Incidents* are a *Campaign*. For example, an hacker logs on to a system using the credentials found on another system.
- **Log Events**: Log all FortiDeceptor system events.

Set up FortiDeceptor

Use the following checklist to verify you have completed all of the general configuration tasks.

Task	Description
☐ Connect to the GUI	Connect the administration interface to a management computer with an Ethernet cable, then configure the management computer to be on the same subnet as the internal interface of the FortiDeceptor unit.
☐ Change the administrator password	You are required to create a create strong password the first time you log into FortiDeceptor.
☐ Change the system hostname	Change the full host name in the *System Information* widget.
☐ Connect to the CLI	If necessary, connect to the CLI console.
☐ Configure the system time	Configure the FortiDeceptor system time manually or synchronize with an NTP server from the *System Information* widget.
☐ Upload the license file to FortiDeceptor	Go to *Dashboard* > *System Information* widget, click *Upload License* beside *Firmware License*.
☐ Review the default port information	FortiDeceptor reserves Port1 for device management. The other ports are used to deploy deception decoys.
☐ Configure Central Management on the manager	Configure the Central Management console to manage remote FortiDeceptor appliances including Decoy VMs deployment, system configuration, and incident alert monitoring.

Connect to the GUI

Use the GUI to configure and manage FortiDeceptor.

To connect to the FortiDeceptor GUI:

1. Using an Ethernet cable, connect the management computer to FortiDeceptor's port1.
2. Configure the management computer to be on the same subnet as the internal interface of the FortiDeceptor unit:
   - Change the IP address of the management computer to `192.168.0.2`.
   - Change the IP address of the network mask to `255.255.255.0`.
3. Go to `https://192.168.0.99`.
4. Type `admin` in the *Name* field, leave the *Password* field blank, and click *Login*.
   You can now proceed with configuring your FortiDeceptor unit.

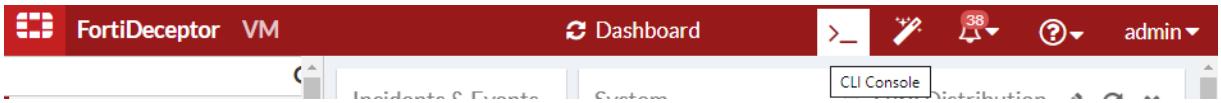
If the network interfaces have been configured differently during installation, the URL and administrative access protocols might not be in their default state.

Connect to the CLI

You can use CLI commands to configure and manage FortiDeceptor.

To connect to the FortiDeceptor CLI:

1. In the FortiDeceptor banner at the top, click the *CLI Console* icon.



   The *CLI Console* pane opens.
2. If necessary, click *Connect* and enter your username and password.
   The *CLI Console* pane has icons to disconnect from the CLI console, clear console text, download console text, copy console text, open the CLI console in its own window, and close the console.
3. To close the CLI console, click the *Close* icon.

Change the system hostname

The *System Information* widget displays the full host name. You can change the FortiDeceptor host name.

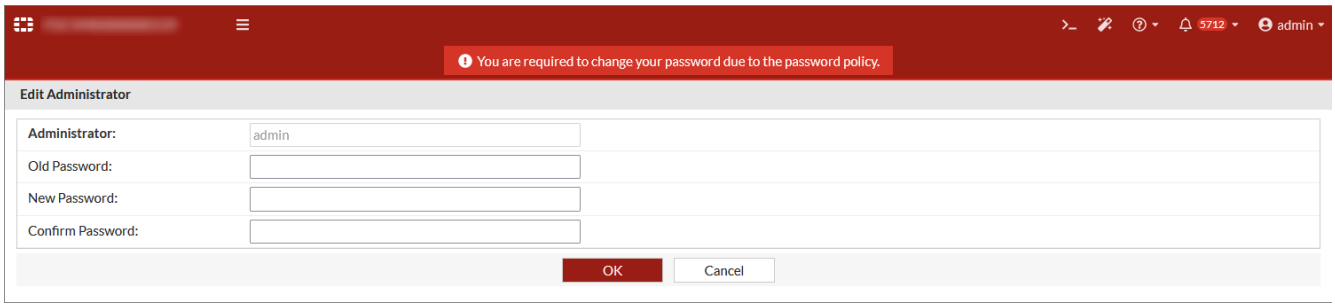
To change the host name:

1. Go to *Dashboard*, *System Information* widget.
2. Click *Change* beside *Host Name*.
3. In the *New Name* field, type a new host name.
   The hostname can start with a character or digit, and cannot end with a hyphen. A-Z, a-z, 0-9, or hyphen are allowed (case-sensitive). Other symbols, punctuation, or white space are not allowed.
4. Click *Apply*.

Change the administrator password

The first time you log into FortiDeceptor you will be prompted to change the administrator password. Passwords must be 8-60 characters long, and contain only upper/lower-case letters, numbers and special characters *!#$%()*.

Due to a higher level of password encryption introduced in version 5.2.0, users upgrading from v5.1.0 to v5.2.0 will be prompted to change their password.



To change the password of the logged in administrator:

1. In the FortiDeceptor banner at the top, click the username and select *Change Password*.
2. Change the password and click *OK*.

To change the administrator password in the Administrators page:

1. Go to *System* > *Administrators*.
2. Select an administrator and click *Edit*.
3. Change the password and click *OK*.

To change the administrator password with the CLI:

Run the following command:

```
passwd
```

Example:

```
> passwd

Old password: *************

New password: *************

Confirm password: *************

Successfully changed password, please re-login with the new password.
```

Configure the system time

You can change the FortiDeceptor system time in the *Dashboard*. You can configure the FortiDeceptor system time manually or synchronize with an NTP server.

To configure the system time:

1. Go to *Dashboard* > *System Information* widget and click *Change* beside *System Time*.
2. Select the *Time Zone* and wait for the widget to refresh.
3. Check that the *System Time* is correct. If necessary, click *Set Time* and manually set the time and date.

4. Click *Apply*.
   You might need to log in again.

If the time is not correct, we recommend configuring the NTP server for time synchronization.

Upload license file to FortiDeceptor

To upload the license to FortiDeceptor:

1. Go to *Dashboard* > *System Information* widget, click *Upload License* beside *Firmware License*.
2. Locate the license and click *Submit*.

Default port information

FortiDeceptor treats Port1 as reserved for device management. The other ports are used to deploy deception decoys.

The following table list the default open ports for each FortiDeceptor interface.

FortiDeceptor default ports:

Configure the FortiDeceptor management IP address on port1.

Configure the FortiDeceptor management IP address on port1.

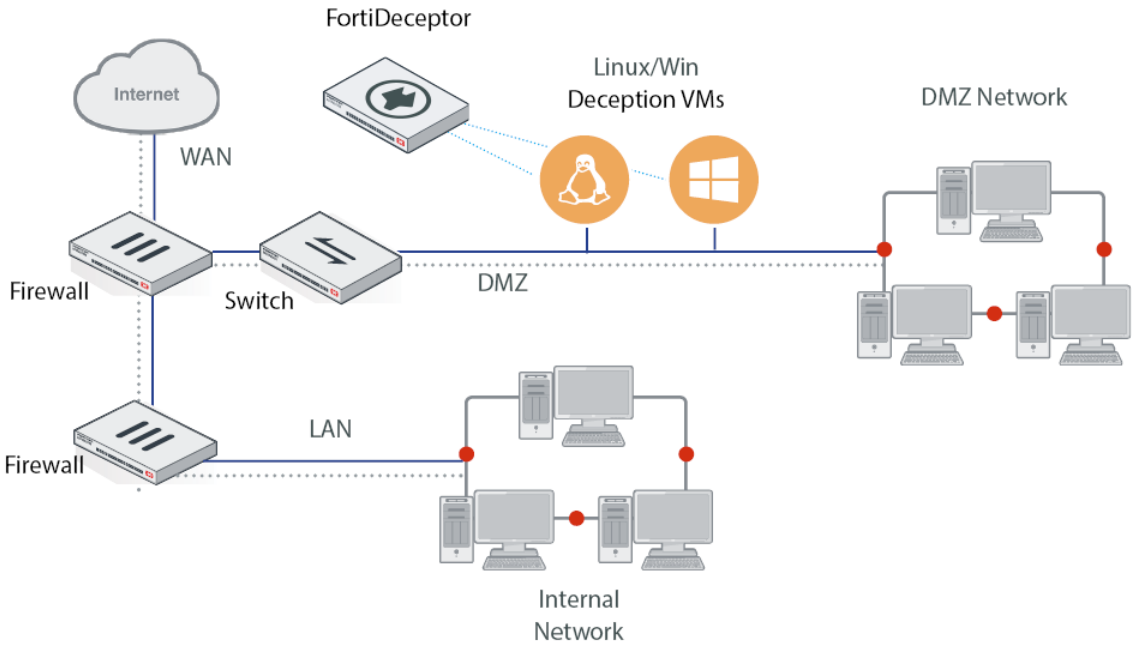
Port (Interface)	Default Open Ports
Port1	TCP ports 22 (SSH), 23 (Telnet), 80 and 443 (GUI). FortiGuard Distribution Servers (FDS) use TCP port 443 or 8890 for download. FortiDeceptor uses a random port picked by the kernel. FortiGuard Web Filtering servers use TCP port 443 or UDP port 53 or 8888. FortiDeceptor uses a random port picked up by the kernel. FortiDeceptor deception VM download uses TCP port 443 for download. FortiDeceptor uses a random port picked by the kernel. FortiDeceptor Manager is required to open port 8443 **from** the client (remote appliance) to the FortiDeceptor Manager. FortiDeceptor Manager is required to have access to *virustotal.com* over port 443 for malware analysis based on MD5 request.
Port2 to port8	Each FortiDeceptor port can be directly connected to a specific VLAN or use the network trunk to communicate with multiple VLANs from a single interface. In DMZ mode, no service listens. In regular mode, token communication service listens on deployment interface monitor IP with port 1443. The token communication uses HTTPS protocol.

The default port for FortiDeceptor VM is 443. To add HTTP, SSH, Telnet or another port, go to *Network >Interfaces > port1> Edit*.

DMZ Mode

Deploy a FortiDeceptor hardware unit or VM in the Demilitarized Zone (DMZ). You can monitor attacks on the DMZ network when FortiDeceptor is installed in the DMZ network.

DMZ mode is useful when you want to deploy decoys to a segment of the network that hosts critical services. When a threat actor attacks a server and attempts to move laterally inside the DMZ segment they are detected by the decoys without exposing the decoys on the Internet.



Limitations of the DMZ Mode

The DMZ Mode in FortiDeceptor functions like regular mode with the following exceptions:

- When DMZ mode is enabled, the banner displays *DMZ-MODE*.
- In *Deception* > *Deployment Network*, *Deception Monitor IP/Mask* is hidden. See Deployment Network on page 67.
- In *Deception* > *Decoy & Lure Status* in the Deception Status view, the Attack Test selection is disabled.
- Decoy VMs are limited to one deploy Interface. For information about IP address range, see Deployment Wizard on page 72.

To enable DMZ mode in the CLI:

```
dmz-mode -e
```

To disable DMZ mode in the CLI:

```
dmz-mode -d
```

Enabling or disabling the DMZ mode removes all previous configurations including Decoy VMs, lures, and tokens. Deception OS is not removed.

JSON API

FortiDeceptor provides a Representational State Transfer (REST) API for interaction with system components. Programs communicate with the REST API over HTTP, the same protocol your web browser uses to interact with web pages.

The REST-API authentication is based on a token generated by the FortiDeceptor.

The FortiDeceptor API has the following capabilities:

- Get the decoy deployment template list.
- Deploy decoys based on the decoy template configuration and the deployment network configuration (both STATIC and DHCP IP).
- Get a decoy deployment status.
- Stop/start the deployed decoys.
- Get incident alerts based on filter requests like time range (last minutes/hours/days) / service name/decoy name.

The *FortiDeceptor JSON API Reference* guide is available in the Fortinet Developer Network (FNDN). To access the guide, log in to FNDN and enter `FortiDeceptor` in the *Search* field.

Fortinet Developer Network is a subscription-based community. For more information about FNDN, visit Fortinet Worldwide Developer Community.

Deploy Decoy VM

Use the *Deception* pages to deploy Decoy VMs on your network. When a hacker gains unauthorized access to Decoy VMs, their movements can be monitored to understand how they attack the network.

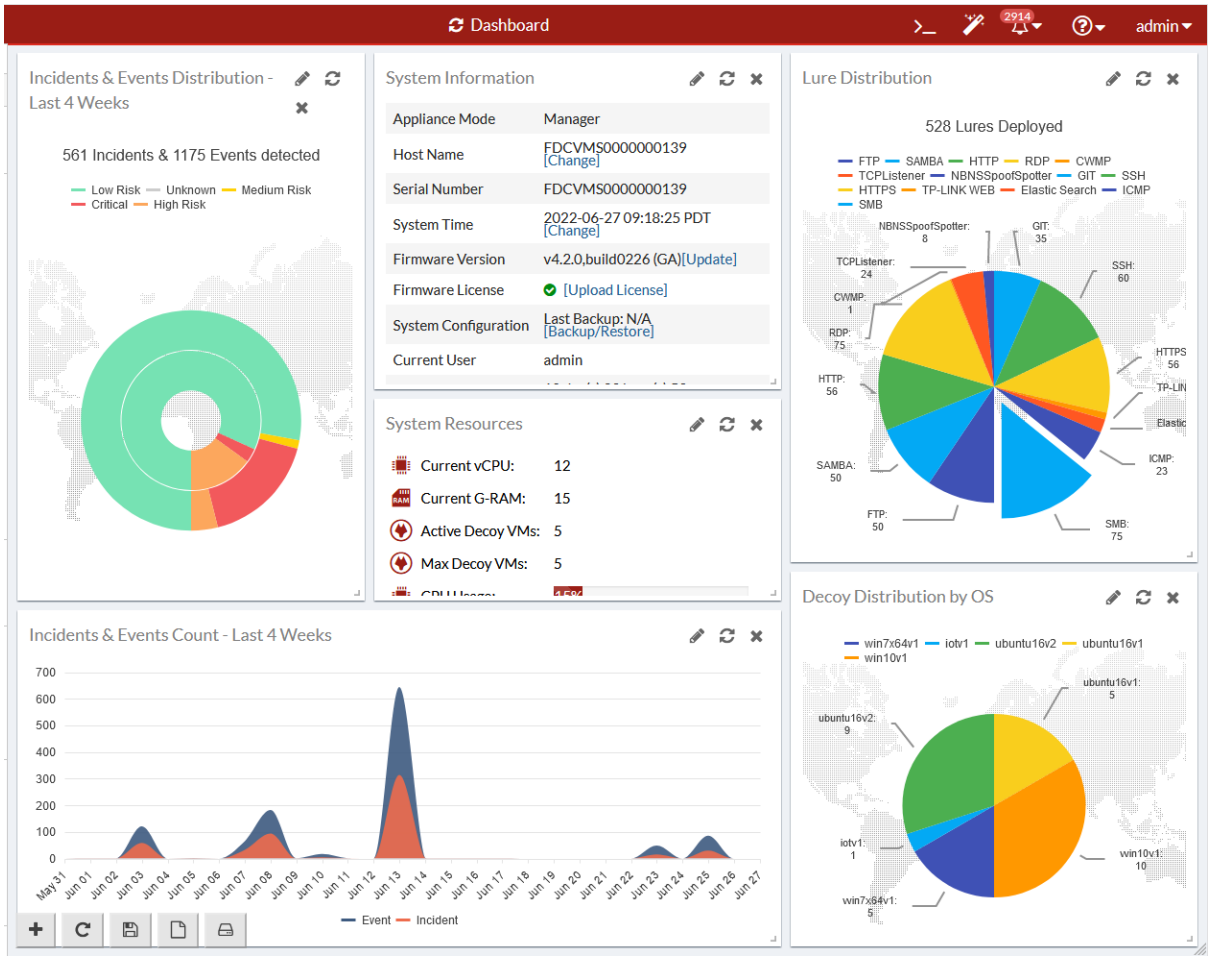
To use FortiDeceptor to monitor the network:

Task	Location in GUI	More information
Check the Deception OS is available	Go to Deception > Deception OS	See Deception OS on page 66.
Auto-detect or specify the network where the Decoy VMs are deployed	Go to *Deception* > *Deployment Network*	See Deployment Network on page 67.
Deploy the Decoy VM on the network	Go to *Deception* > *Deployment Wizard*	See Deployment Wizard on page 72.
Start or stop the deployed Decoy VMs, or download the FortiDeceptor token package to manually install it on computers	Go to *Deception* > *Decoy Status*	See Decoy Status on page 86.
Specify the IP address that is to be considered safe	Go to *Deception* > *Safe List*	See Safe List on page 94. This is useful when you want to log in to the deployment network without being flagged as an attacker.
View and work with lure resources	Go to *Deception* > *Lure Resources*	See Lure Resources on page 69.

For more information, see Deception deployment best practices on page 161.

Dashboard

The *Dashboard* contains system information widgets that allow you to monitor the performance of the FortiDeceptor. The Dashboard also includes widgets that provide an overview of incidents and events over the last 24 hours to 7 days. You can customize the Dashboard by adding and removing widgets.



The following widgets are available:

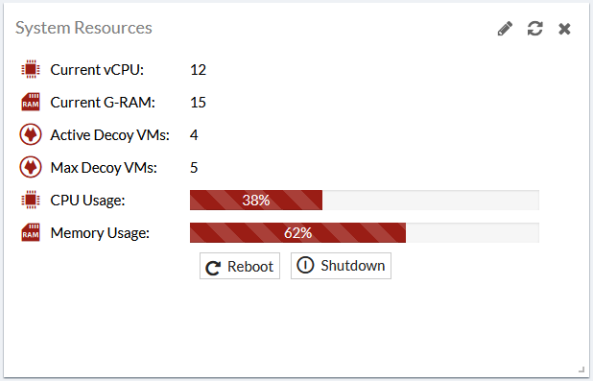
Widget	Description
System Resources	Hardware requirements benchmark for FortiDeceptor Virtual appliances only. This widget provides real-time guidelines for system performance and increasing vCPU & RAM resources during deployment and ongoing maintenance. The widget also provides the overall Real-time usage status of the CPU and memory.
System Information	Basic information about the FortiDeceptor system, such as the serial number, system up time, and license status information.
License Information	The list of VM license keys and their expiry dates.

Widget	Description
Disk Monitor	For hardware models: • The RAID level and status, disk usage, and disk management information. For VM models: • Disk usage.
Incidents & Events Distribution	Information about the number of incidents and events, and their level of severity.
Incidents & Events Count	Number of events occurring each day.
Decoy Distribution by OS	Number of decoys displayed as a pie-chart showing the OS such as Windows or Ubuntu.
Lure Distribution	Number of decoys deployed displayed a pie-chart showing the type of service such as SSH, SAMBA, SMB, SCADA, RDP, HTTP, HTTPS, IIS (HTTP, HTTPS), or MSSQL.
Incidents Distribution by Service	Information about the number and types of incidents, such as SMB, HTTP, TCP, and so on.
Top 10 Attackers by Incidents	The top 10 attackers by the number of incidents. .
Top 10 Attackers by Events	The top 10 attackers by the number of events.
Global Incidents Distribution	Displays the number of Attackers by country on a global map.
Top 10 IPS attacks	Displays the top 10 IPS attackers by the number of events.

For information about adding widgets, see Customizing the dashboard on page 30.

System Resources

The *System Resources* widget displays basic information about the FortiDeceptor system, such as the serial number, system up time, and license status information. Use the *System Resources* to reboot or shutdown the unit.



This *System Resources* widget displays the following information:.

Current vCPU	The current number of vCPUs.
Current G-RAM	The current amount of RAM in GB.
Active Decoy VMs	The current number of active decoy VMs.
Max Decoy VMs	The maximum number of decoy VMs.
CPU Usage	The CPU usage as a percentage.
Memory Usage	The memory usage as a percentage.

Reboot or shut down the unit

To avoid potential configuration or hardware problems, always use the GUI or CLI to reboot or shut down FortiDeceptor.

To reboot the FortiDeceptor unit:

1. Go to *Dashboard* > *System Resources*.
2. Click *Reboot*.
3. Enter a reason for the reboot in the *Reason* field.
4. Click *OK*.

After reboot, the FortiDeceptor VM initialization requires approximately 30 minutes. The Decoy VM icon in the *System Information* widget shows a warning sign until the process completes.

When FortiDeceptor boots or reboots, the following critical event log message is normal:

The VM system is not running and might need more time to start up. Please check system logs for more details. If needed, please reboot system.

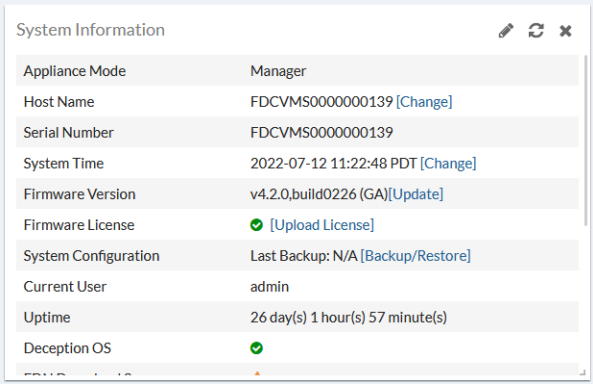
After upgrading FortiDeceptor to a new firmware version, the system might clean up data and a *Database is not ready* message displays. The clean up time depends on the size of historical data.

To shut down the FortiDeceptor unit:

1. Go to *Dashboard* > *System Resources*.
2. Click *Shutdown*.
3. Enter a reason for the shutdown in the *Reason* field.
4. Click *OK*.

System Information

The *System Information* widget displays information about the FortiDeceptor device. Use this widget to configure the device host name, update the firmware version, upload a license or back up the system configuration.



This widget displays the following information and options.

Appliance Mode	The mode of the appliance: Manager, Client, or standalone.
Appliance CM Status	Optional for client appliance. Display the status in Central Management. See Central Management on page 32.
Appliance CM Live Time	Optional for client appliance. The last live timestamp in Central Management. See Central Management on page 32.
Host Name	The name assigned to this FortiDeceptor unit. Click *Change* to edit the FortiDeceptor host name.
Serial Number	Serial number of this FortiDeceptor unit. The serial number is unique to the FortiDeceptor unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
System Time	The current time on the FortiDeceptor internal clock or NTP server. Click *Change* to configure the system time. See Configure the system time on page 13.
Firmware Version	Version and build number of the firmware installed on the FortiDeceptor unit. To update the firmware, you must download the latest version from the Fortinet Customer Service & Support portal. Click *Update* or *UPDATE AVAILABLE* and select the firmware image to load from the local hard disk or network volume. For information, see Update FortiDeceptor firmware on page 22.
Firmware License	To load a firmware license, click *Upload License* and select a license file. See Upload license file to FortiDeceptor on page 14.
System Configuration	Date and time of the last system configuration backup. Click *Backup/Restore* to go to the *System Recovery* page. See Back up or restore the system configuration on page 23.
Current User	The administrator that is currently logged into the system.

Uptime	Duration that the FortiDeceptor unit has been running since it booted up.
Deception OS	Deception OS license activation and initialization status. Displays a green check mark if the Deception OS is activated and initialized. A *Caution* icon is displayed if the Deception OS is initializing or having issues. Hover you mouse over the status icon to view detailed information. For more information, see *Log* > *All Events*. To go to *Deception* > *Deception OS* to see the images available on FortiDeceptor, click *Update* or *UPDATE AVAILABLE*. After purchase, download the license file from the Fortinet Customer Service & Support portal. Then click *Upload License* to select the license file. The system reboots and activates the newly-installed Deception OS.
FDN Download Server	Shows if the FDN download server is accessible. When the FDN download server is inaccessible, no update packages are downloaded.
Web Filtering Server	Shows if the web filtering query server is accessible.
Antivirus DB Contract	Brief information about this contract.
Antivirus Engine Contract	Brief information about this contract.
IDS Engine/DB Contract	Brief information about this contract.
Web Filtering Contract	Brief information about this contract.
ARAE Engine Contract	Brief information about this contract.
Custom VM Contract	Brief information about this contract. This is displayed when FortiDeceptor is running a v1 license.
SSL VPN Contract	Brief information about this contract. These is displayed when FortiDeceptor is running a v4 license.

To change the Host Name:

1. Go to *Dashboard* > *System Information* widget.
2. Click *Change*. The *Edit Host Name* page opens.
3. In the *New Name* field, enter the new Host Name and click Apply.

Update FortiDeceptor firmware

A best practice is to stay up-to-date with patch releases for currently deployed major release. Only update to a new major release or version when you are looking for specific functionality in the new major release or version. For more information, see the *FortiDeceptor Release Notes* or contact Technical Support.

Before any firmware update, complete the following:

- Download the FortiDeceptor firmware image and Release Notes document from the Fortinet Customer Service & Support portal. Review the Release Notes, including the special notices, upgrade information, product integration and support, and resolved and known issues.

- Back up your configuration file. It is highly recommended that you create a system backup file and save it to your management computer. You can also schedule the system to back up system configurations to a remote server. See, Back up or restore the system configuration on page 23.
- Plan a maintenance window for the firmware update. If possible, consider setting up a test environment to check that the update does not negatively impact your network.

To update the FortiDeceptor firmware:

1. Go to *Dashboard* > *System Information* > *Firmware Version*.
2. In the *System Information* widget beside *Firmware Version*, click *Update* or *UPDATE AVAILABLE*.
3. Click *Choose File* and locate the previously downloaded firmware image on your management computer; then click *Submit* to start the upgrade.
   Alternatively, in the *AVAILABLE FIRMWARE* pane *Install* column, click the download icon beside the firmware release you want. The system upgrades and restarts automatically.

When the update is complete, test your FortiDeceptor device to ensure that the update was successful.

Back up or restore the system configuration

We recommend that your regular maintenance includes system backups. Always backup before upgrading firmware or making major system configuration changes. Save configuration backups to a management computer in case you need to restore the system after a network event.

The FortiDeceptor configuration file is in binary format and manual editing is not supported.

To back up the FortiDeceptor configuration to your local management computer:

1. Go to *Dashboard* > *System Information* > *System Configuration*.
2. Click *Backup/Restore*.
3. Click *Click here* to save your backup file.

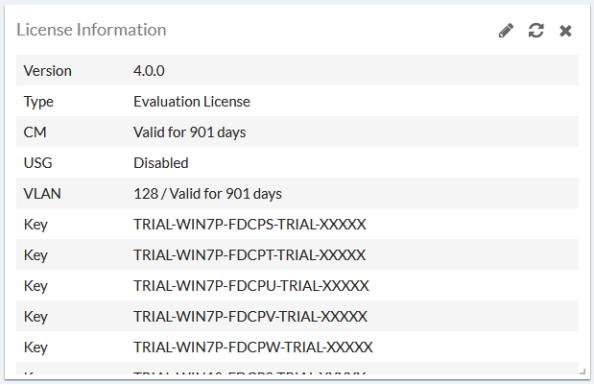
To restore the FortiDeceptor configuration:

1. Go to *Dashboard* >*System Information* > *System Configuration*.
2. Click *Backup/Restore*.
3. Click *Choose File* and locate the backup file on your management computer.
4. Click *Restore* to load the backup file.
5. Click *OK*.
   When the system configuration restore process completes, the login page appears.

When you do a system restore, all configurations are replaced with the backup data. The system reboots automatically to complete the restore. Only the backup configuration file from the previous or the current release is supported.

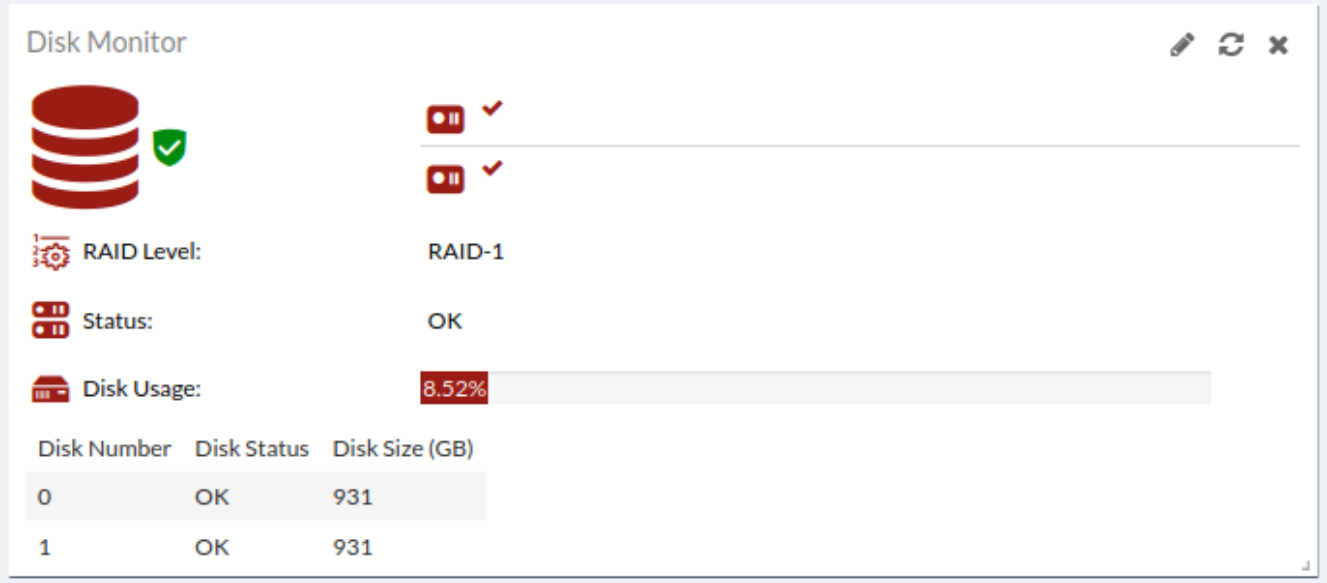
License Information

The License Information widget displays the license version, type, expiration dates and license key.



Disk Monitor

This *Disk Monitor* is only available in hardware-based models. This widget displays the RAID level and status, disk usage, and disk management information.



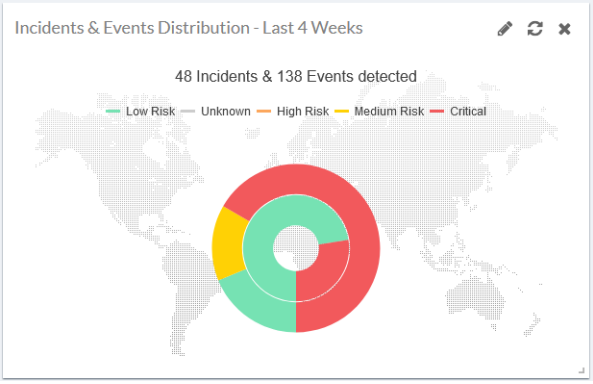
This *Disk Monitor* displays the following information:

RAID Level	The RAID level.
Disk Status	The disk status.
Disk Usage	The current level of disk usage as a percentage.
Disk Number	The disk number.

Disk Size	The disk size in GB.

Incidents & Events Distribution

This *Incidents & Events Distribution* widget displays the number of incidents and events by risk level as a pie chart. Hover the pie chart to see the number of Incidents or Events and their percentage.

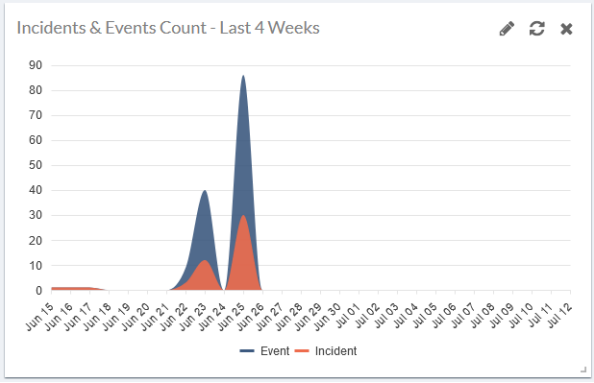


The *Incidents & Events Distribution* widget shows following risk level information:

Unknown	*Incident* or *Event* where the risk level is unknown. Entries are in grey.
Low Risk	*Incident* or *Event* where the risk level is low. Entries are in green.
Medium Risk	*Incident* or *Event* where the risk level is medium. Entries are in yellow.
High Risk	*Incident* or *Event* where the risk level is high. Entries are in orange.
Critical	*Incident* or *Event* where the risk level is critical. Entries are in red.

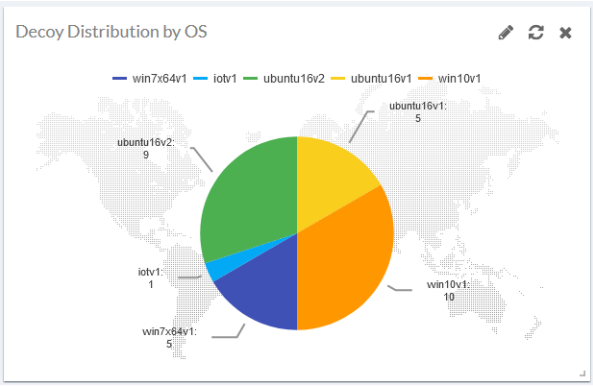
Incidents and Events Count

The *Incidents and Events Count* widget displays the number of Incidents and Events as a chart. The Events are in blue and the Incidents are in orange. Hover over the chart to view the counts by date. To filter the chart, click *Event* or *Incident* in the legend.

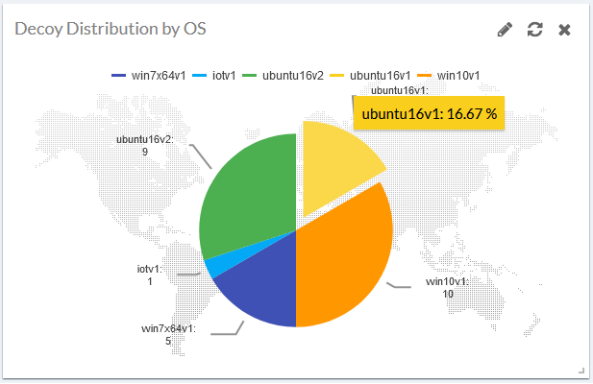


Decoy Distribution by OS

The *Decoy Distribution by OS* widget displays the number and percentage of Decoy VMs by OS as a pie chart. Hover over a piece of the chart to view the distribution by percentage. To filter the chart by OS, click the OS name in the chart legend.



Click a piece of the chart to isolate a Decoy VM from the chart.



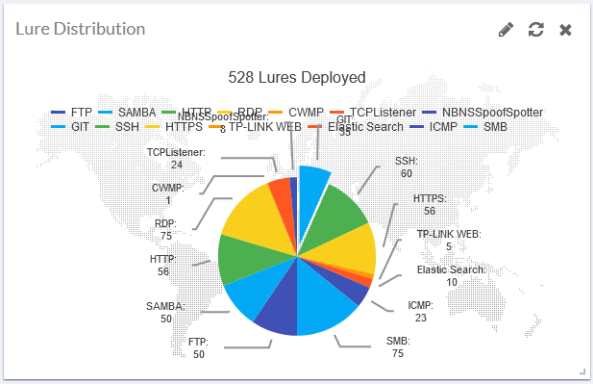
Supported OS types:

The *Decoy Distribution by OS* widget displays the distribution for the following OS types:

Ubuntu, Windows, SCADAV3, SSLVPN, Medical, ERP, POS, IoT and SAP.

Lure Distribution

The *Lure Distribution* widget displays the number of lures deployed as a pie chart. Hover of a piece of chart to view the number and percentage of decoys by service. To filter the chart, click the service name in the legend.



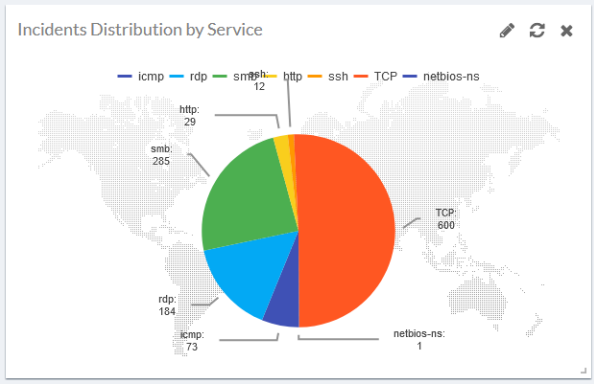
Supported services

The *Lure Distribution* widget displays information for of decoy images using the following services:

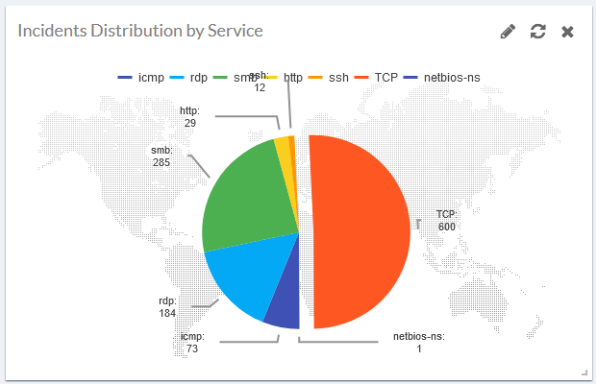
SSH, SAMBA, SMB, TCPLISTENER, NBNSSpoofSpotter, RDP, HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, Guardian-AST, IEC104, MSSQL, IIS, GIT, ENIP, Infusion Pump Telnet, Infusion Pump FTP, POS-WEB, ERP-WEB, PACS, PACS-WEB, DICOM, SSLVPN, DNP3, Telnet, Printer-WEB, JETDIRECT, IP CAMERA-WEB, UPNP, RTSP, SAP WEB, SAP ROUTER, SAP DISPATCHER , TP-LINK WEB and CWMP

Incidents Distribution by Service

The *Incidents Distribution by Service* widget displays the number of incidents by service as a pie chart. Hover over a section of chart to view the percentage by service. To filter the chart by service, click the service name in the chart legend.



Click the pie chart to split a service from the chart.



Supported services

Incidents Distribution by Service widget displays incidents occurring for the following services:

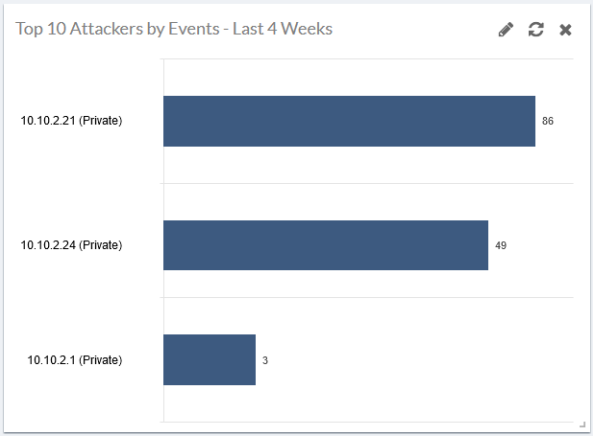
SSH, SAMBA, SMB, RDP, SWIFT Lite2, HTTPS, HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, IEC104, HTTPS, PACSWEB, POSWEB, AST, IPCAMERA, JETIRECT, TELNET, SSLVPN, KAMSTRUP, DICOM, ENIP, UPNP_HTTP, GIT, RTSP, PRINTER, DNP3, SAP_DISPATCHER, SAP_WEB_HTTPS, SAP_WEB,SAP_ROUTER,NETBIOS-NS, and ERPWEB

Top 10 Attackers by Incidents

The *Top 10 Attackers by Incidents* widget displays the top ten attackers by the number of incidents as well as the attacker's IP address. Hover over a bar in the chart to view the number of incidents by IP.

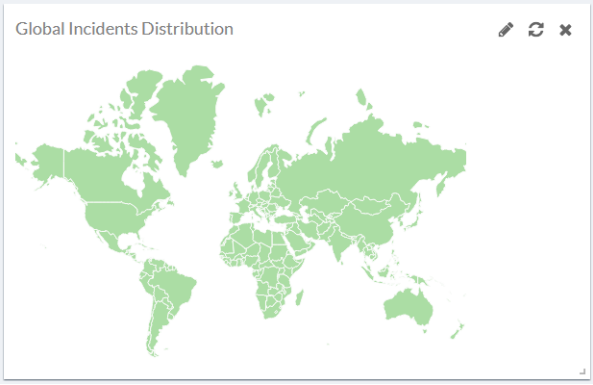
Top 10 Attackers by Events

The *Top 10 Attackers by Events* widget displays the top ten attackers by the number of events as well as the attacker's IP address. Hover over a bar in the chart to view the number of events.



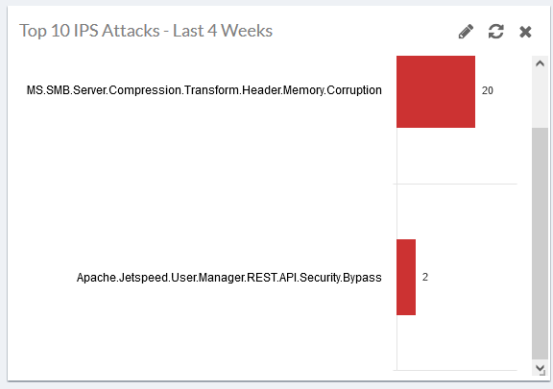
Global Incidents Distribution

The *Global Incidents Distribution* widget displays the number of attackers by country on a global map. Hover over each country to see the number of attackers from each country.



Top 10 IPS Attacks

The *Top 10 IPS Attacks* widget displays the IPS attack name and number of events for the selected time period (24 hours, 7 Days, or 4 weeks).



Customizing the dashboard

You can select which widgets to display on the Dashboard and where they are located on the page. You can also configure the time period and refresh interval for individual widgets.

Dashboard toolbar

The dashboard toolbar is located near the bottom of the pages. You can perform the following tasks:

- Click *Add Widget* to add a widget to the dashboard.

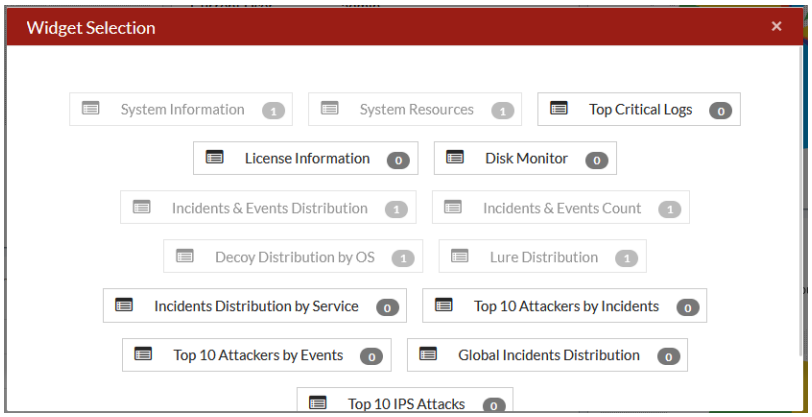
- Click *Reset* to restore the dashboard settings. This will remove any widgets you added to Dashboard and revert any changes you made to the widget settings.

- Click Save to save the current Dashboard view.

- Click *Save as Default* to save the current layout as the default Dashboard view.

To add a widget to the Dashboard:

1. Click the Add icon. The *Widget Selection* dialog opens.



2. Select the widget you want to add to the Dashboard.

Widget toolbar

The widget tools are located in the widget header.

- Click *Edit* to configure the widget Time Period and Refresh Interval. The widgets setting will vary depending on the widget.
- Click *Refresh Data* to refresh the widget data.
- Click *Delete* to remove a widget from the Dashboard.

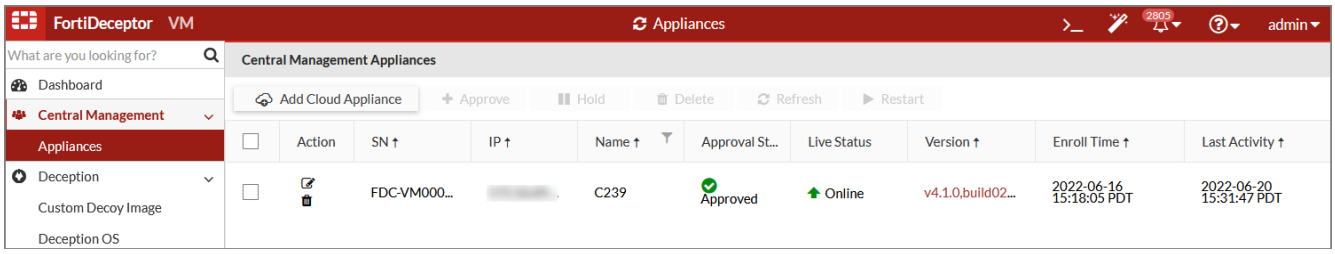
Central Management

Central Management allows you to manage remote FortiDeceptor appliances including Decoy VM deployments, system configuration, and incident alert monitoring.

You can configure a FortiDeceptor hardware or VM appliance to be a Management Device or Remote Client. The Management Device has deception capabilities. You can use the Management Device to deploy decoys and lures to the Remote Clients on the network.

Network communication requirements:

Communication between:	From:
Management device and regular client appliance	Client to manager port1 IP and 8443 port
Management device and cloud client appliance	Management device to cloud client port1 public IP and 8443 port

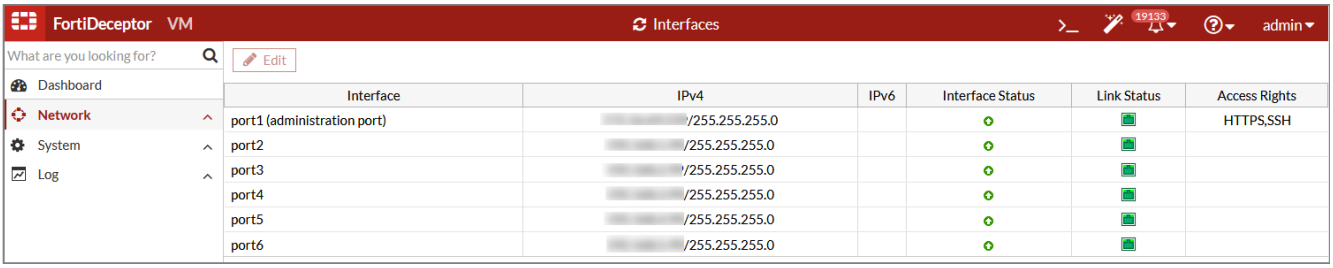


Use the buttons in the *Central Management Appliances* pane to manage Remote Clients.

Button	Description
Approve	Allow the selected clients to participate in Central Management.
Hold	Pause the selected clients' participation in Central Management.
Delete	Pause the selected clients and then permanently delete related data in the Manage Device's local database, including OS, network settings, decoys, and lures. This action does not: • Delete or change any data in the Remote Client. • Change incident and campaign data generated in the past.
Refresh	Force re-sync all data between manager and selected clients.
Restart	Send signal to selected clients to reboot.

Remote Client

When a FortiDeceptor is managed as a Remote Client the navigation pane will only displays the *Network*, *System* and *Log* modules.



To prevent access to a Remote Client outside the Central Management or other trusted IP addresses, go to System > Administrators. See Administrators on page 124.

When the Remote Client is a cloud device, configure the trusted host with the Management Device's IP to ensure only the Management Device can access itself.

On the Management Device, configure the trusted host with regular client IPs to ensure regular clients can access Management Device.

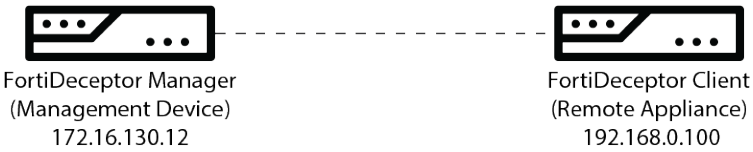
When you deploy a decoy or network, select the local or Remote Client name. Use the local configuration to deploy decoys and lures from the Management Device.

Configuring Central Management

To configure Central Management:

1. Enable Central Management on the Management Device.
2. Enable Central Management the Remote Client.
3. Approve the Remote Client on the Management Device.
4. Configure the Remote Client with the Management Device.

The tasks below are based on the following topology:



To enable Central Management on the Management Device:

```
cm -sc -mM -nManager -a<password>
```

Example:

```
cm -sc -mM -nManager -a1234567890
```

To enable Central Management on the Remote Client:

Before configuring FortiDeceptor as a Remote Client, perform a `factory reset` and basic network configuration to avoid data incompatibility between the Management Device and Remote Client. For more information on manager and client configuration, see the *CLI Reference*.

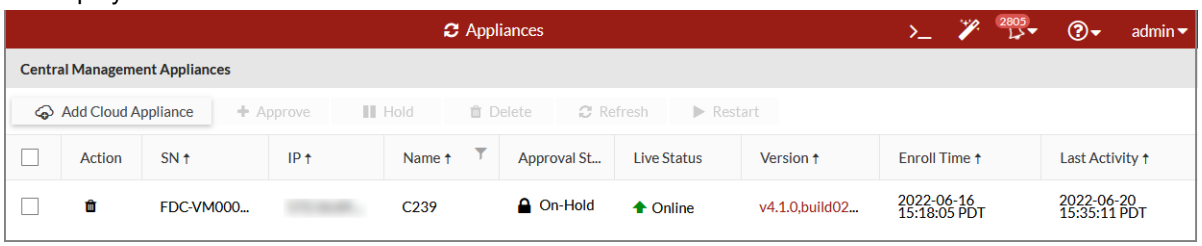
```
cm -sc -mC -nAppliance1 -a<password> -i<manager_ip_address>
```

Example:

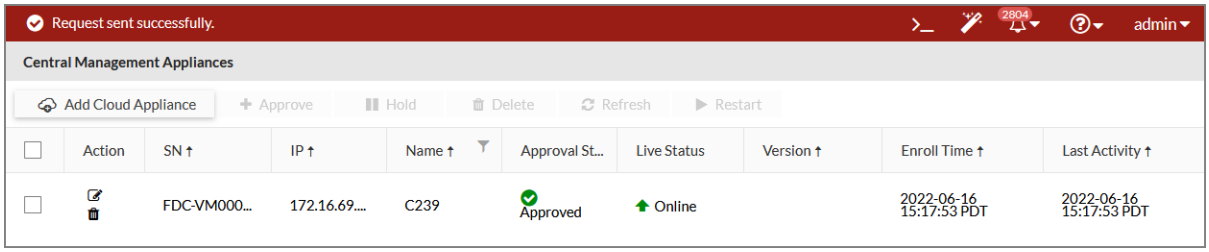
```
cm -sc -mC -nAppliance1 -a1234567890 -i172.16.130.12
```

To approve a Remote Client with the Management Device:

1. On the Management Device, go to *Central Management* > *Appliances*. The *Approval Status* for the Remote Client will display *On-Hold*.



2. Select the appliance and click *Approve*. The *Approval Status* changes to *Approved*.



To configure the Remote Client with the Management Device:

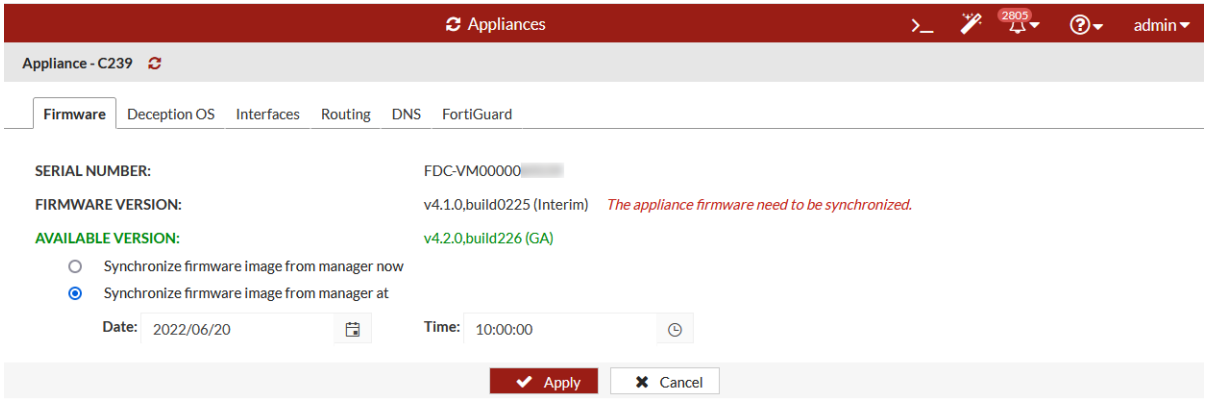
1. On the Management Device, go to *Central Management* > *Appliances*.
2. In the *Action* column, click the *Config* icon ✎. The Appliance - <name> page displays the following tabs.

Firmware	Push FortiDeceptor firmware updates and upgrades to the Remote Client. Synchronization can be immediate or scheduled.
Deception OS	Push deception VM images from the Management Device to the Remote Client. Synchronization can be immediate or scheduled.
	Status — Current status of deception OS image.
	Name — Name of deception OS.
	OS Type — Type of this deception OS.

	VM Type	Category of this deception OS.
	Lures	Lure services can be provided by this deception OS.
Interfaces	Configure the Remote Client network interfaces.	
Routing	Configure the Remote Client network routing table.	
DNS	Configure the Remote Client DNS configuration.	
FortiGuard	Configure the Remote Client FortiGuard configuration.	

3. To synchronize the firmware, click the *Firmware* tab and select one of the following options and then click *Apply*:

Synchronize firmware image from manager now	Click to synchronize the firmware immediately.
Synchronize firmware image from manager at	Click to schedule the synchronization.



To remove a client from Central Management:

1. On the Remote Client, run the following CLI command:
   ```
   cm -sc -mN
   ```
   After a client leaves Central Management, its status on the manager changes to *Offline*.
2. On the Management Device, select that client and click *Delete*.

To remove the Management Device from Central Management:

1. On the Management Device, run the following CLI command:
   ```
   cm -sc -mN
   ```

Deception

Use the *Deception* module to customize, deploy, and monitor decoys.

This section includes the following topics:

- Deception OS on page 66

  View the deception OSes available for creating Decoy VMs. You can also upload a deception OS package or synchronize the deception OS list.

- Custom Decoy Image on page 36

  Create custom OS images for the decoy. FortiDeceptor supports Decoy Customization with a purchased FDC Custom Decoy Subscription.

- Deployment Network on page 67

  Set up a monitoring interface in a VLAN or a subnet.

- Lure Resources on page 69

  View the current lure, upload resources such as Word and PDF files to automatically generate lures, and import a user name list from an LDAP server.

- Deployment Wizard on page 72

  Create and deploy Decoy VMs on your network. Decoy VMs appear as real endpoints to hackers and can collect valuable information about attacks

- Decoy Status on page 86

  Monitor the status of the Decoys on your network.

- Deception Token on page 88

  Use a FortiDeceptor token package to add breadcrumbs on real endpoints and lure an attacker to a Decoy VM.

- Deployment Map on page 90

  View the entire network showing real endpoints and decoy VMs.

- Asset Discovery on page 92

  Generate Asset Inventory by passively fingerprinting the OS and other parameters for the assets in OT/IT/IoT networks.

- Safe List on page 94

  Add an IP address that is considered legitimate without generating an Event or Incident when accessing decoys.

Custom Decoy Image

For most deployments, the decoys included with FortiDeceptor are enough and are easier to deploy. However, you have the option to build a decoy from your gold image using the custom decoy feature that is included under the subscription license.

Some examples of using Decoy Customization include:

- Windows 10/11/2016/2019/2022 decoy joining AD.
- Windows 10/11 Enterprises users with SQL Server (without IIS server).
- Windows Server 2016/2019/2022 Enterprises users with SQL Server, web applications using an IIS server, and more.

This version only supports Decoy Customization for Windows 10/11 and Windows Server 2016/2019/2022. Windows Server 2016/2019/2022 supports customized MSSQL and IIS services. Windows 10/11 supports customized MSSQL.

Overview of implementing Decoy Customization:

1. Order the FortiDeceptor Custom Decoy Subscription for FortiDeceptor hardware appliance only.
   The Decoy Customization subscription is for FortiDeceptor hardware appliances only. This subscription license is already included in the FortiDeceptor VM bundle.
2. Install FortiDeceptor.
   After installing FortiDeceptor with the Decoy Customization subscription, the *Help* menu in the toolbar will display an option for the *Custom Decoy Image Cookbook*.
3. Follow the instructions in the *Customization Cookbook*. The high-level instructions are:
   a. Upload an ISO image.
   b. Install ARAE engine on image.
   c. Use the Deployment Wizard to install the customized decoy.

Customize the deception base OS image

Overview of customizing the deception base OS image:

1. Import Windows ISO image.
2. Customize VM image.
3. Deploy custom image.

Import Windows ISO image

Before importing an ISO image into FortiDeceptor, ensure you have completed the following:

- Purchased a FortiDeceptor Custom Decoy Subscription
  The FortiDeceptor Custom Decoy Subscription is for FortiDeceptor hardware appliances only. This subscription license is already included in the FortiDeceptor VM bundle.
- Set up an ISO image with the licenses for your environment. For example, if you want to allow Active Domain (AD) accounts to access decoys, configure the settings on the AD servers, such as create dummy accounts, and so on.

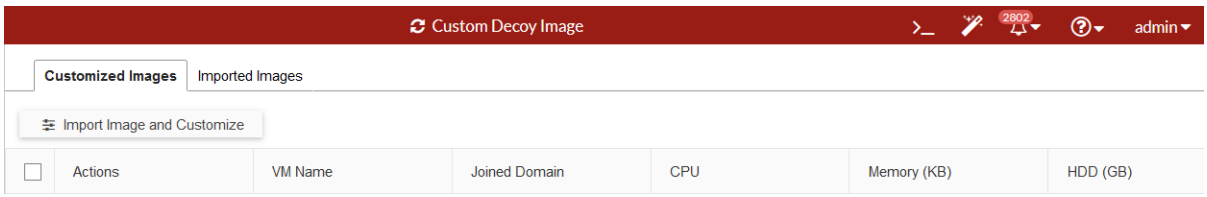
To import an ISO image using the Imported Images page:

1. Go to *Deception* > *Custom Decoy Image* and click the *Imported Images* tab.

2. Click *Import New ISO Image*.
3. Click *Choose a file* or drag and drop an image file into that pane.

To import an ISO image using the Customized Images page:

1. Go to *Deception* > *Custom Decoy Image* and click the *Customized Images* tab.



2. Click *Import Image and Customize*.
3. Click *Choose a file* or drag and drop an image file into that pane.

To delete an ISO image:

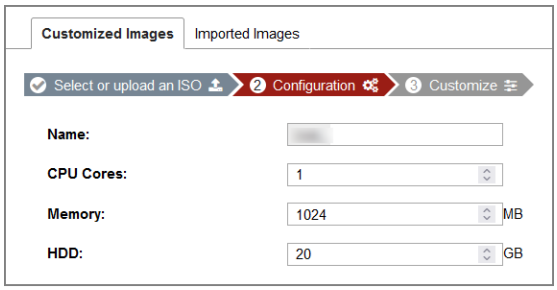
1. Go to *Deception* > *Custom Decoy Image* and click the *Imported Images* tab.
2. Select one or more images and then click *Delete*.

Customize VM image

To initialize the VM instance:

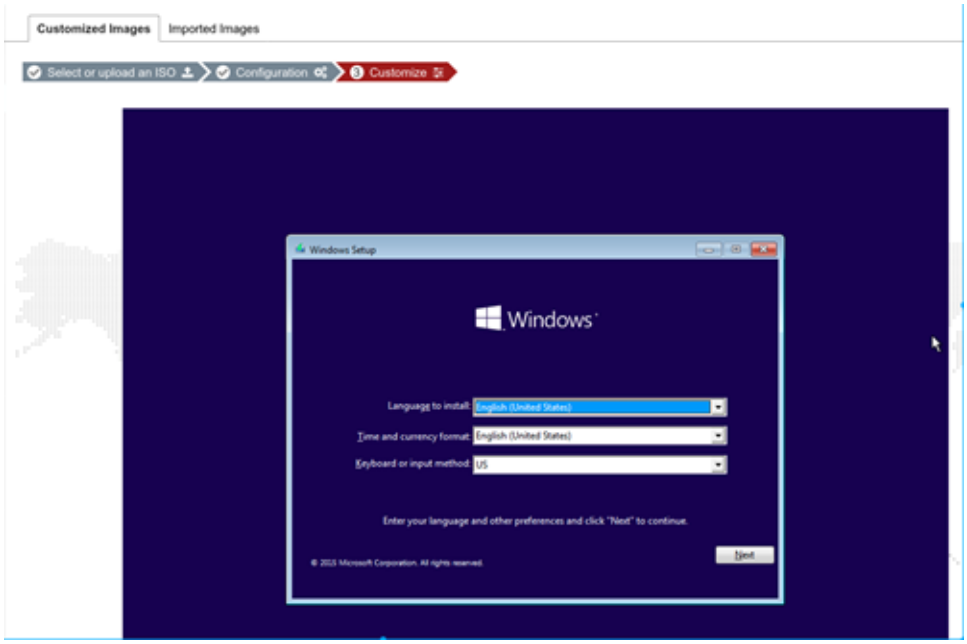
1. Go to *Deception* > *Custom Decoy Image* and click the *Customized Images* tab.
2. Click *Import Image and Customize*. The custom image wizard opens.
3. In the *Select an imported ISO image* dropdown list, select an ISO image. Then click *Next*.
4. In the *Configuration* step, specify the following and then click *Next*.

Name	Upper and lowercase letters and numbers totaling under 48 characters.
CPU Cores	1–4 cores.
Memory	1024–8192 MB.
Storage	20–50 GB.

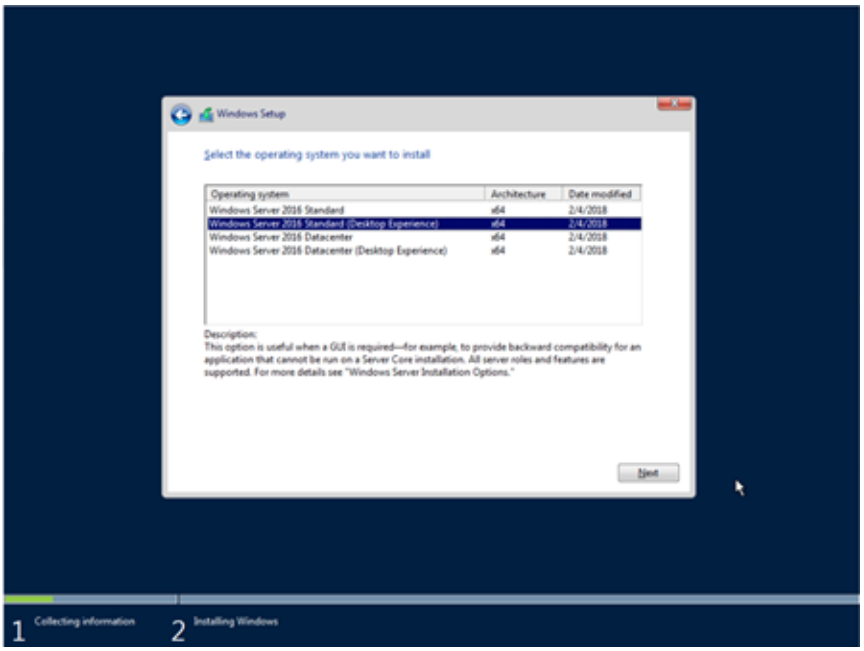


This configuration is applied to the VM instance for customizing the image, This configuration is **not** applied to decoys.

5. In the *Customize* step, install the OS from the ISO image.

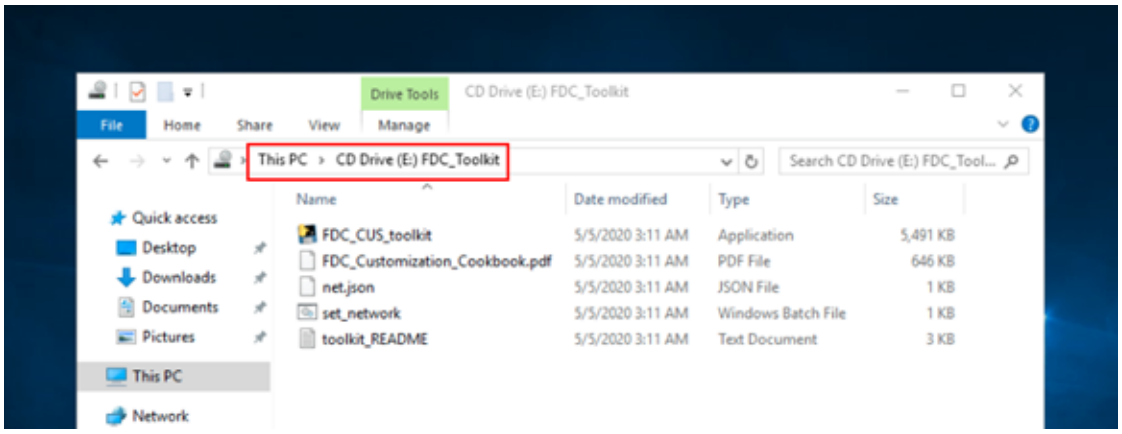


Follow the prompts until the installation is complete.



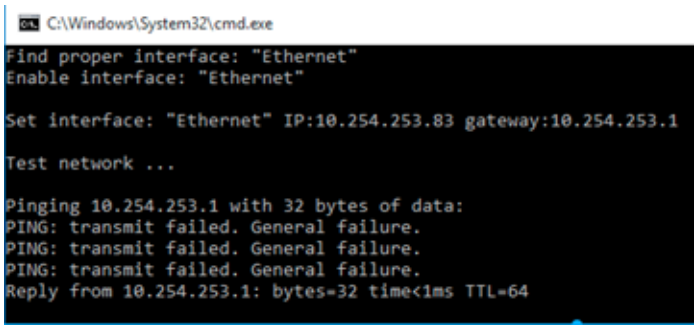
To customize the VM:

1. Ensure the OS is installed and then log in with an admin account.
2. In Windows Explorer, locate the *FDC_Toolkit* folder and read the instructions in *toolkit_README.txt*.



3. Configure the network using one of the following options.
   - Right-click *set_network.bat* and then click *Run as Administrator*.
   - Follow the instructions in *net.json* to configure the IP address, gateway, and DNS in Windows *Control Panel* >

Network and Internet > *Network Connections*.



10.254.253.0/24 set by the script is the internal NAT IP address that is temporarily used by the customization VM to allow downloading files and accessing other network resources via the FortiDeceptor default route.

To customize the system for Windows 2016:

1. Ensure your license is activated.
2. If you are using Windows 2016, enter the following commands in the PowerShell window to prevent lure configuration failures in the Decoy Deployment wizard.
```
secedit /export /cfg c:\secpol.cfg
(gc C:\secpol.cfg).replace("PasswordComplexity = 1", "PasswordComplexity = 0") | Out-
     File C:\secpol.cfg
secedit /configure /db c:\windows\security\local.sdb /cfg c:\secpol.cfg /areas
     SECURITYPOLICY
rm -force c:\secpol.cfg -confirm:$false
```

To customize the system for standalone Windows Server 2016:

1. Go to *Server Manager* > *Tools* > *Local Security Policy*. The *Local Security Policy* directory opens.
2. In the *Security Settings* folder, go to *Account Policies* > *Password Policy* folder, and double-click *Password must meet complexity requirements*.
3. Select *Disabled* and then click *OK*.
4. Open a Command Prompt as an Administrator and type the following command to update the group policy:
```
gpupdate /force
```
You should get the following response:
```
C:Users\Administrator>gpupdate /force
Updating policy...
Computer policy update has completed successfully.
```

To customize the system for Server 2016 Domain Controller :

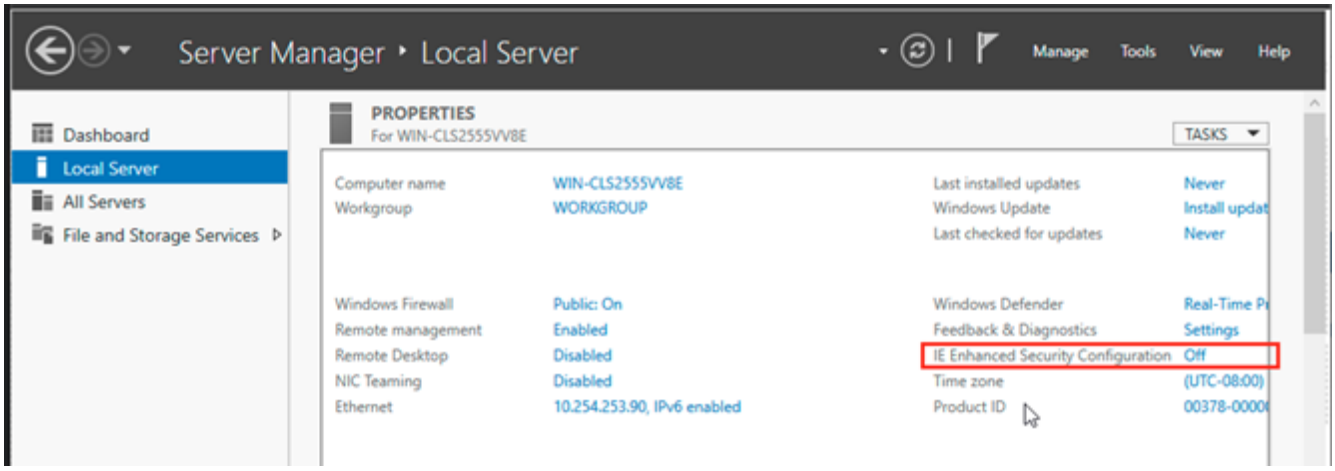
1. In the *Domain Controller*, go to *Server Manager* > *Tools* > *Group Policy Management*.
2. Right-click *Default Domain Policy* and click *Edit*. The *Group Policy Management Editor* opens.
3. In the *Computer Configuration* folder, go to *Policies* > *Windows Settings* > *Security Settings\Account Policies* > *Password Policy* > *Password must meet complexity requirements*.
4. Select *Disabled* and click *OK*.
5. Open a Command Prompt as Administrator and type the following command to update the group policy:
```
gpupdate /force
```

Optional: Install the Microsoft SQL Server

The following SQL Server versions are supported.

- SQL Server 2016: https://www.microsoft.com/en-us/download/details.aspx?id=56840
- SQL Server 2017: https://www.microsoft.com/en-us/download/details.aspx?id=55994
- SQL Server 2019: https://www.microsoft.com/en-us/sql-server/sql-server-downloads
- QL Server 2022: https://www.microsoft.com/en-ca/sql-server/sql-server-downloads
- SQL Server Management Studio for SQL server management and customization. https://aka.ms/ssmsfullsetup

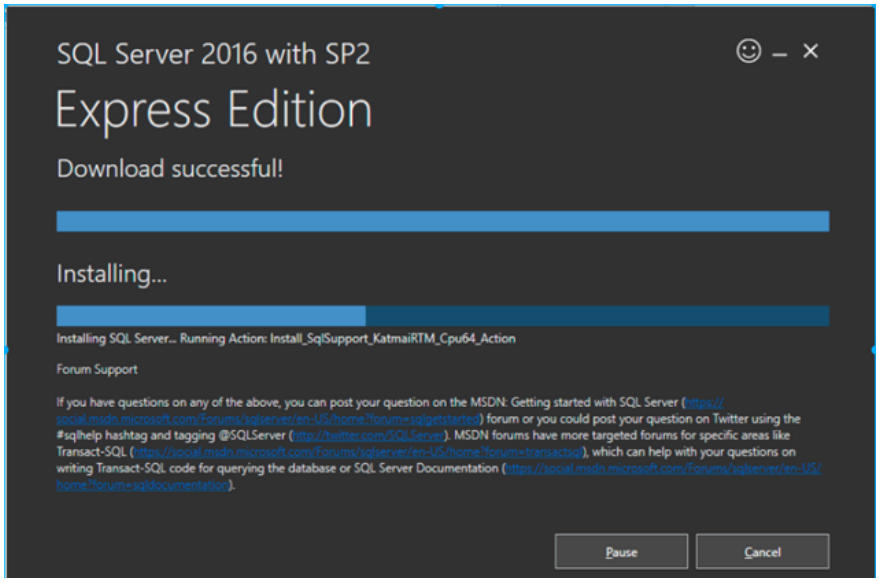
If you are downloading with Internet Explorer, it is recommended you disable *IE Enhanced Security Configuration*.



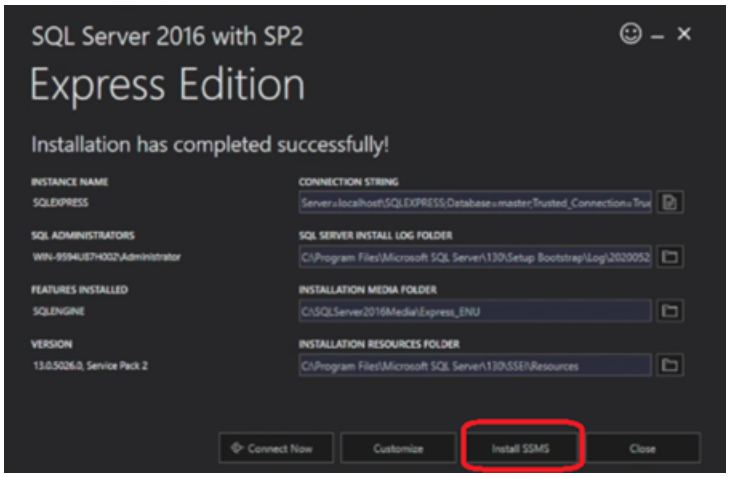
Since there is no desktop for Windows Server core OS, you must download the installation file on another computer and then use SMB to install the SQL Server.

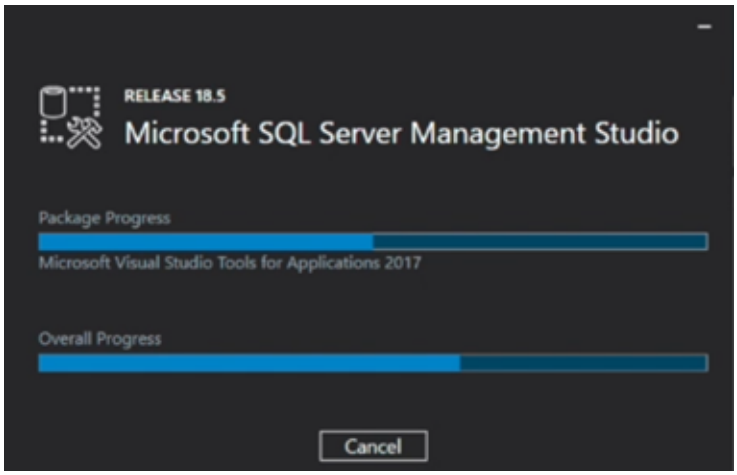
To install SQL server:

1. Download and install the SQL server on another computer.



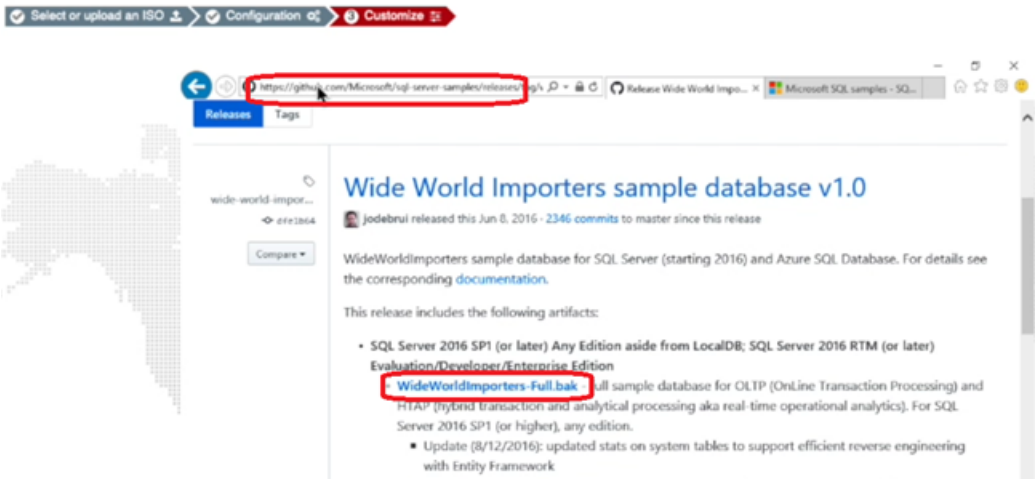
2. When the SQL Server installation is complete, click *Install SMSS* to download and install the SQL Server Management Studio to manage and customize the SQL Server.



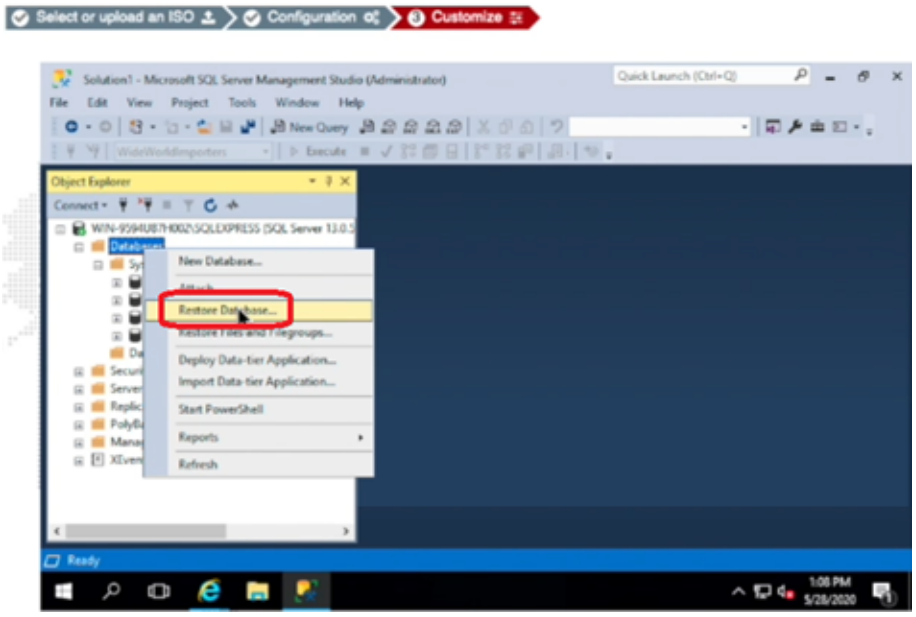


To further customize the SQL database:

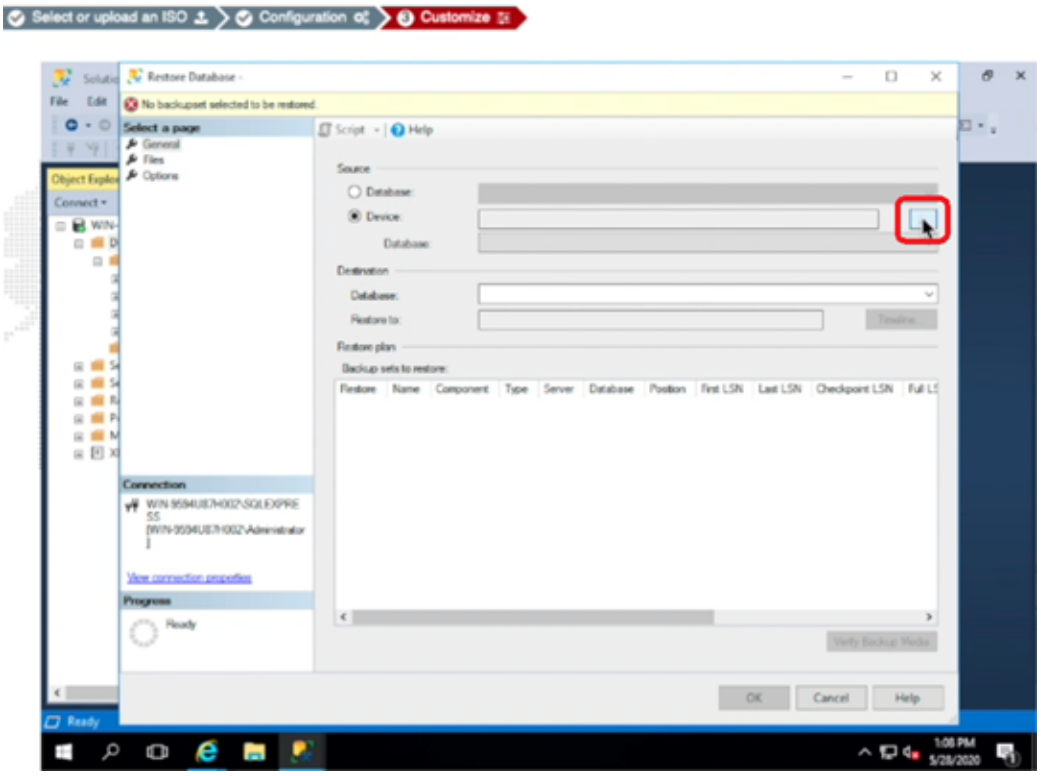
1. Download a sample database from https://github.com/Microsoft/sql-server-samples/releases/download/wide-world-importers-v1.0/WideWorldImporters-Full.bak.

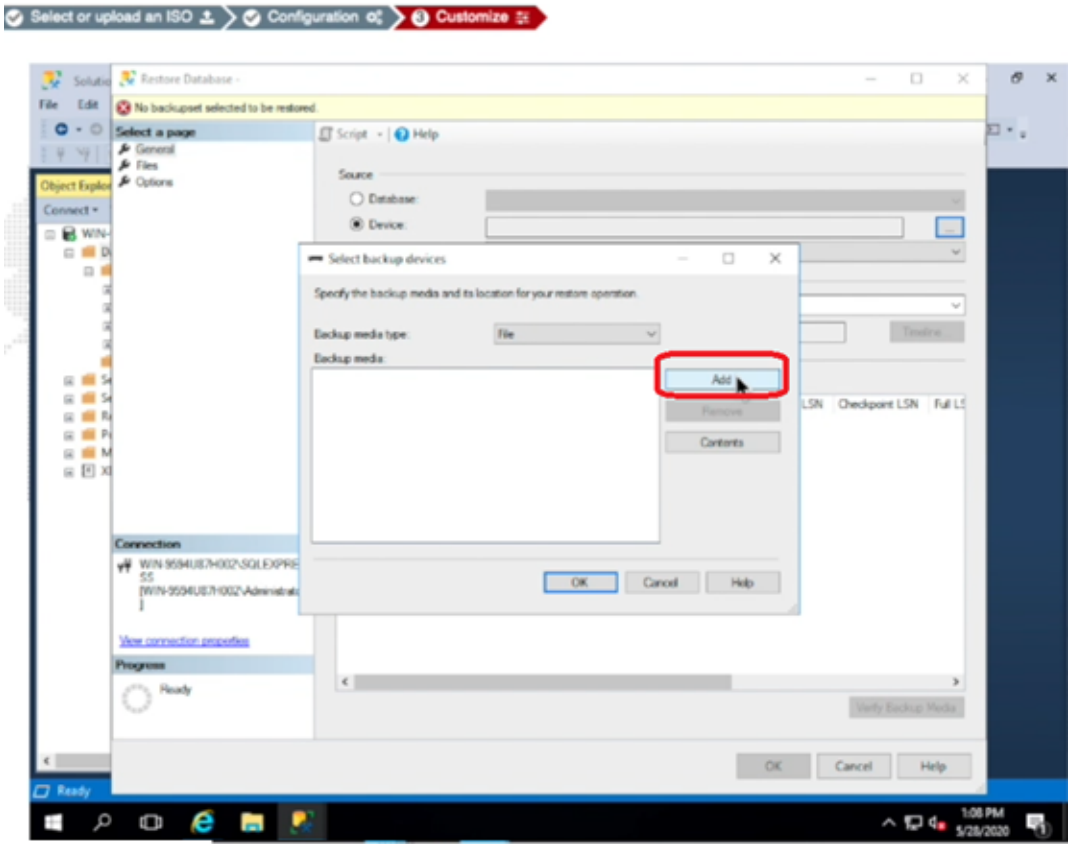


2. In the FortiDeceptor Customize Decoy console, open SQL Server Management Studio.
3. Right-click the database object and select *Restore Database*.

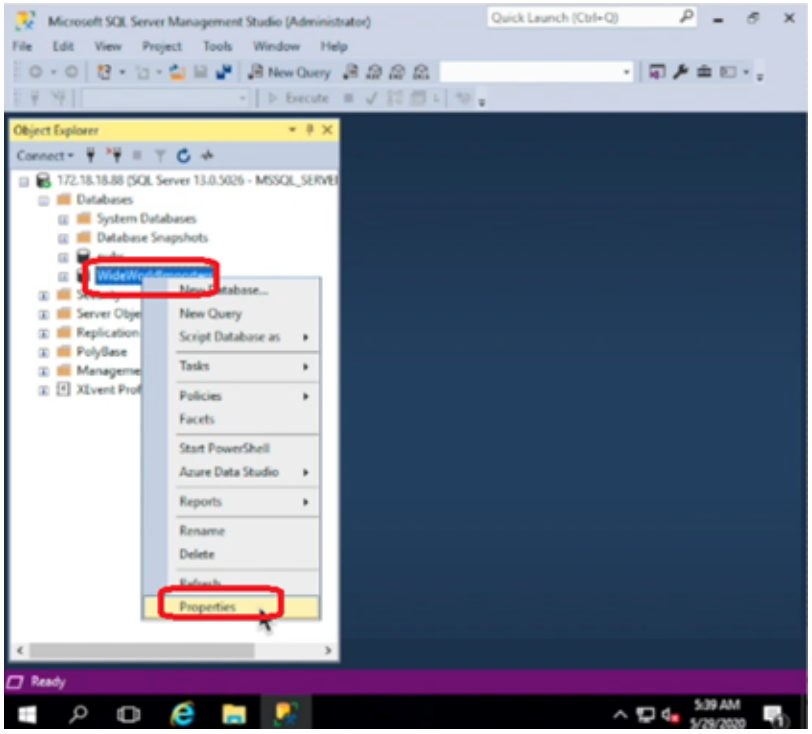


4. Locate and add the sample DB you downloaded.

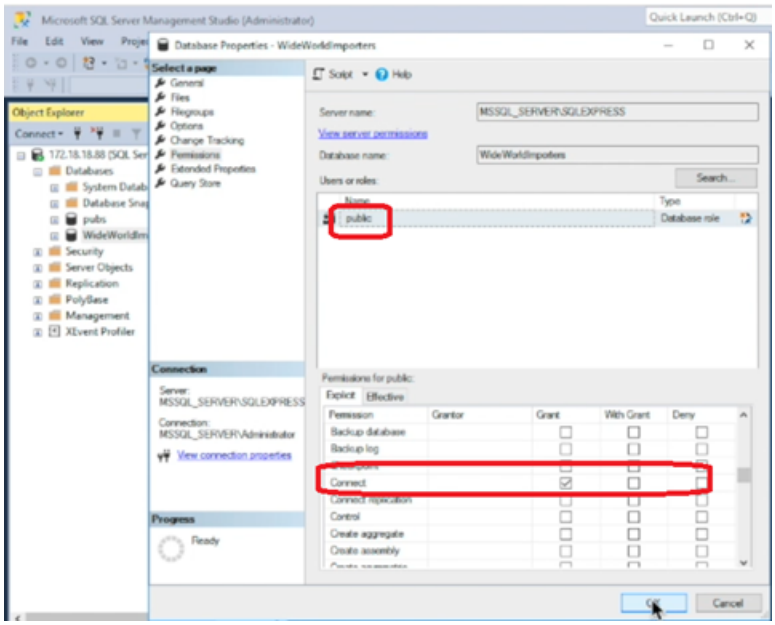




5. When the sample DB is restored, right-click that DB and select *Properties* to change access permission to make the decoy DB more attractive to attackers.



6. Give *Grant* permission to *Select* and *Connect*.



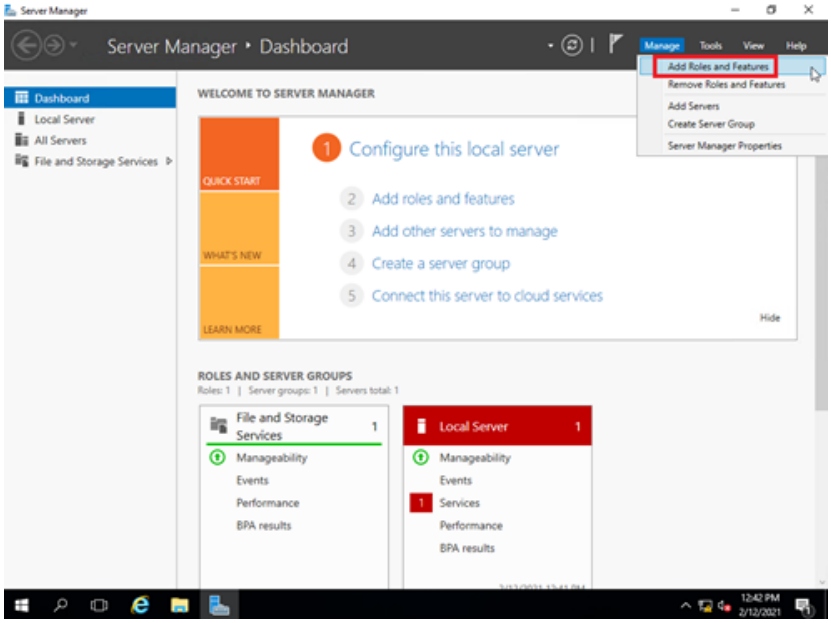
7. Close SQL Server Management Studio.
8. Verify that your DB is up using the command `netstat -an | findstr 1433`.
9. The listening port on the SQL Express Database is disabled by default. To enable the port:
   a. Click *Start* > *Programs* > *Microsoft SQL Server 20XX* and select *SQL Server Configuration Manager*.
   b. Select *SQL Server Network Configuration*.
   c. Double-click *Protocols for SQLEXPRESS*
   d. Right-click *TCP/IP* and select *Properties*. If necessary, first enable *TCP/IP*.
   e. Scroll down to *IPAll* and verify *TCP Dynamic Ports* is blank and that *TCP Port* is set to *1433*.
   f. Click *OK*.

Optional: Install Internet Information Service (IIS)

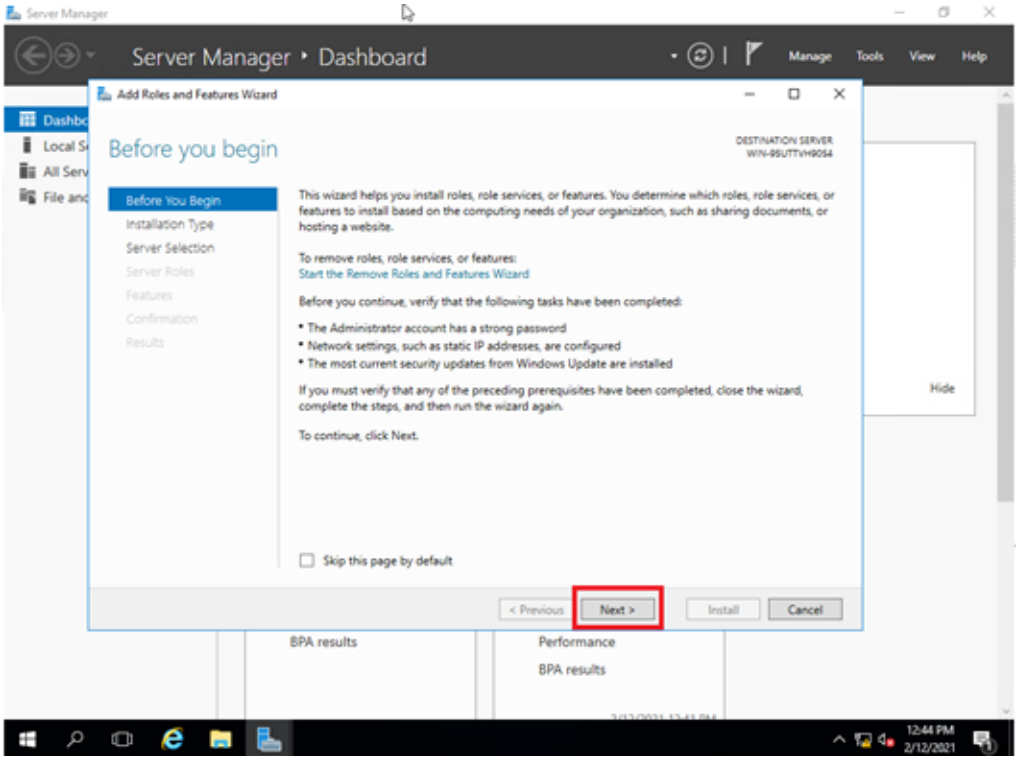
IIS 10 is supported on Windows Server 2016/2019/2022.

To add the IIS role and service:

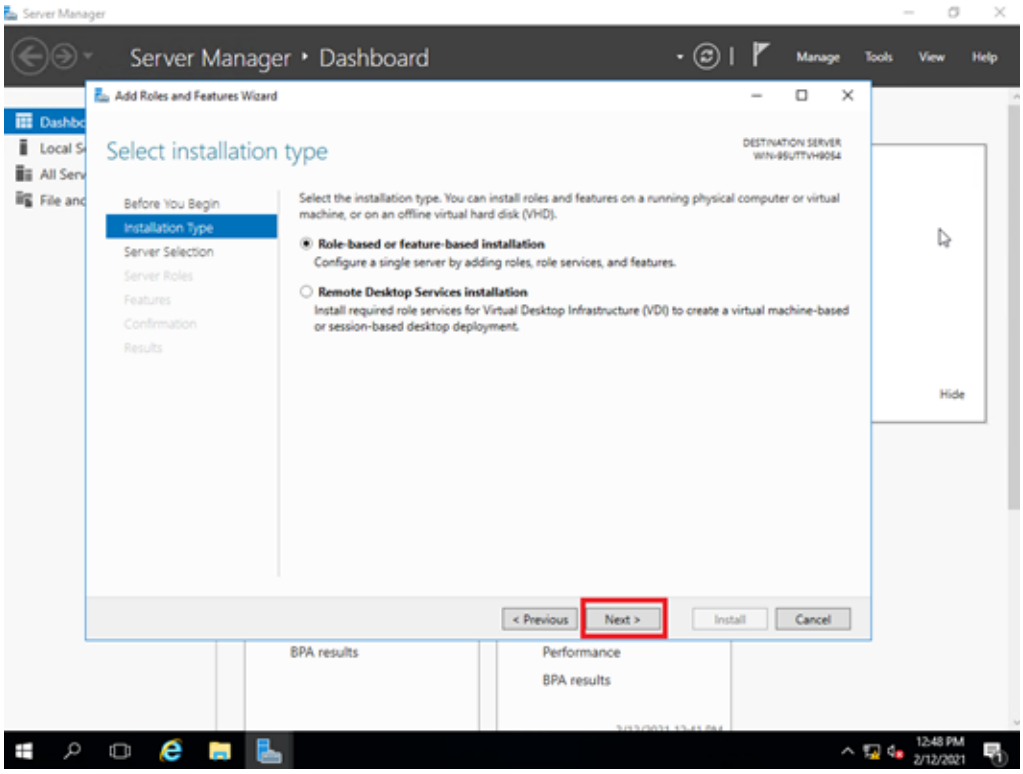
1. Go to *Server Manager >Dashboard*.
2. Click *Manage > Add Roles and Features*.



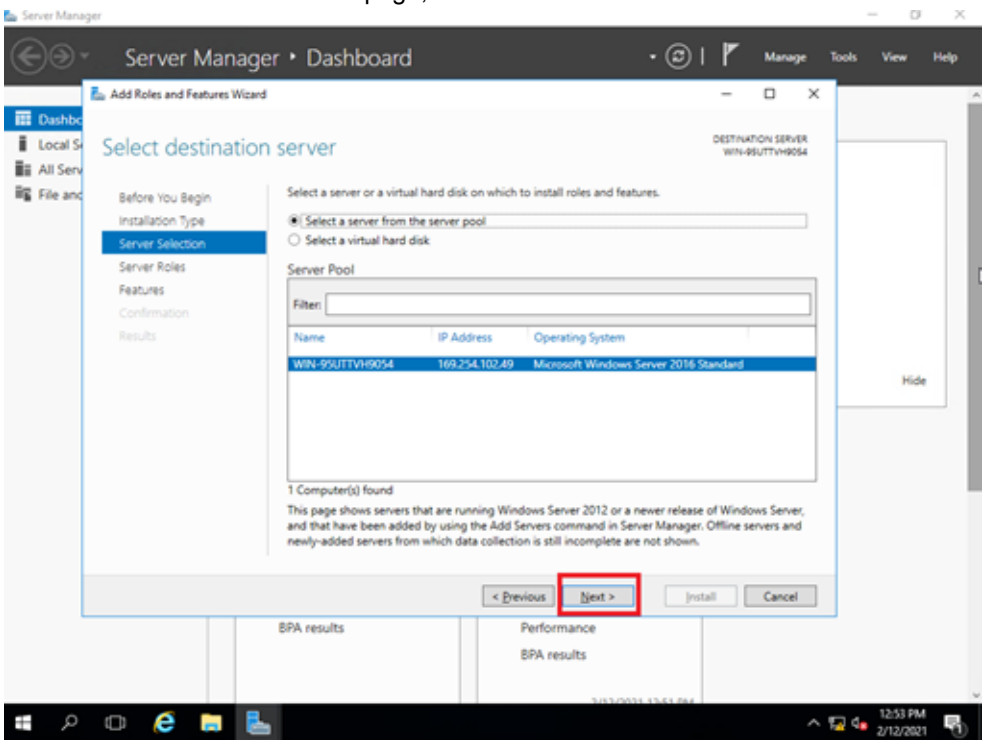
3. On the *Before you begin* page, click *Next*.



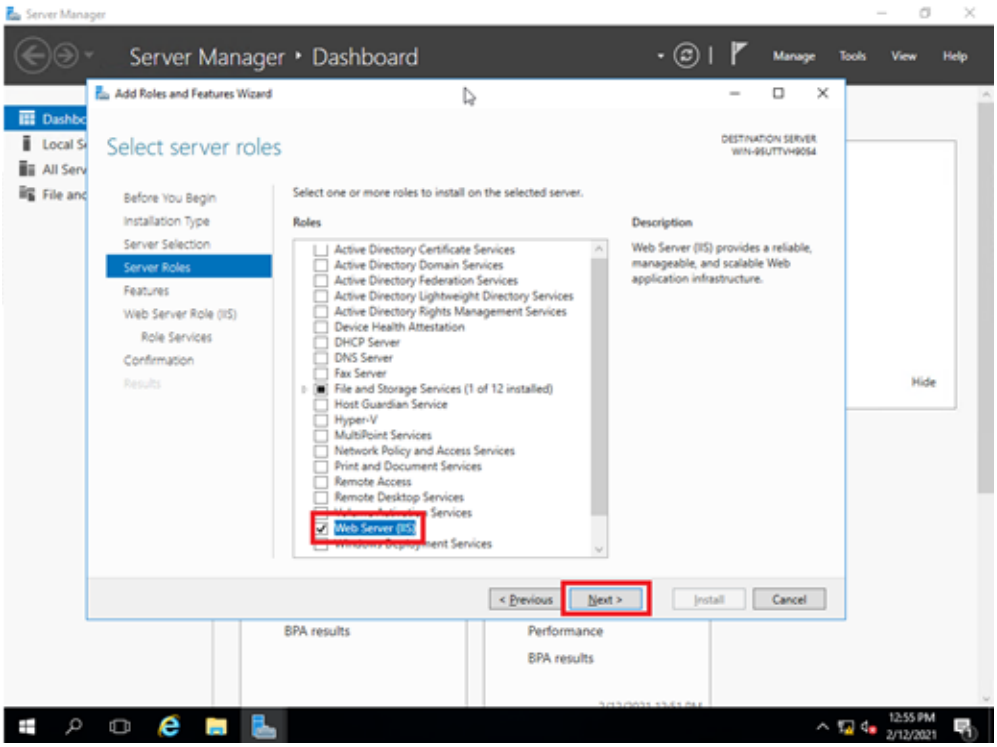
4. On the *Select installation type* page, click *Next*.



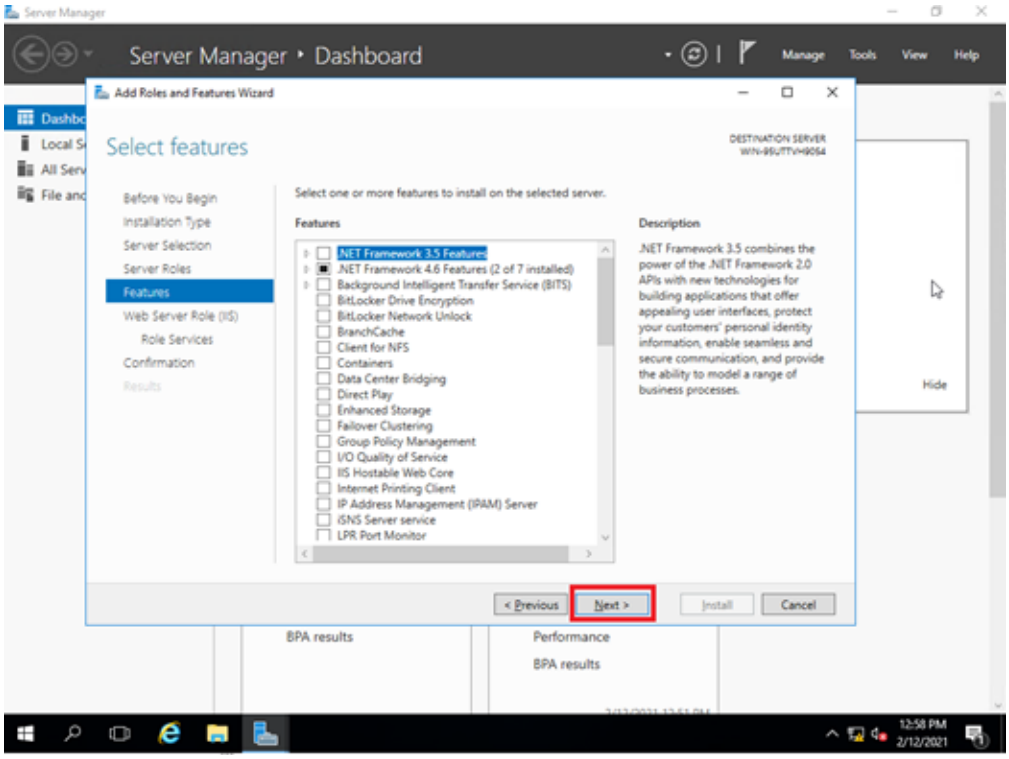
5. On the *Select destination server* page, click *Next*.



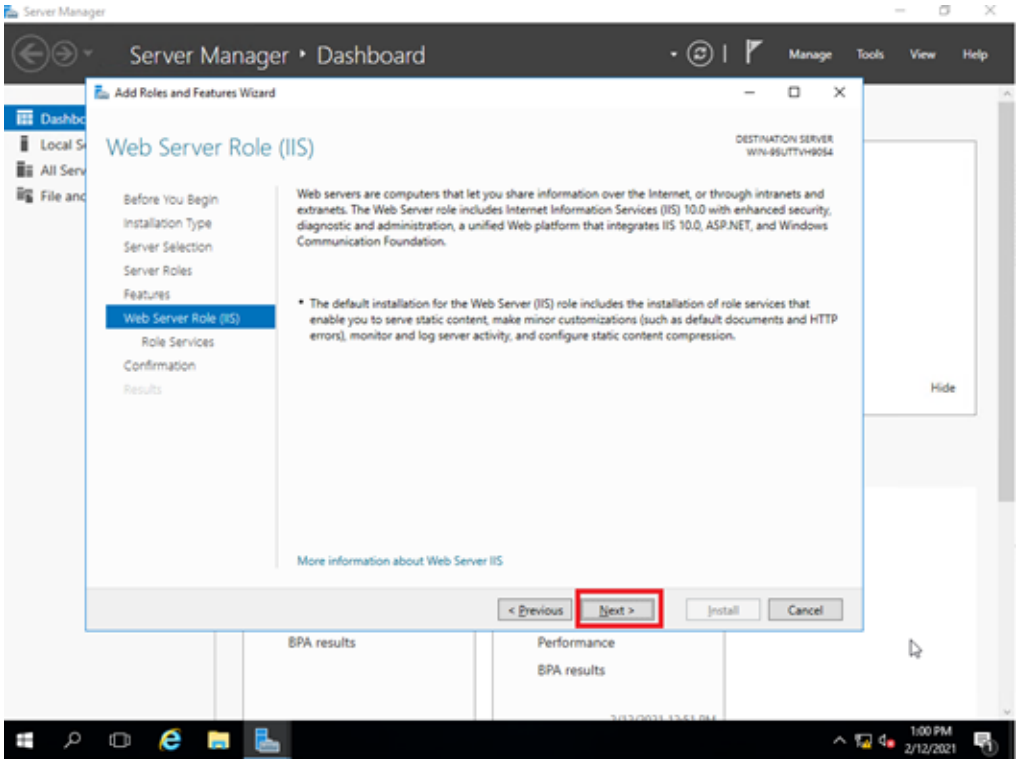
6. On the *Select server roles* page, click *Web Server (IIS)*.



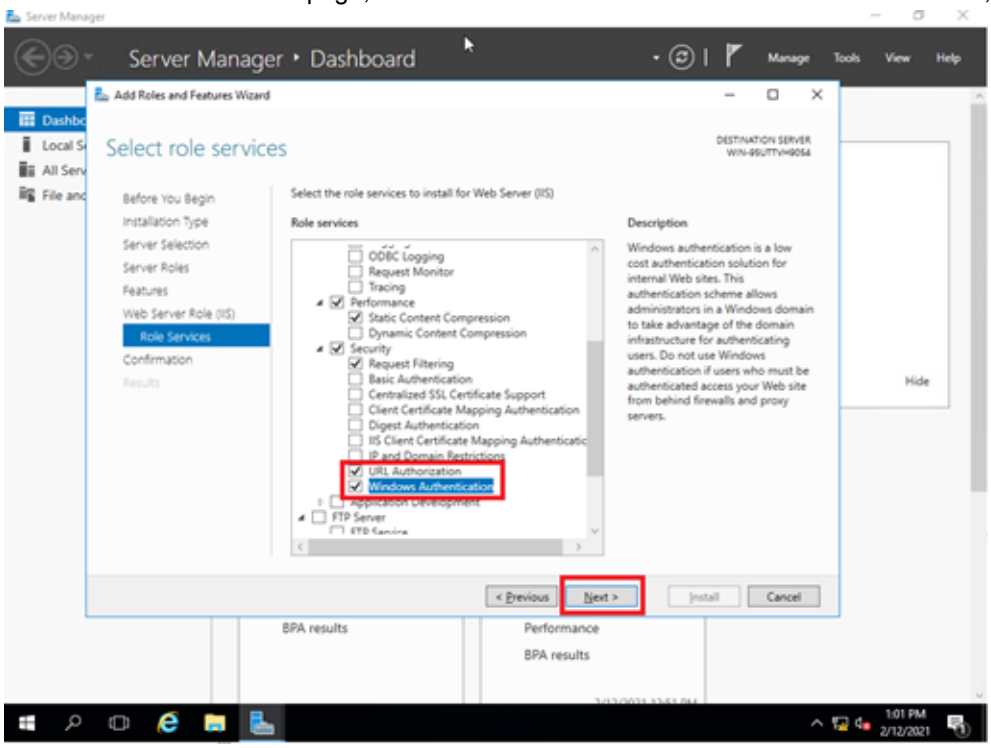
7. In the pop-up dialog box, click *Add Features*.
8. On the *Select features* page, click *Next*.



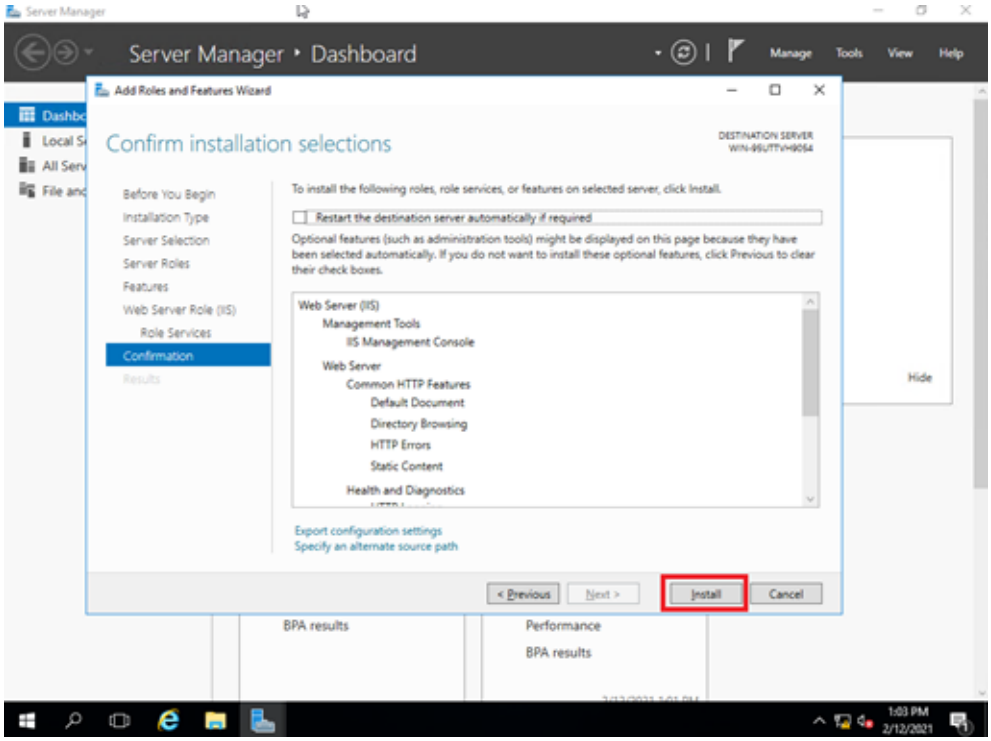
9. On the *Web Server Role (IIS)* page, click *Next*.



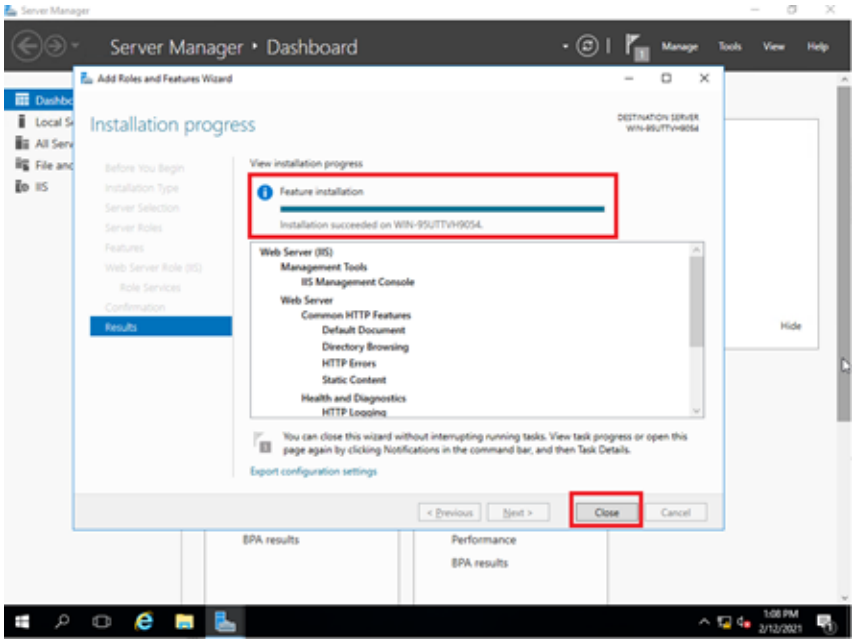
10. On the *Select role services* page, enable *URL Authorization* and *Windows Authentication*, then click *Next*.



11. On the *Confirm installation selections* page, click *Install*.

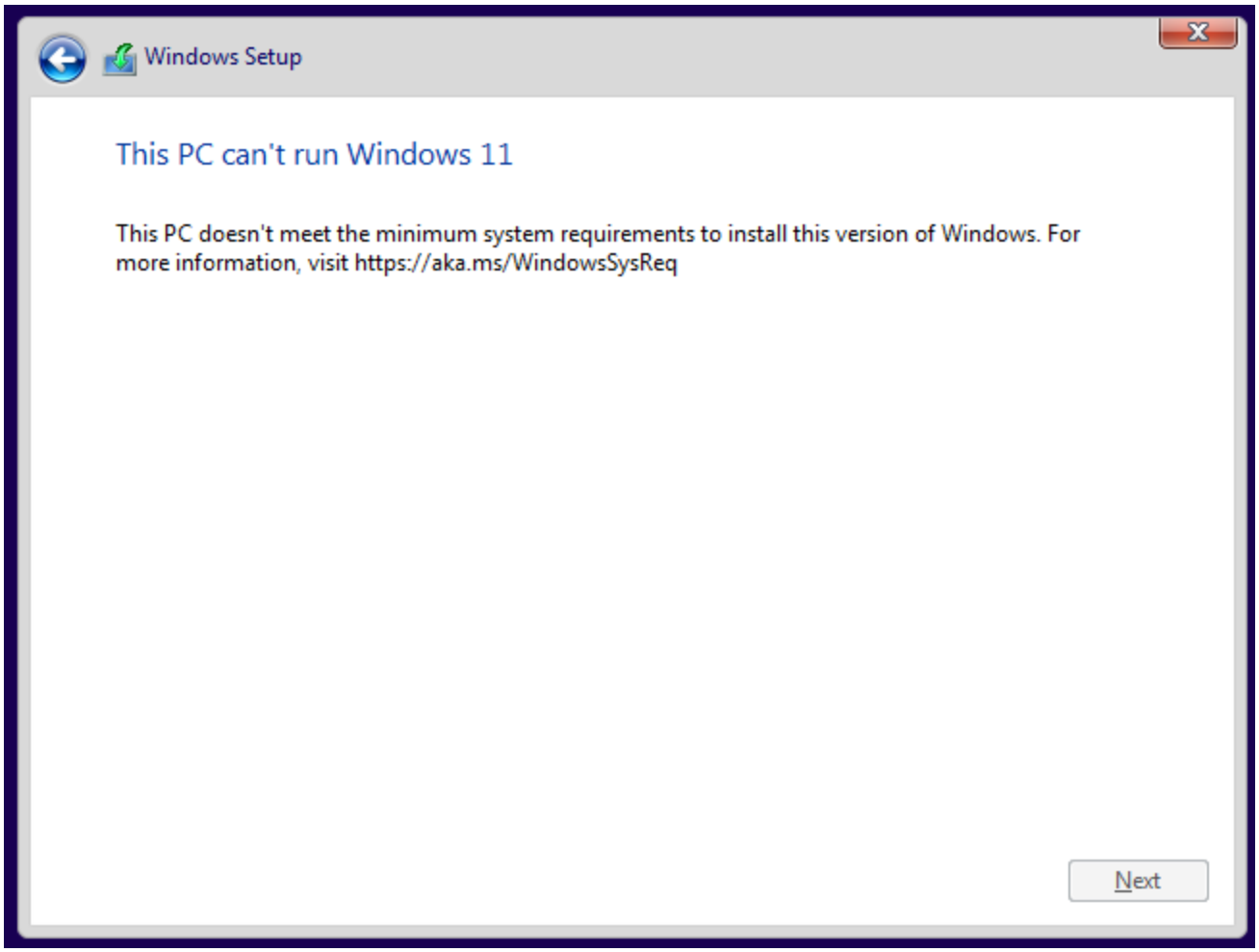


12. Wait for the installation to finish, then check the results and click *Close*.

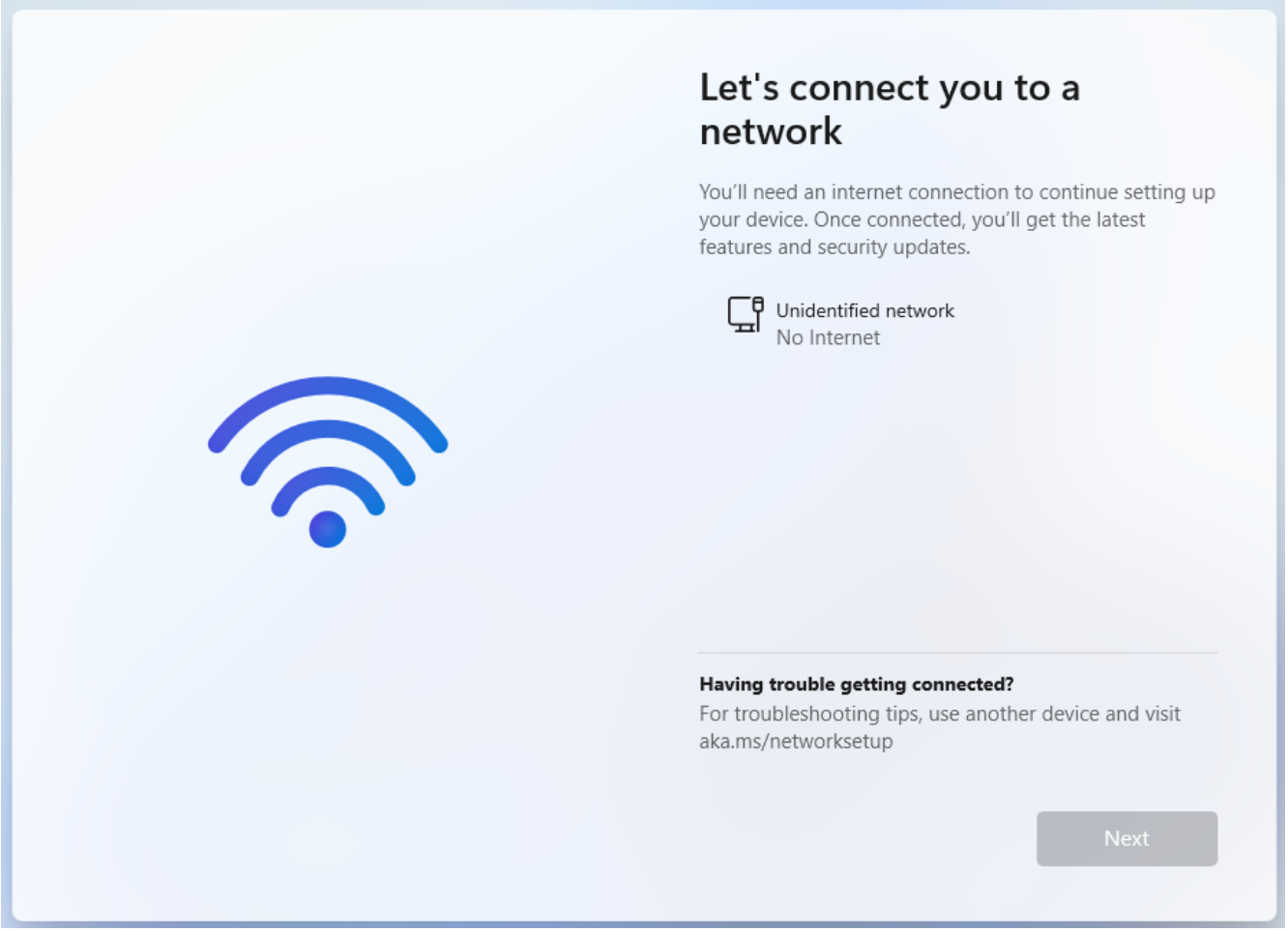


Custom OS Windows 11

The OS Windows 11(64 bits) deception OS is similar to Windows 10 services: however, the GUI restricts the CPU Cores, Memory and Storage. Since Windows 11(64 bits) requires more resources, you may see the following messages:

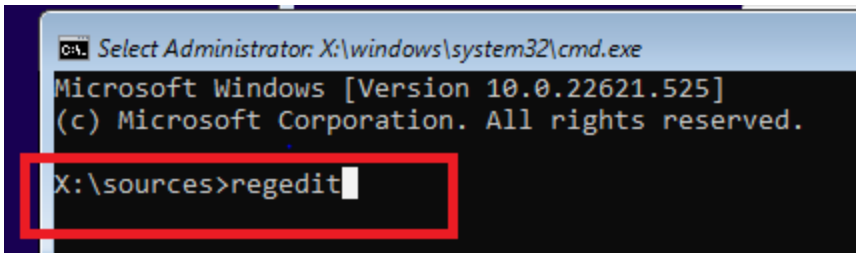


You may also be blocked on the following OOBE page.

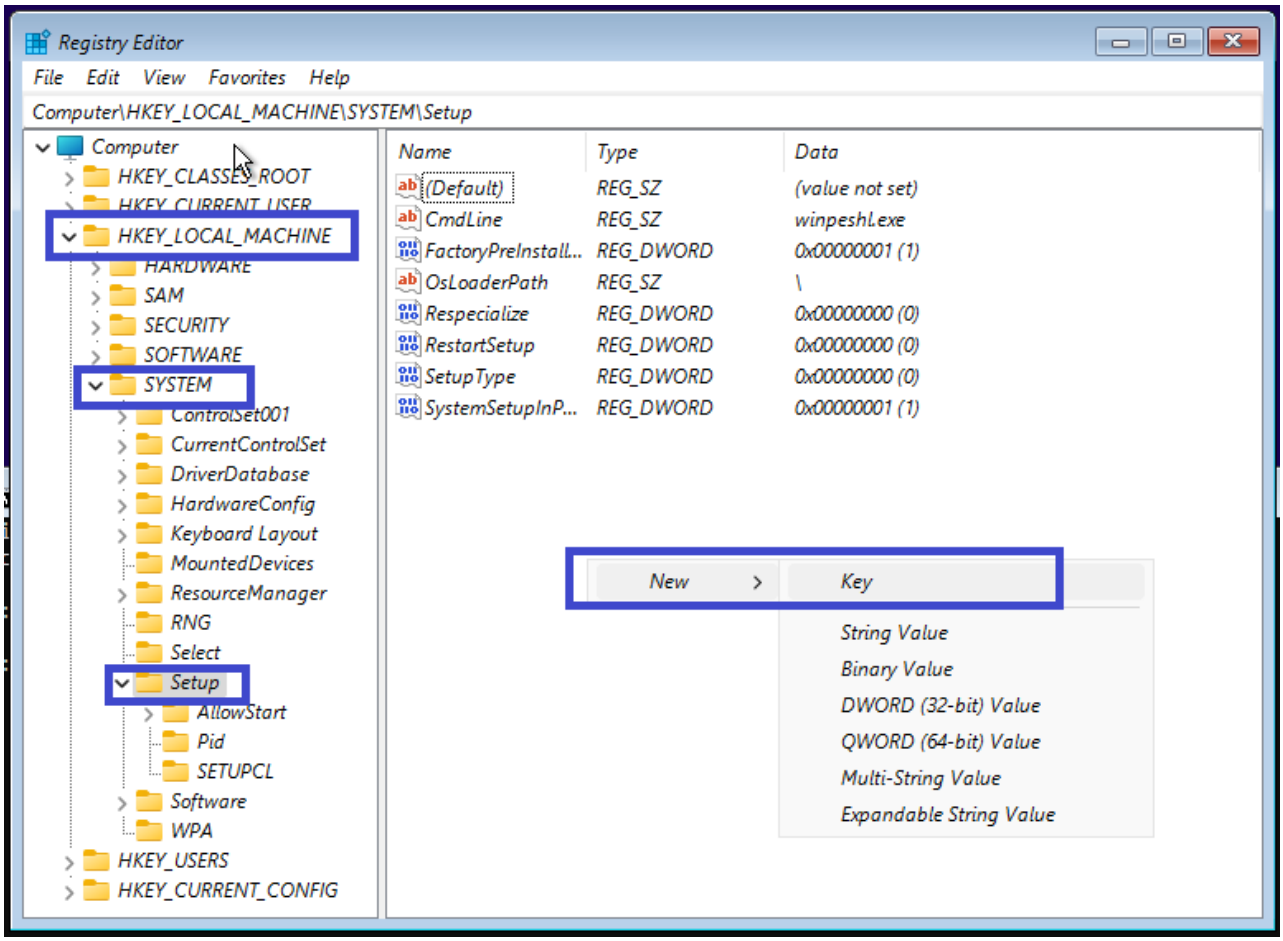


To run Set Bypass TPM and SecureBoot check:

1. Boot off of your Windows 11 install disk.
2. Press SHIFT + F10 to launch the command prompt (If this does not work, you can try SHIFT + F10 +FN).
3. Enter `regedit` and press Enter.

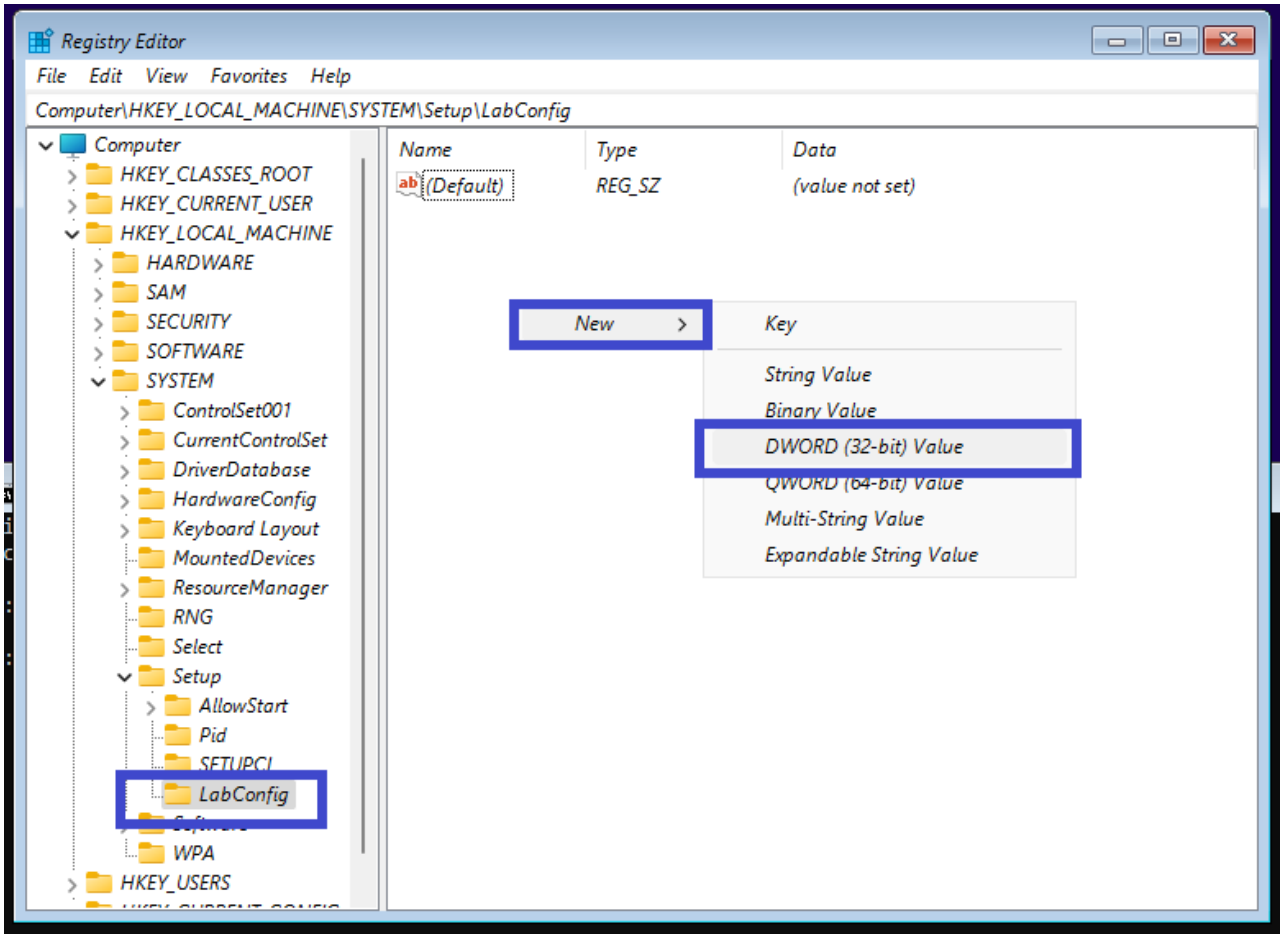


4. Go to *HKEY_LOCAL_MACHINE* > *SYSTEM*> *Setup*. Right-click the folder to add a new key folder called `LabConfig`.

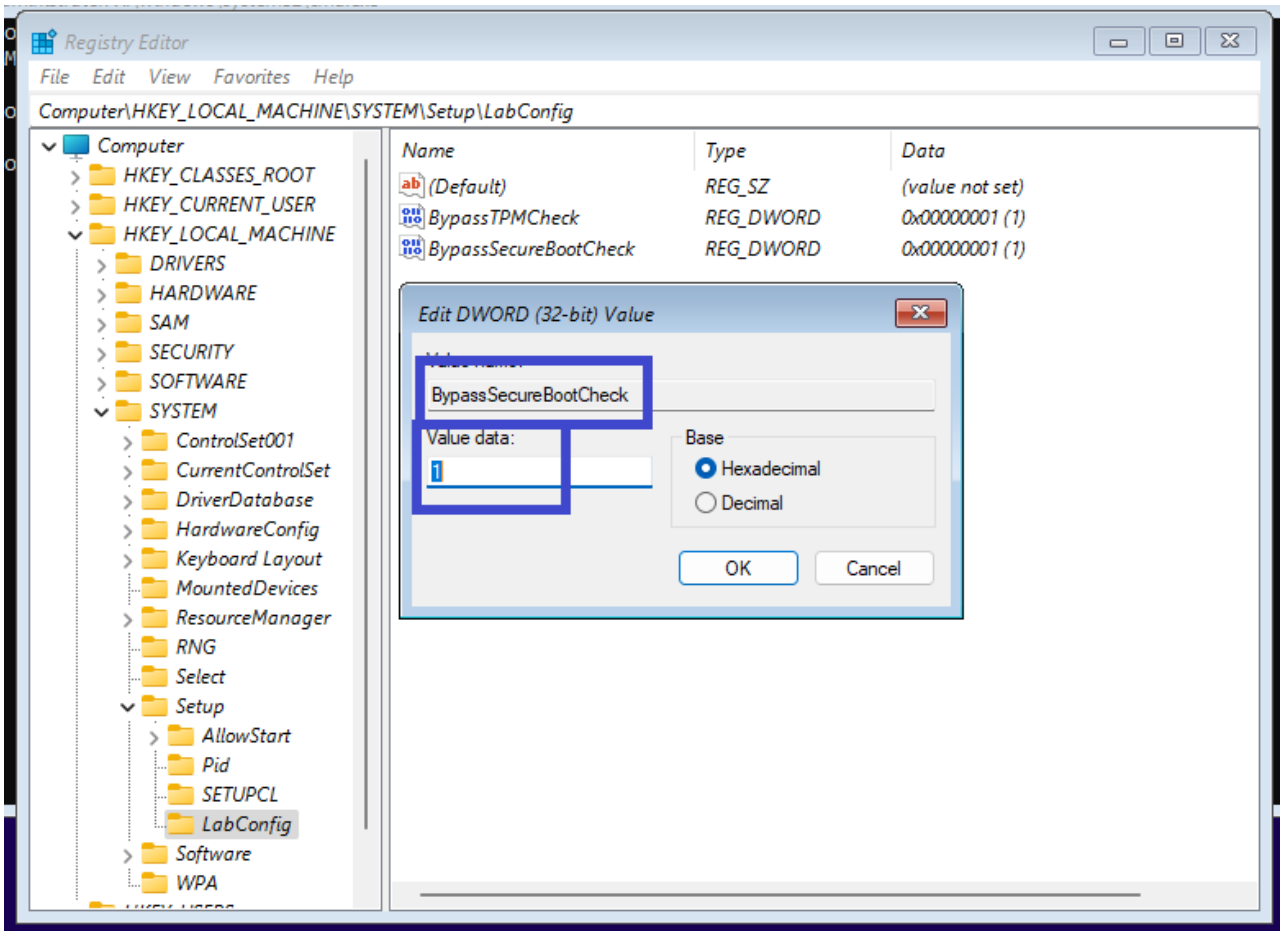


5. Add new value named `BypassTPMCheck`.

6. In the *LabConfig* folder, type *REG_DWORD*", set it to *1*.



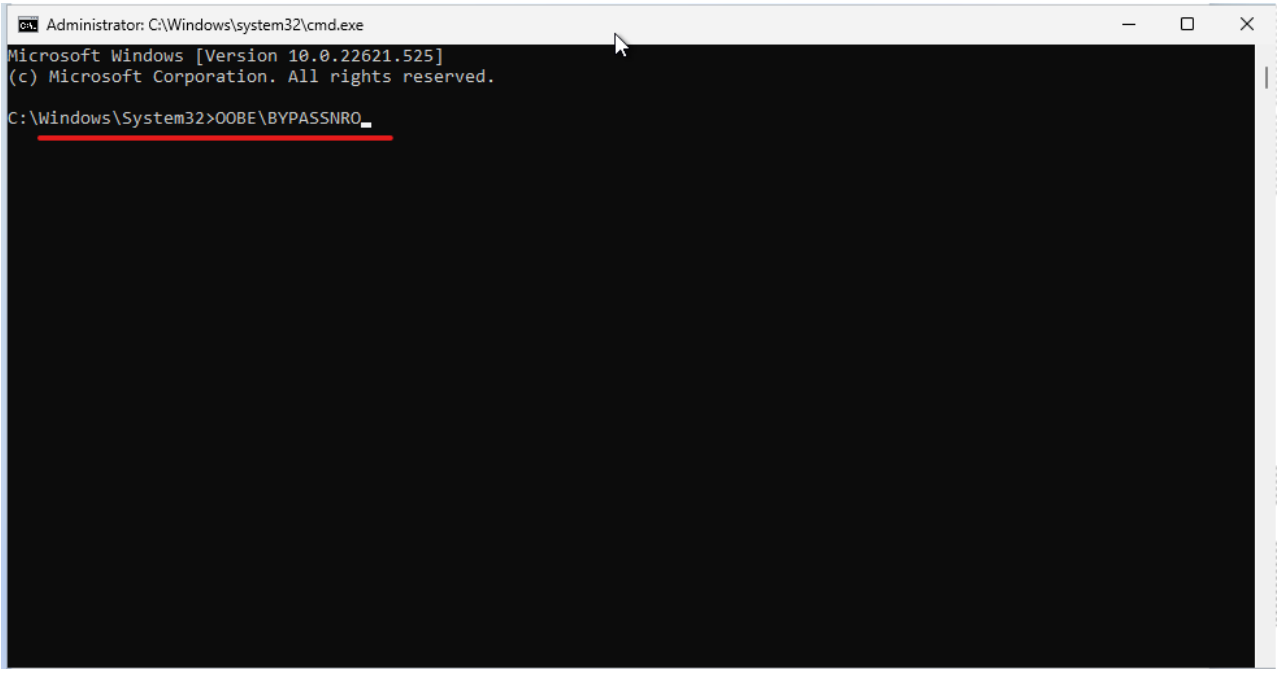
7. In the *LabConfig* folder, add a new value called *BypassSecureBootCheck* then type *REG_DWORD*, and set it to *1*.



You can set the RAM larger or equal to 4G during configuration, but If the RAM is less than 4G, you can add another new value called *BypassRAMCheck* to the *LabConfig* folder, and type *REG_DWORD*, and set to *1*.

To set the bypass network setup during OOBE:

1. Press SHIFT + F10 or SHIFT +Fn+ F10 to launch the command prompt when asked to setup network
2. Enter "`OOBE\BYPASSNRO`" and press Enter.



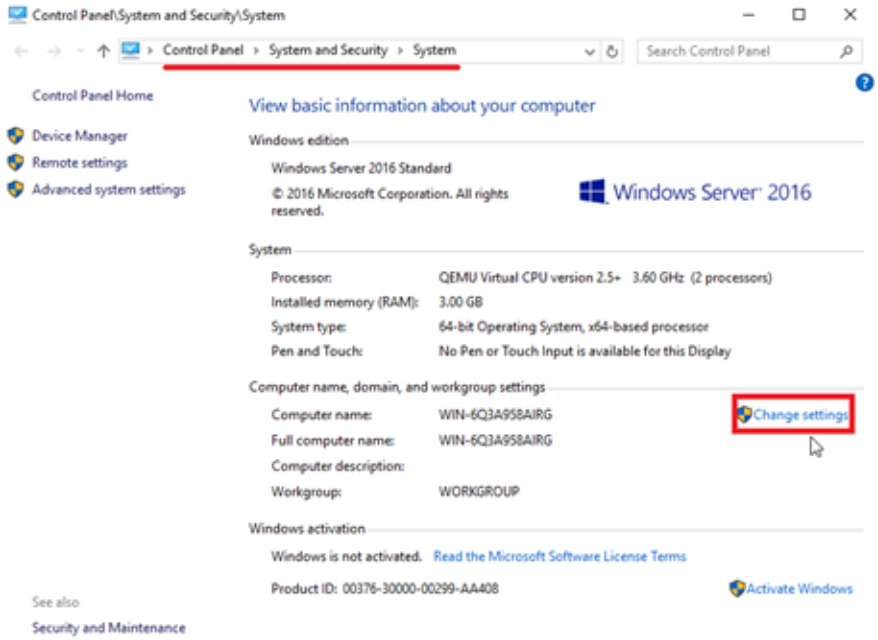
Join a domain

Before joining a custom Windows OS to a domain, change its DNS server to the DNS server of the domain.

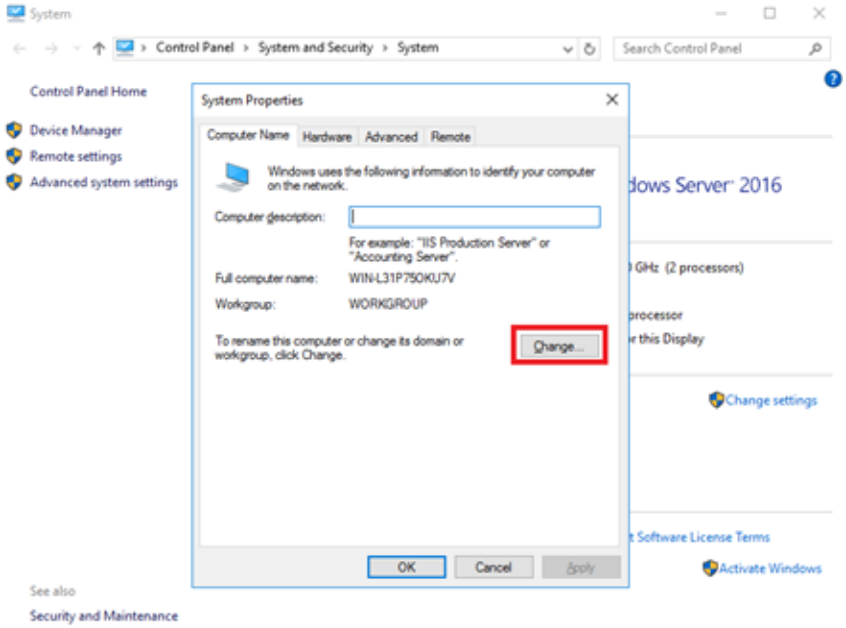
This task is optional.

To join a domain:

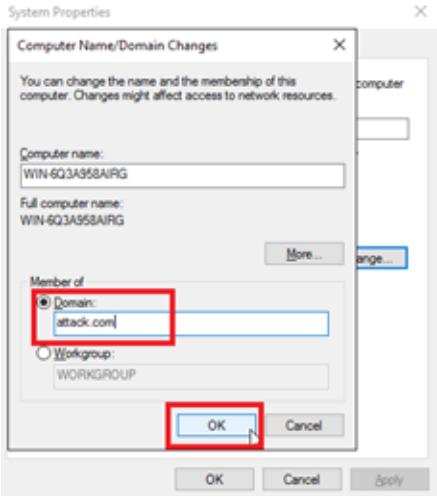
1. Go to *Control Panel* > *System and Security* > *System* and click *Change settings*.



2. On the *System Properties* dialog box, click *Change*.



3. Enter the *Domain* and click *OK*.



4. Click *Close* and restart the computer to join the domain.

Install the FortiDeceptor customization toolkit

When system customization is complete, right-click *FDC_CUS_toolkit.exe* and select *Run as Administrator* and wait for the installation to finish.

Another option is to run the CLI command `FDC_CUS_toolkit.exe` as an administrator.

Save the custom image

When the customization status in the GUI displays *Ready*, click *Start -> Power > Shut down* to shut down Windows and then click *Save* to save this image.

If the Windows Server is connected to a domain, there may not be a Power option in the GUI. In this case, run the command `shutdown /s /t 1 /f` as administrator.

It might take several minutes to save the entire image. When the image is saved, the page lists the image in *Customized Images*.

In *Deception* > *Customization*, the *Customized Images* tab lists the custom images.

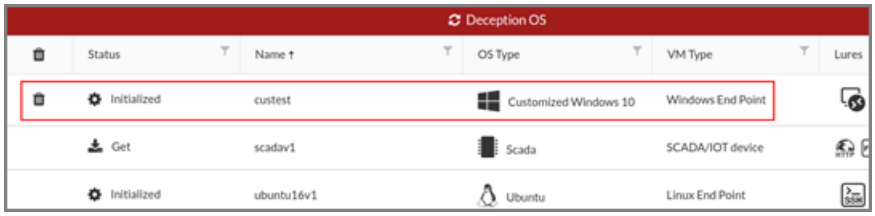
The *Actions* column has icons for you to view logs, apply the image, or delete the image.

Deploy custom image

To apply a custom image:

1. Go to *Deception* > *Custom Decoy Image* and click the *Customized Images* tab.
2. Select a custom image and click the *Apply* button or click the *Apply* icon beside a custom image.

It might take a few minutes to apply the custom image. When applied, the custom image is listed in *Deception* > *Deception OS*.



To deploy decoys with custom images–generic image:

1. Go to *Deception* > *Deployment Wizard*.
2. Click a custom image and deploy it like a standard decoy.
3. Select whether to domain users to access RDP and SMB.
   For normal users:

RDP (2) + Add Lure

Username	Password
loretta	
lawrence	

SMB (2) + Add Lure

Username	Password	Sharename
rhonda		
maurice		

For domain users:

RDP (2) + Add Lure

Allow domain user to access RDP

Username	Password
david@name.com	
ethan@name.com	

SMB (1) + Add Lure

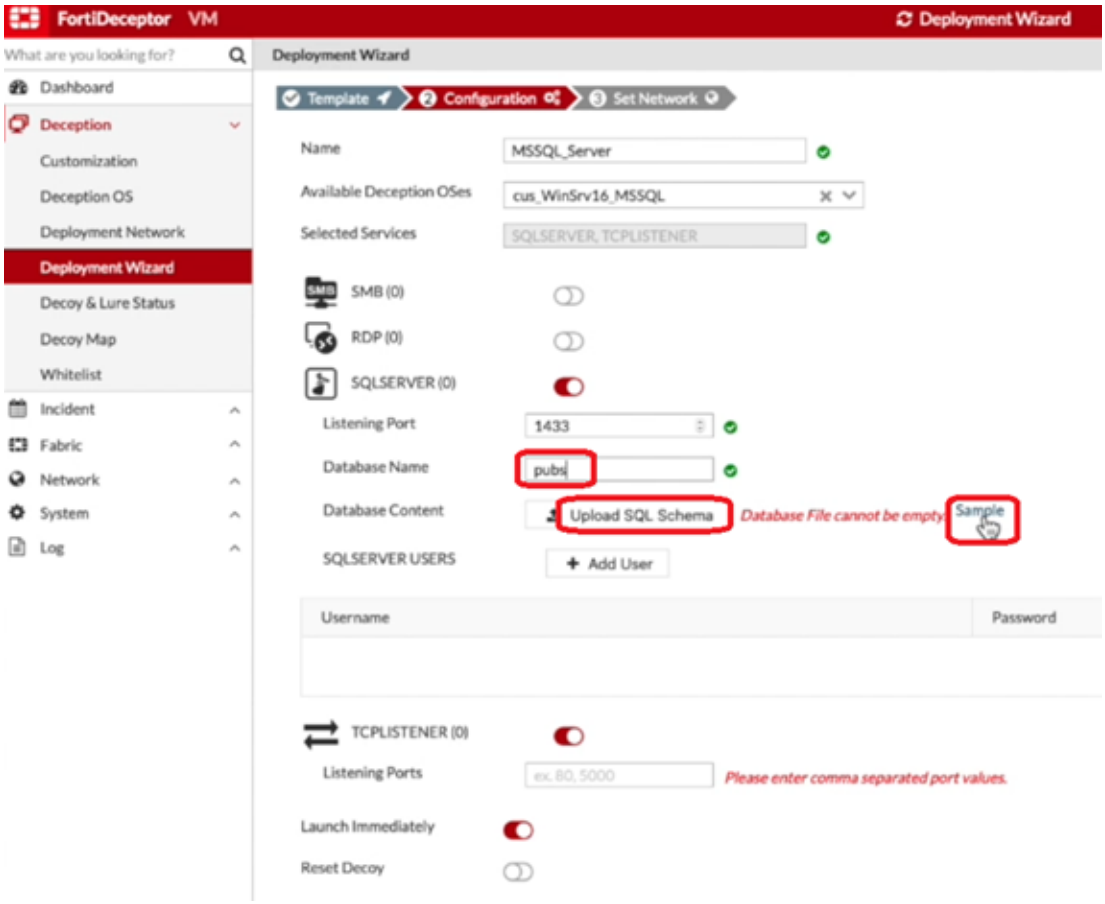
Allow domain user to access SMB

Username	Password	Sharename
robert@name.com		

We highly recommend enabling RDP and SMB services for decoys joined in the domain and not set in any local lure accounts. Many domains have different policies for account name and password which may cause the decoy to fail to initialize.

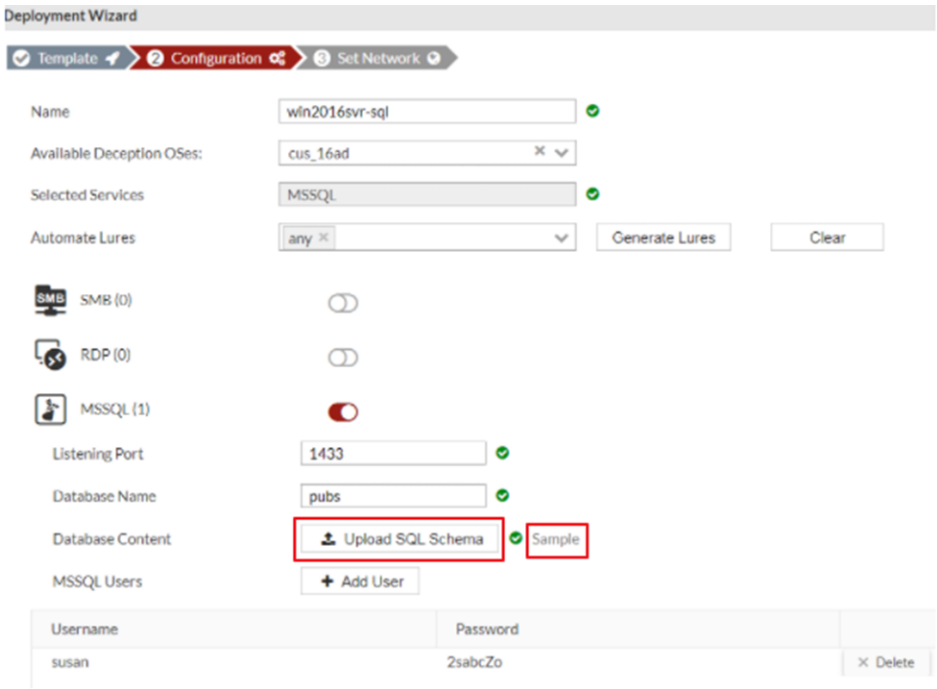
To deploy decoys with custom images–SQL Server:

1. Go to *Deception* > *Deployment Wizard*.
2. Click a custom SQL server image.



3. (Optional) Click *Sample* to download a sample *.sql* file.

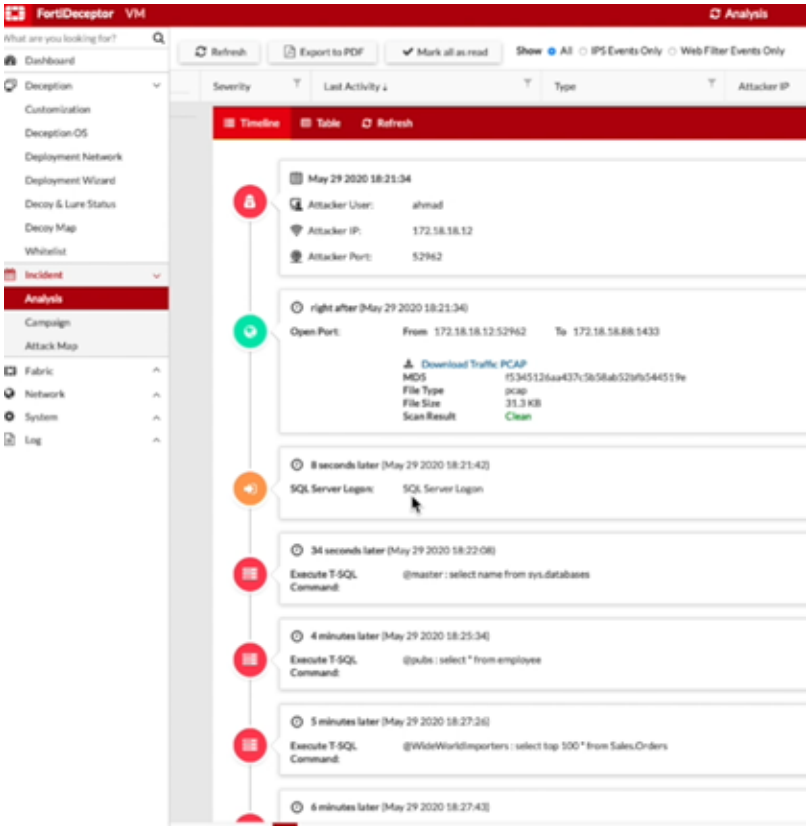
4. Click *Upload SQL Schema* to upload your own custom *.sql* file .



To generate SQL alerts:

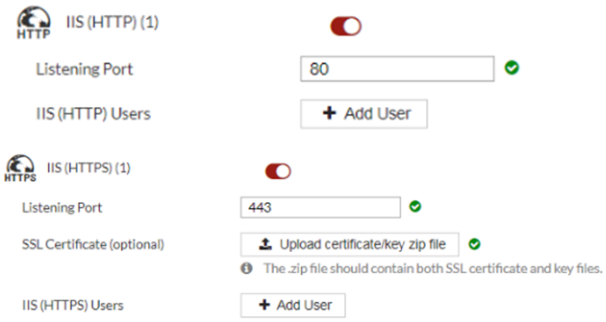
1. You can generate SQL alerts using the `SQLCMD` tool or using `WideWorldImporters`.
   - To use `SQLCMD`, run the following commands.
     ```
     sqlcmd -S "IP Address" -U "username" -P "password"
     use WideWorldImporters;
     SELECT name
     from SYSOBJECTS
     WHERE
     xtype = 'U'
     go
     ```
   - To use `WideWorldImporters`, run the following commands.
     ```
     use WideWorldImporters;
     select top 100 * from Sales.Orders;
     go
     ```

The *Incident* > *Analysis* page displays the alerts for the SQL server attack.



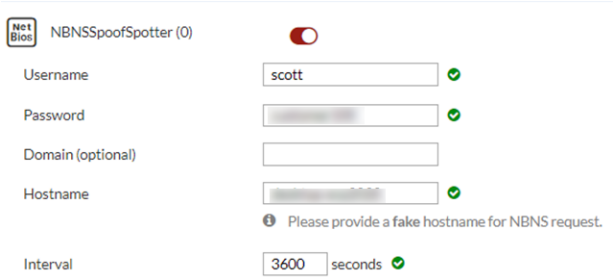
To deploy decoys with custom images–IIS (HTTP/HTTPS):

1. Go to *Deception* > *Deployment Wizard*.
2. Click a custom IIS image.



To deploy decoys with custom images–NBNSSpoofSpotter:

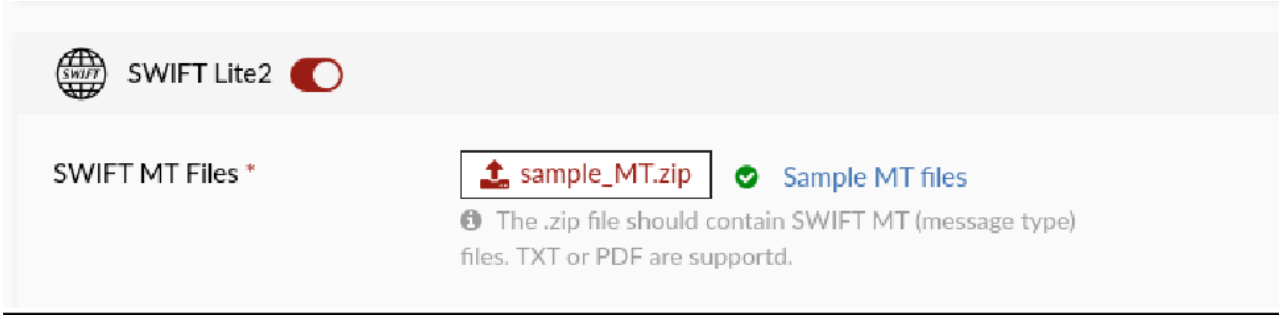
1. Go to *Deception* > *Deployment Wizard*.
2. Click a custom NBNSSpoofSpotter image.



NBNSSpoofSpotter feature detects attacks using the *Responder* tool and includes a link to https://github.com/SpiderLabs/Responder with more information about the attack.

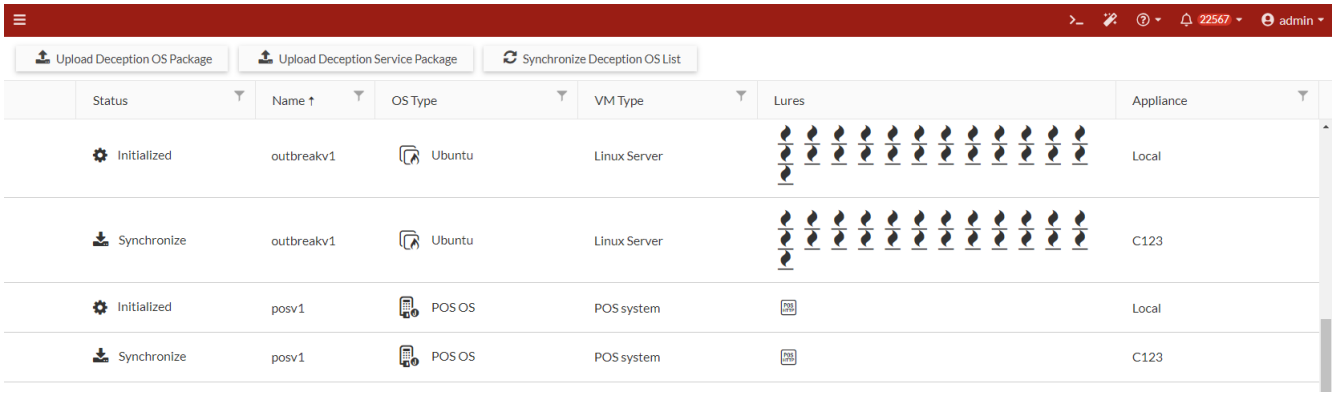
To Deploy decoys with custom images-SWIFT Lite2

1. Go to *Deception* > *Deployment Wizard*.
2. Click *SWIFT Lite2 service.*
3. Upload the MT Files.



Deception OS

The *Deception OS* page displays the deception OS or deception packages available for creating Decoy VMs. Use this page to upload a deception OS package or to synchronize the deception OS list.



The *Deception OS* page displays the following in formation:

Column	Description
Status	Status of the Deception OS.
Name	Name of the Deception OS.
OS Type	Operating System type.
VM Type	VM type of the Deception OS endpoint.
Lures	Lures used by the Decoy VM such as SSH, SAMBA, SMB, RDP, TCPLISTENER, HTTP, NBNSSpoofSpotter, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, Guardian-AST, IEC104, DNP3, ENIP, KAMSTRUP, Infusion Pump (Telnet), Infusion Pump (FTP), PACS, PACS-WEB, DICOM server, POS-WEB, ERP-WEB, SSLVPN, ScadaBR (HTTP), SRTP, Tomcat(HTTP, HTTPS), MariaDB and Elastic Search(HTTP).

To upload a deception OS or service package:

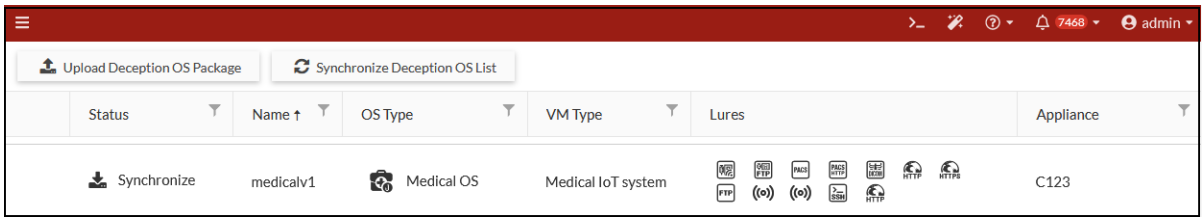
1. Go to *Deception* > *Deception OS*.
2. Click *Upload Deception OS Package* or *Upload Deception Service Package*.
3. Click *Choose a file* or drag and drop the file onto the field.

To synchronize the list:

Click *Synchronize Deception OS List*.

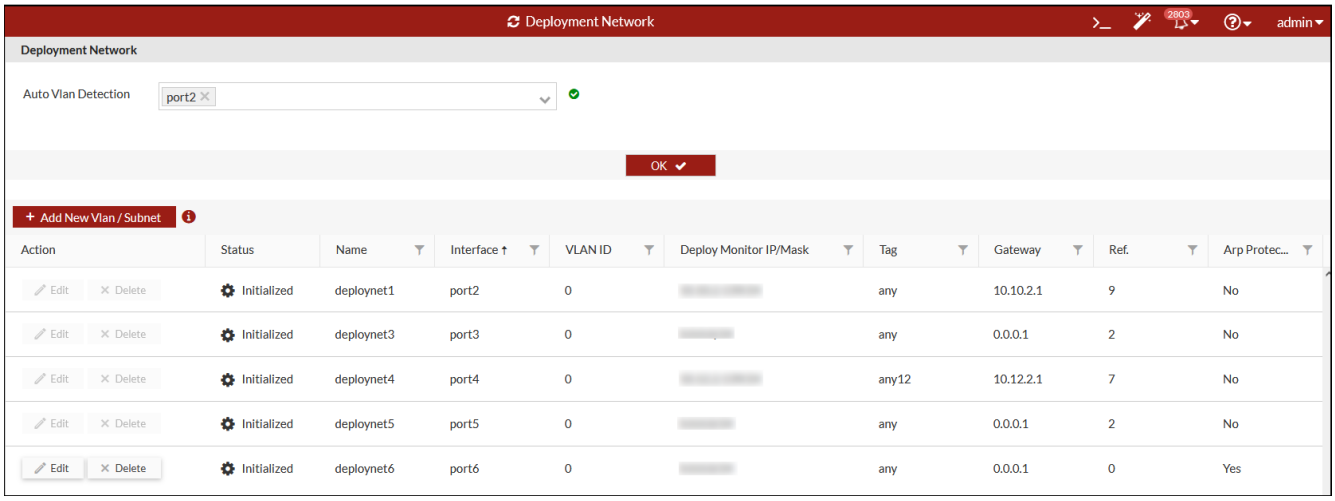
To install a Deception OS on a device:

In the *Status* column, click the Synchronize button next to the OS name.



Deployment Network

Use the *Deployment Network* page to set up a monitoring interface into a VLAN or a subnet.



The *Deployment Network* page displays the following information:

Action	Click *Edit* to edit the VLAN or subnet entry. The *Edit* button is visible only after the entry is saved. Click *Delete* to remove a VLAN or Subnet.
Status	Status of the IP address, such as if it is initialized.
Name	Name of the VLAN or subnet.
Interface	The port that connects to the VLAN or subnet.
VLAN ID	The VLAN's unique integer ID.
Deploy Monitor IP/Mask	The monitor IP provides the dynamic content for the online token, collects the token installation information, and acts as the probing client for active asset discovery when auto-deployment is triggered.
Tag	The tag for the VLAN or subnet.
Gateway	The gateway IP address of the deployment network.
ARP Protection	Indicates ARP Protection is enabled (*Yes*) or disabled (*No*).

Setting up the deployment network

To add a VLAN or subnet to FortiDeceptor:

1. Go to *Deception* > *Deployment Network*.
2. Enable *Auto VLAN Detection* to automatically detect the VLANs on your network.
   Auto VLAN detection allows FortiDeceptor to detect the available VLANs on the deployment network interface and display them in the GUI. You can select and add the VLANs for the deployment of Decoys later.
3. Select the *Detection Interface* and click *OK*. You can select multiple ports.
4. Click *Add New VLAN/Subnet* to manually add a VLAN or a subnet. Configure the following settings:

Name	Name of the VLAN or subnet.
Interface	The port that connects to the VLAN or subnet.
Tagged Interface	Select to enable vlan tag. Default is untagged.
VLAN ID	The VLAN's unique integer ID.
Deploy Monitor	The IP address to monitor. The deploy monitor IP/Mask must be an IP address and not a subnet. You must use the following guidelines to set the network IP/mask: • Interface name and VLAN ID must be unique among all network IP/masks. • If VLAN ID is 0, the network IP/mask must be unique among all the network IP/masks without VLAN and all system interfaces. • If VLAN is not 0, the network IP/mask must be unique among all subnets in the same VLAN.
Gateway	The gateway IP address of the deployment network.
ARP Protection	Select to enable ARP poisoning detection. ARP Protection is disabled by default. Upgrading FortiDeceptor will disable this setting.
Tag	You can specify a tag for the VLAN or subnet.
Ref	The number of objects referring to this object.

Each *VLAN/Subnet* with a network mask of */24* and higher is counted as one seat of the VLAN license.

Each *VLAN/Subnet* with a network mask less than */24* is counted as two seats of the VLAN license.

5. Click *Save*.

Lure Resources

Use the *Lure Resources* page to view the current lure, upload resources such as Word and PDF files to automatically generate lures, and import a user name list from an LDAP server.

Uploading lure resources

Upload a lure resource to automatically generate lures. There are two types of lure resource:

- **Documents**: Word and PDF files that generate authentic directories and files over the Decoy network shares.
- **Credential**: Username (with password) list files that generate authentic credentials access to the network Decoys.

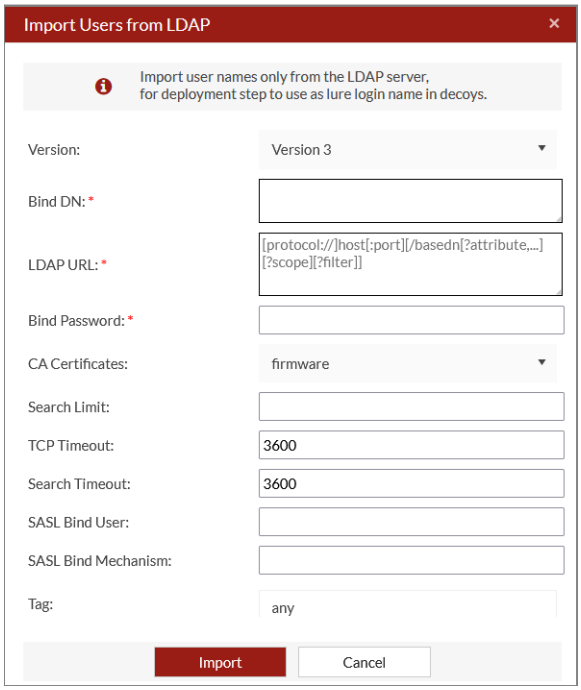
To upload a lure resource:

1. Go to *Deception* > *Lure Resources*.
2. Click *Upload*. The *Upload New Lure Resource* dialog opens.
3. From the *Lure Type* dropdown, select the lure type.

Credential - Fake Users (txt)	Upload a list file with fake users and passwords.
Documents - Template (docx,pdf,zip)	Upload files as a template. FortiDeceptor will insert content to build honey docs.
Documents - Fake Content (zip)	1. Upload Zip Word Document (.docx), PDF, Excel (.xlsx,.xlsm,.xltm,.xltx) then upload .zip file directly to FortiDeceptor.
Credential – AWS Key (txt)	Upload a list file with AWS users and passwords. Requirements: • Create AWS IAM users with no permissions. (Without real AWS user, the AWS platform will not generate a log that indicates the user access.) • Upload a text file with the correct AWS Region, AWS Access Key ID, AWS Secret Access in the format below. `AWS Access Key ID:AWS Secret Access:AWS Region:AWSusername` For more information, see Deploying AWS deception keys on page 200.
Credential – Azure Keys (txt)	Upload a list file with Azure Application IDs and Tenant IDs. Requirements: • Register Azure Application to get Application ID and Tenant ID.

	• Upload a text file with the correct Azure Application IDs, Tenant IDs in the format below.
	`Application ID:display name:Tenant ID`
	For example,
	`35739ab1-0682-783a-88b3-722eb2ef51f1:MyAzureApplication:933b88cd-1b19-02a1-8dcf-1b21dabc61ba`
	For more information, see .Deploying Azure deception keys on page 210.

Certificate – Azure Certificate (pem,crt,cer)	Upload a certificate with private Key and certificate.
	For example,
	`-----BEGIN PRIVATE KEY-----`
	`<private_key>`
	`-----END PRIVATE KEY-----`
	`-----BEGIN CERTIFICATE-----`
	`<certificate>`
	`-----END CERTIFICATE-----`
	For more information, see .Deploying Azure deception keys on page 210.



The *Credential - Fake Users (txt)* and *Documents - Template (doc,docx,pdf,zip)* options include sample files to help you create a resource.

4. Enter an optional *Tag*, such as *any*.
5. In the *Resource File* field, click *Choose a file* to upload the resource, or drag and drop it onto the field.
6. Click *Save*.

Importing users from LDAP

To import an LDAP user list:

1. Go to *Deception* > *Lure Resources*.
2. Click *Import Users from LDAP*.
3. Configure the import settings.

Version	Select the version from the dropdown.
Bind DN	Username used to connect to the LDAP service on the specified LDAP Server.
LDAP URL	Enter the LDAP URL using the following format: `[protocol///]host[:port][/basedn[?attribute,...][?scope][?filter]]`
Bind Password	Enter the Bind DN's password.
CA Certificates	Select a certificate from the dropdown.
Search Limit	Search sub-tree depth.
TCP Timeout	Enter the TCP connection timeout in seconds.
Search Timeout	Enter the search timeout in seconds.
SASL Bind User	The username to authenticate a DN on the directory server using SASL.
SASL Bind Mechanism	The username and password for authentication.
Tag	Enter a tag for the import.
Scheduler Type	Select One Time or Recurring
Scheduler Timezone	Select the timezone.
Scheduler Start	Select the scheduler start time.
Scheduler End	Select the scheduler end time.
Scheduler Interval	Select the Interval including *Daily*, *Weekly* or *Monthly*.
Days	Select the day.
Time	Select the time.

4. Click *Save*.

Examples: Import Users from LDAP

Open LDAP example:

```
"dn": "uid=test,o=org,dc=example,dc=com",
"url": "ldap://192.168.0.100/o=org,dc=example,dc=com?uid?sub?(objectclass=*)",
"password": "password"
```

Windows AD example:

```
"version": "3",
"dn": "cn=users,cn=usergroup,dc=example,dc=com",
"url": "ldap:192.168.0.100/cn=usergroup,dc=example,dc=com?sAMAccountName?sub?
     (objectClass=user)",
"password": "password"
```

Support is offered if the format of the tree can parse `uid/sAMAccountName` in the search results. Ensure the URL queries the proper data.

Deployment Wizard

Use the *Deployment Wizard* to create and deploy Decoy VMs on your network. Decoy VMs appear as real endpoints to hackers and can collect valuable information about attacks.

To deploy Decoys on the network:

1. Go to *Deception* > *Deployment Wizard*.
2. Click + *Create a new decoy* to add a Decoy VM.
3. Configure the following:

Name	Specify the name of the deployment profile. Maximum 15 characters using A-Z, a-z, 0-9, dash, or underscore. No duplicate profile names.
Appliance Name	Destination of the Decoy VM. This can be local (manager) or remote client (remote appliance). This column only shows in Central Management mode on manager.
Available Deception OSes	Select a Deception OS. The OS you select determines the services that are available.
Available Deception Decoys	Select a deception decoy. This option is only available in SCADAV3/IoT. Ubuntu16v2, Ubuntu18v1, VoIPv1 and Medicalv1 deception OSes. The decoy you select determines the options in the *Selected Services* dropdown. See Available Deception OSes, Decoys and Selected Services on page 74.
Selected Services	Select a service based on the Deception OS. See Available Deception OSes, Decoys and Selected Services on page 74.
Automate Lures	Select one or more tag names to automate lure generation and to generate related contents. Selecting *any* and *all* generate random content. Click *Generate Lures* to automatically generate lures and list them in the panes below. Click *Clear* to delete the lures on this page.

4. If applicable, click *Generate lures* or *Add Lure* for the service and configure the lure settings. See, Lure Settings on page 78.
5. To launch the decoy VM immediately, scroll to the bottom of the page and enable *Launch Immediately*.
6. To reset the decoy VM after it detects incidents, enable *Reset Decoy* and specify the *Reset Interval* value in seconds.

7. In the *HTTP/HTTPS Merge Time Window* field, enter a range between 0-300 seconds. The default is 30 seconds.

When the time difference between last activity of the first HTTP request and the first activity of next HTTP request is less than the configured time, FortiDeceptor will merge the activities into the same HTTP incident.

8. In the *Monitor Admin Behaviors for* field, enter the number of minutes to trigger the reset. Enter `0` to shutdown the decoy immediately after admin activities are found. The decoy will re-launch in approximately 30 seconds.

Configure this option for deployments with the RDP service is enabled.

9. Click *Next*. The *Set Network* tab opens.
10. Configure the network IP and Hostname. You can enter up to two DNS IP addresses.

DNS	Enter the network IP address. You must set Domain DNS server IP to be the 1st DNS when custom Windows decoys are in the domain(s).
DNS2	(Optional) Enter a second network IP address. Two DNS IP addresses are not supported in t FortiGate SSLVPN decoy deployments.
Hostname	Enter the hostname for the network. The *Hostname* can start with an English character or a digit, and must not end with a hyphen. Maximum 15 characters using A-Z, a-z, 0-9, or hyphen (case-sensitive). Other symbols, punctuation, or white space are not supported. The *Hostname* cannot conflict with decoy names.

11. Click *Deploy Into Network*.
12. Select the *Deploy Interface*. Set this to the VLAN or subnet added in Deployment Network on page 67
13. Configure the following settings in the *Add Interface for Decoy* pane:

Addressing Mode	Select *Static* or *DHCP*. *Static* allows you to configure the IP address for all the decoys. *DHCP* allows the decoys to receive IP address from the DHCP server. If you select *DHCP*, *IP Count* is automatically set to 1 and all other fields are not applicable.
Network Mask	This field is set automatically.
Gateway	Specify the gateway.
MAC Address OUI	The first three octets of the MAC address for the device vendor. Only the xx:xx:xx format is supported.
IP Count	Specify the number of IP addresses to be assigned, up to 24 (for both STATIC and DHCP).
Min	The minimum IP address in the IP range.

Max	The maximum IP address in the IP range.
IP Ranges	Specify the IP range between *Min* and *Max*.

14. Click *Done*.
15. To deploy the decoys on the network, click *Deploy*.
16. To save this as a template in *Deception* > *Deployment Wizard*, click *Template*.

For deception strategies and examples, see Deployment best practices checklist on page 186 and Deception decoy best practices on page 180

Available Deception OSes, Decoys and Selected Services

The following table shows the *Available Deception OSes* and their corresponding *Available Deception Decoys* and *Selected Services* in the *Deployment Wizard*.

The *Available Deception Decoys* are only available for SCADAV3/IoT, Ubuntu16v2, Ubuntu18v1, VoIPv1 and Medicalv1 deception OSes. The decoy you select determines the available *Selected Services*.

Available Deception OSes	Available Deception Decoys	Selected Services
centosv1		SSH, SAMBA, STMP, HTTP, HTTPS, GIT, TCPListener. ICMP, FTP, RADIUS
fgt601v1		SSLVPN
fgt601v2		SSLVPN
crmv1		ERP-WEB

Available Deception OSes	Available Deception Decoys	Selected Services
scadav3	Liebert Spruce UPS	TFTP, SNMP, HTTP
	Schneider Power Meter - PM5560	SNMP, BACNET, HTTP, DNP3, ENIP
	MOXA NPORT 5110	SNMP, Telnet, HTTP, MOXA
	Rockwell 1769-L35E Ethernet Port	SNMP, ENIP, HTTP
	GE PLC 90	SNMP, HTTP, SRTP
	Kamstrup 382	KAMSTRUP
	Siemens S7-200 PLC	HTTP, TFTP, SNMP, MODBUS, S7COMM
	VAV-DD BACnet controller	SNMP, BACNET
	Niagra4 Station	SNMP, HTTP, BACNET
	Schneider EcoStruxure BMS server	SNMP, HTTP, TRICONEX, BACNET
	Rockwell PLC	HTTP, TFTP, SNMP, ENIP
	NiagaraAX Station	SNMP, HTTP, BACNET
	Rockwell 1769-L16ER/B LOGIX5316ER	SNMP, ENIP, HTTP
	Guardian-AST	Guardian-AST
	Schneider SCADAPack 333E	SNMP, DNP3, Telnet
	Siemens S7-300 PLC	TFTP, SNMP, IEC104
	IPMI Device	HTTP, FTP, SNMP, IPMI
	Siemens S7-1500 PLC	HTTP, TFTP, SNMP, IEC104, PROFINET
	Phoenix contact AXC 1050	HTTP, SNMP, PROFINET, FTP
	PowerLogic ION7650	SNMP, MODBUS, DNP3, HTTP
	Ascent Compass MNG	HTTP, FTP, SNMP, IPMI, BACNET
	C-More HMI	SNMP, HTTP, FTP, HTTPS
	Modicon M241	TFTP, SNMP, MODBUS, ENIP, HTTP
	Modicon M580	TFTP, SNMP, MODBUS, ENIP, HTTP
	Emerson iPro by Dixell	SNMP, MODBUS, HTTP
	Lantronix XPORT V1.8	SNMP, HTTP, Lantronix Discovery Protocol
	Lantronix XPORT V2.0	SNMP, HTTP, Lantronix Discovery Protocol

Available Deception OSes	Available Deception Decoys	Selected Services
ubuntu16v2	Elastic Search	Elastic Search
	Linux Decoy	SSH, SAMBA, SMTP, TCPListener, HTTP, HTTPS, GIT, ICMP, FTP, RADUIS, vnc
	ESXI Decoy	SSH, HTTP, HTTPS
	Mac Decoy	SSH, vnc
Ubuntu16v1		SSH, SAMBA, SMTP, TCPListner, HTTP, HTTPS, GIT, ICMP, FTP, RADIUS, vnc
Ubuntu18v1	Tomcat Decoy	HTTP, HTTPS, SSH
	MySql MariaDB Decoy	MariaDB, SSH
	ESXI Decoy	SSH, HTTP, HTTPS
	Elastic Search	Elastic Search
	Linux Decoy	SSH, SAMBA, SMTP, HTTP, HTTPS, GIT, TCPListener, ICMP, FTP, RADIUS, vnc
	ScadaBR Decoy	ScadaBR
	Webmin Decoy	TTP, HTTPS
win7x64v1		RDP, SMB, SMTP, TCPListener, NBNSSpoofSpotter
Custom Windows 2016/2019/2022		RDP, SMB, TCPListener, NBNSSpoofSpotter, ICMP, FTP, SWIFT Lite2
Custom Windows 10/11		RDP, SMB, MSSQL, SMTP, TCPListener, NBNSSpoofSpotter, ICMP, SWIFT Lite2, FTP
Custom French Windows 2016/ French Windows 10		RDP, SMB, MSSQL, HTTP/HTTPS, SMTP, TCPListener, NBNSSpoofSpotter, ICMP, SWIFT
Custom Redhat Linux		HTTP, HTTPS, GIT, SAMBA, SSH, SMTP, TCPListener, FTP, RADIUS
win10ltsc2021v1		RDP, SMB, SMTP, TCPListener, NBNSSpoofSpotter, ICMP, SWIFT Lite2, FTP
win10v1		RDP, SMB, SMTP, TCPListener, NBNSSpoofSpotter, ICMP, SWIFT Lite2, FTP
***outbreakv1**	Spring4Shell	Spring4Shell

Available Deception OSes	Available Deception Decoys	Selected Services
		Spring4Shell services need time to download. There may be a delay displaying these services in the *Deception OS* and *Deployment Wizard* pages after the *outbreakv1* OS is installed.
	Log4j2	Log4j2
		Log4j2 services need time to download. There may be a delay displaying these services in the *Deception OS* and *Deployment Wizard* pages after the *outbreakv1* OS is installed.
posv1		POS-WEB
iotv1	Lexmark Printer Decoy	SNMP, Jetdirect, Printer-WEB
	HP Printer Decoy	SNMP, Jetdirect, Printer-WEB
	Cisco Router Decoy	Telnet, HTTP, SNMP, CDP
	Brother MFC Printer	SNMP, Jetdirect, Printer-WEB
	TP-LINK Router Decoy	TP-LInk WEB, CWMP
	IP Camera Decoy	IP Camera-WEB, UPnP, SNMP, RTSP
	SWIFT VPN Gateway	Telnet, HTTPS
	HP Switch Decoy	SNMP, Telnet, CDP, HTTP
medicalv1	PACS Decoy	Infusion Pump (Telnet), Infusion Pump (FTP)
	SPACECOM Decoy	HTTP, HTTPS, FTP, CAN bus Protocol, SSH
	INFUSOMAT Decoy	HTTP, HTTPS, FTP, CAN bus Protocol, B.BRAUN
sapv1		SAP ROUTER, SAP DISPATCHER, SAP WEB
voipv		MQTT WEB, CoAP, SIP, XMPP WEB

***Outbreakv1**: When a cybersecurity incident/attack/event occurs that has large ramifications for the cybersecurity industry and affects numerous organizations, *FortiGuard Outbreak Alerts* will be the mechanism for communicating important information to Fortinet's customers and partners. These Outbreak Alerts will help you understand what happened, the technical details of the attack and how organizations can protect themselves from it and others like it. The FortiDeceptor Deception VM called *Outbreakv1* provides the outbreak vulnerabilities that the *FortiGuard Outbreak Alerts*

cover. For example, you can deploy a network decoy based on *FortiGuard Outbreak Alerts* such as *Spring4Shell* and *Log4j2*.

fgt601v1 / fgt601v2 comparison chart

	fgt601v1	fgt601v2
Support models	FGT-60E, FGT-100F, FGT-1500D, FGT-2000E, FGT-3700D	FGT-60F, FGT-100F, FGT-1500D, FGT-2000E, FGT-3700D, FGT-60F-DMZ, FGT-100F-DMZ, FGT-1500D--DMZ, FGT-2000E-DMZ, FGT-3700D-DMZ
Incidents reported	All logins are recorded.	DMZ models: • Only imported LDAP user logins are recorded as an incident. All other events, including connection, url, logins are dropped. • Login incident only have sslvpn login events. All other models are the same as fgt601v1.
OUI	E0:23:FF, 90:6C:AC, E8:1C:BA	E0:23:FF, 90:6C:AC, E8:1C:BA

Lure Settings

The lure settings will vary depending on the service. The character limits and requirements in FortiDeceptor may differ from the requirements implemented in the service.

Character restrictions and guidelines

Lure setting	Service	Requirements
Hostname	Windows: NBNSSpoofSpotter SAP DISPATCHER	Maximum of 15 characters. Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-) and underscores (_) are supported.

Lure setting	Service	Requirements
Client Number	SAP DISPATCHER	Alphanumeric characters (A-Z, a-z, 0-9), periods (.), commas (,), hyphens (-), underscores (_), and spaces are supported.
Database Name	MariaDB	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-) and underscores (_) are supported.
DICOM Listening Port	Medical	Enter a value between 1-65535. Default is 4242.
DICOM Server Name	Medical	Maximum of 16 characters. Name cannot begin with a digit. Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-) and underscores (_) are supported.
Domain (optional)	Windows: NBNSSpoofSpotter	Alphanumeric characters (A-Z, a-z, 0-9) and periods (.), are supported.
DSN Description	Windows: ODBC lure	Maximum of 256 characters. Alphanumeric characters (A-Z, a-z, 0-9), special characters (.-_!@(~)?:|+;*/'") and spaces are supported.
DSN Name	Windows: ODBC lure	Maximum of 32 characters. Alphanumeric characters (A-Z, a-z, 0-9), periods (.), hyphens (-), underscores (_), and spaces are supported.

Lure setting	Service	Requirements
ES Cluster Name	Elastic Search	Alphanumeric characters (A-Z, a-z, 0-9), periods (.), hyphens (-), underscores (_), and spaces are supported.
ES Node Name	Elastic Search	Alphanumeric characters (A-Z, a-z, 0-9), periods (.), hyphens (-), underscores (_), and spaces are supported.
FTP Banner	SCADAV3, Ubuntu, Centos	Alphanumeric characters (A-Z, a-z, 0-9), Periods (.), hyphens (-), underscores (_), and spaces are supported.
HTTP Listening Port	Ubuntu, Centos, Tomcat	Enter a value between 1-65535. • Ubuntu, Centos: Default is 80. • Tomcat: Default is 9200.
HTTPS Listening Port	Ubuntu, Centos, Tomcat	Enter a value between 1-65535. • Ubuntu, Centos: Default is 443 • Tomcat: Default is 9200
HTTPS SSL Certificate	Ubuntu, Centos	Optional. Upload using default settings is supported.
Instance Name	SAP DISPATCHER	Alphanumeric characters (A-Z, a-z, 0-9), periods (.), commas (,), hyphens (-), underscores (_), and spaces are supported.
Interval(sec)	Windows: NBNSSpoofSpotter	Enter a value between 60-3600.
Listening Port	ERP (CRM), POS, SAP Router, SAP DISPATCHER, TP-LINK, CWMP, ScadaBR,MariaDB, Elastic Search(HTTP)	Enter a value between 1-65535. • ERP (CRM), POS, and TP-LINK:

Lure setting	Service	Requirements
		Default is 80. • SAP Router: Default is 3299 • SAP DISPATCHER: Default is 3200 • CWMP: Default is 7547 • ScadaBR: Default is 9090 • MariaDB: Default is 3306 • Elastic Search (HTTP): Default is 9200
Listening Port Over HTTPS	SAP WEB	Enter a value between 1-65535. Default is 443
Location	SCADAV3	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), period (,), comma (,), underscores (_) and space are supported
Module type	SCADAV3	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), underscores (_), and spaces are supported.
MQTT WEB port	VoIP	Enter a value between 1-65535. Default is 18083.
PACS Listening Port	Medical	Enter a value between 1-65535. Default is 80.
PACS System Name	Medical	Maximum of 16 characters. Name cannot start with a digit. Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), and underscores (_) are supported.

Lure setting	Service	Requirements
Page title	SCADAV3	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), underscores (_), and spaces are supported.
Password	Windows: RDP & SMB, Ubuntu and Centos: SSH & SAMBA, RADIUS, NBNSSpoofSpotter French Windows:RDP, SMB, MSSQL, HTTP/HTTPS, SMTP, FTP GIT Users, ERP (CRM), Medical, POS, FortiGate, Cisco Router (Telnet/HTTP), HP Printer (HTTP), IP Camera (HTTP), Centos, SAP Router, SAP WEB, Brother MFC Printer (HTTP), Lexmark Printer (HTTP), TP-LINK	Maximum of 32 characters. Alphanumeric characters (A-Z, a-z, 0-9) and special characters (- ! @ # $ (~) ^ & ? <> : | + ; * / , . " ' _) are supported. The password is optional in *GIT repository import*.
Plant Identification	SCADAV3	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), underscores (_), and spaces are supported.
PLC name	SCADAV3	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), underscores (_), and spaces are supported.
Repository Name	GIT Users	Maximum of 100 characters. Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-) and underscores (_) are supported.
Serial number	SCADAV3	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), underscores (_), and spaces are supported.
Serial number for ENIP	SCADAV3	Only 0-9 allowed

Lure setting	Service	Requirements
Sharename	French Windows:RDP, SMB, MSSQL, HTTP/HTTPS, SMTP, FTP Windows:RDP & SMB, Ubuntu Centos-SSH & SAMBA Centos	This option is only available for SAMBA (Ubuntu) or SMB (Windows). Enter a Sharename between 3-63 characters. Alphanumeric characters (a-z, 0-9) and hyphens are supported.
SID	SAP DISPATCHER	Alphanumeric characters (A-Z, a-z, 0-9), periods (.), commas (,), hyphens (-), underscores (_), and spaces are supported.
SIP port	VoIP	Enter a value between 1-65535. TCP Default is 5060, 5061. UDP Default is 5060.
SMTP Banner	Windows, Ubuntu, Centos	Alphanumeric characters (A-Z, a-z, 0-9), periods (.), hyphens (-), underscores (_), and spaces are supported.
SMTP Domain	Windows, Ubuntu, Centos	Alphanumeric characters (A-Z, a-z, 0-9) and periods (.), and hyphens (-) are supported.
SNMP	SCADAV3, Cisco Router (Telnet/HTTP), HP Printer (HTTP), IP Camera (HTTP), Brother MFC Printer (HTTP), Lexmark Printer (HTTP)	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-) and underscores (_) are supported.
SNMP Banner	SCADAV3, Ubuntu, Centos	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), underscores (_), and spaces are supported.

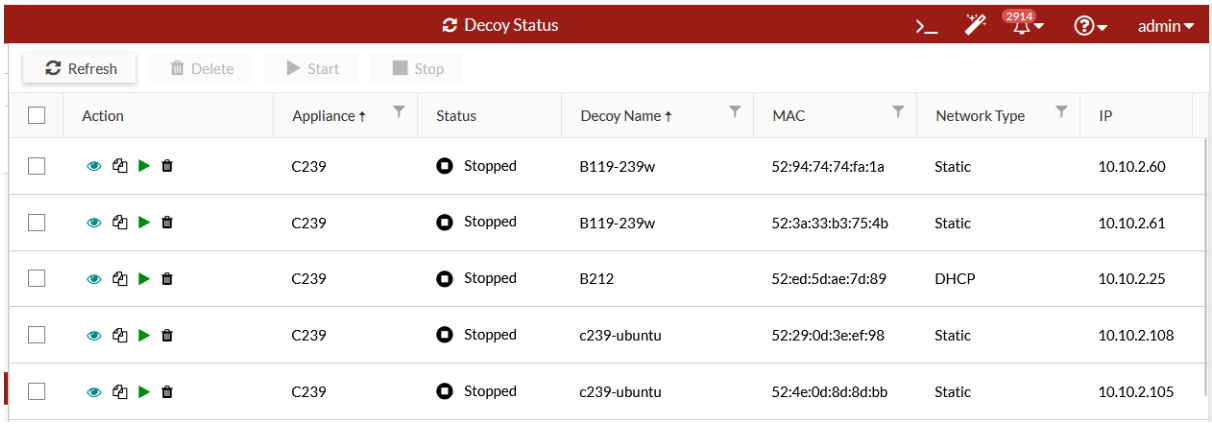
Lure setting	Service	Requirements
SSH Banner	Ubuntu, Centos	Alphanumeric characters (A-Z, a-z, 0-9), periods (.), hyphens (-), underscores (_), and spaces are supported.
SSLVPN Bookmarks Name	FortiGate	Maximum of 15 characters. Alphanumeric characters (A-Z, a-z, 0-9), periods (.), hyphens (-), underscores (_), and spaces are supported.
SSLVPN Bookmarks URL	FortiGate	Required field. Alphanumeric characters (A-Z, a-z, 0-9), spaces, and special characters (-@#~?:./_=) are supported.
SSLVPN Listening Port	FortiGate	Enter a value between 1-65535. Default is 10443.
TCP Banner	Windows: TCP Listener Ubuntu, Centos	Alphanumeric characters (A-Z, a-z, 0-9), periods (.), hyphens (-), underscores (_), and spaces are supported.
TCP Listener	Windows: TCP Listener Ubuntu, Centos	Separate multiple ports with a comma (,).
Telnet	SCADAV3	Telnet username password is the same as ERP
Token	GitHub repository import	Alphanumeric characters (A-Z, a-z, 0-9), and periods (.) are supported.

Lure setting	Service	Requirements
Update or Cancel	Windows: RDP & SMB, Ubuntu and Centos: SSH & SAMBA	Click *Update* to save the username and password. Click *Cancel* to discard the username and password. Click *Delete* to delete an existing lure.
URL	GitHub repository import	Required field. Alphanumeric characters (A-Z, a-z, 0-9), spaces, and special characters (-@#~?:./_=) are supported.
Username	LINK Windows (FTP/NBNSSpoofSpotter/RDP/SMB/SMTP), Ubunbu and Centos (Elastic Search/FTP/GIT/HTTP/HTTPS/MariaDB/RADIUS/SAMBA/SMTP), CRM (ERP-WEB), FortiGate (SSLVPN), Brother MFC Printer (HTTP), Cisco Router (HTTP/Telnet), HP Printer (HTTP), HP Switch (HTTP), IP Camera (HTTP), Lexmark Printer (HTTP), TP-LINK Router (HTTP), Medical (B.BRAUN/FTP/HTTP/HTTPS/Telnet), POS (HTTP), SAP (HTTP), Schneider SCADAPack 333E (Telnet), Phoenix contact AXC 1050 (FTP)	Maximum of 32 characters. Alphanumeric characters (a-z, 0-9), hyphens (-) and underscores (_) are supported. Usernames should start with letters or underscores (_) and could end with dollar sign ($).
	Ubuntu and Centos (SSH), Medical (SSH),	Maximum of 32 characters Alphanumeric characters (a-z, 0-9), hyphens (-) and underscores (_) are supported. Usernames should start with letters or underscores (_) and could end with dollar sign ($).
XMPP WEB port	VoIP	Enter a value between 1-65535.Default is 5280.

Decoy Status

The *Decoy Status* page shows the status of the Decoys on your network. Use the page to start, stop or delete a decoy. You can also view the decoy's configuration details and copy the decoy template.

We recommend operating Decoy VMs with the same status for expected behavior.

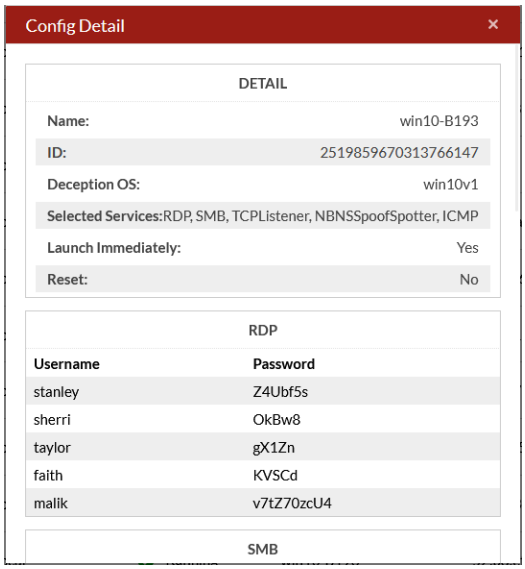


The *Decoy Status* page displays the following information:

Status	The status of the decoy can be *Initializing*, *Running*, *Stopped*, or *Cannot Start*. If the Decoy VM cannot start, hover over the VM to see the reason.
Decoy Name	Name of the decoy.
Initialize Time and Start Time	The decoy's initialization time and its last start time.
OS	Operating system of the decoy.
VM	The name of the Decoy VM.
IP	The IP address of the Decoy VM.
Services	List of services enabled. Hover over an icon to see a text list.
Network Type	Shows if the IP address is *Static* or *DHCP*.
DNS	DNS of the Decoy VM.
Gateway	Gateway of the Decoy VM.

To view the decoy configuration details:

1. Go to *Deception* > *Decoy Status* and select a decoy.
2. In the *Action* column, click *View Details*. The *Config Detail* page opens.



To copy a decoy the Deployment Wizard:

1. Go to *Deception* > *Decoy Status* and select a decoy.
2. Click *Copy to Template*. The template is copied to the *Deployment Wizard*.

To delete Decoy VMs:

1. Go to *Deception* > *Decoy Status* and select one more decoys.
2. In the *Action* column, click *Delete*.
3. Click *OK*.

To start a Decoy VM:

1. Go to *Deception* > *Decoy Status* and select one more decoys that are stopped.
2. In the *Action* column, click *Start*.

To stop a Decoy VM:

1. Go to *Deception* > *Decoy Status* and select one more decoys that are running.
2. In the toolbar, click *Stop*. The decoy status changes to *Stopped*.

Deception Token

Use a FortiDeceptor token package to add breadcrumbs on real endpoints and lure an attacker to a Decoy VM. Tokens are normally distributed within real endpoints and other IT assets on the network to maximize the deception surface.

For information about using FortiDeceptor to generate a deception lure package based on the decoy service configuration, see Deploying tokens using AD GPO logon script on page 195.

The following token types are available:

Token type	Description
SMB (hidden mapped network disk)	Map the shared directory to a remote decoy that acts as file server while the shared disk is hidden. The username and password are saved in the Windows Vault (Credentials Manager). SMB remote folders are Windows folders.
SAMBA (hidden mapped network disk)	Same as SMB but for Linux SAMBA shares. SAMBA remote folders are Linux folders.
RDP (Remote Desktop)	The username, password and the windows Decoy IP are saved in the Windows Vault (Credentials Manager). Additionally, it creates RDP shortcuts in `%USERPROFILE%\Documents`. The file name format is `rdp_USERNAME_IP.rdp` and created files are hidden. The RDP Lure username and password are saved in Windows Vault.
SSH (Secure Shell)	Create a hidden Putty shortcut in `%USERPROFILE%\Documents`. If Putty (putty.exe) is not installed in the specified directory, no shortcut is created.
Credential Cache Lure	In Domain environment, add a new credentials entry to the real desktop or server process `lsass.exe`.
HoneyDocs	Add fake files (Word & PDF) to Windows directories. The default is to the most recent folder. You can specify the location in the Windows directory. Please use the Linux decoy to deploy the HoneyDocs token campaign.
ODBC	The ODBC lure saves a DSN connection string using the Trusted Connection mechanism. To deploy an effective ODBC token, the following is required: • Deploy with domain DNS and SQL SERVER service based on a custom windows image joining a domain. See, *Custom Decoy Image on page 36* > *To deploy decoys with custom images–SQL Server*. • Install ODBC lures into domain user accounts that are on the same domain as the custom Windows server.
SAP token	Add fake SAP configuration files to Windows SAP installation path that contains decoy IP and other SAP related configuration data.

Token type	Description
AWS Key	Add a JSON file including AWS Keys to Windows directories. You can specify the location in the Windows directory. The default location is the most recent folder.
Azure Key	Add a JSON file including Azure Keys to Windows directories. You can specify the location in the Windows directory. The default location is the most recent folder. You can also specify a certificate with Azure Keys in the same directory.

To create a FortiDeceptor token campaign:

1. Go to *Deception* > *Deception Token* > *Token Campaign*.
2. Click *+Campaign*.
3. Configure the campaign *Name* and *Mode*.

Name	Enter the campaign name.
Mode	• **Offline**: The complete Deception Tokens package will be downloaded from the FDC manager and copied to the endpoint using the external distribution system like the A/D logon script for deployment. • **Online**: A light Deception Tokens package will download from the FDC manager and copied to the endpoint using the external distribution system like the A/D logon script. The package will have the binary file and one configuration file that points to the endpoint to download the deception campaign from the FDC manager over a secure port. Use *Online* mode to change the campaign at any time on the FortiDeceptor server. Any changes you make will be applied to the endpoint.

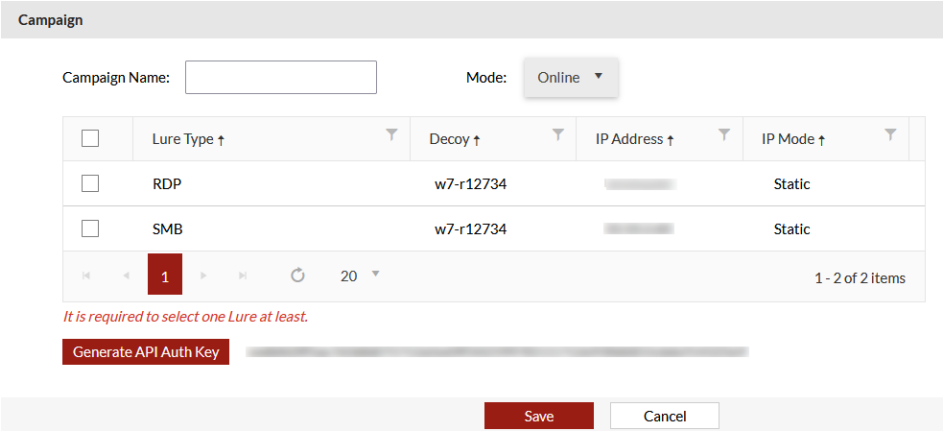
4. Select the lures. At least one lure must be selected.

You can only select lures with valid Static IP addresses.

The related decoys must have a status of *Initialized*, *Stopped*, *Running*, or *Failed*. We recommend keeping the related decoys with a status of Running for successful lure deployment.

5. (Optional) Click *Generate API Auth Key* to generate an API key.

6. Click *Save*.



To view campaign list:

1. Go to *Deception* > *Deception Token*.
2. Select a campaign from the list. In the column:
   - Click *Edit* to edit the campaign.
   - Click *Delete* to delete the campaign.
   - Click *Download* to download the campaign.

To deploy FortiDeceptor token campaign on an existing endpoint:

1. Download FortiDeceptor token campaign package
2. Copy the downloaded FortiDeceptor token campaign package to an endpoint such as a Windows or Linux endpoint.
3. Unzip the FortiDeceptor token campaign package.
4. In the OS folder, follow the instructions in README.txt file to install the token package.
   - **Windows**: Open the windows folder, and double-click the *windows_token.exe* to run it.
   - **Ubuntu**: Open Terminal and run python script *./ubuntu_token.py*.
5. In the OS folder, uninstall the token campaign package.
   - By default, the new token installation process will automatically clear the lure information before installing the new ones.

When the FortiDeceptor token package is installed on a real Windows or Ubuntu endpoint, it increases the deception attack surface and lures the attacker to a Decoy VM

To review Token Deployment Status:

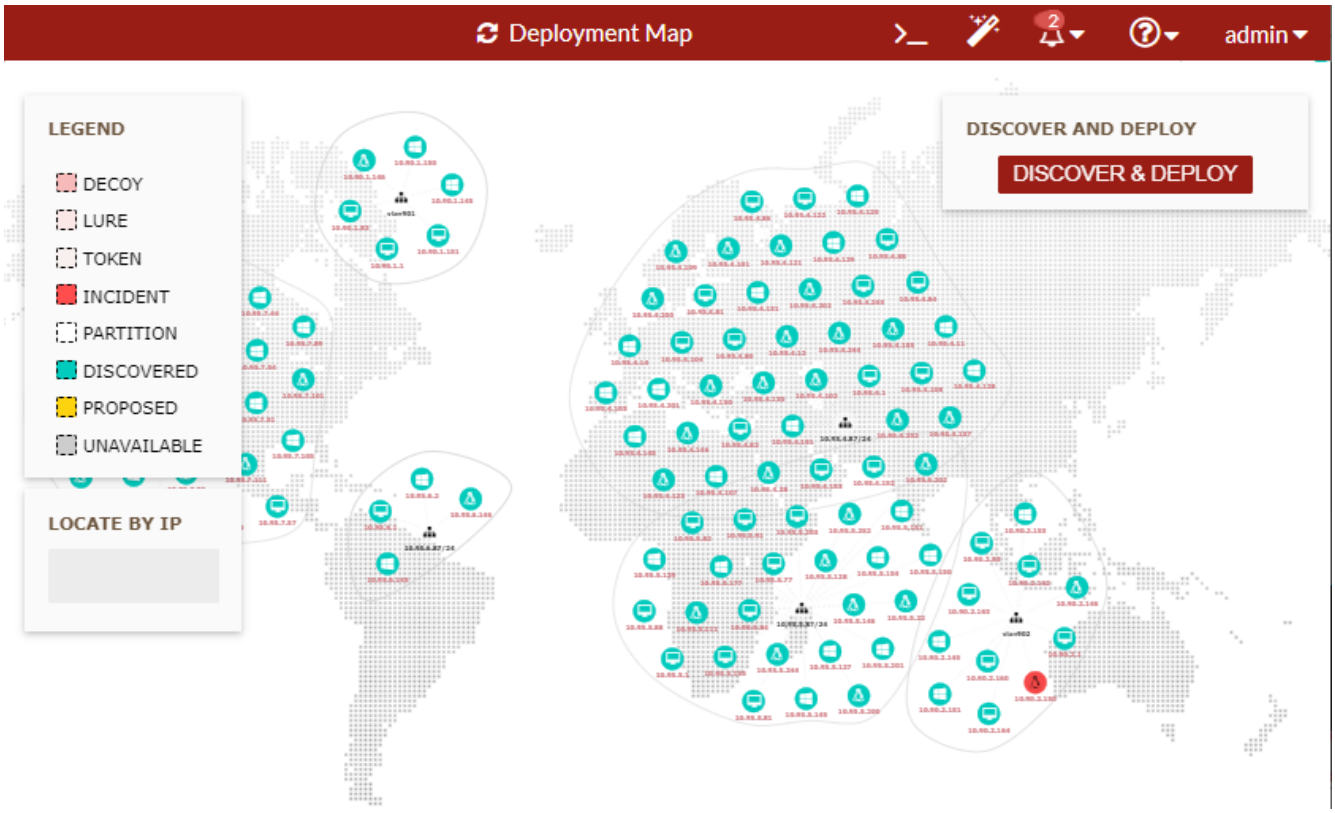
1. Go to *Deception* > *Deception Token* > *Token Deployment Status*.
2. Expand the *Endpoint Name* to view the *Deployment Details* for the endpoint.

Deployment Map

The *Deployment Map* is a visual representation of the entire network showing real endpoints and decoy VMs. Click a node on the map to view its details. Use *Discover & Deploy* to detect the OSes for all the assets on the network and

automatically deploy decoys for those OSes.

If you know the IP of an endpoint or partition, you can search for it with the *Locate By IP* box.



The nodes on the map are color-coded by importance:

Node	Color	Description
Partition	White	Click the node to view the Network Partition ID, Interface port, and subnet.
Incident	Red	A glowing red node indicates the decoys have been attacked. Click the node to view the Decoy ID, view incidents in the *Analysis* page.
Decoy	Pink	Click to start or stop the, view its configuration, save the decoy as a template, or delete it.
Lure	Coral	Click to view the Decoy type, Service, and data such as the username and password.
Endpoint	Green	Click to view the IP, MAC address, and OS.
Proposed	Yellow	Click a yellow node to edit its settings, generate lures, duplicate, or delete it.
Unavailable	Grey	FortiDeceptor cannot retrieve data for the asset.

Discover & Deploy

Use *Discover & Deploy* to detect the OSes for all the assets on the network. After the OSes are discovered, FortiDeceptor will attempt to create decoys to auto-fit the assets in the network.

To discover OSes and auto-deploy decoys:

1. Click *Discover & Deploy*. The *Discovery & Deployment* dialog opens.
2. Configure the discover settings.

Select Networks to Scan	Select the ports on the network you want to discover.
Add Deployment Network	Click to open the *Add New Vlan/Subnet* dialog. See Deployment Network on page 67.
Additional TCP Scan Port	Enter the additional scan ports. The default scan ports are 21, 22, 23, 25, 53, 69, 80, 110, 135, 137, 1378, 139, 143, 443, 445, 993, 995, 1433, 3306, 3389, 5900, 8080.
Decoys per VLAN/Subnet	Enter the number of decoys per VLAN based on the asset discovery results.

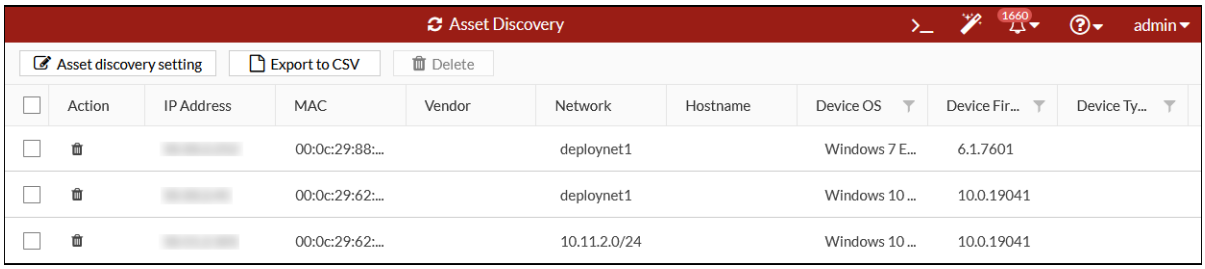
3. Click *Discover* and wait a few minutes for the system to complete the discovery. The results are displayed.

OS Covered	The OSes FortiDeceptor can cover with a suitable decoy for auto-deployment.
Total auto-deploy decoys	The number of decoys that are suitable for auto-deployment.
Total coverage	The percentage of assets that will be covered by the deployment.
Download assets list CSV	Click to download the asset list as CSV file.

4. Click *Accept & Deploy*. FortiDeceptor deploys the decoys.

Asset Discovery

The *Asset Discovery* module generates Asset Inventory by passively fingerprinting the OS and other parameters for the assets in OT/IT/IoT networks. This improves threat visibility for the networks and helps with optimizing decoy placement.



The Asset Discovery page displays the following information:

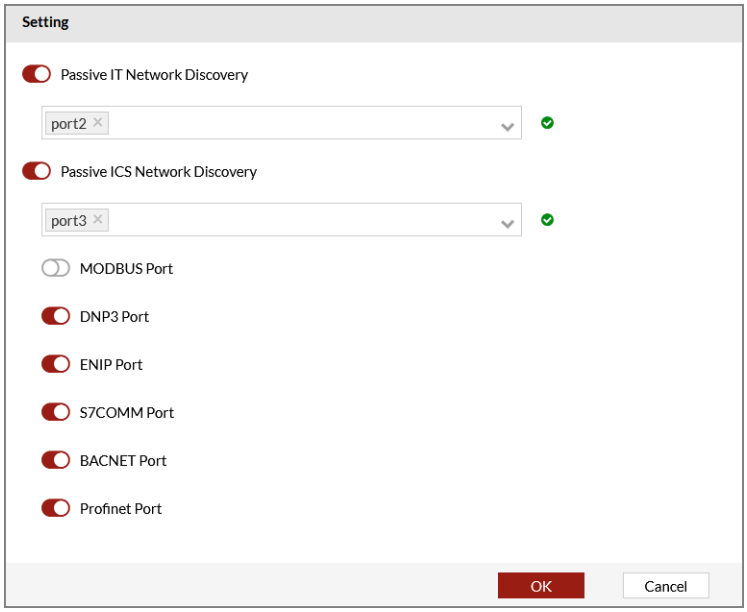
Action	Click *Delete* to remove the asset.

IP Address	The IP address of the asset.
MAC	The MAC address of the asset.
Vendor	The vendor identified by the asset MAC address.
Network	The network this asset was discovered.
Hostname	The hostname of the asset.
Device OS	The Device OS of the asset.
Device Firmware	The firmware version of the asset.
Device Type	The type of the asset.

To enable Asset Discovery:

1. Go to *Deception > Asset Discovery*.
2. Click *Asset discovery setting*.
3. Enable the following the settings:

Passive IT Network Discovery	Enable to allow FortiDeceptor to identify common IT devices such as servers, laptops, and routers by sniffing network traffic. Select all the ports connected to the network for discovery.
Passive ICS Network Discovery	Enable to allow FortiDeceptor to identify industrial control devices such as PLC controllers. Select all the ports connected to the network and ICS protocols for discovery. The available protocols are, MODBUS, DNP3, ENIP, S7comm/S7comm plus, BACNET, Profinet, FINS, ATG, Kamstrup, Moxa, IEC104, FL-net, GE-EGD, GE-SRTP, Triconex and PCOM.



4. Click *OK*.

To delete multiple assets at the same time:

1. Select the assets you want to delete.
2. In the toolbar, click *Delete*.

To export the asset details as a CSV file:

In the toolbar, click *Export CSV*.

Safe List

Use the *Deception* > *Safe List* page to add an IP address that is considered legitimate so that it does not generate an *Event* or *Incident* when accessing decoys. For example, the IP address of a monitoring system that is polling the network.

To add a new Safe List IP address:

1. Go to *Deception* > *Safe List*.
2. Click *Add New Safe List IP* and configure its settings:

IP/Mask	Specify the IP address or subnet from where the connection originate.
Source Ports	Specify the source ports from where the connection originates.
Destination Ports	Specify the destination ports on the network where the connection terminates.
Description	Specify a description. For example, you can name it as *Safe_Network*.
Services	Select the name of the services used to connect to the network.
Status	Select *Enabled* or *Disabled*.
Action	Click *Update* or *Cancel*.

Incident

The *Incident* module displays the incidents and attacks detected by FortiDeceptor.

This section contains information about the following topics:

- Analysis on page 95
  View incidents and related events detected by FortiDeceptor
- Campaign on page 97
  View attacks and related events detected by FortiDeceptor.
- Attack Map on page 99
  View ongoing attacks and related events detected by FortiDeceptor.

Analysis

The *Analysis* page displays the list of incidents detected by FortiDeceptor. Use this page to generate the *Incidents Report* PDF. The *Incidents Report* can be generated one at time, or you can schedule the report to generate on a recurring basis. You can also export incidents list as a CSV file.

When you expand an incident to the view the details, the incident is marked as *read*. Newly-detected incidents are in bold to indicate they are unread. To refresh the data click the *Refresh* button in the toolbar.

You can configure the table settings by clicking the gear icon at the bottom-right of the page or go to *System* > *Table Customization.* For more information, see Table Customization on page 146.

The *Analysis* page displays the following information:

Severity	Severity of the event.
Protocol	Network protocol the attacker used to perform the attack.
Last Activity	Date and time of the last activity.
Type	

Event Type	Triggered By
Connection	**1.** Port scan (SYNConnection). **2.** Ping. **3.** SYN connection. **4.** Access to the service with no other interaction like accessing a web server without entering any credentials.
Reconnaissance	**1.** Port scan (Full TCP Connection). **2.** Access the decoy network share and browse files. **3.** Access the decoy web application and browse the

	Event Type	Triggered By
		web application. **4.** Access decoy FTP server and browse files.
	Interaction	**1.** The attacker accesses the decoy and passes the log in phase. **2.** Attacker logs into a decoy and runs commands inside the session like RDP.
	Infection	**1.** Attacker copies files to the decoy. **2.** Attacker accesses the decoy and downloads files from the internet. **3.** The attacker runs an exploit against the decoy and injects a binary file.
Attacker IP	Attacker IP address.	
Attacker User	Attacker username.	
Victim IP	IP address of the victim.	
Victim Port	Port of the victim.	
Decoy ID	Unique ID of the Decoy VM.	
ID	ID of the incident.	
Attacker IP	Attacker IP address and domain name.	
Attacker Port	Port where the attack originated.	
Tag Key	Unique key string for the incident.	
Attacker Password	Password used by the attacker.	
Start	Date and time when the attack started.	

The infected files captured by the decoy are saved as a password protected .zip file you can download. The password for the file is `FortiDeceptor`.

To generate the Incidents Report:

1. Go to *Incidents* > *Analysis*.
2. In the toolbar, click *PDF Report*.

3. Configure the report settings.

Mail Address	Enter the destination email for the report.
Scheduler Type	Select *One Time* or *Recurring*.
User Timezone	For one time reports, set the recipient's timezone.
Generate report for data From	For one time reports, select the report start date and time.
Generate report for data To	For one time reports, select the report end date and time.
Scheduler Timezone	For recurring reports, select the scheduled timezone.
Scheduler Start	For recurring reports, select the schedule start date and time.
Scheduler End	For recurring reports, select the schedule end date and time.
Scheduler Interval	Select *Daily*, *Weekly*, or *Monthly*.
Days	For Weekly reports, select the day of the week to generate the report. For Monthly reports, select the date to generate the report.
Time	Select the time to generate the report for the selected day.

4. Click *Generate*.

To export the Incidents list a CSV file:

- In the toolbar, click *Export to CSV*.

It may take some time to export the report depending on the number of incidents in the list.

Campaign

The *Campaign* page displays a list of attacks detected by FortiDeceptor. An attack consists of multiple incidents.

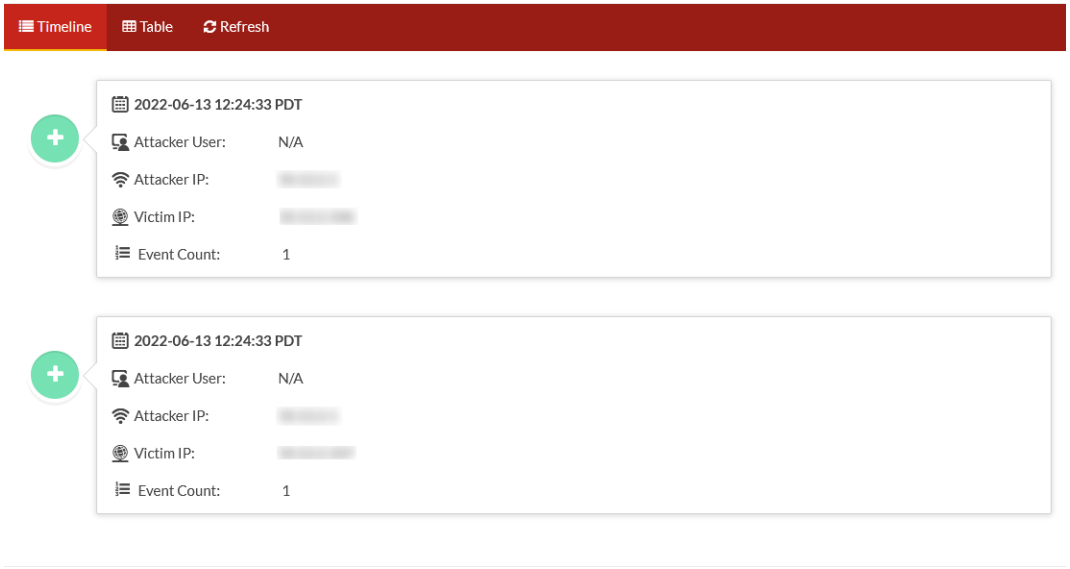
You can configure the table settings by clicking the gear icon at the bottom-right of the page or go to *System* > *Table Customization.* For more information, see Table Customization on page 146.

The *Campaign* page displays the following information:

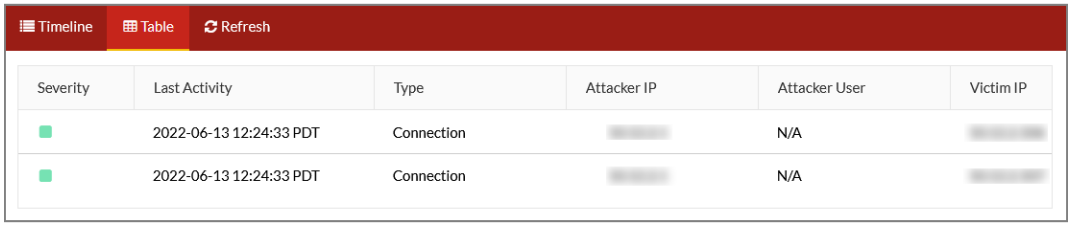
Severity	Severity of the event.
Start	Date and time when the attack started.
Attacker IP	IP mask of the attacker.
ID	ID of the campaign record.
Last Activity	Date and time of the last activity.

To view the attack details:

1. Go to *Incident* > *Campaign*.
2. Expand an attack in the list. The campaign *Timeline* is displayed.



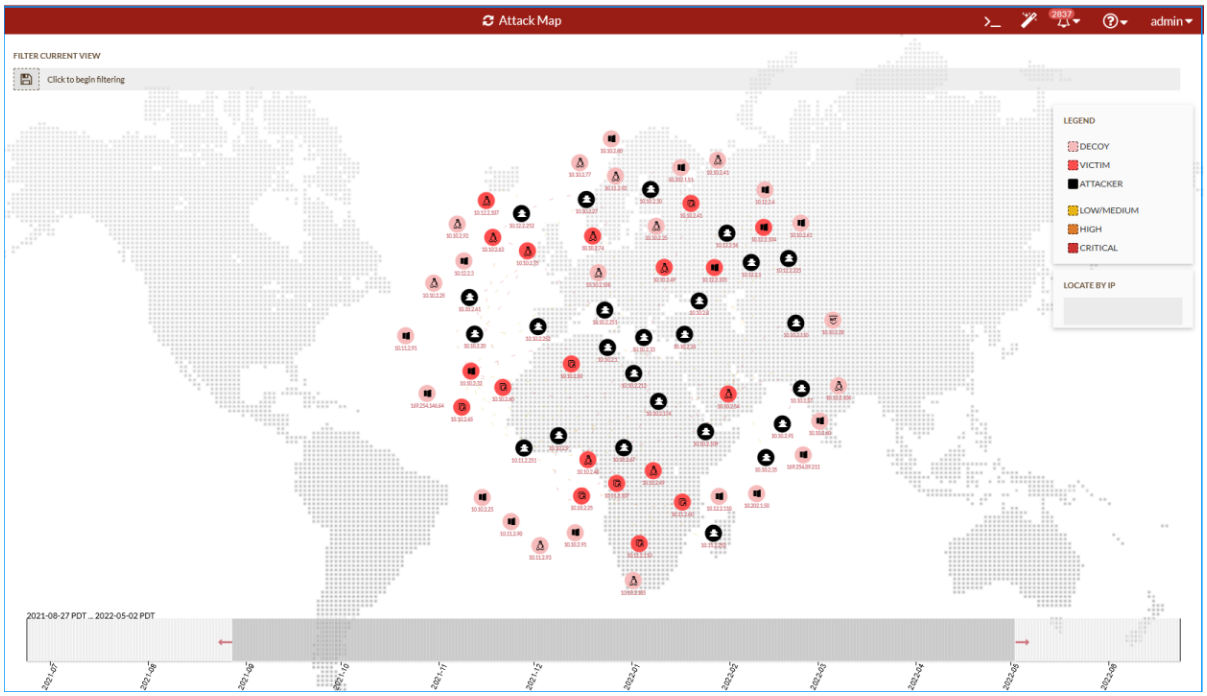
3. Click table to view the attack *Severity*, *Last Activity*, *Type*, *Attacker IP*, *Attacker User*, *Victim IP*, and *Victim Port*.



4. (Optional) Click *Refresh* to refresh the data.

Attack Map

The *Attack Map* is a visual representation of the entire network showing real endpoints, Decoy VMs, and ongoing attacks.



The nodes on the map are color-coded by severity.

Node	Color	Description
Decoy	Pink	Click to view the *Name*, *MAC address*, *IP*, *DNS*, and Gateway.
Victim	Red	Click to view the attack history including *Attacker*, *Start Time* and *Incident ID*. When a node is both Victim and Attacker, the node will appear as Attacker.
Attacker	Black	Click to view the attacker's history including *Attacker*, *Start Time* and *Incident ID*.

To filter the Attack Map by IP:

1. Under *Filter Current View*, click in inside *Click to begin filtering*. The options menu is displayed.
2. Select one of the following options:
   - *Attacker IP*
   - *Victim IP*
   - *Decoy IP*
3. Enter the IP address. FortiDeceptor sorts the nodes on the map.

To save the current view of the map:

Under *Filter Current View*, click the *Save View* icon .

To filter the map by date:

Drag the red arrows at the bottom of the page to set the start and end dates.

To search for a node by IP:

In the *Locate by IP box*, enter the IP address.

MITRE ICS

The *MITRE ICS* matrix provides an overview of the tactics and techniques in the *ATT&CK for the ICS* Knowledge Base. ATT&CK for ICS is a Knowledge Base used to describe an adversary's actions during an attack. The *MITRE ICS* page visually aligns individual techniques under the tactics where they can be applied. Some techniques span more than one tactic because they can be used for different purposes.

MITRE ICS is relevant to IoT/OT networks. To identify the network, you will need to tag each FortiDeceptor appliance.

To tag MITRE ICS a FortiDeceptor client with the CLI:

```
set tag ICS
```

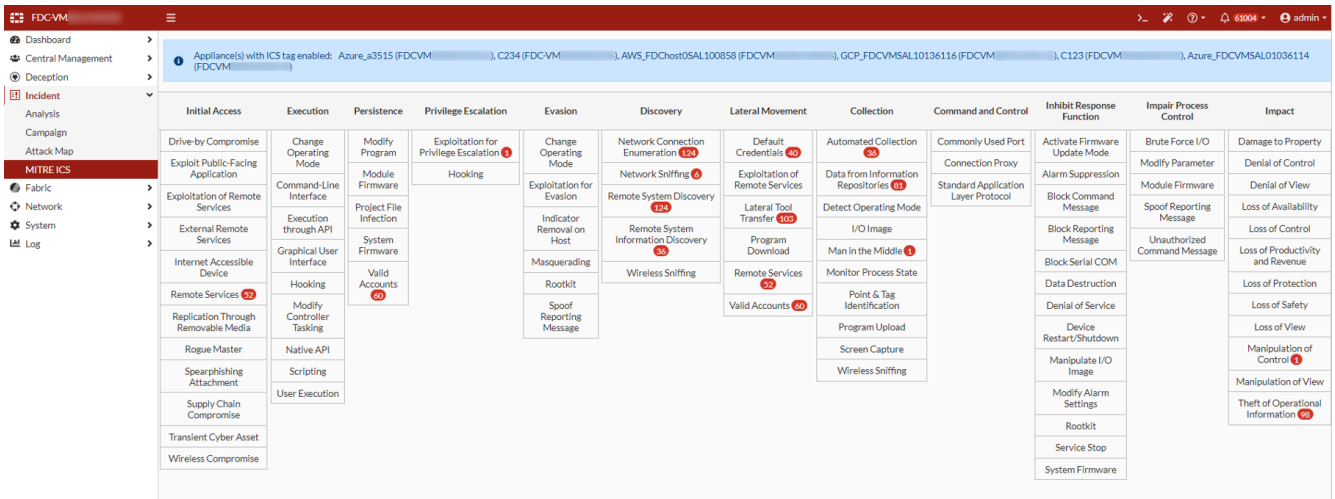
To remove a tag from a FortiDeceptor client with the CLI:

```
unset tag
```

Viewing the MITRE ICS matrix

After the FortiDeceptor appliance is tagged, go to *Incident* > *MITRE ICS* to view the matrix. The matrix displays the *Tactics* as columns and the *Techniques* as tiles. Management devices display a blue banner at the top of the matrix that shows the tagged appliances in the network. Standalone devices do not display the banner. When an incident meets the Tactic criteria, the Technique tile displays a red dot with the number of incidents.

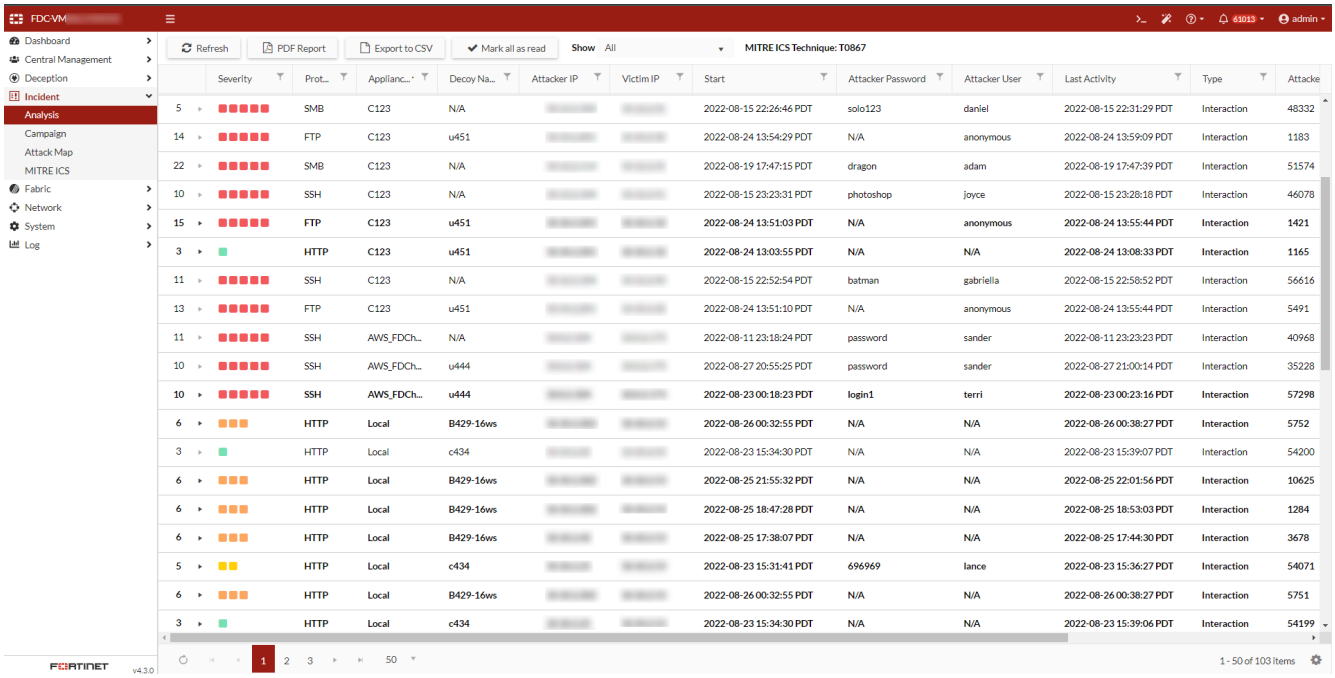
To view the MITRE ICS incidents, click a *Technique* tile in the *Tactics* column.



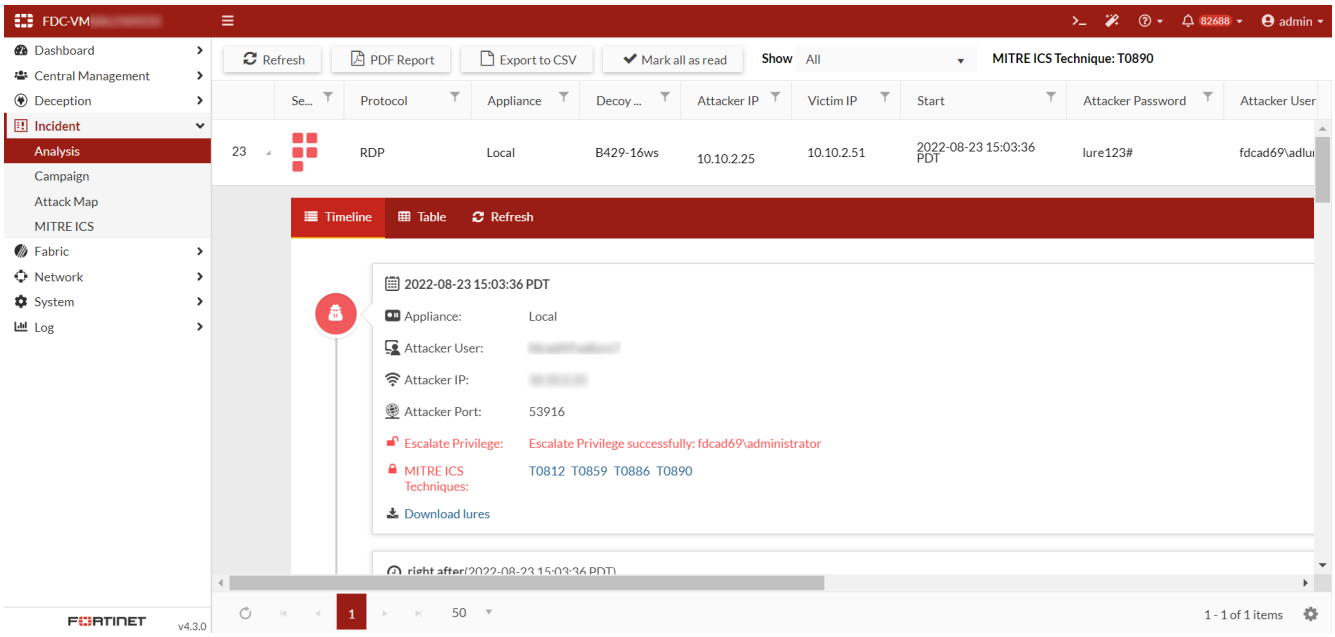
After you click a technique, you are redirected to the *Incidents* > *Analysis* page. The *Analysis* page displays the incidents that meet conditions for the technique you selected.

The MITRE ICS page is only available in the FortiDeceptor appliances tagged with *set tag ICS*.

In the image below, the *Analysis* page displays the incidents that match *MITRE ICS Technique: T0867*.



Click an attack to view its details. Scroll down to the *MITRE ICS Techniques* field to view the techniques linked to the attack. Click a *TXXX* link to view a description of technique in the *ATT&CK for the ICS* Knowledge Base.


FDC-VM
admin
Dashboard
Central Management
Deception
Incident
Analysis
Campaign
Attack Map
MITRE ICS
Fabric
Network
System
Log
Refresh
PDF Report
Export to CSV
Mark all as read
Show All
MITRE ICS Technique: T0890
Se...
Protocol
Appliance
Decoy ...
Attacker IP
Victim IP
Start
Attacker Password
Attacker User
23
RDP
Local
B429-16ws
10.10.2.25
10.10.2.51
2022-08-23 15:03:36 PDT
lure123#
Timeline
Table
Refresh
2022-08-23 15:03:36 PDT
Appliance:
Local
Attacker User:
Attacker IP:
Attacker Port:
53916
Escalate Privilege:
Escalate Privilege successfully: fdcad69\administrator
MITRE ICS Techniques:
T0812 T0859 T0886 T0890
Download lures
1
50
1 - 1 of 1 items
v4.3.0

Fabric

Use the *Fabric* pages to manage and configure FortiGate information for integration with FortiDeceptor. This includes blocking settings and Security Fabric status information. Blocking from FortiGate is an API call from FortiDeceptor which allows instant quarantine from FortiGate once an incident is detected. The quarantined IP is under user quarantine in the FortiGate GUI.

This section includes the following topics:

- Detection Devices on page 103
  Configure the third-party malware detection devices for FortiDeceptor integration.
- Quarantine Integration on page 105

  Configure the quarantine devices for FortiDeceptor integration.
- Quarantine Status on page 117

  Status of blocked IP addresses.
- IOC Export on page 118

  Export the IOC file in CSV format for a specified time period.

Detection Devices

The *Detection Devices* page allows you to configure integrations with FortiSandbox, Cuckoo Sandbox, and Virus Total devices.

FortiSandbox

The integration between FortiDeceptor and FortiSandbox will provide a complete static and dynamic analysis against malicious code captured by the network decoys. The malware analysis report will be available on the FortiDeceptor admin console.

To configure integration with FortiSandbox:

1. Go to *Fabric* > *Detection Devices*.
2. Enable *FortiSandbox*.
3. Configure the following parameters:

Type	Select *Appliance* or *Cloud*.
IP/URL	Type the FortiSandbox appliance or cloud IP address or URL
Port	Type the FortiSandbox API port. Default is 443.
Username	Type the API username for the FortiDeceptor appliance. You can configure the

	API username in FortiSandbox.
Password	Type the API password for the FortiDeceptor appliance. You can configure the API password in FortiSandbox.
Token Access	Type the Token for FortiSandbox Cloud. You can find this in FortiSandbox Cloud CLI with the following command: `login-token`
User ID	Type the FortiSandbox Cloud User ID.

4. Click the *Test* button to ensure the API connection is working properly.
5. Click *Save* to store the configuration

Cuckoo Sandbox

The integration between FortiDeceptor and Cuckoo Sandbox will provide a complete static and dynamic analysis against malicious code captured by the network decoys. The malware analysis report will be available on the FortiDeceptor admin console.

To configure integration with Cuckoo Sandbox:

1. Go to *Fabric* > *Detection Devices*.
2. Enable *Cuckoo Sandbox* .
3. Configure the following parameters:

Name	The Fabric connector name
IP/URL	Type the Cuckoo Sandbox IP address or URL
Port	Type the Cuckoo SandboxAPI port. (default is 1337)
API Token	Type the API Token located in the Cuckoo Sandbox's configuration file.

4. Click on the *Test* button to ensure the API connection is working properly.
5. Click *Save* to store the configuration

Virus Total

The integration between FortiDeceptor and the well-known Virus Total service allows the submission of suspicious files (MD5) for malware analysis. When integrated, Virus Total detection ratios will be displayed in the incident analysis alert Workflow for relevant events.

Virus Total engages with multiple service providers to perform the same file inspection. Some service providers return a score of *0*, meaning it is not malware, whereas other providers return a score of *1*, meaning it is malware. Virus Total then returns a ratio such as *15/36* that indicates *15* out of *36* service providers determined the file is malware.

To configure integration with VirusTotal:

1. Join the VirusTotal Community.
2. In your personal settings section find your personal API key in your personal settings section.
3. Go to *Fabric* > *Detection Devices*.

4. Enable *VirusTotal*.
5. In *VT API Key* field enter the your Virus Total personal API key.
6. Click *Save*.

Quarantine Integration

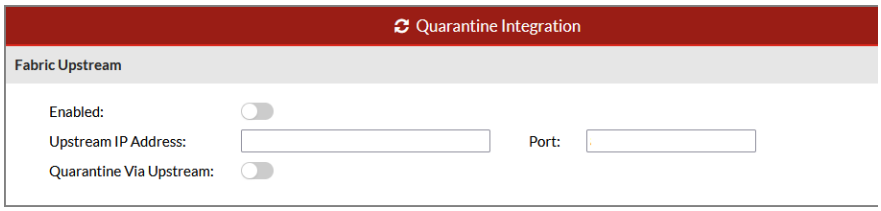
FortiDeceptor on FortiGate Security Fabric topology map

Security Fabric integration allows FortiDeceptor and deception decoys to be visible through the Fabric network topology map.

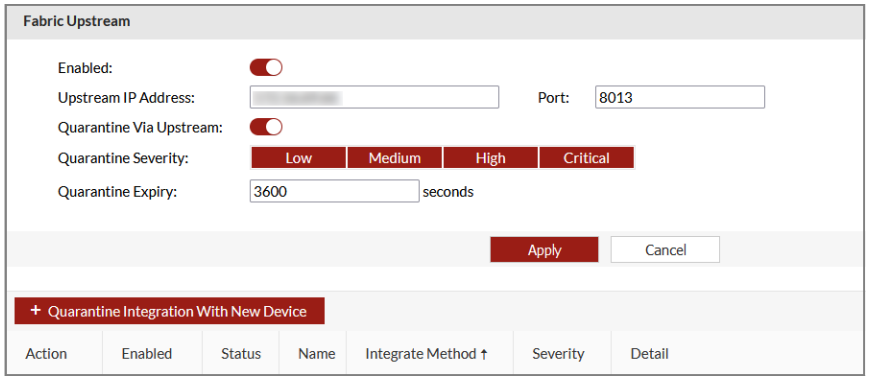
To configure Security Fabric integration, enter the upstream device IP in Port in FortiDeceptor. Next you will add the FortiDeceptor fabric connector in FortiGate.

To configure FortiGate for Security Fabric integration in FortiDeceptor:

1. In FortiDeceptor, go to *Fabric* > *Quarantine Integration*.
2. Under *Fabric Upstream* section, select *Enabled*.

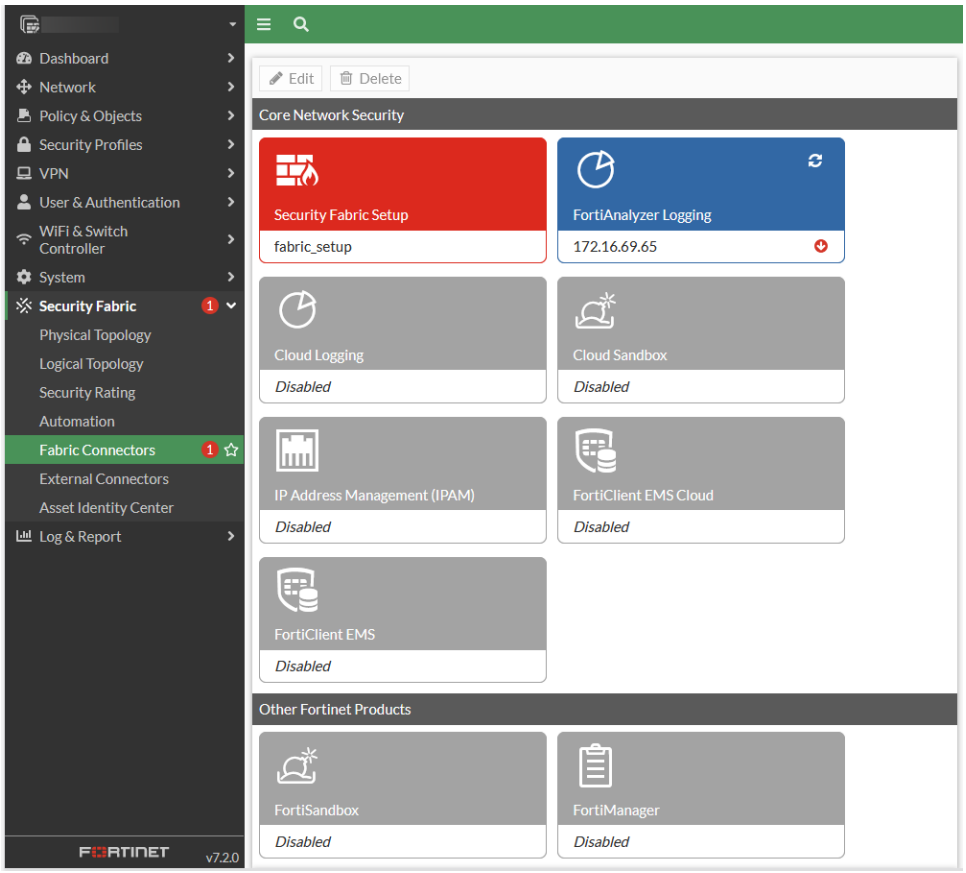


3. Enter the FortiGate IP address in *Upstream IP Address* and the FortiGate connector port in *Port*.

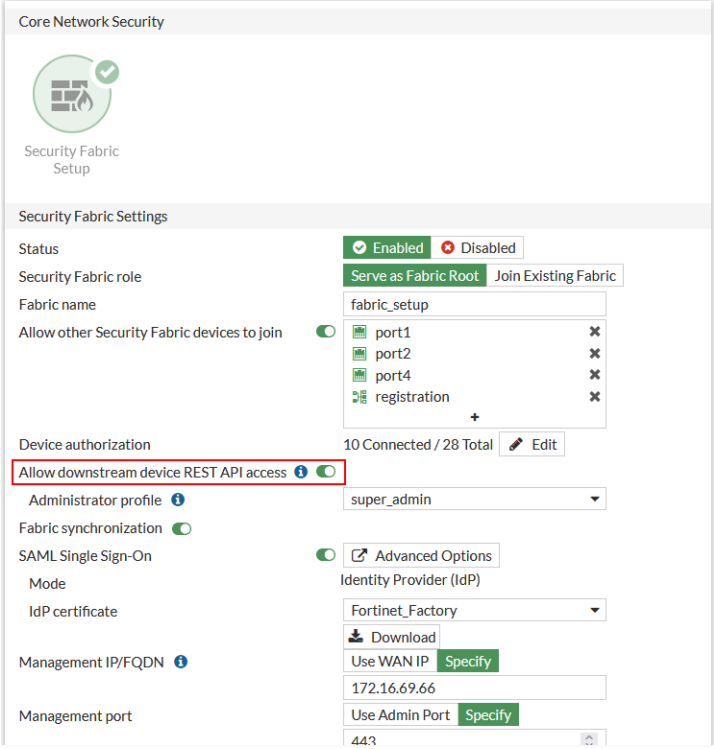


To add the FortiDeceptor fabric connector in FortiGate:

1. In FortiGate, log in as an admin and go to *Security Fabric* > *Fabric Connectors*.
2. Add the FortiDeceptor connector for this integration. For information, see Configuring other Security Fabric devices > FortiDeceptor in the *FortiGate Administration Guide*.



When configuring the Fabric Connector in FortiGate, you must enable *Allow downstream device REST API*.



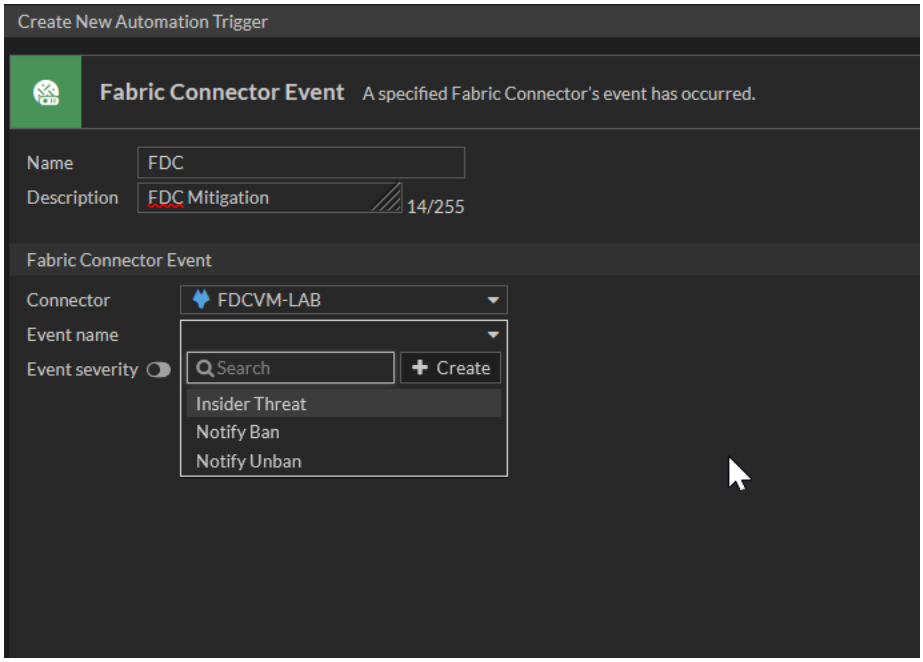
FortiDeceptor supports the CSF protocol that triggers automatic mitigation-isolation of the infected endpoint from the network and prevents the attack from moving laterally.

The CSF integration provides access to more fabric devices for isolation like FortiSwitch through the FortiGate.

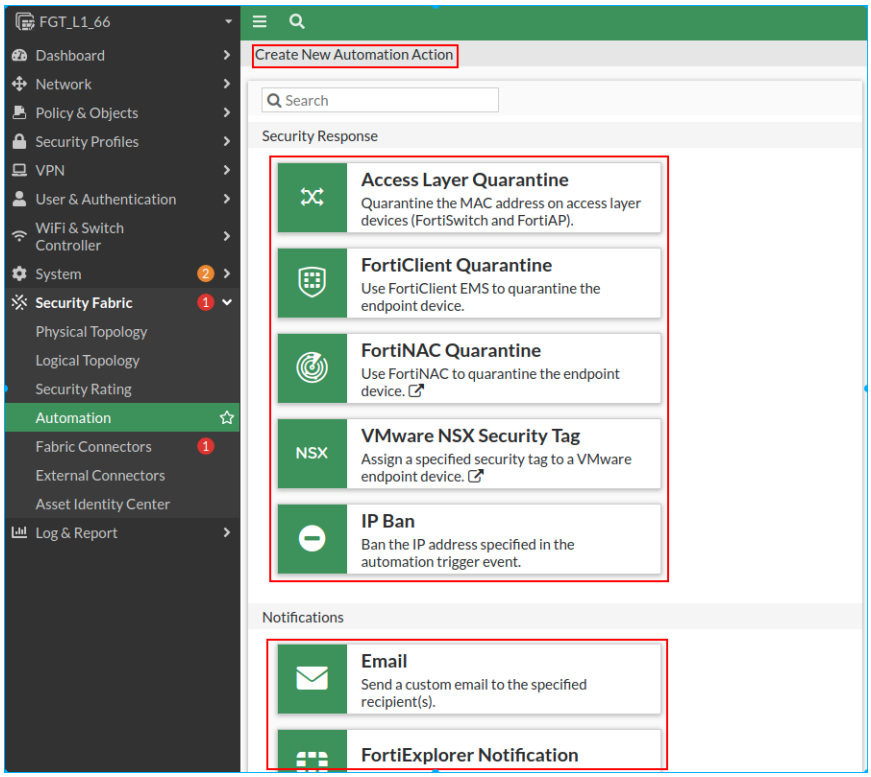
SAML support between FortiGate WEB-UI to FortiDeceptor to allows SSO login from FortiGate to FortiDeceptor.

Cooperative Security Fabric (CSF), also known as a Fortinet Security Fabric, spans across an entire network linking different security sensors and tools together to collect, coordinate, and respond to malicious behavior in real time. CSF can be used to coordinate the behavior of different Fortinet products in your network, including FortiGate, FortiAnalyzer, FortiClient, FortiSandbox, FortiAP, FortiSwitch, and FortiClient Enterprise Management Server (EMS).

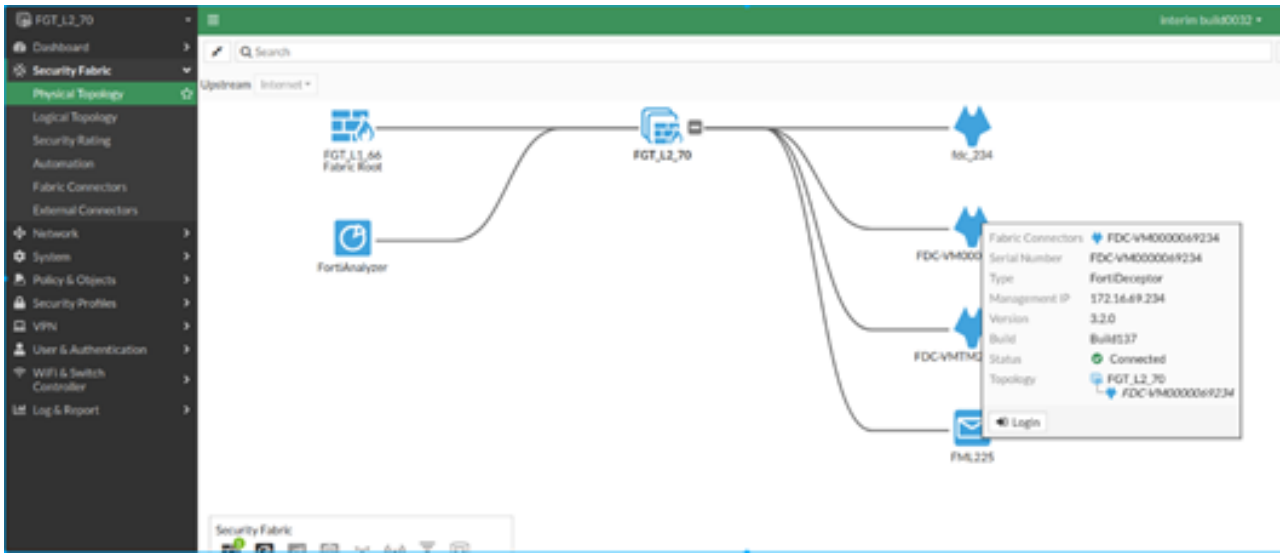
3. To trigger automatic mitigation using the CSF:
   a. In FortiGate, log in as an admin and go to *Security Fabric* > *Automation*.
   b. Click *Trigger* > *Create New*.
   c. Configure the *Fabric Connector Event*:
      i. Enter the *Name* of the event.
      ii. Enter a *Description* of the event.
      iii. Select a *FDC* appliance from the connector menu.
      iv. Select an event.
      v. Select the *Event Severity*.
      vi. Click *OK*.



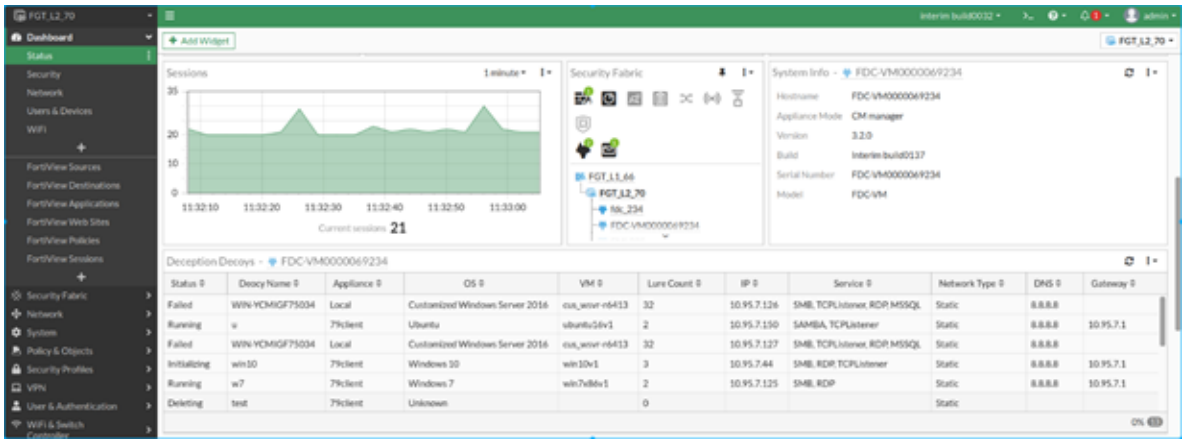
4. In the same screen, go to *Action* > *Create New* and choose any mitigation response you would like to execute once the FortiDeceptor pushes an incident alert to FortiGate.



5. In FortiGate, go to *Security Fabric* > *Physical Topology* to verify that the FortiDeceptor is on the topology map.



6. In FortiGate, go top *Dashboard* > *Status* to view FortiDeceptor information and deception decoys configuration status.



FortiDeceptor integration for threat response mitigation

Use *Fabric* > *Quarantine Integration* to view and configure FortiGate and other device settings for integration with FortiDeceptor. Integration uses REST APIs, XML APIs, or webhooks. When decoys are accessed, FortiDeceptor makes quarantine calls and attackers are immediately quarantined on the device for further analysis.

The following information is displayed:

Action	Click *Edit* to edit the integration settings. Click *Delete* to delete the device.
Enabled	Shows if the device is enabled or disabled.
Status	Device status.
Name	Alias of the integrated device.
Integrate Method	• A/D Connector Isolation • Aruba ClearPass • CheckPoint-FW-Isolation • Cisco-ISE • CrowdStrike-Isolation • FGT-REST-API • FGT-WEBHOOK • FNAC-WEBHOOK • FortEDR-Isolation • FSM-Watch-List • GEN-WEBHOOK • IR Collector (see, Integrate Windows IR collector on page 318) • Microsoft-ATP • PAN-XMLAPI • SentinelOne Isolation • Windows Network Isolation

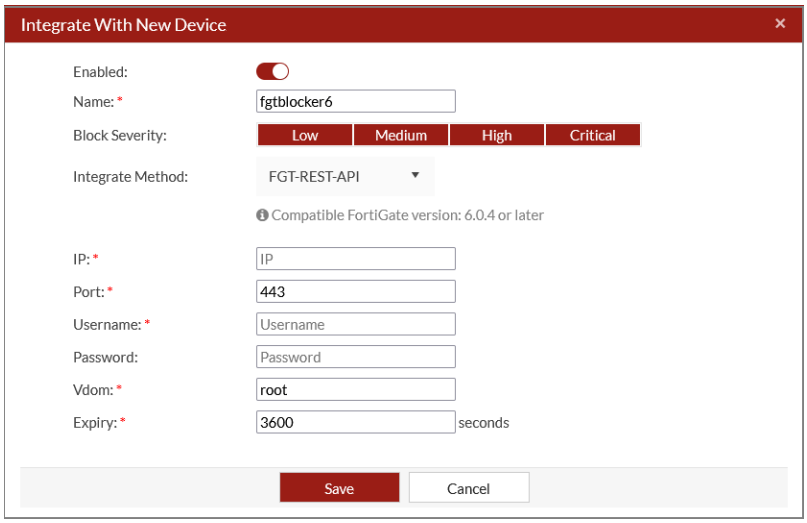
Severity	Security level. The selected level and all levels above it are blocked. For example, if you select *Medium*, then when any attack reaches medium, high, or critical levels, the attacker IP address is blocked. If you select *Critical*, then only the critical level is blocked.
Detail	Device integration details.

To integrate a device:

1. Go to *Fabric* > *Integration Devices*.
2. Click *Quarantine Integration With New Device*.

3. Configure the device for integration. Then click *Save*.

Enabled	Enable or disable this device.
Name	Specify a name for this device.
Block Severity	The selected level and all levels above it are blocked. For example, if you select *Medium*, then when any attack reaches medium, high, or critical levels, the attacker IP address is blocked. If you select *Critical*, then only the critical level is blocked.
Appliance	Option for Central Management manager device to integrate the incidents from the specified appliances only.
Integrate Method	The integration method of this device: • FGT-REST-API (Default) • FGT-WEBHOOK • PAN-XMLAPI • GEN-WEBHOOK • FNAC-WEBHOOK • Windows Network Isolation • FortEDR-Isolation • Cisco-ISE • Microsoft-ATP • CrowdStrike-Isolation • FSM-Watch-List Different integration methods have different settings. To view the settings for each integration type, see Integrate Method settings on page 112
IP or Device IP	IP address of the integrated device.
Port	Port number of the integrated device API service. Default is 8443.
Username and Password	Username and password of the integrated device.
VDOM	For FortiGate devices, the default access VDOM.
Verify SSL	Enable to verify SSL.
Expiry	Default blocking time in second. Default is 3600 seconds.



Integrate Method settings

A/D Connector Isolation

Hostname	IP address or Hostname of the Active Directory (AD) server.
Port	Port number used for connecting to the AD server.
Username	Valid AD service account with a minimum of *account operators* access.
Password	Password for your AD user.

Base DN	The base, or node from where the search should start.
	All connector operations are carried out using the Base DN as a root to the AD organization tree. You can restrict the AD lookup by providing appropriate filters in this parameter.
	Some examples are as follows:
	`DC=fdc,DC=com`
	`OU=workstation,DC=fdc,DC=com`
	`OU=Finance,OU=workstation,DC=fdc,DC=com`

Bind DN	The fully distinguished name, which is used to bind to the AD server.
Use TLS	Specifies whether SSL and TLS. SSL is used by default.
Limit	The number of quarantine attackers per 24 hours.

Aruba ClearPass

Server URL	The Aruba ClearPass URL or IP address.
Client ID	Client ID of the Aruba ClearPass application which is used to access Aruba ClearPass.

Auth Type	Select *Username/Password* or *Client Secret*.
Username	If the *Auth Type* is *Username/Password*, enter the Aruba ClearPass username.
Password	If the *Auth Type* is *Username/Password*, enter the Aruba ClearPass password.
Client Secret	If the *Auth Type* is *Client Secret*, enter the Aruba ClearPass client secret.
Verify SSL	Enable to verify Secure Sockets Layer.
Expiry	Default blocking time in seconds. Default is 3600 seconds

AWS Keys

AWS Region	AWS region to access the AWS CloudTrail.
AWS Access Key ID	ID of the AWS Access Key to access AWS services.
AWS Secret Access Key	Key of the AWS Secret Access to access AWS services.
Verify SSL	Specifies whether the SSL certificate for the server is to be verified or not. By default, this option is set as *True*.

Azure Keys

Client ID	Also called *Application ID;Unique ID* of the Azure Active Directory application.
Client Secret	Client Secret of the Azure Active Directory application that is used to create an authentication token required to access the API.
Tenant ID	Tenant ID provided for your Azure Active Directory.
Verify SSL	Specifies whether the SSL certificate for the server is to be verified or not. By default, this option is set as *True*.

CheckPoint-FW-Isolation

Compatible CheckPoint version: R81 build392 or later

IP/URL	IP address or URL of the integrated device.
Port	Port number of the integrated device API service. Default is 443.
IP Block Policy(Network Group Name)	Enter the Network Group Name.
Username	Username of the integrated device.
Password	Password of the integrated device.
Verify SSL	Enable to verify Secure Sockets Layer.
Install Policy After Publish	Enable to install the policy after it is published.

Cisco-ISE

Compatible Cisco ISE version: 2.7 or later.

Server URL/IP	The Cisco server URL and IP address.
Port	Port number of the integrated device API service. Default is 8443.
Username	Username of the integrated device.
Password	Password of the integrated device.
Verify SSL	Enable to verify SSL.
Expiry	Default blocking time in seconds. Default is 3600 seconds.

CrowdStrike-Isolation

Server URL	CrowdStrike server URL.
Client ID	Client ID of the Crowdstrike application which is used to access CrowdStrike isolation service.
Client Secret	Secret string of the Crowdstrike application which is used to access CrowdStrike isolation service.
Verify SSL	Enable to verify SSL.
Expiry	Default blocking time in seconds. Default is 3600 seconds.

FGT-REST-API

Compatible FortiGate version: 6.0.4 or later

IP	IP address of the integrated device.
Port	Port number of the integrated device API service. Default is 8443.
Username	Username of the integrated device.
Password	Password of the integrated device.
VDOM	For FortiGate devices, the default access VDOM.
Expiry	Default blocking time in second. Default is 3600 seconds.

FGT-WEBHOOK

Compatible FortiGate version: 6.4.0 or later

Block Action	**Expiry**	Default blocking time in seconds. Default is 3600 seconds.
	URL	Enter the request API URI.
	Authorization	Enter the API key.

Unblock Action	**Expiry**	Default blocking time in seconds. Default is 3600 seconds.
	URL	Enter the request API URI.
	Authorization	Enter the API key.

FNAC-WEBHOOK

Compatible FortiNAC version: 8.8.2.1714 or later.

IP:	IP address of the integrated device.
Port:	Port number of the integrated device API service. Default is 8443.
Authorization Token:	The FortiNAC-WEBHOOK authorization token generated by FNAC.
Expiry:	Default blocking time in seconds. Default is 3600 seconds.

FortiEDR-Isolation

Compatible FortiEDR version: 5.0.2.305 or later.

IP	IP address of the integrated device.
Port	Port number of the integrated device API service. Default is 8443.
Organization\Username	The FortiEDR organization and username.
Password	Password of the integrated device.
Expiry	Default blocking time in seconds. Default is 3600 seconds.

FSM-Watch-List

IP	IP address of the integrated device.
Port	Port number of the integrated device API service. Default is 8443.
Username:	Username of the integrated device.
Password:	Password of the integrated device.
Organization	Type the organization name for the integration device.
Verify SSL	Enable to verify SSL.
Watch-List Name	Type Watch-List Name as defined in FortiSIEM.
Lure Users-Manual Mode	Type the other lures you want to watch.
Polling Time Interval	Default polling time in seconds. Default is 3600 seconds.

GEN-WEBHOOK

Compatible FortiNAC version: 8.8 or later (Firmware: 8.8.2.1714)

Block Action:	**Expiry**	Default blocking time in seconds. Default is 3600 seconds.
	Http Method	Select GET, POST, PUT, or PATCH
	URL	Enter the request API URI.
	Authorization	Enter the API key.
	HTTP Header	Select Empty, Hacker-IP, Hacker-MAC, or Expiry-Time.
	HTTP Data	Select Empty, Hacker-IP, Hacker-MAC, or Expiry-Time.
Unblock Action:	**Http Method**	Select GET, POST, PUT, or PATCH
	URL	Enter the request API URI.
	Authorization	Enter the API key.
	HTTP Header	Select Empty, Hacker-IP, Hacker-MAC, or Expiry-Time.
	HTTP Data	Select Empty, Hacker-IP, Hacker-MAC, or Expiry-Time.

IR Collector

Domain	The device domain.
Username	Username of the integrated device.
Password	Password of the integrated device.
Limit	The number of collections per endpoint per 24 hour.

Microsoft-ATP

Server URL	Service base URI to connect and perform the automated operations. For example, https://api.securitycenter.microsoft.com.
Client ID	Client ID of the Azure application that is used to access Windows Defender ATP
Client Secret	Secret string that the application (used to access Windows Defender ATP) uses to prove its identity
Tenant ID	Tenant ID of the Azure application
Verify SSL	Enable to verify SSL.
Expiry	Default blocking time in seconds. Default is 3600 seconds.

PAN-XMLAPI

Compatible PAN-device version: 10.0.0 or later

Device IP	IP address of the integrated device.
Port	Port number of the integrated device API service. Default is 8443.
Username	Username of the integrated device.
Password	Password of the integrated device.
Vsys	The virtual system which is configured on PAN
Policy Index	Select *Top* or *Bottom*.
Expiry	Default blocking time in seconds. Default is 3600 seconds.

SentinelOne Isolation

Server URL	SentinelOne server URL.
API Token	The SentinelOne authorization token.
API Version	The version of the SentinelOne token.
Verify SSL	Enable to verify SSL.
Expiry	Default blocking time in seconds. Default is 3600 seconds.

Windows Network Isolation

Domain	The device domain.
Username	Username of the integrated device.
Password	Password of the integrated device.

Quarantine Status

The *Fabric* > *Quarantine Status* page displays the status of blocked and quarantined IP addresses. It also lets you manually block or unblock devices. The following options are available:

Refresh	Refresh the page to get the latest data.
Block	Manually send a blocking request for the selected attacker IP addresses.
Unblock	Manually send an unblocking request for the selected attack IP addresses.

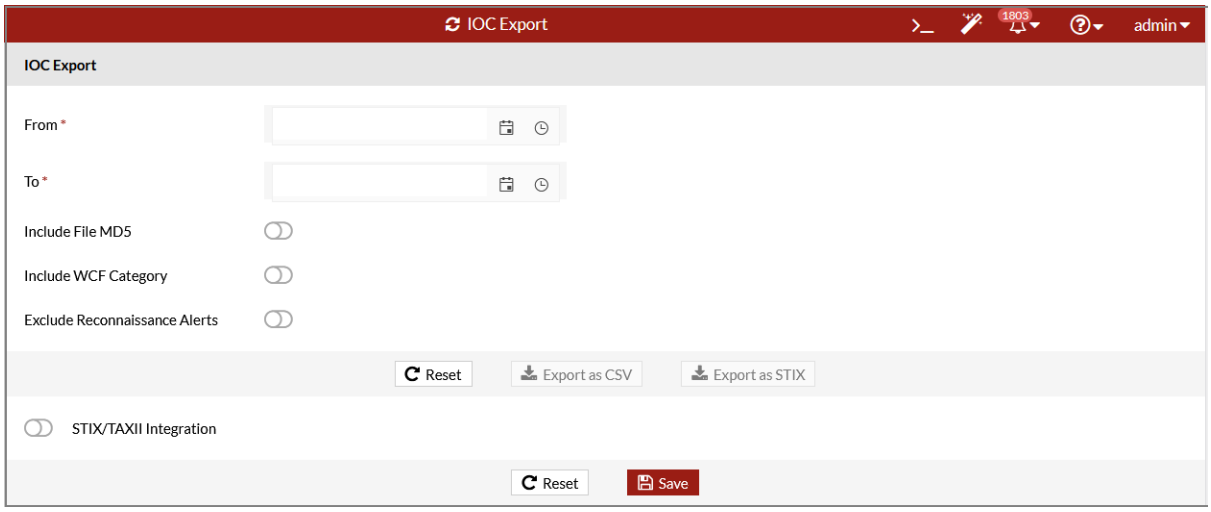
The following information is displayed:

Attacker IP	IP addresses of blocked attacker.
Start	Start time of blocking behavior.
End	End time of blocking behavior.

Type	Blocking type, manual, or automatic quarantine.
Integrated Device	Alias of the device which blocks the *Attacker IP* address. This is the *Name* field in *Fabric > Integration Devices*.
Time Remaining	The remaining blocking time.
Status	Current status of the attacker.
Message	Additional message for the quarantine operation.

IOC Export

The *IOC Export* page allows you to export the IOC file in CSV or STIX format for a specified time period. The CSV file can be processed by third party Threat Intelligence Platforms. The file contains the TimeStamp, Incident ID, Attacker IP, related files, and WCF (Web Content Filtering) events. You can include MD5 checksums, WCF category, and reconnaissance alerts.



To export the IOC as a CSV file:

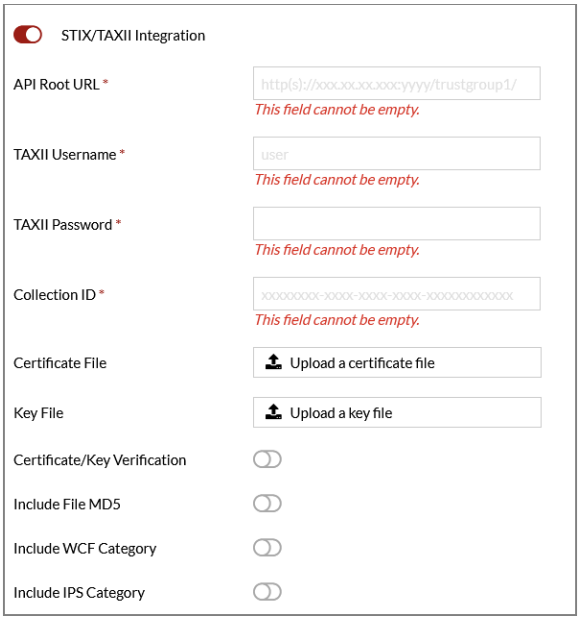
1. Go to *Fabric > IOC Export*.
2. Specify the date range by setting the date and time in the *From* and *To* fields.
3. (Optional) Include or exclude the following files and alerts:
   - *Include File MD5*
   - *Include WCF Category*
   - *Exclude Reconnaissance Alerts*
4. Click *Export as CSV*

To Push the IOC over STIX/TAXII server

1. Go to *Fabric > IOC Export*.
2. Specify the date range by setting the date and time in the *From* and *To* fields.

3. Enable *STIX/TAXII Integration*.
4. Configure the export settings:

API Root URL	Enter the API Root URL.
TAXII Username	Enter the TAXII username.
TAXII Password	Enter the TAXII password.
Collection ID	Enter the Collection ID.
Certificate File	Click Upload a certificate file to upload the certificate file.
Key File	Click to upload the API key file.
Certificate/Key Verification	Enable Certificate/Key Verification.
Include File MD5	Enable to include the MD5 file.
Include WCF Category	Enable to include the WCF category.
Include IPS Category	Enable to include the IPS category.



5. Click *Export as STIX* to push the export over the protocol in real time.

Network

The *Network* page provides interface, DNS, and routing management options.

This section includes the following topics:

- Interfaces
- System DNS
- System Routing

Interfaces

To view and manage interfaces, go to *Network* > *Interfaces*. All of the columns in the table are searchable and support custom filters.

This page displays the following information and options:

Interface	The interface name and description. Failover IP is listed under this field with the descriptor: *(cluster external port)*.
port1 (administration port)	Port1 is hard-coded as the administration interface. You can enable or disable HTTP, SSH, and Telnet access rights on port1. HTTPS is enabled by default and cannot be disabled. You can use port1 for Device mode although a different, dedicated port is recommended.
port2	Decoy VM deployment.
port3	Decoy VM deployment.
port4	Decoy VM deployment.
port5/port6	Decoy VM deployment.
port7/port8	Decoy VM deployment.
IPv4	The IPv4 IP address and subnet mask of the interface.
IPv6	The IPv6 IP address and subnet mask of the interface.
Interface Status	The state of the interface: • Interface up • Interface down • Interface is being used by sniffer
Link Status	The link status: • Link up • Link down
Access Rights	The access rights associated with the interface. HTTPS is enabled by default on port1. You can enable HTTP, SSH, and Telnet access on port1.

Edit	Select the interface and click *Edit* in the toolbar to edit the interface.

To filter the columns in the table:

1. Click the plus sign in the Search field. The *Filterable Columns* menu opens.

2. Select a column in the list to *Resize to Contents*, *Group By This column* or create a custom filter.
3. Click *Apply*.

To show or hide columns in the table:

1. Hover the header row until the *Configure Table* icon appears.

2. Click *Configure Table*. The *Best Fit Columns* menu opens.
3. Select the columns to appear in the table and click *Apply*.
4. To restore the default table, click *Reset Table*.

To edit an interface:

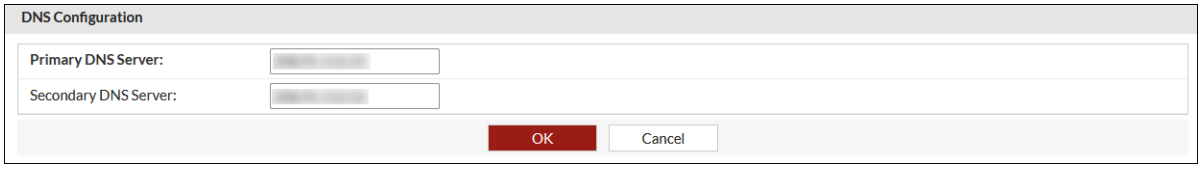
1. Select the *IPv4* or *IPv6* address of an interface name and click *Edit* in the toolbar.
2. Edit the *IP Address / Netmask*. The Confirmation dialog opens.
3. (Optional) Change the *Interface Status*.
4. In the *IP Address / Netmask* pane, update the IPv4 and IPv6 address.
5. Click *OK*.

To edit administrative access:

1. Select *port1 (administration port)* and click *Edit* in the toolbar.
2. Edit the *Access Rights*.
   HTTPS is enabled by default. You can also enable HTTP, SSH, and Telnet support.
3. If necessary, edit the *IP Address / Netmask*.
4. Click *OK*.

System DNS

You can configure the primary and secondary DNS server addresses in *Network* > *System DNS*.



To configure the System DNS:

1. Go to Network > System DNS.
2. In the *Primary DNS Server* and *Secondary DNS Server* fields, enter the address of the primary and secondary servers.

System Routing

Use the *Network* > *System Routing* page to manage static routes of your FortiDeceptor device. All of the columns in the table are searchable and support custom filters.

The following options are available:

Create New	Create a new static route.
Edit	Edit the selected static route.
Delete	Delete the selected static route.

The following information is displayed:

IP/Mask	IP address and subnet mask.
Gateway	Gateway IP address.
Device	The interface associated with the static route.

To create a new static route:

1. Click *Create New*.
2. Enter the *Destination IP* address, *Mask*, and *Gateway*.

   You can enter the *Destination IP/Mask* in the format `192.168.1.2/255.255.255.0`, `192.168.1.2/24`, or `fe80:0:0:0:0:0:c0a8:1fe`.

3. Select a *Device* (or interface).
4. Click *OK*.

To edit a static route:

1. Select a Static Route
2. Click *Edit*.
3. Edit the destination IP address and mask, gateway, and device (or interface) as required.
4. Click *OK* to apply the edits to the static route.

To delete a static route or routes:

1. Select one or more Static Routes.
2. Click *Delete*.
3. Confirm the deletion.

To filter the columns in the table:

1. Click the plus sign in the Search field. The *Filterable Columns* menu opens.

2. Select a column in the list to *Resize to Contents*, *Group By This column* or create a custom filter.
3. Click *Apply*.

To show or hide columns in the table:

1. Hover the header row until the *Configure Table* icon appears.

2. Click *Configure Table*. The *Best Fit Columns* menu opens.
3. Select the columns to appear in the table and click *Apply*.
4. To restore the default table, click *Reset Table*.

System

Use the *System* pages to manage and configure the basic system options for FortiDeceptor. This includes administrator configuration, mail server settings, and maintenance information.

This section includes the following topics:

Administrators	Configure administrator user accounts.
Admin Profile	Configure admin profiles to define admin privileges.
Certificates	Configure CA certificates.
LDAP Servers	Configure LDAP servers.
RADIUS Servers	Configure RADIUS servers.
Mail Server	Configure the mail server.
SNMP	Configure SNMP.
FortiGuard	Configure FortiGuard settings and upgradeable packages.
FDC License	Upload license files and input confirmation ID.
Settings	Configure the idle timeout or reset all widgets to their default state.
Login Disclaimer	Configure the Login Disclaimer.
Table Customization	Define columns and order of *Incident* and *Event* tables.

Administrators

Use the *System* > *Administrators* page to configure administrator user accounts.

If the admin user's Admin Profile does not have *Read Write* privilege under *System* > *Admin Profiles*, the user can only view and edit their own information.

The following options are available:

Create New	Create a new administrator account.
Edit	Edit the selected entry.
Delete	Delete the selected entry.
Test Login	Test the selected user's login settings. If an error occurs, a debug message appears.

The following information is displayed:

Name	The administrator account name.

Type	The administrator type: • **Local**: User information is stored in the FortiDeceptor local database and authenticated locally by FortiDeceptor. • **LDAP**: User information is stored in the remote LDAP server. A copy of the username is stored in the FortiDeceptor local database (without password and other information), and is authenticated remotely by the LDAP server. See, LDAP Servers on page 131. • **RADIUS**: User information is stored in the remote RADIUS server. A copy of the username is stored in the FortiDeceptor local database (without password and other information), and is authenticated remotely by the RADIUS server. See, RADIUS Servers on page 132. **NOTE**: For Single Sign-On (SSO), user information is stored in a remote Identity Provider (IdP) server. No user information is stored locally. Instead, FortiDeceptor acts as a Service Provider (SP). When a login request is received, FortiDeceptor redirects the request via SAML protocol to the IdP to complete the authentication. See Single Sign-On on page 133.
Profile	The Admin Profile the user belongs to.

To create a new user:

1. Log in using an account with *Read/Write* access and go to *System* > *Administrators*.
2. Click *Create New*.

3. Configure the following:

Administrator	Name of the administrator account. The name must be 1 to 30 characters using upper-case letters, lower-case letters, numbers, or the underscore character (_) for *Local* and LDAP administrators. The character limit for RADIUS server administrators is 64 characters.
Password, Confirm Password	Password of the account. The password must be 6 to 64 characters using upper-case letters, lower-case letters, numbers, or special characters. This field is available when *Type* is set to *Local*.
Type	Select *Regular Admin*, *Local*, *LDAP*, or *RADIUS*.
LDAP Server	When *Type* is *LDAP*, select an *LDAP Server*. For more information, see LDAP Servers on page 131.
RADIUS Server	When *Type* is *RADIUS*, select a *RADIUS Server*. For more information, see RADIUS Servers.
Regular Admin	When *Type* is *Regular Admin*, the user will have almost all the same privileges of a *Super admin*, but cannot see or can change the Super Admin user profile. Only Super Admin and Regular Admin accounts can choose the Regular Admin type to create a new Regular Admin. When a Regular Admin logs in, they will not see the Super User account. Regular Admins can see and edit all other users. Regular Admins have access to the same Menu items and CLI Commands settings as a Super Admin.
Push notification to mobile if applicable	Enable FortiToken push notifications for mobile devices. This option is available when *Type* is *RADIUS*.
Admin Profile	Select the Admin Profile.
Trusted Host 1, Trusted Host 2, Trusted Host 3	Enter up to three IPv4 trusted hosts. Only users from trusted hosts can access FortiDeceptor.
Trusted IPv6 Host 1, Trusted IPv6 Host 2, Trusted IPv6 Host 3	Enter up to three IPv6 trusted hosts. Only users from trusted hosts can access FortiDeceptor.
Comments	Enter an optional comment.

Setting trusted hosts for administrators limits the computers an administrator can use to log into FortiDeceptor. When you identify a trusted host, FortiDeceptor only accepts the administrator's login from the configured IP address or subnet. Attempts to log in with the same credentials from another IP address or subnet are dropped.

4. Click *OK*.

To edit a user account:

1. Log in using an account with *Read/Write* access and go to *System* > *Administrators*.
2. Select and account and click *Edit*.
   Only the *admin* user can edit its own settings.
   You must enter the old password before you can set a new password.

3. Edit the account and click *OK*.

To delete one or more user accounts:

1. Log in using an account with *Read/Write* access and go to *System* > *Administrators*.
2. Select the user account you want to delete.
3. Click *Delete* and confirm that you want to delete the user.

To test LDAP or RADIUS logins:

1. Log in using an account with *Read/Write* access and go to *System* > *Administrators*.
2. Select an LDAP or RADIUS user to test.
3. Click *Test Login*.
4. Enter the user password.
5. Click *OK*.
   If an error occurs, a debug message appears.

When a remote RADIUS server is configured for two-factor authentication, RADIUS users must enter a FortiToken code or the code from email/SMS to complete login or to test login.

Admin Profiles

Use administrator profiles to control administrator access privileges to system features. When you create an administrator account, you assign a profile to the account.

You cannot modify or delete the following predefined administrator profiles:

- *Read Write* has access to all functionality. This includes creating, editing, and deleting administrator profiles
- *Read only* has read-only access.

The *Menu Access* section has the following settings:

None	User cannot view or make changes to that page.
Read Only	User can view but not make any change to that page, except session-related user settings such as Table Customization, Dashboard, or Attack Map filter.
Read Write	User can view and make changes to that page.
Super Admin	User cannot view or make changes to that page.
Regular Admin	User cannot view or make changes to that page.

The *CLI Commands* section has the following settings:

None	User cannot execute CLI commands.
Execute	User can execute CLI commands.

To create an Administrator Profile:

1. Go to *System* > *Admin Profiles*.
2. Select the *Profile Name*.
3. Click *Create New*.
4. Specify the *Profile Name*.
5. If you wish, add a *Comment*.
6. Specify the privileges for *Menu Access*:

Dashboard	Dashboard
Central Management	Appliances
Deception	• Custom Decoy Image • Deception OS • Deployment Network • Deployment Wizard • Decoy Status • Deployment Map • Asset Discovery • Safe List • Lure Resources • Deception Token
Incident	• Analysis • Campaign • Attack Map
Fabric	• Integration Devices • Quarantine Status • IOC Export • Detection Devices
Network	• Interfaces • System DNS • System Routing
System	• Administrators • Admin Profiles • Certificates • LDAP Servers • RADIUS Servers • Mail Server • SNMP • Login Disclaimer • FortiGuard • FDC License • System Settings • Table Customization

Log	• All Events • Log Servers
REST API	• Decoy • Attack

7. Specify the privileges for *CLI Commands*:

Configuration	• Set • Unset
System	• Reboot • Shutdown • Reset Configuration • Factory Reset • Firmware Upgrade • Reset Widgets • IP Tables • test-network • usg-license • Set Confirm ID for Windows VM • List VM License • Show VM Status • VM reset • DC Image Status • Set Maintainer • Set Timeout for Remote Auth • Data Purge • Log Purge • DMZ Mode • FDN Package Information • Fabric Binding • Central Management Settings
Utilities	• TCP Dump • Trace Route
Diagnostics	• Diagnose

8. Click *Save*.

Certificates

Use this page to import, view, and delete certificates. Certificates are used for secure connection to an LDAP server, system HTTPS, and SSH services. FortiDeceptor has one default certificate named *firmware*.

FortiDeceptor does not support generating certificates. FortiDeceptor supports importing certificates for SSH and HTTPS access using `.crt`, `PKCS12`, or `.pem` format.

The following options are available:

Import	Import a certificate.
Service	Configure specific certificates for HTTP and SSH servers.
View	View the selected CA certificate details.
Delete	Delete the selected certificate.

The following information is displayed:

Name	Name of the certificate.
Subject	Subject of the certificate.
Status	The certificate status, active or expired.
Service	HTTPS or SSH service that is using this certificate.

To import a certificate:

1. Go to *System* > *Certificates*.
2. Click *Import*.
3. Enter the *Certificate Name*.
4. If you want to import a password protected PKCS12 certificate, select *PKCS12 Format*.
5. Click *Choose File* and locate the certificate and key files on your management computer.
6. Click *OK* to import the certificate.

To view a certificate:

1. Go to *System* > *Certificates*.
2. Select a certificate and click *View*.
   The following information is available:

Certificate Name	Name of the certificate.
Status	Certificate status.
Serial number	Certificate serial number.
Issuer	Issuer of the certificate.
Subject	Subject of the certificate.
Effective date	Date and time that the certificate became effective.
Expiration date	Date and time that the certificate expires.

To delete a CA certificate:

1. Go to *System* > *Certificates*.
2. Select the certificate you want to delete.
3. Click *Delete* and confirm you want to delete the certificate.

You cannot delete the *firmware* certificate.

LDAP Servers

FortiDeceptor supports remote authentication of administrators using LDAP servers. To use this feature, configure the server entries in FortiDeceptor for each authentication server in your network.

If you have configured LDAP support and require users to authenticate using an LDAP server, FortiDeceptor contacts the LDAP server for authentication. To authenticate with FortiDeceptor, the user enters a user name and password. FortiDeceptor sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, FortiDeceptor authenticates the user. If the LDAP server cannot authenticate the user, FortiDeceptor refuses the connection.

Due to the security enhancement requirement, FortiDeceptor requires peer servers to use strong cipher algorithm for certificates.

The following options are available:

Create New	Add an LDAP server.
Edit	Edit the selected LDAP server.
Delete	Delete the selected LDAP server.

The following information is displayed:

Name	LDAP server name.
Address	LDAP server address.
Common Name	LDAP common name.
Distinguished Name	LDAP distinguished name.
Bind Type	LDAP bind type.
Connection Type	LDAP connection type.

To create a new LDAP server:

1. Go to *System* > *LDAP Servers*.
2. Click *Create New*.

3. Configure the following settings:

Name	A unique name to identify the LDAP server.
Server Name/IP	IP address or FQDN of the LDAP server.
Port	The port for LDAP traffic. The default port is 389.
Common Name	Common name identifier of the LDAP server. Most LDAP servers use `cn`. Some servers use other common name identifiers such as `uid`.
Distinguished Name	Distinguished name used to look up entries on LDAP servers. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier.
Bind Type	The type of binding for LDAP authentication: • *Simple* • *Anonymous* • *Regular*
Username	When the *Bind Type* is set to *Regular*, enter the user name.
Password	When the *Bind Type* is set to *Regular*, enter the password.
Enable Secure Connection	Use a secure LDAP server connection for authentication.
Protocol	When *Enable Secure Connection* is selected, select *LDAPS* or *STARTTLS*.
CA Certificate	When *Enable Secure Connection* is selected, select a *CA Certificate*.

4. Click *OK*.

RADIUS Servers

FortiDeceptor supports remote authentication of administrators using RADIUS servers. To use this feature, configure the server entries in FortiDeceptor for each authentication server in your network.

If you have configured RADIUS support and require users to authenticate using a RADIUS server, FortiDeceptor contacts the RADIUS server for authentication. To authenticate with FortiDeceptor, the user enters a user name and password. FortiDeceptor sends this user name and password to the RADIUS server. If the RADIUS server can authenticate the user, FortiDeceptor authenticates the user. If the RADIUS server cannot authenticate the user, FortiDeceptor refuses the connection.

The following options are available:

Create New	Add a RADIUS server.
Edit	Edit the selected RADIUS server.
Delete	Delete the selected RADIUS server.

The following information is displayed:

Name	RADIUS server name.
Primary Address	Primary server IP address.
Secondary Address	Secondary server IP address.
Port	Port used for RADIUS traffic. The default port is 1812.
Type	Select either *FortiAuthenticator* or *Other* from the dropdown.
Auth Type	The authentication type the RADIUS server requires. Select *Any*, *PAP*, *CHAP*, or *MSv2*. *Any* means FortiDeceptor tries all authentication types.
Primary Secret	Primary RADIUS server secret.
Secondary Secret	Secondary RADIUS server secret.
NAS IP	NAS IP address.

To add a RADIUS server:

1. Go to *System* > *RADIUS Servers*.
2. Click *Create New*.
3. Configure the following settings:

Name	A unique name to identify the RADIUS server.
Primary Server Name/IP	IP address or FQDN of the primary RADIUS server.
Secondary Server Name/IP	IP address or FQDN of the secondary RADIUS server.
Port	Port for RADIUS traffic. The default port is 1812.
Auth Type	Authentication type the RADIUS server requires. Select *Any*, *PAP*, *CHAP*, or *MSv2*. *Any* means FortiDeceptor tries all authentication types.
Primary Secret	Primary RADIUS server secret.
Secondary Secret	Secondary RADIUS server secret.
NAS IP	NAS IP address.

4. Click *OK*.

Single Sign-On

Go to *System* > *Single sign-on* to allow administrators to log into FortiDeceptor with a single ID. User information is stored in a remote Identity Provider (IdP) server. No user information is stored locally. Instead, FortiDeceptor acts as a

Service Provider (SP). When a login request is received, FortiDeceptor redirects the request via SAML protocol to the IdP to complete the authentication.

To enable Single Sign-On:

1. Go to *System* > *Single sign-on* and click *Enable* . The Single Sign-On settings are displayed.
2. Configure the Single Sign-On settings and click *Apply*.

Service Provider Configuration	
Address	The address the identify provider will send SAML authentication requests to.
Entity ID	Click the *Copy* icon to copy the Entity ID.
Assertion consumer service URL	Click the *Copy* icon to copy the URL.
Single logout service URL	Click the *Copy* icon to copy the URL.
Enable Certificate	Service provider will use this certificate to sign or encrypt the request. When this option is disabled , the request will not be signed or encrypted.
Certificate	Allow the service provider to sign or encrypt the request. Select the certificate to use from the list. You can also download the public key of the certificate and upload it to the identity provider to verify and decrypt the request.
Identity Provider Configuration	
Entity ID	Enter the entity ID of identity provider
Single sign-on service URL	Enter the identity provider's sign on URL.
Single logout service URL	Enter the identity provider's logout URL.
Certificate	Upload the public X.509 certificate of the identity provider .
Additional SAML Attributes	
Attribute used to identify users	The identity provider will use this attribute in the request to report the sign-on user name.

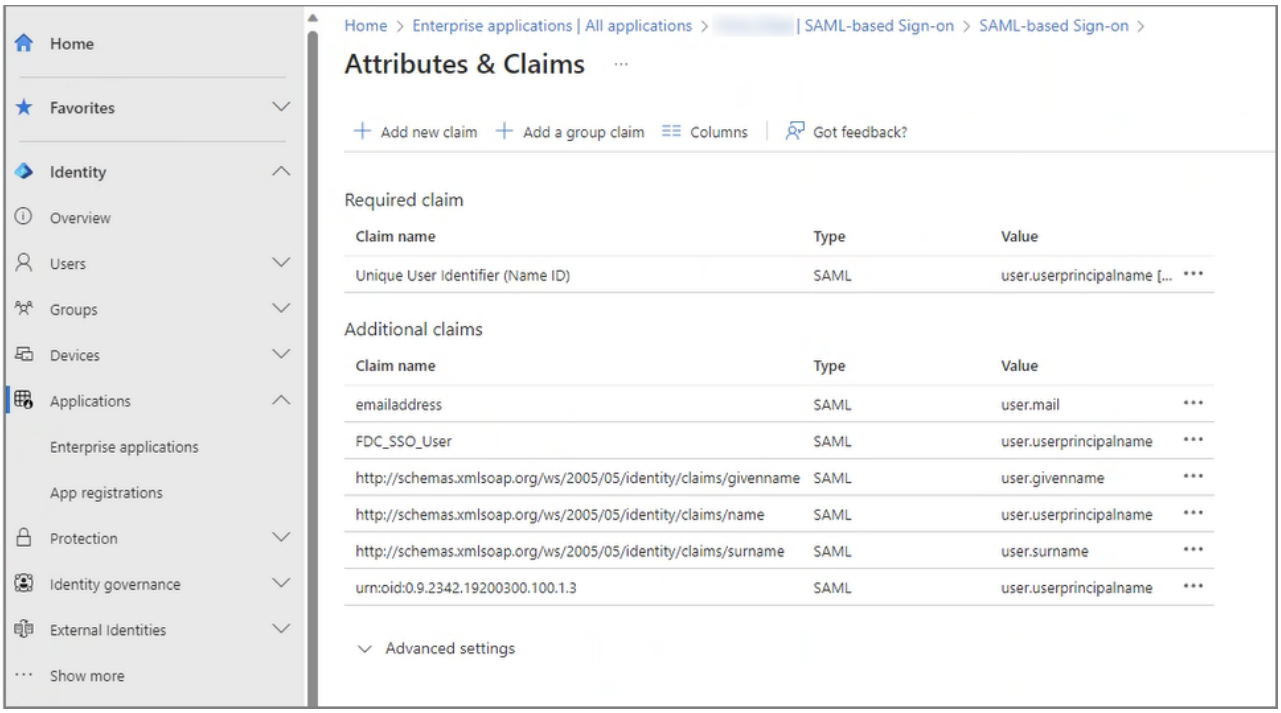
Configuring SSO with Azure

Configuring SSO with Azure requires a *Claim Attribute*. This section provides an overview on how to configure a new Claim Attribute in Azure and where to enter it in FortiDeceptor. For more information about Claim Attributes, see the Azure product help.

As SSO is a standard method, setting Claim Attribute on the IDP side can be applied to any IDP servers.

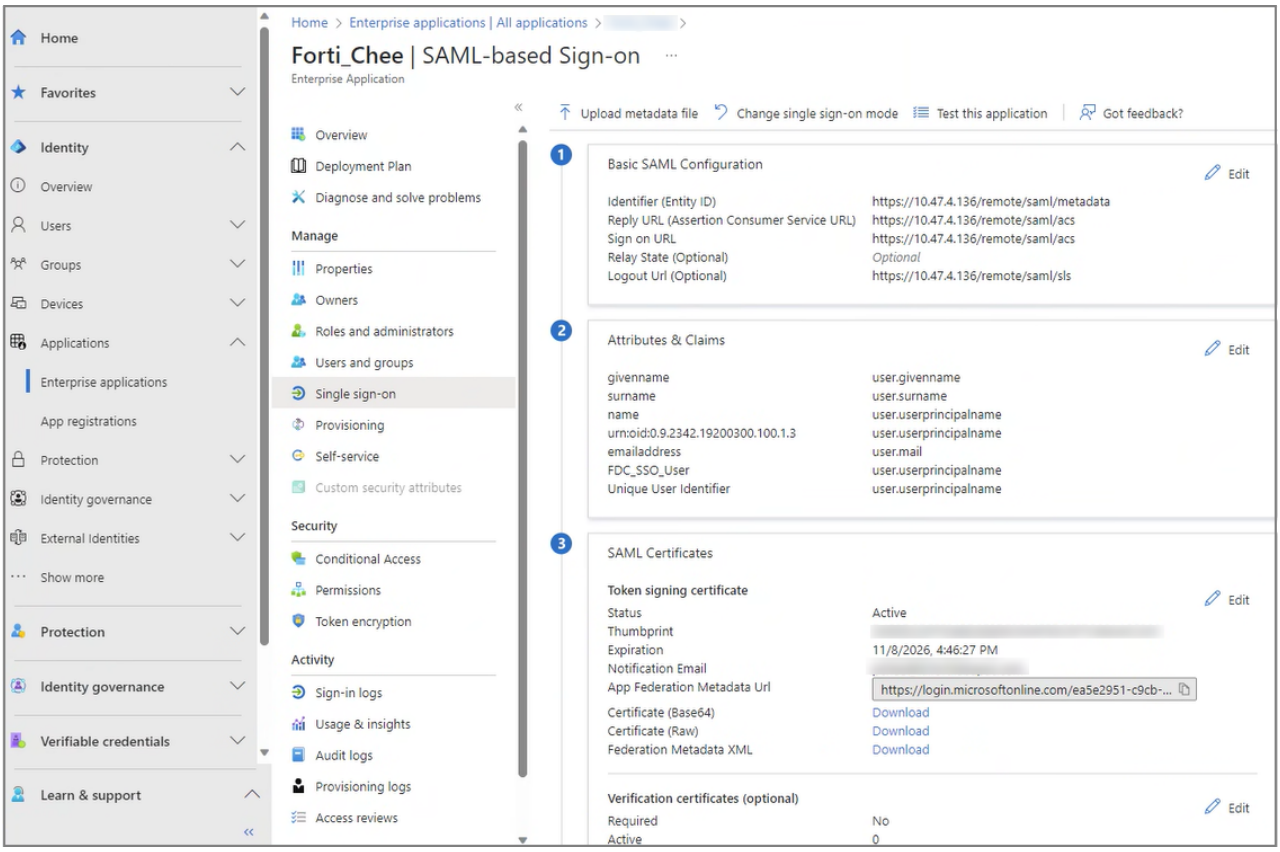
To configure SSO for Azure:

1. In Azure, go to *Identity* > *Applications* > *Enterprise applications* > *All applications*.
2. Select the application, select *Single sign-on* in the left-hand menu, and then select *Edit* in the *Attributes & Claims* section.

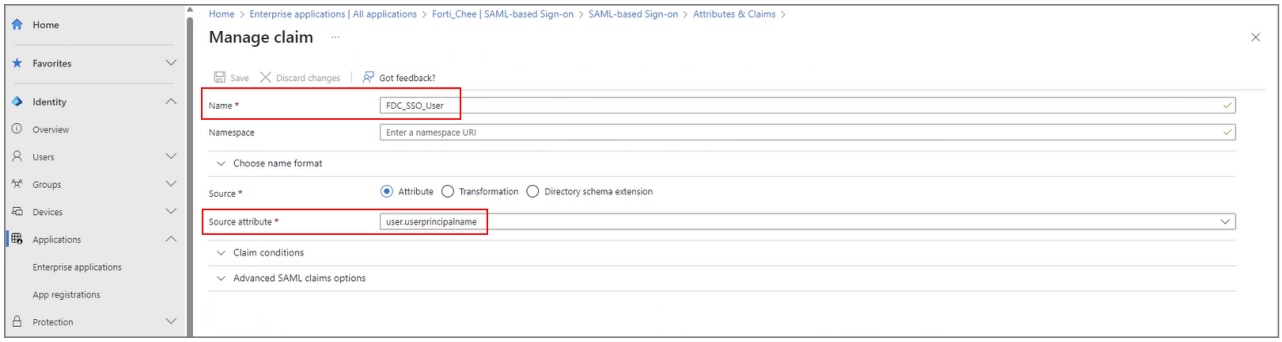


3. Go to *Manage Claim*.

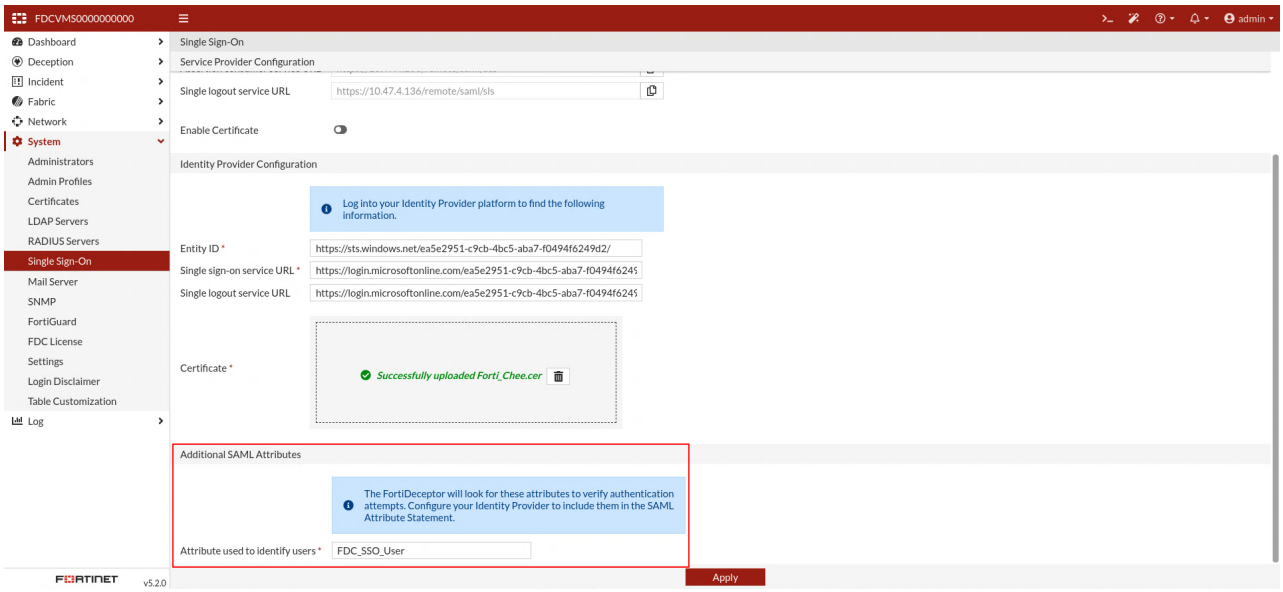
4. Go to *Manage* > *Single-Sign On*.



5. Specify the attribute *Name* and the *Source Attribute*.

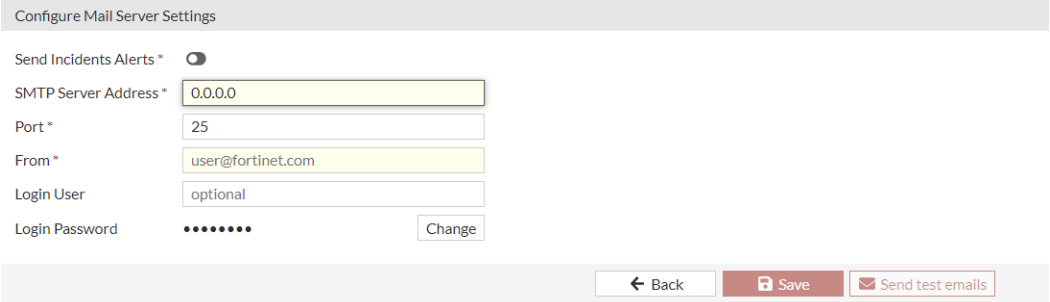


6. In FortiDeceptor enter the attribute claim in the *Attribute used to identify users* field.



Mail Server

Use the *Mail Server* page to send incident alerts. You can also create custom delivery rules.



Creating incident alerts

To send incident alerts:

1. Go to *System* > *Mail Server*. The *Mail Server* page opens.
2. Enable *Send Incidents Alerts*.
3. Configure the mail server settings.

SMTP Server Address	SMTP server address.
Port	SMTP server port number.
From	The mail server email account. This is the "from" address.

Login User	The mail server login account.
Login Password	Enter and confirm the password.

4. (Optional) Click *Send Test Email* to send a test email to one or more email addresses. If an error occurs, the error message appears at the top of the page and is recorded in the System Logs.
5. Click *Save*.
6. Click *Back* to return to the *Mail Server* page.

Creating alert delivery rules

To create a alert delivery rule:

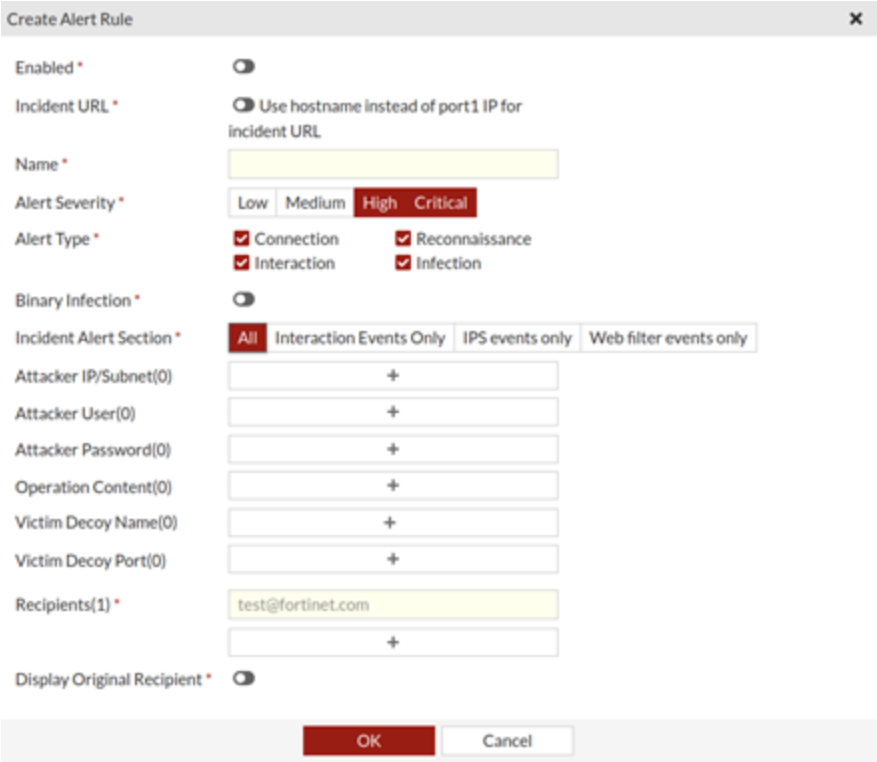
1. Click *Alert Deliver Rule*. The *Alert Rule* dialog opens.
2. *Enable* the rule. When enabled, FortiDeceptor sends an email alert to the Receiver Email List according to the rule
3. Configure the rule settings.

Name	Enter a name for the rule.
Incident URL	When enabled, the device hostname is used instead of the management IP. **Note**: The device hostname must be able to be resolved in your DNS server for the Incident URL link to work.
Alert Severity	Select *Low*, *Medium*, *High*, or *Critical*.
Alert Type	Select *Connection*, *Reconnaissance*, *Interaction*, and *Infection*.
Binary Infection	This options is available when the *Alert Type* is *Interaction* or *Infection* . Select *Yes* to be alerted when an attacker drops or downloads suspicious files into decoys.
Incident Alert Section	Select *All*, *Interaction Events Only*, *IPS events only*, or *Web filter events only*.
Attacker IP/Subnet	Enter one or more values for the attacker IP address or attacker IP network.
Attacker User	Enter one or more values for the attacker username. To trigger the rule, the username entered by the attacker and the value for *Attacker User* must be exactly same. The string is case sensitive.
Attacker Password	Enter one or more values for the attacker password. To trigger the rule, the password entered by the attacker and the value for *Attacker Password* must be exactly same. The string is case sensitive.
Operation Content	Enter one or more key words that will trigger the rule. Operation Content supports exact and partial matches. For example, if the value is `Monkey` and the attacker enters `Key`, the rule is triggered. However, the rule is not triggered if the attacker only enters `ey`. Operation Content is not case sensitive.
Victim Decoy Name	Select one or more deployed decoys from the *Select Entries* pane that slides open.

Victim Decoy Port	Enter one or more decoy service port numbers.
Recipients	Enter one or more receiver email addresses.
Display Original Recipient	Enable to view the original recipient of the alert email message.

The relationship between each of the lines in the rule is *And*. To trigger the rule, all the values must be met. For example, the rule is not triggered if the value for *Attacker User* is met, but the value for *Attacker Password* is not.

The relationship for each line of the rule is *Or*. To trigger the rule, only one of the values must be met. For example, if the values for *Attacker User* are `Admin` and `Administrator`, the rule is triggered if only `Admin` is entered.



4. Click *Save*.

SNMP

SNMP is a method to monitor your FortiDeceptor system on your local computer. You need an SNMP agent on your computer to read the SNMP information. Using SNMP, your FortiDeceptor system monitors for system events including CPU usage, memory usage, log disk space, interface changes, and malware detection.

SNMP has two parts:

- The SNMP agent or the device that is sending traps.
- The SNMP manager that monitors those traps.

The SNMP communities on the monitored FortiDeceptor are configured in the SNMP page.

The FortiDeceptor SNMP implementation is read-only. SNMP v1, v2c, v3 compliant SNMP manager applications, such as those on your local computer, have read-only access to FortiDeceptor system information and can receive FortiDeceptor system traps.

You can also download FortiDeceptor and Fortinet core MIB files.

Configure the SNMP agent

The SNMP agent sends SNMP traps that originate on FortiDeceptor to an external monitoring SNMP manager defined in one of the FortiDeceptor SNMP communities. Typically, an SNMP manager is an application on a local computer that can read the SNMP traps and then generate reports or graphs.

The SNMP manager can monitor FortiDeceptor to determine if it is operating properly or if critical events are occurring. The description, location, and contact information for this FortiDeceptor system is part of the information an SNMP manager collects. This information is useful if the SNMP manager is monitoring many devices, and it enables a faster response when FortiDeceptor requires attention.

To configure SNMP agents:

1. Go to *System* > *SNMP*.
2. Configure the following settings:

SNMP Agent	When enabled, the FortiDeceptor SNMP agent sends FortiDeceptor SNMP traps.
Description	Description of this FortiDeceptor to identify this unit.
Location	Location of this FortiDeceptor if it requires attention.
Contact	Contact information of the person in charge of this FortiDeceptor.
SNMP v1/v2c	Create, edit, or delete SNMP v1 and v2c communities. You can enable or disable communities in the edit page. Columns include: *Community Name*, *Queries*, *Traps*, *Enable*.
SNMP v3	Create, edit, or delete SNMP v3 entries. You can enable or disable queries in the edit page. Columns include: *Username*, *Security Level*, *Notification Host*, and *Queries*.

To create an SNMP v1/v2c community:

1. Go to *System* > *SNMP*.
2. In the SNMP v1/v2c section, click *Create New*.

3. Configure the following settings:

Enable	Enable the SNMP community.
Community Name	The name that identifies the SNMP community.
Hosts	The list of hosts that can use the settings in this SNMP community to monitor FortiDeceptor.
IP/Netmask	IP address and netmask of the SNMP hosts. Click *Add* to add additional hosts.
Queries v1, Queries v2c	Port number and if it is enabled. Enable queries for each SNMP version that FortiDeceptor uses.
Traps v1, Traps v2c	Local port number, remote port number, and if it is enabled. Enable traps for each SNMP version that FortiDeceptor uses.
SNMP Events	Events that cause FortiDeceptor to send SNMP traps to the community: • CPU usage is high • Memory is low • Log disk space is low • Incident is detected

4. Click *OK*.

To create an SNMP v3 user:

1. Go to *System* > *SNMP*.
2. In the SNMP v3 section, click *Create New*.

3. Configure the following settings:

Username	Name of the SNMPv3 user.
Security Level	Security level of the user: • None • Authentication only • Encryption and authentication
Authentication	Authentication is required when *Security Level* is either *Authentication only* or *Encryption and authentication*.
Method	Authentication method: • MD5 (Message Digest 5 algorithm) • SHA1 (Secure Hash algorithm)
Password	Authentication password of at least eight characters.
Encryption	Encryption is required if *Security Level* is *Encryption and authentication*.
Method	Encryption method: • DES • AES
Key	Encryption key of at least eight characters.
Notification Hosts (Traps)	
IP/Netmask	IP address and netmask. Click *Add* to add more hosts.
Query	
Port	Port number and if it is enabled.
SNMP V3 Events	SNMP events associated with that user: • CPU usage is high • Memory is low • Log disk space is low • Incident is detected

4. Click *OK*.

To download MIB files:

1. Go to *System* > *SNMP*.
2. Scroll down to *FortiDeceptor SNMP MIB* and click one of the following links:
   - *Download FortiDeceptor MIB File*
   - *Download Fortinet Core MIB File*

To filter the columns in the table:

1. Click the plus sign in the Search field. The *Filterable Columns* menu opens.

2. Select a column in the list to *Resize to Contents*, *Group By This column* or create a custom filter.
3. Click *Apply*.

905416

To show or hide columns in the table:

1. Hover the header row until the *Configure Table* icon appears.

2. Click *Configure Table*. The *Best Fit Columns* menu opens.
3. Select the columns to appear in the table and click *Apply*.
4. To restore the default table, click *Reset Table*.

FortiGuard

The FortiGuard Distribution Network (FDN) provides FortiGuard services for your FortiDeceptor system. The FDN is a worldwide network of FortiGuard Distribution Servers (FDS), which update the FortiGuard services on your FortiDeceptor system on a regular basis so that your FortiDeceptor system protects against the latest threats.

The FortiGuard services available on the FortiDeceptor system include:

Service	Description
Antivirus	Malware scanning against files that get captured by the decoys.
IDS engines	• Scanning the traffic between the threat actor and the decoys to detect network attacks • Contain the industrial signature pack for the ICS network .
Web filtering engine	Databases and look-ups against access from the decoy to the internet.
Anti-Recon and Anti-Exploit Service	The Anti-Reconnaissance and Anti-Exploit Service (ARAE) service is available on FortiDeceptor and is responsible for tracking hackers' activities on decoys with real-time alerts. Similar to how FortiSandbox traces malware behavior activities, ARAE will record malicious activities such as files extracted, intrusions activities, planted malware, and web sites visited. ARAEs goal is to Deceive, Expose and Eliminate threats.
AI Malware Engine	AI Pallas malware detection engine used for backend file inspection.

To configure FortiGuard updates:

1. Go to *System* > *FortiGuard*.
2. The following options and information are available:

Module Name	The FortiGuard module name, including: AntiVirus Scanner, AntiVirus Extended Signature, AntiVirus Active Signature, AntiVirus Extreme Signature, IDS Engine, IDS Signature, Anti-Reconnaissance & Anti-Exploit Engine. All modules automatically install update packages when they are available on the FDN.
Current Version	The current version of the module.
Release Time	The time that module was released.
Last Update Time	The time that module was last updated.
Last Check Status	The status of the last update attempt.
Upload Package File	Select *Browse* to locate a package file on the management computer, then select *Submit* to upload the package file to the FortiDeceptor. When the unit has no access to the Fortinet FDN servers, the user can go to the Customer Service and Support site to download package files manually.
FortiGuard Server Settings	
Use override FDN server to download module updates	Select to enable an override FDN server, or FortiManager, to download module update, then enter the server IP address or FQDN in the text box. When an overridden FDN server is used, FortiGuard Server Location will be disabled. Click *Connect FDN Now* button to schedule an immediate update check. The default port on FDN server is *443* and can be changed to *53* or *8888*.
Use Proxy	Select to use a proxy. Configure the *Proxy Type* (*HTTP Connect*, *SOCKS v4*, or *SOCKS v5*), *Server Name/IP*, *Port*, *Proxy Username*, and *Proxy Password*.
FortiGuard Web Filter Settings	
Use override server address for web filtering query	Select to enable an override server address for web filtering query, then enter the server IP address (IP address or IP address:port) or FQDN in the text box. By default, the closest web filtering server according to the unit's time zone is used. The default port on FDN server is 443.
Use Proxy	Select to use a proxy. Configure the *Proxy Type* (*HTTP Connect*, *SOCKS v4*, or *SOCKS v5*), *Server Name/IP*, *Port*, *Proxy Username*, and *Proxy Password*.
VM Image Download Proxy Settings	
Use Proxy	Select to use a proxy. Configure the *Proxy Type* (*HTTP Connect*, *SOCKS v4*, or *SOCKS v5*), *Server Name/IP*, *Port*, *Proxy Username*, and *Proxy Password*.

3. Click *Connect FDN Now* to connect the override FDN server/proxy.
   - Click *Test Connection* to test your connection.
   - Click *Apply* to apply your changes.

FDC License

FortiDeceptor is a subscription-based model that calculates the amount of Network VLANs the system can connect to. Single Class C (/24) will consume 1 VLAN, while other network classes with /23 and below will consume 2 VLANs (max).

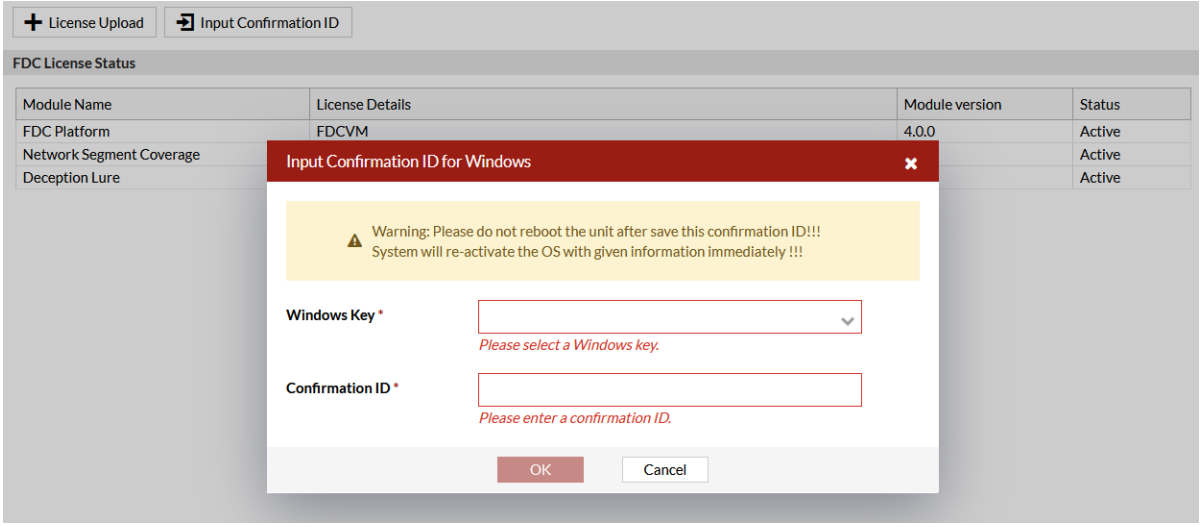
To upload a FortiDeceptor license:

1. Go to *System* > *FDC License*.
2. Click *License Upload*. The *Firmware License Upload* page opens.
3. Click *Browse* and navigate to the license file on your computer.
4. Click *Submit*.

FortiDeceptor will reboot after the license file is installed.

To input the confirmation ID for Windows:

1. Go to *System* > *FDC License*.
2. Click *Input Confirmation ID* . The *Input Confirmation ID for Windows* dialog opens.
3. From the *Windows Key* dropdown, select a Windows key.
4. In the *Confirmation ID* field, enter the confirmation ID.
5. Click *OK*.



Do not reboot FortiDeceptor until the activation is complete.

Settings

Configure the idle timeout for the administrator account or reset all the widgets in the *Dashboard*.

To configure idle timeout:

1. Go to *System* > *Settings*.
2. Enter a value between *1* and *480* minutes.
3. Click *OK*.

To reset all widgets:

Click the *Reset* button to revert the *Dashboard* to the default settings. This removes any widgets you added to the *Dashboard* and restores the widget settings.

To enable Mitre ICS tag:

1. Go to *System* > *Settings*.
2. Under *Mitre ICS settings* select *Enable Mitre ICS*.
3. Click *Apply*.

To Upload deception statistics to FortiGuard:

1. Go to *System* > *Settings*.
2. Enable *FortiDeceptor Attack Detection Exchange Program*.
3. Click *Apply*.

Login Disclaimer

Create a custom disclaimer message to display when a user logs into the FortiDeceptor unit.

To create a custom log in disclaimer:

1. Go to *System* > *Login Disclaimer*.
2. In the *Disclaimer* field, enter the disclaimer text.
3. (Optional) Select *Show disclaimer on login*, to display the disclaimer when a user logs in.
4. Click *OK*.

Table Customization

You can customize the page layout for the *Incidents* and *Events* pages.

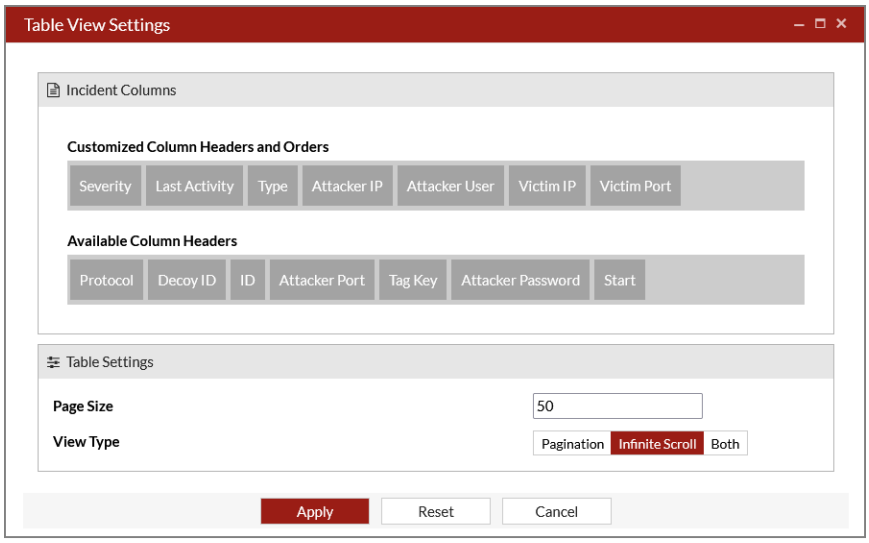
To customize the columns available for Incidents or Events:

1. In the *Incident Columns* pane:

To show a column	Drag and drop the headers from the *Available Column Headers* to *Customized Column Headers and Orders*.
To hide a column	Drag and drop the headers from the *Customized Column Headers and Orders* to *Available Column Headers*.
To change the column order	Drag and drop the position of the headers in *Customized Column Headers and Orders*.

2. In the *Table Settings* pane, configure the table size and view.

Page Size	Enter the number of incidents to display per page when *View Type* > *Pagination* is selected.
View Type	Select *Pagination*, *Infinite Scroll* or *Both*.



3. Click *Apply*.

You may need to refresh the page to see your changes.

Raw logs

You can download and save raw logs to the management computer. Raw logs are saved as a text file with the extension *.log.gz*.

To download raw logs:

1. Go to *Log* > *All Events* and select a log.
2. In the toolbar, click *Download Log*.

Sample raw logs file content

```
itime=1535413204 date=2018-08-27 time=16:40:04 logid=0106000001 type=event subtype=system
     pri=debug user=system ui=system action= status=success msg="SNMP TRAP sent out:
     Service=SSH AttackerIp=10.95.5.83 AttackerPort=57190 VictimIp=10.95.5.21 VictimPort=22
     Operation=Established SSH connection Description=10.95.5.83 Username=NA Password=NA"
itime=1535413204 date=2018-08-27 time=16:40:04 logid=0106000001 type=event subtype=system
     pri=debug user=system ui=system action= status=success msg="SNMP TRAP sent out:
     Service=SSH AttackerIp=10.95.5.83 AttackerPort=57190 VictimIp=10.95.5.21 VictimPort=22
     Operation=SSH connection closed Description=83ssh Username=83ssh Password=83ssh"
itime=1535413204 date=2018-08-27 time=16:40:04 logid=0106000001 type=event subtype=system
     pri=debug user=system ui=system action= status=success msg="SNMP TRAP sent out:
     Service=SSH AttackerIp=10.95.5.83 AttackerPort=57190 VictimIp=10.95.5.21 VictimPort=22
     Operation=Authentication Failure Description=83ssh Username=83ssh Password=83ssh"
itime=1535413204 date=2018-08-27 time=16:40:04 logid=0106000001 type=event subtype=system
     pri=debug user=system ui=system action= status=success msg="SNMP TRAP sent out:
     Service=SAMBA AttackerIp=10.95.5.83 AttackerPort=NA VictimIp=10.95.5.21 VictimPort=445
     Operation=Change to dir Description=/home/share/samba Username=83samba
     Password=83samba"
itime=1535413204 date=2018-08-27 time=16:40:04 logid=0106000001 type=event subtype=system
     pri=debug user=system ui=system action= status=success msg="SNMP TRAP sent out:
     Service=SAMBA AttackerIp=10.95.5.83 AttackerPort=NA VictimIp=10.95.5.21 VictimPort=445
     Operation=Access path Description=samba Username=83samba Password=83samba"
itime=1535413204 date=2018-08-27 time=16:40:04 logid=0106000001 type=event subtype=system
     pri=debug user=system ui=system action= status=success msg="SNMP TRAP sent out:
     Service=SAMBA AttackerIp=10.95.5.83 AttackerPort=NA VictimIp=10.95.5.21 VictimPort=445
     Operation=Disconnect net share Description=samba Username=83samba Password=83samba"
itime=1535413201 date=2018-08-27 time=16:40:01 logid=0106000001 type=event subtype=system
     pri=alert user=system ui=GUI action=update status=success msg="Service=SSH
     AttackerIp=10.95.5.83 AttackerPort=57190 VictimIp=10.95.5.21 VictimPort=22
     Operation=SSH connection closed Description=83ssh Username=83ssh Password=83ssh"
itime=1535413201 date=2018-08-27 time=16:40:01 logid=0106000001 type=event subtype=system
     pri=alert user=system ui=GUI action=update status=success msg="Service=SSH
     AttackerIp=10.95.5.83 AttackerPort=57190 VictimIp=10.95.5.21 VictimPort=22
     Operation=Authentication Failure Description=83ssh Username=83ssh Password=83ssh"
itime=1535413198 date=2018-08-27 time=16:39:58 logid=0106000001 type=event subtype=system
     pri=alert user=system ui=GUI action=update status=success msg="Service=SSH
     AttackerIp=10.95.5.83 AttackerPort=57190 VictimIp=10.95.5.21 VictimPort=22
     Operation=Established SSH connection Description=10.95.5.83 Username=NA Password=NA"
itime=1535413198 date=2018-08-27 time=16:39:58 logid=0106000001 type=event subtype=system
     pri=alert user=system ui=GUI action=update status=success msg="Service=SAMBA
     AttackerIp=10.95.5.83 AttackerPort=NA VictimIp=10.95.5.21 VictimPort=445
     Operation=Disconnect net share Description=samba Username=83samba Password=83samba"
itime=1535413197 date=2018-08-27 time=16:39:57 logid=0106000001 type=event subtype=system
     pri=alert user=system ui=GUI action=update status=success msg="Service=SAMBA
     AttackerIp=10.95.5.83 AttackerPort=NA VictimIp=10.95.5.21 VictimPort=445
```

```
      Operation=Change to dir Description=/home/share/samba Username=83samba
      Password=83samba"
itime=1535413197 date=2018-08-27 time=16:39:57 logid=0106000001 type=event subtype=system
      pri=alert user=system ui=GUI action=update status=success msg="Service=SAMBA
      AttackerIp=10.95.5.83 AttackerPort=NA VictimIp=10.95.5.21 VictimPort=445
      Operation=Access path Description=samba Username=83samba Password=83samba"
```

Log

Use the *Log* pages to view and download FortiDeceptor system logs. You can put logs locally on FortiDeceptor or on a remote log server.

Log Servers

You can send FortiDeceptor logs to a remote syslog server, FortiAnalyzer, or common event type (CEF) server. In *Log* > *Log Servers*, you can create new remote log servers, and edit and delete remote log servers. You can configure up to 30 remote log server entries.

The following options are available:

Create New	Create a log server entry.
Edit	Edit the selected log server entry.
Delete	Delete the selected log server entry.

This page displays the following information:

Name	Name of the server entry.
Type	Server type: syslog, syslog over TLS, FortiAnalyzer or CEF.
Log Server Address	Log server address.
Port	Log server port number.
Status	Log server status, *Enabled* or *Disabled*.

To create a server entry:

1. Go to *Log* > *Log Servers*.
2. Click *Create New*.
3. Configure the following settings:

Name	Name of the new server entry.
Type	Select *Syslog Protocol*, *FortiAnalyzer*, or *Common Event Format*.
Log Server Address	Log server IP address or FQDN.
Port	Port number. The default port is 514.
Status	Enable or disable sending logs to the server.
Log Level	Select the logging levels to forward to the log server. For logging levels, see Logging Levels on page 151.

4. Click *OK*.

To edit or delete a log server

1. Go to *Log* > *Log Servers*.
2. Select an entry and click *Edit* or *Delete*.

Log Categories

Log > *All Events* shows all logs.

The following options are available.

Download Log	Download the raw log file to the management computer.
History Logs	Enable to include historical logs in Log Search.
Refresh	Refresh the log message list.
Search	Click *Search* to add search filters. You can select different categories to search the logs. Search is not case sensitive. Click the **+** button to choose from *Date/Time*, *Level*, *User*, *Message*, or *Appliance*.
Details	Click to view the *Log Details*.

The following information is displayed.

#	Log number.
Date/Time	Date and time the log message was created.
Level	Level of the log message. For logging levels, see Logging Levels on page 151.
User	The user to which the log message relates. User can be a specific user or system.
Message	Detailed log message.

Logging Levels

FortiDeceptor log level can be Emergency (reserved), Alert, Critical, Error, Warning, Information, or Debug. The following table provides example logs for each log level.

Log Level	Description	Example Log Entry
Alert	Immediate action is required.	Suspicious URL visit domain.com from 192.12.1.12 to 42.156.162.21:80.
Critical	Functionality is affected.	System database is not ready. A program should have started to rebuild it and it shall be ready after a while.

Log Level	Description	Example Log Entry
Error	An erroneous condition exists and functionality is probably affected.	Errors that occur when deleting certificates.
Warning	Functionality might be affected.	Submitted file AVSInstallPack.exe is too large: 292046088.
Information	General information about system operations.	LDAP server information that was successfully updated.
Debug	Detailed information for debugging.	Launching job for file. jobid=2726271637747836543 filename=log md5=ebe5ae2bec3b653c2970e8cec9f5f1d9 sha1=06ea6108d02513f0d278ecc8d443df86dac2885b sha256=d678da5fb9ea3ee20af779a4ae13c402585 ebb070edcf20091cb20509000f74b

Appendix A - Deploying FortiDeceptor in offline or air-gapped networks

This section shows how to deploy FortiDeceptor in an offline or air-gapped network with no internet access, using the following procedures.

- Applying the license in an offline or air-gapped network on page 153
- Importing deception VMs in an offline or air-gapped network on page 155
- Importing firmware in an offline or air-gapped network on page 157
- Importing an FDS package via FDC GUI in an offline or air-gapped network on page 157
- Importing FDS package and license file via FortiManager in an offline or air-gapped network on page 158

FortiDeceptor uses deception VMs to deploy decoys across the network. Deploying FortiDeceptor VMs in a closed network requires downloading the required images directly from the FortiDeceptor VM external repository and manually uploading the deception VMs. For information about downloading the deception VMs, see Importing deception VMs in an offline or air-gapped network on page 155

You can also use the *Deception* > *Deception OS* page or the `fw-upgrade` CLI command to download and import packages.

Because FortiDeceptor also uses FDS services (IPS/AV/WEB) in offline and air-gapped networks, you must also import these packages.

Deception VM security

You can download deception VMs via the HTTPS protocol. Each image is compressed, encrypted, and packed by the FDC tool separately. The metafile describes the MD5 of each VM image.

The security layers that protect deception images are:

- Download via HTTPS.
- Deception VMs do not have any Fortinet propriety software.
- We provide the file's MD5 so that you can confirm the MD5 checksum for the downloaded files.
- FortiDeceptor always verifies the VM image by encryption and multiple layer checksum inside the package before installing it.

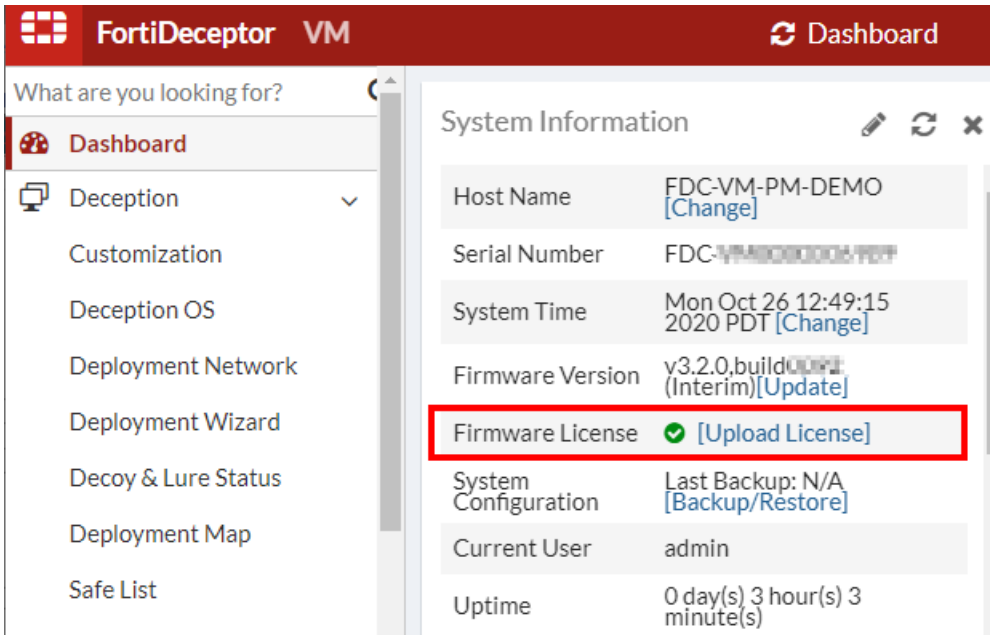
Applying the license in an offline or air-gapped network

To download the FortiDeceptor license file from the Fortinet support site:

1. Log into Customer Service and Support. The Asset Portal opens.
2. Go to *My Assets* and locate the device then click the *Serial Number*. The product details page opens.
3. In the *License & Key* widget, click *Get The License File* and save it to the local disk.

To upload the license file to FortiDeceptor:

1. Log into FortiDeceptor.
2. Configure the management IP address on port1.
3. In the *Dashboard System Information* widget, click *Upload License* beside *Firmware License*.



4. Locate the license and click *Submit*.

FortiDeceptor extracts the serial number, IP addresses, decoy keys, expiry date; and then performs the following verifications.

- Verify the expiration time of the license.
- Verify that the embedded management IP address is the same as the current management IP address. You can view the IP address in the *Product Information* widget in the product details page.
- Verify the expiration time of the decoys keys if the keys are subscription type.

If all the verifications pass, the unit is ready to import deception images.

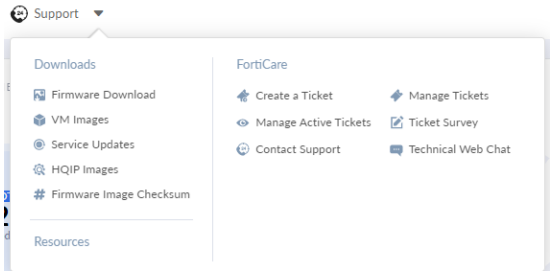
- FortiDeceptor decoy WCF lookup (any URLs visiting from decoys) are **not** categorized.
  - You can use FortiManager to resolve this. Because FortiDeceptor supports override FDS server, you can enter the FortiManager IP address there.
- Subscription-based decoys, that is, SSL VPN Windows customization, is in the `*.lic` file from the support site, which you can run offline.
- FortiDeceptor Custom Decoy Subscription Service includes:
  - FC-10-FDCVM-292-02-DD (for VM).
  - FC-10-FDC1K-292-02-DD (for HW).

Importing deception VMs in an offline or air-gapped network

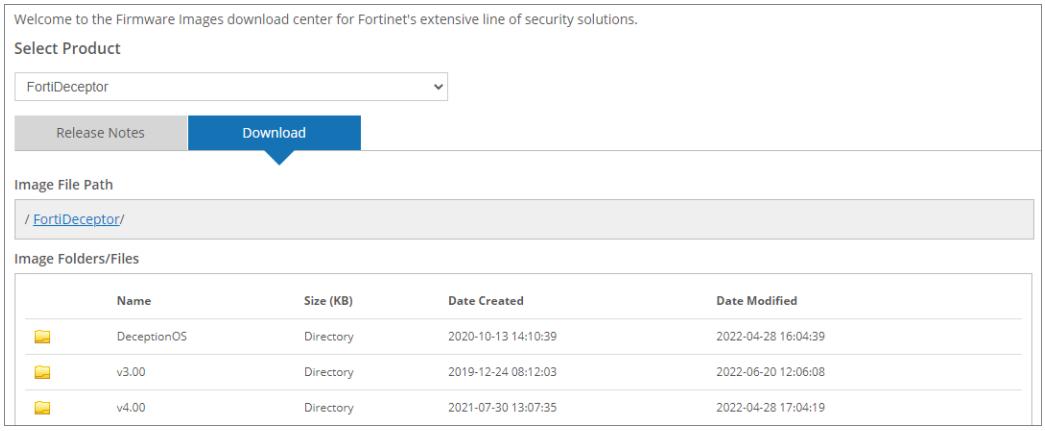
This topic shows how to download and import deception VMs in an offline or air-gapped network.

To download and import a deception VM:

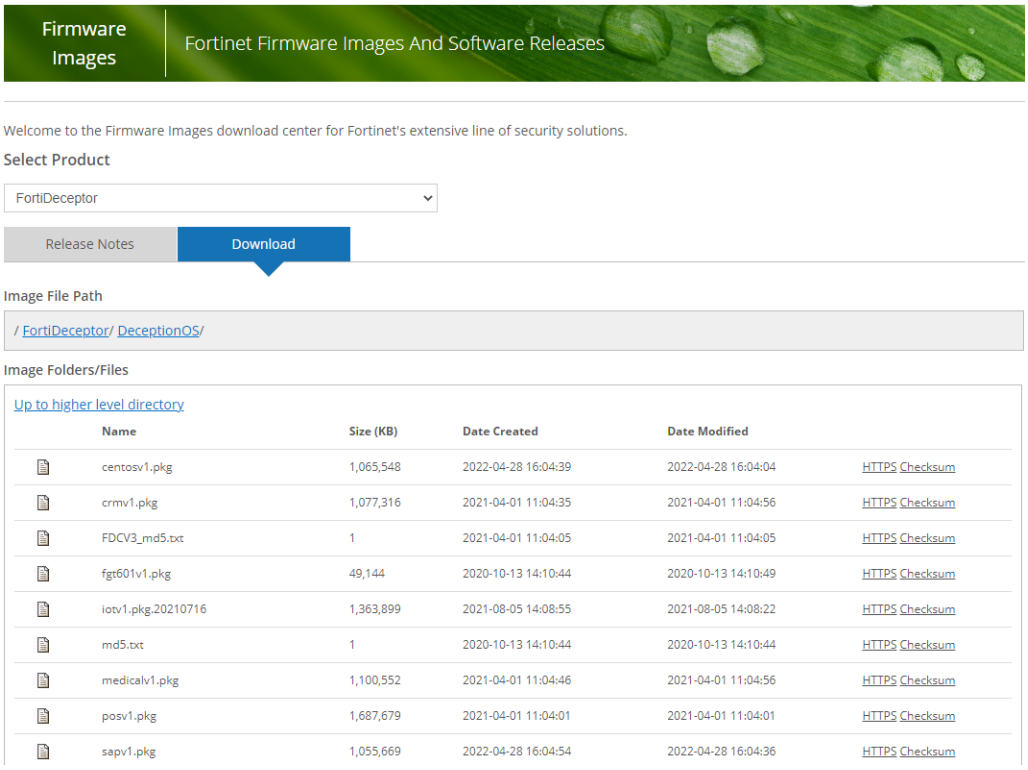
1. Log into Customer Service and Support. The *Asset Portal* opens.
2. In the banner, click *Support* > *Downloads* > *Firmware Download*.



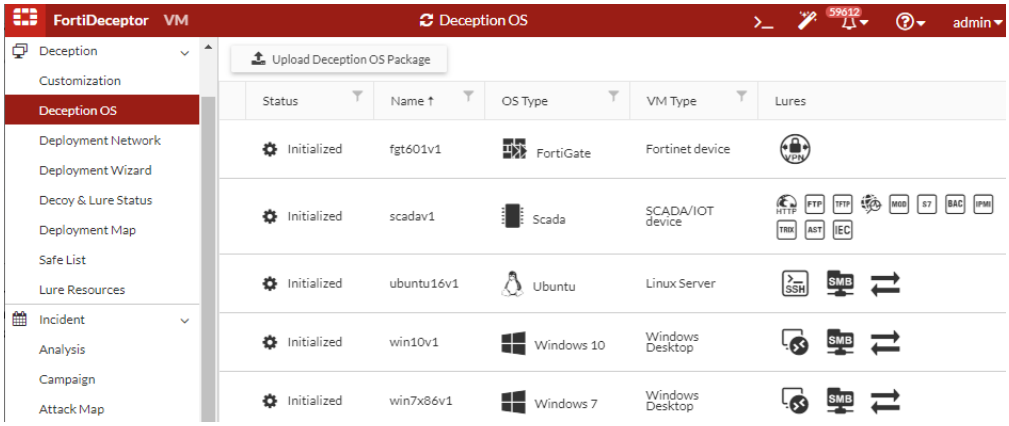
3. In the *Select Product* dropdown list, select FortiDeceptor and then click *Download*.



4. Click *Deception OS* to see the list of deception OS VM files.



5. Download all the deception OS VM *.pkg* files in this directory.
6. Copy the downloaded files to the offline or air-gapped network.
7. In FortiDeceptor, go to *Deception* > *Deception OS* and click *Upload Deception OS Package* to import the FortiDeceptor images.

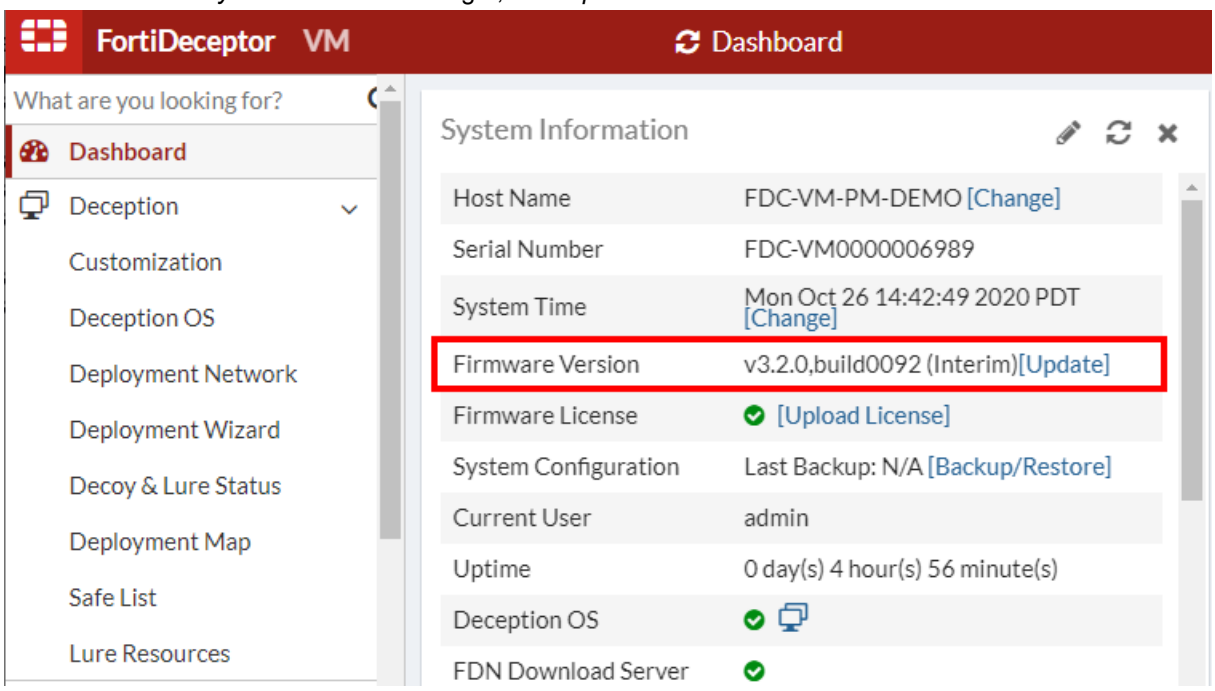


FortiDeceptor imports the images, verifies image integrity and other security layers, confirms that the images are the originals, and then initializes them. After initialization the *Deception OS* window *Status* column shows these images as *Initialized*.

Importing firmware in an offline or air-gapped network

To download and import FortiDeceptor firmware:

1. Log into Customer Service and Support.
2. Go to *Download* > *Firmware Images*.
3. In the *Select Product* dropdown list, select FortiDeceptor and then click *Download*.
4. Click the version you want.
5. Download the FortiDeceptor firmware file (the `.out` file).
6. Copy the downloaded file to the offline or air-gapped network.
7. Log into FortiDeceptor.
8. In the *Dashboard System Information* widget, click *Update* beside *Firmware Version*.



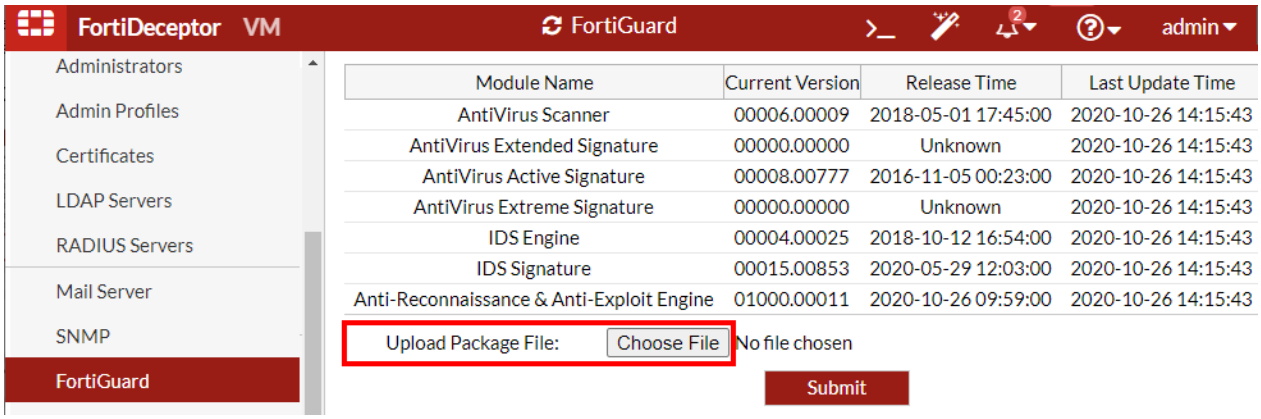
9. Click *Choose file*, then locate the firmware file and click *Submit*.
   FortiDeceptor reboots after the update.

Importing an FDS package via FDC GUI in an offline or air-gapped network

To download and import a FortiDeceptor FDS package:

1. Log into Customer Service and Support.
2. Go to *Download* > *FortiGuard Service Updates*.
3. Locate and download the FortiDeceptor FDS package (the `.pkg` file).
4. Copy the downloaded file to the offline or air-gapped network.

5. In FortiDeceptor, go to *System* > *FortiGuard*; then beside *Upload Package File*, click *Choose File* and locate the FDS package.



6. Click *Submit*.
   Ensure you receive a confirmation that installation is successful.

Importing FDS package and license file via FortiManager in an offline or air-gapped network

This topic shows how to download and import a FortiDeceptor license in an offline or air-gapped network using FortiManager.

When FortiManager is operating in a closed network, you can create a support ticket to request account entitlement files from Fortinet Customer Service & Support for devices, and then upload the files to FortiGuard. This allows devices in the closed network to check licenses.

To request the FortiDeceptor entitlement license file for FortiManager:

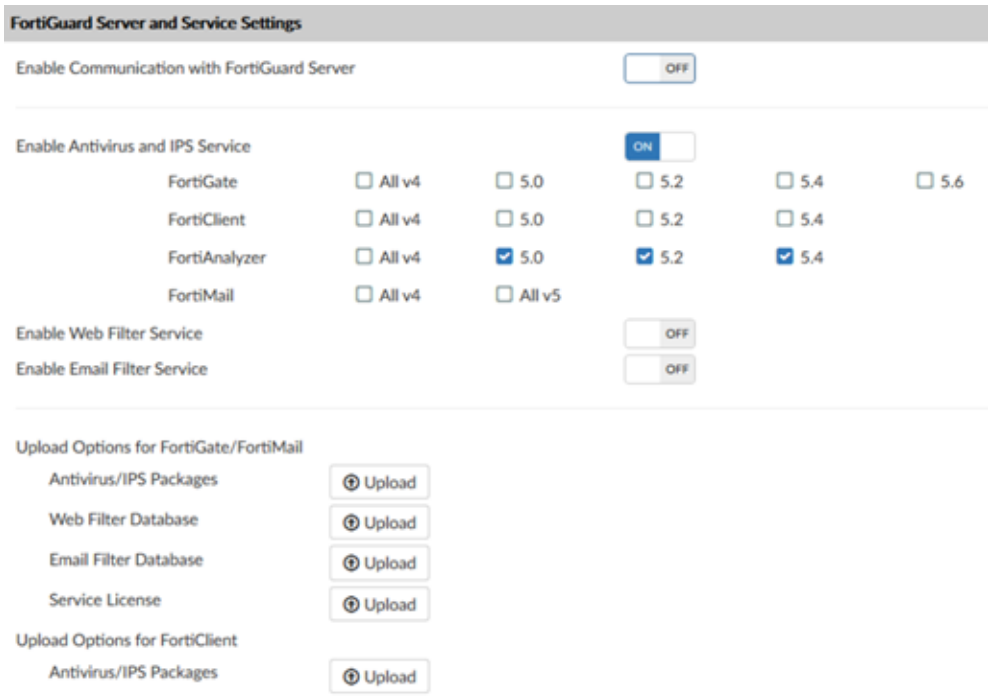
1. Log into Customer Service and Support.
2. Go to *Assistance* > *Create a Ticket*.
3. Expand *Customer Service* and click *Submit Ticket*.
4. Enter the required information.
   - For *Subject*, enter *Entitlement file*.
   - For *Category*, select *CS Contract/License*.
5. Complete and submit the ticket.
6. When you receive the entitlement file via email, download it to your computer.

Without a connection to a FortiGuard server, update packages and licenses must be manually downloaded from support, and then uploaded to FortiManager.

To upload the FortiDeceptor entitlement license file to FortiManager:

1. In FortiManager, go to *FortiGuard* > *Settings*.
2. Set *Enable Communication with FortiGuard Server* to *OFF* so that you can configure FortiManager as a local FDS server.

3. In the *Upload Options for FortiGate/FortiMail* section, click *Upload* besides *Service License*.

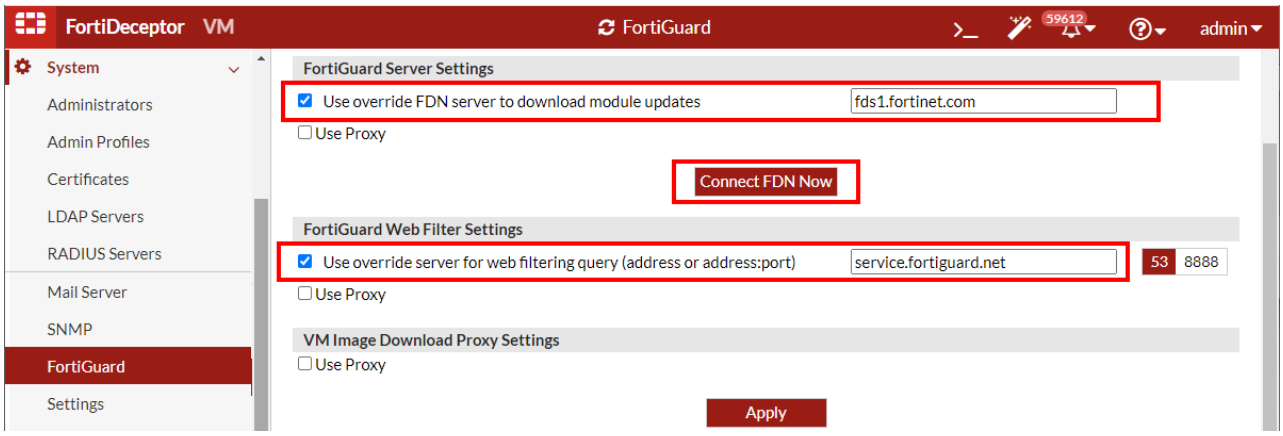


Enable Communication with FortiGuard Server	Toggle *OFF* to disable communication with FortiGuard servers.
Enable AntiVirus and IPS Service	Toggle *ON* to enable antivirus and intrusion protection service. When on, select the versions of FortiGate, FortiClient, FortiAnalyzer, and FortiMail to download updates.
Enable Web Filter Service	Toggle *ON* to enable web filter services. When uploaded to FortiManager, the web filter database displays.
AntiVirus/IPS Packages	Click *Upload* to upload antivirus and IPS packages you downloaded from the Customer Service & Support portal.
Web Filter Database	Click *Upload* to upload the web filter database you downloaded from the Customer Service & Support portal. As the database can be large, uploading with CLI is recommended.
Service License	Click *Upload* to import the FortiGate license. You can get a license file from support by requesting your account entitlement for the device.

To configure FortiDeceptor to use FortiManager for FortiGuard services:

1. Go to *System* > *FortiGuard*.
2. In the *FortiGuard Server Settings* section, select *Use override FDN server to download module updates* and enter the FortiManager IP address.
3. In the *FortiGuard Web Filter Settings* section, select *Use override server for web filtering query (address or address:port)* and enter the FortiManager IP address.

4. In the *FortiGuard Server Settings* section, click *Connect FDN Now* to test the FDN connection.



5. If the test passes, click *Apply*.

Appendix B - Deception deployment best practices

This section provides best practices principles and use cases on how to deploy FortiDeceptor in different network topologies.

The section covers the following topics:

- Deception strategy on page 161
- FortiDeceptor platform on page 167
- Deploying deception on page 180
- Attack vectors vs deception on page 191
- Deploying tokens using AD GPO logon script on page 195
- Deploying AWS deception keys on page 200
- Deploying Azure deception keys on page 210
- Configuring trunk ports on FortiDeceptor VM on page 216

Deception strategy

The ancient war strategies by Sun Tzu says: "Know thy self, know thy enemy. A thousand battles, a thousand victories."

This means if you know the strengths and weaknesses of your enemy, and if you know the strengths and weaknesses in your defense system, you can win any battle. To win against cyber attackers and hackers or users with malicious intention, the cyber security team needs to understand the attacker's techniques and tools, as well as shortfalls in the organization's defense system.

To understand the attack techniques and hackers' interests in your environment, we need to understand three tools that can help security professionals stop attackers before a data breach happens.

- **Sandboxing**: This technique allows the malware to install and run in an enclosed environment where the security team can monitor the malware's actions to identify potential risks and countermeasures.
- **Honeypots**: These are intentionally vulnerable systems that are meant to attract attackers. Honeypots entice attackers to attempt to steal valuable data or further scope out the target network. Honeypots help you to understand the process and strategy of attackers.
- **Deception technologies**: These are more advanced honeypot and honeynet products that offer more automation for both detection and implementation of defenses based on the data they gather.

Deception technology is like honeypots on steroids. It has more advanced capabilities like deception lure, deception automation, threat analysis, threat hunting, and more.

The core technology behind deception is the decoy. In general, there are several kinds: low, medium, and high. To align with FortiDeceptor technology, let's focus on two types of decoys: Low Interaction and High Interaction.

- **Low interaction honeypot**: This decoy has limited capability of emulating enterprise applications and is used only to detect from where the attackers are coming and what they attempt to exploit. These are easy for attackers to fingerprint and bypass.
- **High interaction honeypot**: This decoy is identical to the enterprise systems and can run real operating systems, applications, and services with dummy data. They allow the attacker to log in and they respond to the attacker's

request. In this way, the decoy helps you understand the attacker's intentions, lures them for a long time to identify how command and control infrastructure is set up.

Deception technology systems are more advanced and have more components, breadcrumbs, baits, and lures. Deception systems are implemented alongside enterprise systems but still remain in an isolated environment.

Deception technology systems are used to interrupt the attacker's kill chain, prolong the attack either to exhaust the attacker’s resources or encourage attackers by providing obvious vulnerabilities to help identity the details of their network and arsenals.

Deception strategy components

Deployment of enterprise-scale deception includes the following components:

- Medium interaction decoy and high interaction decoy that are deployed everywhere.
- Customizable decoys to match infrastructure and applications.
- Create and deploy lures to redirect attackers toward decoys.
- Create and deploy lures with trackable misinformation.
- Threat analysis capabilities.
- Integration with existing security infrastructure for mitigation and remediation (Security Fabric and third-party).

Deception strategy goals

Deployment of enterprise-scale deception should achieve the following cyber security requirements and goals:

- Generate actionable, high-fidelity alerts.
- Reduce the “dwell time” of an initial compromise.
- Confuse the attacker with false assets and misinformation.
- Block the human attacker or Advanced Persistent Threat (APT).
- Collect threat intelligence regarding tactics, techniques, and procedures.
- Integrate with existing defense-in-depth architecture.

Deception philosophy

Deception philosophy is a straightforward concept. You deploy deception across the whole network infrastructure and location which generates a fake virtual network layer that masks the real assets with a fake one.

The networks today are fluid and dynamic, so we need to be sure that every network segment and location has this deception layer and capability.

For example:

- **IT Endpoint segment** — Requires deployment of lures and decoys.
- **IT Servers segment** — Requires deployment of lures and decoys.
- **Network Devices** — Requires deployment of decoys.
- **IoT Devices** — Requires deployment of decoys.
- **OT Devices** — Requires deployment of decoys.
- **Data Repository** — Requires deployment of honey files and decoys.
- **Application segment** — Requires deployment of lures and decoys.

- **Network Traffic** — Require decoys that generates fake network traffic and lure that creates fake network connections and entries on the endpoint level.
- **Public/Private Cloud** — Requires deployment of decoys.

Deception light stack vs full stack

Deception light stack concept

The light deception concept uses a combination of endpoint lures with several high interaction decoys only as destination targets.

Using the light deception concept against a sophisticated adversary has some significant drawbacks:

- Deception lures reside on the endpoint and if there is no in-depth customization, this can be fingerprinted.
- A sophisticated adversary that controls several endpoints might fail once and learn the deception lure logic so that the adversary will not make the same mistake next time.
- A sophisticated adversary might not touch the deception lures if it can get high privilege at the beginning of the attack, and the probability of finding several decoys from several thousand assets is non-existent.
- Lack of visibility around unmanaged devices (IoT/OT) where an adversary has plenty of time and space to attack without detection.
- Simple malware spread vectors like pass the hash / single vulnerability attacks are not detected due to a lack of decoys in the network segment level. For example, the Wannacry malware will not get detected using this deployment stack.

Deception full stack concept

A simple explanation of the deception full stack concept is “do not let the sophisticated adversary / malware fingerprint your fake story!”

The deception full stack addresses the drawback of the light deception concept using several deception layers’ architectures:

- Server / endpoint lures are the first layer that engages with the adversary / APT.
- A large scale of decoys that creates a fake network surface on top of the real one offering false endpoints, servers, network devices, IoT/OT, database, files, applications, cloud, and more. This is the deception everywhere concept.
- Some of the decoys are generated from a customer “gold image” and are part of the network domain to increase the authentic deception level.

The dynamic deception decoys module prevents the sophisticated adversary from fingerprinting the decoys by changing the decoys' IP addresses and profile based on time or trigger.

The FortiDeceptor full stack deception concept runs deception lures with a large scale of decoys using a hybrid mode engine that provides medium and high-level interaction decoys against the adversary / APT malware.

Deception for FortiGuard Outbreak Alerts

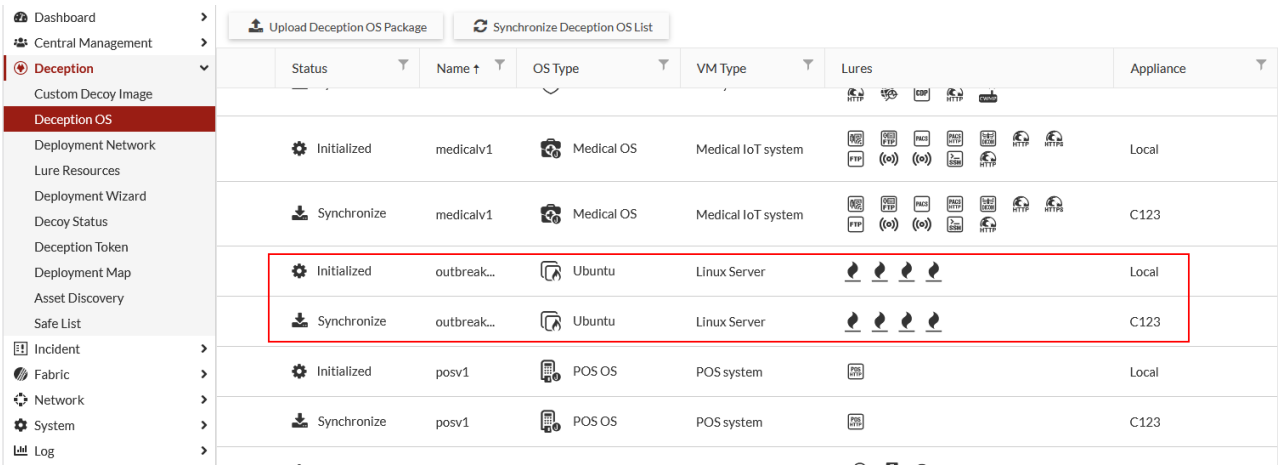
FortiGuard Outbreak Alerts communicate important information about cybersecurity attacks and the Fortinet products that will break the attack sequence. When a cybersecurity incident/attack/event occurs that affects numerous organizations, the Outbreak Alerts page is updated with a link to an individual FortiGuard Outbreak Alert. For more information, visit the *Outbreak Alerts* page.

FortiDeceptor's *outbreakv1* Deception OS contains Deception Decoys that are designed to target and mitigate vulnerabilities identified in the FortiGuard Outbreak Alerts page.

The following steps describe how to configure the *outbreakv1* Deception OS for Log4j2 attacks.

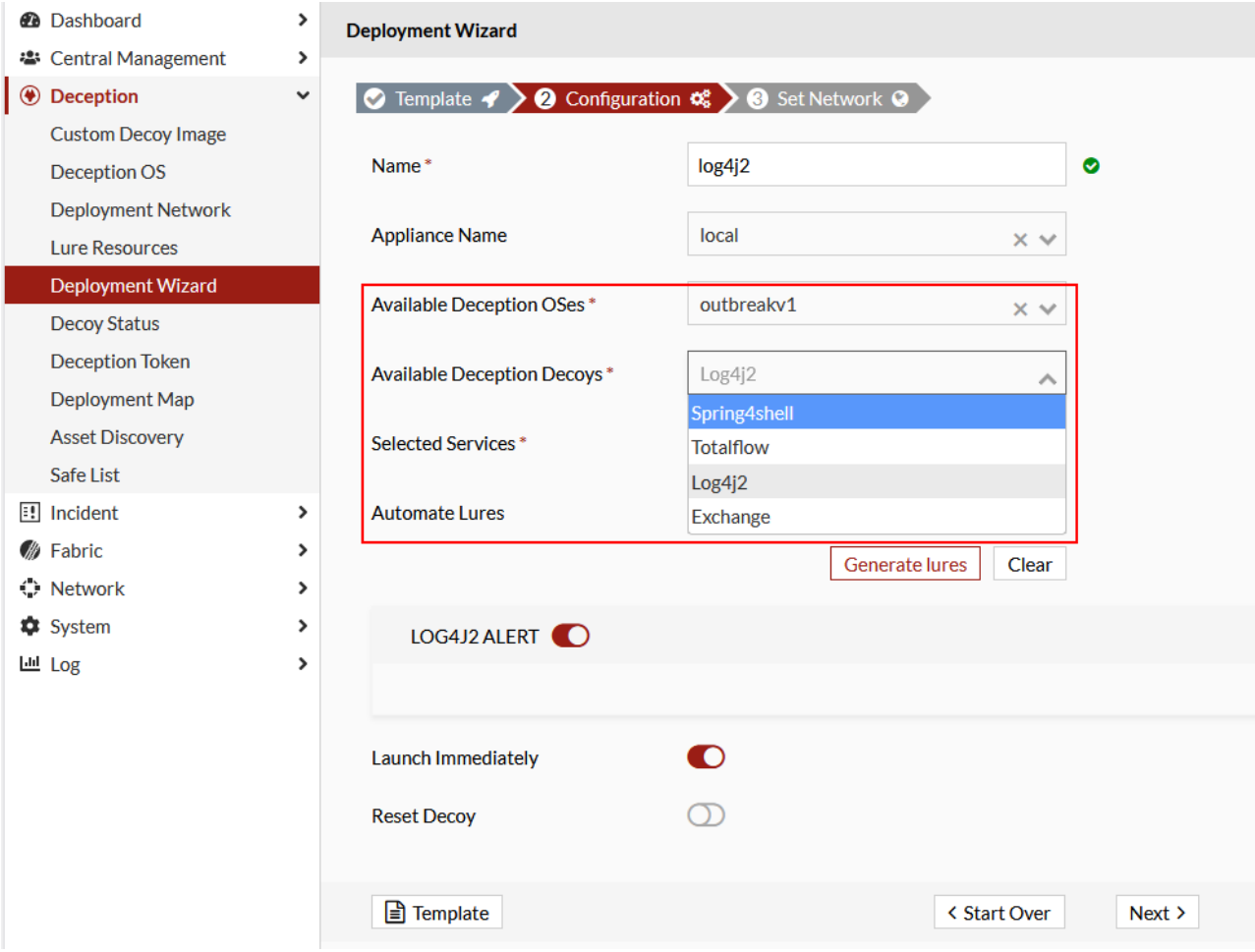
To deploy deception decoys for Outbreak Alerts:

1. Install the *outbreakv1* deception OS.
   a. Go to *Deception* > *Deception OS*.
   b. In the *Status* column, click *Synchronize* next to *outbreakv1*. The status changes to *Initialized*.



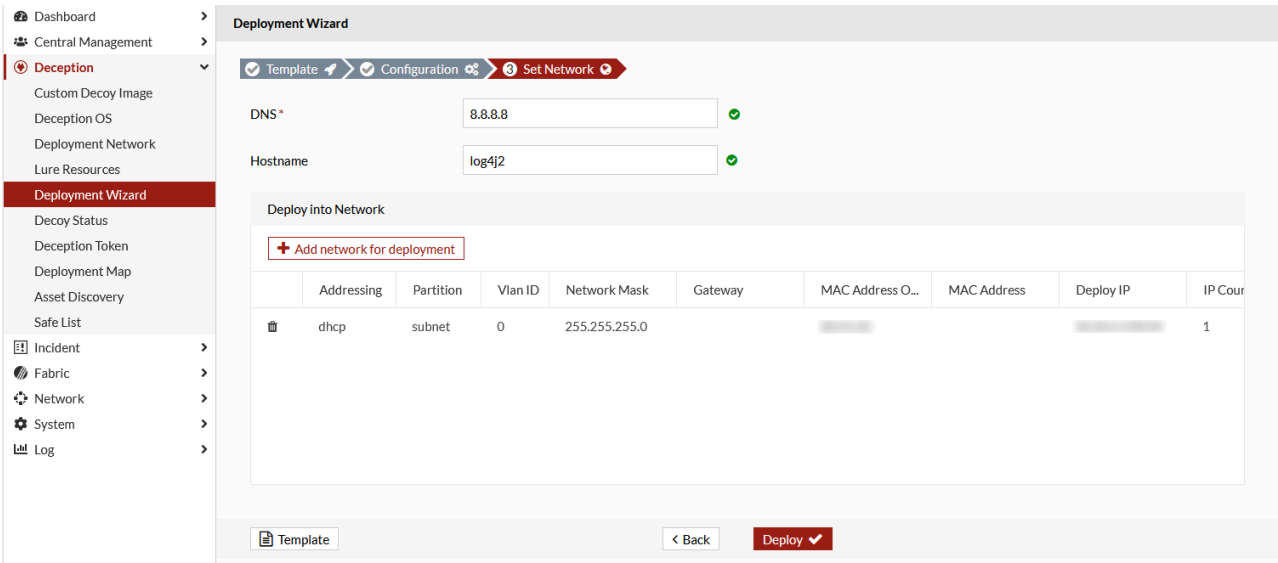
2. Go to *Deception* > *Deployment Wizard* and click *Create a new decoy*. The *Configuration* page opens.
3. Configure the following deployment settings.

Available Deception OSes	Select *outbreakv1*.
Available Deception Decoys	Select and outbreak deception decoy. For example, *Log4j2*.

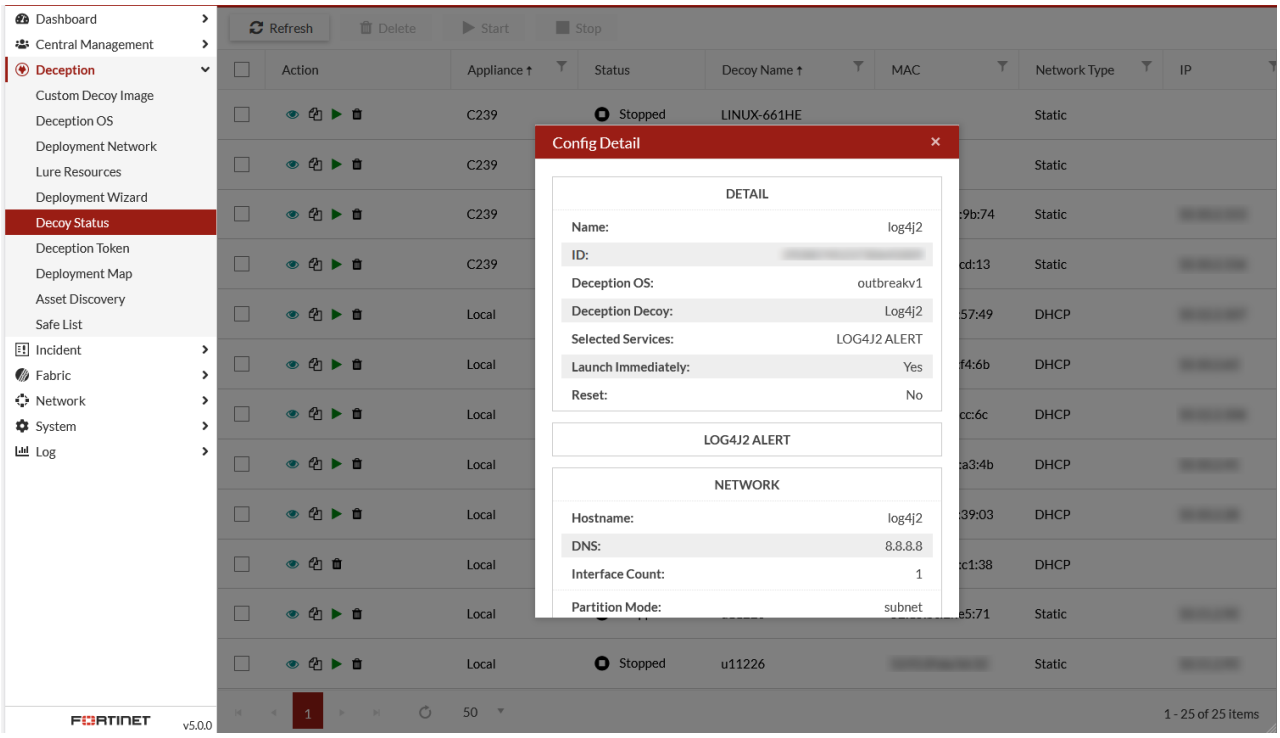


For more information about configuring deployment, see Deployment Wizard on page 72.

4. Continue to follow the steps in the Deployment Wizard and then click *Deploy*.

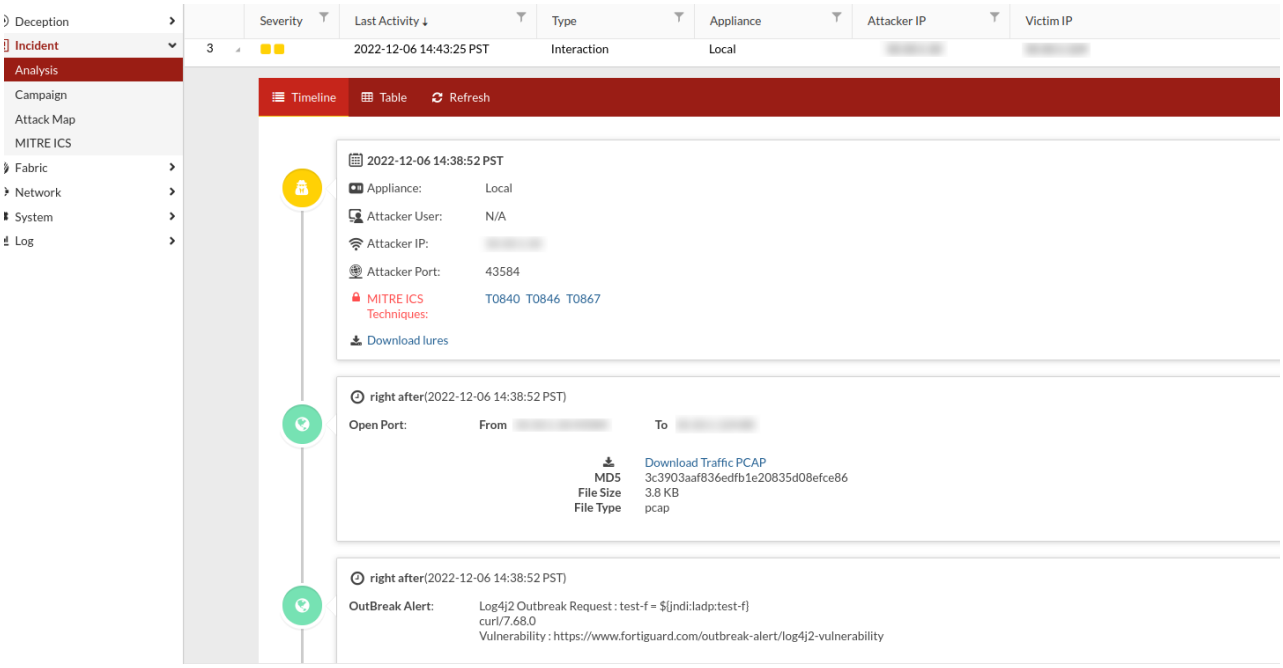


5. Go to *Deception* > *Decoy Status* to verify the decoy is running and configured correctly.



6. Run a simulated attack with the Log4j2 traffic pattern from an endpoint machine located within same deployment network as the outbreak decoy. For example, `curl -X POST http://10.10.1.124/login -F "test-f=\${jndi:ladp:test-f}"`

7. Go to *Incident* > *Analysis* to verify the attack results.



FortiDeceptor platform

The FortiDeceptor platform includes the following:

- FortiDeceptor components on page 167
- FortiDeceptor Token Package on page 167
- FortiDeceptor decoys on page 168

FortiDeceptor components

The FortiDeceptor platform includes the following components:

- The FortiDeceptor management console manages and operates the whole platform including deployment, configuration, alerting, analysis, and ECO system integration.
- FortiDeceptor offers a highly-scalable three-tier architecture that combines three levels of deception:
  - Server / endpoint lures.
  - Medium interaction decoys (IoT / OT).
  - High interaction decoys.

You can deploy deception lures using existing infrastructure tools such as A/D GPO, MS SCCM, and so on.

A single FortiDeceptor appliance can run up to 16 deception VMs that support a total of 256 IP addresses. Each IP address represents a single decoy.

You can download a deception VM from the FortiDeceptor marketplace. You can also allow the end user admin bring their own gold image and convert it to a decoy using the FortiDeceptor decoy customization wizard.

FortiDeceptor Token Package

The FortiDeceptor Token package adds breadcrumbs on real endpoints and servers, and redirects an attacker to engage with a decoy instead of a real asset. Deception tokens are typically distributed within real endpoints and servers on the network to expand the deception surface.

Effective deception lure technology should support the following:

- Deploy deception lure data and configurations where attackers collect information.
- Deception lure location must be invisible to end users, and doesn't affect endpoint functionality.
- Deception lure is accessible with user level permissions so that attackers can access it early on and get detected. This saves the privileged escalation attack time.

The current FortiDeceptor token packages are:

Windows	• Cached Credential • HoneyDocs • Network Connection (static MAC address) • ODBC • RDP • SMB
Linux	• RDP (xfreerdp)

	• SMB (SAMBA) • SSH
MAC	• RDP (xfreerdp) • SMB (SAMBA) • SSH
SAP	• SAP
AWS Key	• AWS Keys
Azure Key	• Azure Keys

When the FortiDeceptor token package is installed on a real Windows, Linux, or MAC endpoint, it increases the deception surface and redirects an attacker to engage with a decoy instead of a real asset.

FortiDeceptor decoys

FortiDeceptor creates a network of decoys to lure attackers and monitor their activities on the network. When a hacker attacks a decoy, an alert is generated and their malicious activities are captured and analyzed in real-time. This analysis generates a mitigation and remediation response that protects the network.

The current FortiDeceptor decoy OS are:

Windows	Windows 7, Windows 10, Windows 10ltsc2021v1
Linux	Ubuntu Desktop, CentOS, ESXi and ELK
IoT/OT	SCADA version 3, Medical OS, IoT OS, and d VoIP version1.
VPN	Fortinet SSL-VPN (FG-60E, FG-100F, FG-1500D, FG-2000E, FG-3700D)
Customized Windows	Windows 10, Windows 11, Windows Server 2016, Windows Sever 2019, Windows Sever 2022, French Windows 10, French Windows Server 2016

The current FortiDeceptor application decoys are:

Application Decoys	POS OS, ERP OS PACS and SAP

The current FortiDeceptor lure services are:

Windows	RDP, SMB, TCPListener, NBNSSpoofSpotter, ICMP, FTP, SMTP, SWIFT Lite2. Does not contain (Windows 7.
Linux	SSH, SAMBA, TCPListener, HTTP, HTTPS, GIT, ICMP and FTP

IoT/OT	HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, ENIP, Kamstrup, DNP3, Telnet, PACS-WEB, PACS, DICOM server, Infusion Pump (TELNET), Infusion Pump (FTP), POS-WEB, ERP-WEP, GUARDIAN-AST, IEC104, Jetdirect, Printer-WEB, IP Camera-WEB, UPnP, RTSP, CDP, TP-link WEB, CWMP, SAP DISPATCHER, SAP WEB, MOXA, MQTT WEB, CoAP, SIP, and XMPP WEB
SSL VPN	HTTPS
Customized Windows	RDP, SMB, NBNSSpoofSpotter, MSSQL, IIS (HTTP/HTTPS), ICMP, TCPListener, SMTP, SWIFT Lite2 and FTP

The current FortiDeceptor IP address capacity are:

- A single EOL can host up to 16 deception VMs.
- A single FDCIKG can host up to 20 deception VMs.
- A single FDCVMS can host up to 20 deception VMs.
- A single deception VM supports up to 24 IP addresses or decoys. Each IP represents a decoy.
- A single FortiDeceptor appliance (HW/VM) can support up to 480 IP addresses.
- A single FortiDeceptor appliance (HW/VM) can support up to 128 segments (VLANS).

VPN only supports 8 IPs.
Cisco Decoy only supports 1VLAN.

Decoy services details

- IoT OS on page 169
- Medical on page 172
- POS on page 172
- CRM(ERP) on page 172
- SAP on page 172
- SCADA
- VOIP V1 OS on page 179

IoT OS

Brother MFC Printer Decoy

Service	Description
SNMP	• Enable this service to open port 161 on the decoy VM, and respond to SNMP (v1 or v2c) request from within the network. • Community name is user-defined. • SNMP response is customized for Brother MFC Printer decoy.

Service	Description
Jetdirect	Enable this service to open port 9100 on the decoy VM and respond to PJL (Printer Job Language) requests.
Printer-WEB	A web GUI that simulates the administration GUI of Brother NC-340h printer.

Cisco router decoy

Service	Description
Models*	4 Cisco images (models) are supported: 2691, 3660, 3725 and 3745. An error is displayed if you upload an image that is not supported.
Router Running-Config (optional)	Allows you to upload a customized Cisco *config* file to predefine the Cisco router setting
Telnet service	A login-required service that enables attackers to utilize all Cisco router functions.
HTTP service	A login-required GUI service similar to the telnet service but with less functionality.
SNMP service	• Enable this service to open port 161 on the decoy VM, and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for Cisco router decoy.
CDP service	Enable this service to allow the decoy VM to send CDP traffic within the network.

*Please provide Cisco IOS software to run the Cisco decoy. You can copy the IOS from any Cisco router/switch flash by using TFTP server and running the `copy flash tftp:` command on the Cisco router/switch side, and then completing the deployment wizard.

HP printer decoy

Service	Description
SNMP service	• Enable this service to open port 161 on the decoy VM, and respond to SNMP (v1 or v2c) requests from within network • Community name is user-defined • SNMP response is customized for HP printer decoy.
Jetdirect	• Enable this service to open port 9100 on the decoy VM, and respond to PJL (Printer Job Language) requests.
Printer-WEB	• A web GUI that simulates the administration GUI of HP Officejet Pro X451dw printer.

IP camera decoy

Service	Description
IP Camera-WEB	• A login-required service that displays videos to simulate IP cameras. Default

Service	Description
	videos are available. However, we strongly recommend uploading 1-8 *.mp4* videos that fit best with the working environment.
SNMP service	• Enable this service to open port 161 on the decoy VM, and respond to SNMP (v1 or v2c) requests from within the network • Community name is user-defined. • SNMP response is customized for IP camera decoy.
UPnP service	• Enable this service to open port 8080 on the decoy VM and simulate UPnP service. • A UPnP msg will broadcast within the network. Within the msg there is a URL for the attacker to download a *.xml* file showing device information.
RTSP service	• When this service is enabled, you will also need to upload a video to a predefined location so the attacker can watch the video. • The RTSP port can be adjusted. • To upload the video, you can use *ffmpeg*, or any other method to infinitely loop a video so it is available to the attacker **Example:** To infinitely loop a video:`sudo ffmpeg -re -stream_loop -1 -i {path_to_local_video} -c copy -f rtsp rtsp://{ip}:{port}/{name_you_choose};` From the attacker perspective, the live camera stream is available at `rtsp://{ip}:{port}/{name_you_choose}`

Lexmark Printer decoy

Service	Description
SNMP	• Enable this service to open port 161 on decoy VM, and respond to SNMP(v1 or v2c) request from within the network. • Community name is user-defined. • SNMP response is customized for Lexmark Printer decoy
Jetdirect	Enable this service to open port 9100 on the decoy VM and respond to PJL (Printer Job Language) requests.
Printer-WEB	A web GUI that simulates the administration GUI of Lexmark MX410de printer.

TP-LINK decoy

Service	Description
TP-LINK WEB	Enable this service to allow attackers to login to a fake TP-link setting site.
CWMP	Enable this service to send data using CWMP protocol to *{ip}:{port}/cpe*.

Medical

Service	Description
Infusion Pump (Telnet) service	• Simulates Infusion Pump (telnet) • A username/password is required to login.
Infusion Pump (FTP)	• Simulates Infusion Pump (FTP) • A username/password is required to login.
PACS service	• A user-defined name for the PACS system.
PACS-WEB service	• Login-required web GUI for PACS, with existing medical data • Port can be adjusted
DICOM Server service	• Server port can be adjusted • Server name can be adjusted • DICOM operations (e.g. C-STORE, C-FIND) are supported
B. Braun Infusomat service	• HTTP/S: Built-in web services to retrieve medical data • CAN Bus Protocol (enable/disable) • B.BRAUN (port 8080): Login-required web GUI for the B.Braun Infusomat device

POS

Service	Description
POS-WEB service	• Login-required web GUI simulate POS website • Port can be adjusted

CRM(ERP)

Service	Description
ERP-WEB service	• Login-required web GUI simulates ERP website • Port can be adjusted

SAP

Service	Description
SAP ROUTER	• Enable SAP ROUTER Service so SAP Logon can configure the SAProuter String. • Use the default port to ensure SAP Logon can connect.
SAP DISPATCHER	• Enable SAP DISPATCHER so SAP Logon can get responses from the SAP decoy.

Service	Description
	• Use the default port to ensure SAP Logon can connect.
SAP WEB	A fake SAP HTTP and HTTPS GUI for SAP Fiori Launchpad or Legacy WebGUI.

SCADA (version3) OS

Ascent Compass MNG decoy

Service	Description
HTTP service	• Enable this service to capture attacks through HTTP on the default HTTP port.
FTP service	• Enable this service to capture attacks through FTP on the default FTP port • FTP banner is user-defined.
SNMP service	• Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) request from within the network • Community name is user-defined • SNMP response is customized for Ascent Compass MNG decoy.
BACNET service	• Enable this service to capture attacks through BACNET on the default BACNET port.

Guardian-AST decoy

Service	Description
Guardian-AST service	• Enable this service to simulate an AST's satellite communications remote asset tracking system named *Guardian*. • To deploy a Guardian-AST decoy, this service must be enabled since it is the only service available

IPMI Device decoy

Service	Description
HTTP service	• Enable this service to capture attacks through HTTP on the default HTTP port.
SNMP service	• Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for IPMI Device decoy.
FTP service	• Enable this service to capture attacks through FTP on the default FTP port. • FTP banner is user-defined.
IPMI service	• Enable this service to capture attack through IPMI on the default IPMI port.

KAMSTRUP 382 decoy

Service	Description
KAMSTRUP service	• Toggle to enable/disable this service. Enable this service to simulate a Kamstrup device • To deploy a KAMSTRUP decoy, this service must be enabled since it is the only service available

Liebert Spruce UPS decoy

Service	Description
TFTP	Enable this to service capture attacks through TFTP on default TFTP port
SNMP	• Enable this service to open port 161 on decoy VM and respond to SNMP(v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for Liebert Spruce UPS decoy.
HTTP	Enable this service to capture attacks through HTTP on default HTTP port.

Niagara4 Station decoy

Service	Description
SNMP	• Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for IPMI Device decoy.
HTTP	Enable this service to capture attacks through HTTP on default HTTP port.
BACNET	Enable this service to capture attack through BACNET on default BACNET port.

NiagaraAX Station decoy

Service	Description
SNMP	• Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for IPMI Device decoy.
HTTP	Enable this service to capture attacks through HTTP on the default HTTP port.
BACNET	Enable this service to capture attacks through BACNET on the default BACNET port.

PowerLogic ION7650 decoy

Service	Description
SNMP	• Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for PowerLogic ION7650 decoy.
MODBUS	Enable this service to capture attacks through MODBUS on the default MODBUS port.
DNP3	Enable this service to capture attacks through DNP3 on the default DNP3 port.
HTTP	Enable this service to capture attacks through HTTP on the default HTTP port.

Rockwell 1769-L16ER/BLOGIX5316ER decoy

Service	Description
SNMP	• Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for Rockwell 1769-L16ER/B LOGIX5316ER decoy.
ENIP	Enable this service to capture attacks through ENIP on the default ENIP port.
HTTP	Enable this service to capture attacks through HTTP on the default HTTP port.

Rockwell 1769-L35E Ethernet Port decoy

Service	Description
SNMP	• Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for Rockwell 1769-L35E Ethernet Port decoy.
ENIP	Enable this service to capture attacks through ENIP on the default ENIP port.
HTTP	Enable this service to capture attacks through HTTP on the default HTTP port.

Rockwell PLC decoy

Service	Description
HTTP service	• Enable s this service capture attack through HTTP on the default HTTP port. • HTTP page title is user defined.
TFTP service	• Enable this service to capture attacks through TFTP on the default TFTP

Service	Description
	port.
SNMP service	• Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) request from within the network. • Community name is user-defined. • SNMP response is customized for Siemens Rockwell PLC decoy.
ENIP service	• Enable this service to capture attack through ENIP on the default ENIP port. • ENIP serial number is user-defined.

GE PLC decoy

Service	Description
HTTP service	• Enable this service to capture attacks through HTTP on the default HTTP port. • HTTP page title is user defined.
TFTP service	• Enable this service to capture attacks through TFTP on the default TFTP port.
SNMP service	• Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) request from within the network. • Community name is user-defined. • SNMP response is customized for GE PLC decoy.
ENIP service	• Enable this service to capture attacks through ENIP on the default ENIP port. • ENIP serial number is user-defined.

Schneider EcoStruxure BMS server decoy

Service	Description
SNMP service	• Enable this service to open port 161 on decoy VM and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for Schneider EcoStruxure BMS server decoy.
BACNET service	• Enable this service to capture attacks through BACNET on the default BACNET port.
HTTP service	• Enable this service to capture attacks through HTTP on the default HTTP port.
TRICONEX service	• Enable this service to capture attacks with the TRICONEX service.

MOXA NPORT 5110 decoy

Service	Description
SNMP service	• Enable this service to open port 161 on decoy VM and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for moxa nport 5110 decoy.
Telnet service	• Login-required telnet service simulates moxa nport 5110 command line environment. • Two command choices: 1 and 2
HTTP service	• Enable this service to capture attacks through HTTP on the default HTTP port.
MOXA service	• Download MOXA script from GitHub is required (https://github.com/Z-0ne/MoxaNportScan)

Schneider Power Meter - PM5560 decoy

Service	Description
SNMP service	• Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network • Community name is user-defined. • SNMP response is customized for Schneider Power Meter - PM5560 decoy.
BACNET service	• Enable this service to capture attacks through BACNET on the default BACNET port.
HTTP service	• Enable this service to capture attacks through HTTP on default HTTP port.
DNP3 service	• Enable this service to capture attacks through DNP3 on the default DNP3 port.
ENIP service	• Enable this service to capture attacks through ENIP on the default ENIP port.

Schneider SCADAPack 333E decoy

Service	Description
SNMP service	• Enable this service to open port 161 on decoy VM, and respond to SNMP(v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for Schneider SCADAPack 333E decoy.
DNP3 service	• Enable this service to capture attacks through DNP3.
Telnet service	• Login-required telnet service simulates SCADAPack E Smart RTU command line environment.

Siemens S7-200 PLC decoy

Service	Description
HTTP service	• Enable this service to capture attacks through HTTP on the default HTTP port. • HTTP page title is user defined. • Plant Identification is user-defined. • Serial Number is user-defined.
TFTP service	• Enable this to service capture attacks through TFTP on the default TFTP port.
SNMP service	• Enable this service to open port 161 on decoy VM, and respond to SNMP(v1 or v2c) request from within the network. • Community name is user-defined. • SNMP response is customized for Siemens S7-200 PLC decoy.
MODBUS service	• Enable this service to capture attacks through MODBUS on the default MODBUS port.
S7COMM service	• Enable this service to capture attacks through S7COMM on the default S7COMM port. • Module Type is user-defined. • PLC Name is user-defined.

Siemens S7-300 PLC decoy

TFTP service	• Enable this service to capture attacks through TFTP on the default TFTP port.
SNMP service	• Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for Siemens S7-300 PLC decoy.
IEC104 service	• Enable this service to capture attacks through IEC104 on the default IEC104 port.

Siemens S7-1500 PLC decoy

Service	Description
HTTP service	Enable this service to capture attacks through HTTP on the default HTTP port. HTTP page title is user defined. Plant Identification is user-defined. Serial Number is user-defined.
TFTP service	Enable this to service capture attacks through TFTP on the default TFTP port
IEC104 service	Enable this to service capture attacks through IEC104 on the default IEC104 port.

Service	Description
SNMP service	Enable this service to open port 161 on decoy VM, and respond to SNMP (v1 or v2c) request from within the network. Community name is user-defined. SNMP response is customized for Siemens S7-1500 PLC decoy.
S7COMM service	Enable this service to capture attacks through S7COMM on the default S7COMM port. Module Type is user-defined. PLC Name is user-defined.
PROFINET service	Enable this service to capture attacks through PROFINET

Phoenix contact AXC 1050 decoy

Service	Description
HTTP service	Enable this service to capture attacks through HTTP on the default HTTP port. HTTP page title is user defined. Plant Identification is user-defined. Serial Number is user-defined.
SNMP service	Enable this service to open port 161 on decoy VM, and respond to SNMP (v1 or v2c) request from within the network. Community name is user-defined. SNMP response is customized for Phoenix contact AXC 1050 decoy.
FTP service	Enable this service to capture attacks through FTP on the default FTP port FTP banner is user-defined Anonymous Access can be enabled which let user enters "anonymous" as a user ID and eliminate the need to authenticate themselves
PROFINET service	Enable this service to capture attacks through PROFINET

VAV-DD BACNET controller decoy

Service	Description
SNMP service	• Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for VAV-DD BACNET controller decoy.
BACNET service	• Enable this service to capture attacks through BACNET on the default BACNET port.

VOIP V1 OS

MQTT decoy

Service	Description
MQTT WEB	• Enable this service to capture attacks through MQTT WEB on the default MQTT WEB port. • Supports custom listening port. Default port is 18083. • Supports adding User/Password.

Service	Description
CoAP	• Enable this to service capture attacks through CoAP on the default CoAP port. • Download `libcoap` from GitHub is required. Go to https://github.com/miri64/libcoap and follow the command `libcoap` command rule.

SIP decoy

Service	Description
SIP	• Enable this service to capture attacks through MQTT WEB on the default SIP port. • Supports adding User/Password. • Users can connect to the SIP server from SIP client service (like Linphone) through UDP or TCP, and register an account, text message, voice call, and video call each other.

XMPP decoy

Service	Description
XMPP WEB	• Enable this service to capture attacks through XMPP WEB on the default XMPP WEB port. • Supports custom listening port (default port is 5280). • Supports adding User/Password. • Can be reached through HTTP.

Deploying deception

To deploy FortiDeceptor to optimize the deception surface, see the following best practices.

Deception decoy best practices on page 180

Deception token best practices on page 184

AD integration best practices on page 185

Deployment best practices checklist on page 186

Network topology best practices on page 187

Deception decoy best practices

Deception effectiveness requires deployment across all network segments and locations.

This topic provides deception deployment best practices for the decoy layer, including deployment guidelines for each kind of network VLAN that can exist on an enterprise network.

Example of 5-8 decoys per data-center segment (VLAN)

OS

Deploy a matching decoy OS for each type of critical / sensitive IT system in this segment.

Services

Enable matching services for each type of critical / sensitive IT system in this segment and customize the services:

- Apply banner matching the network.
- Apply user access rule such as fake user and password.
- Upload fake data (SMB, FTP, HTTP).

If you do not have out-of-the-box matching services, you can use the custom TCP port listener.

Data

Upload fake data to the decoys to provide authentic engagement. If you do not have matching files, ask the customer to provide a public files package that you can upload and generate fake data using the same structure.

Application

Enable a false matching application for each type of critical / sensitive IT system on this segment If you do not have a matching application, enable high profile fake applications like ERP, POS, or PACS, and so on.

Hostname

Follow corporate standard server's names for half the decoys and assign enticing names to the remaining half, such as JumpHost001, ERP-XXX, MNG-XXX, Net-Monitor, and so on. Remember that we need to configure these hostnames on the AD level as we use single deception VM across 16 IP address and we can have just one real hostname per OS. For the rest of the IP address, we should have it virtual on the DNS level.

Attackers also like to attack servers with a hostname that has names like "-test" or "-dev" as attackers assume that these servers are less protected.

Gold Image

Ensure you use at least two Windows servers as customer gold images that host critical applications and data. To increase authenticity, configure them to be part of the organization domain.

STATIC / DHCP IP Address

For datacenter segment hosting servers that always use static IP addresses, also use static IP configuration for the decoys.

Example of 2-4 decoys per endpoint segment (VLAN)

OS

Deploy a matching decoy OS and also an “old’ OS like Win7.

Services

Enable matching services for the endpoint on this segment.

If you do not have out-of-the-box matching services, you can use the custom TCP port listener.

Data

Upload fake data to the decoys to provide authentic engagement. If you do not have matching files, ask the customer to provide a public files package that you can upload and generate fake data using the same structure.

Hostname

Follow corporate standard server’s names for half the decoys and assign enticing names to the remaining half, such as IT Admin, HelpDesk, DBA, Finance, and so on. Remember that we need to configure these hostnames on the AD level as we use single deception VM across 16 IP address and we can have just one real hostname per OS. For the rest of the IP address, we should have it virtual on the DNS level.

Gold Image

Ensure you use at least 3–4 Windows servers as customer gold images. To increase authenticity, configure them to be part of the organization domain.

STATIC / DHCP IP Address

For endpoints segment hosting desktops that always use DHCP IP addresses, also use the DHCP IP configuration for the decoys. The DHCP configuration in FortiDeceptor 3.1 and 3.2 allows us to configure one IP per segment, so use the static configuration in this stage to have more decoys per segment.

Example of 7-10 decoys per OT segment (VLAN)

OS

Deploy a matching decoy SCADA OS.

Deploy a matching regular IT OS such as Win7, Win10, or Win2016.

Services

Enable matching services for the OT assets on this segment and customize the services.

- Apply banner matching the network.
- Apply access rule such as fake user and password.
- Upload fake data (SMB, FTP, HTTP).

If you do not have out-of-the-box matching services, you can use the custom TCP port listener.

Data

Upload fake data to the decoys to provide authentic engagement. If you do not have matching files, ask the customer to provide a public files package that you can upload and generate fake data using the same structure. You can also use a search engine like SHODAN.IO to find this data on the Internet and use it to customize the decoys.

Hostname

Follow the OS SCADA names for half the decoys and assign enticing names to the remaining half, such as IT Admin, SCADA-MNG, PLC_ADMIN, HMI_SERVER, NET-MONITOR, and so on.

Application

Check if the customer is willing to provide you access to his OT software. Otherwise, use open-source OT software or use the customize decoy option to generate this kind of decoy.

MAC ADDRESS

Ensure the OT decoy uses the appropriate MAC ADDRESS per vendor.

STATIC / DHCP IP Address

OT networks are mainly a static environment that does not has a DHCP server, so use static IP configuration as well for the decoys.

Example of 8-10 decoys per cloud segment (VPC, VNET)

OS

Deploy a matching decoy OS for each type of critical / sensitive IT system in this segment.

Services

Enable matching services for each type of critical / sensitive IT system in this segment and customize the services:

- Apply banner matching the network.
- Apply user access rule such as fake user and password.
- Upload fake data (SMB, FTP, HTTP).

If you do not have out-of-the-box matching services, you can use the custom TCP port listener.

Data

Upload fake data to the decoys to provide authentic engagement. If you do not have matching files, ask the customer to provide a public files package that you can upload and generate fake data using the same structure.

Application

Enable a false matching application for each type of critical / sensitive IT system on this segment. If you do not have a matching application, enable high profile fake applications like ERP, POS, or PACS, and so on.

Hostname

Follow corporate standard server's names for half the decoys and assign enticing names to the remaining half, such as JumpHost001, WEB-XXX, DB-XXX, Sec-Monitor, and so on. Remember that we need to configure these hostnames on the AD level as we use single deception VM across 16 IP address and we can have just one real hostname per OS. For the rest of the IP address, we should have it virtual on the DNS level.

Attackers also like to attack servers with a hostname that has names like "-test" or "-dev" as attackers assume that these servers are less protected.

Gold Image

Ensure you use at least two Windows servers as customer gold images that host critical applications and data. To increase authenticity, configure them to be part of the organization domain.

STATIC / DHCP IP Address

Cloud environments mainly host servers that always use static IP addresses, so use static IPs configuration as well for the decoys.

Deception token best practices

Deception effectiveness requires deployment across all managed endpoints and servers.

This topic provides deception deployment best practices for the deception token layer. For token deployment over AD logon script, see appendix A.

Example of deception tokens on Windows, MAC, or Linux endpoint segment (VLAN)

RDP token

- Set up several Windows server decoys that support RDP access.
- Set up appropriate decoy hostnames like Terminal-XX, VDI-XX, and so on. This increases the level of authenticity when you add the Windows server decoys to the company domain.
- Follow company username and password policy.
- Generate 2-3 deception lures and deploy them over several different AD user groups.

SMB token

For Windows endpoints, use either SMB token or SAMBA token. Do not use both.

- Set up at least two Windows server decoys that support two fake network share access.
- Generate at least two tokens with two different share names.
- Use a share name similar to the company structure.
- Set up appropriate hostnames like FileSRV-XX, File-Server, and so on. This increases the level of authenticity when you add the Windows server decoy to the company domain.
- Follow company username and password policy.
- Generate a single deception token package and deploy it over all the network endpoints.

SAMBA token

For Windows endpoints, use either SMB lure or SAMBA token. Do not use both.

- Set up at least two Linux server decoys that support network share access.
- Set up appropriate hostnames like Storage-XX, Backup-Server, and so on.
- Generate at least two tokens with two different share names.
- Use a share name similar to the company structure.
- Follow company username and password policy.
- Generate a single deception token package and deploy it over all the network endpoints.

SSH lure

- Set up several Linux server decoys that support SSH access.
- Set up appropriate hostnames like JumpHost-XX, Control-XX, Cloud-XXX, and so on.
- Use a complicated password. This gives the attacker the impression that this is a critical server.
- Generate 2-3 deception tokens and deploy them over the IT endpoints group only. Attackers do not expect to see SSH clients on a regular desktop.

AD integration best practices

Active Directory (AD) is Microsoft's proprietary directory service. It runs on Windows Server and allows administrators to manage permissions and access to network resources. Active Directory stores data as objects. An object is a single element, such as a user, group, application; or device, such as a printer.

To detect AD attack using deception technology, use the following deception configuration example.

- Deploy custom Windows decoys (Windows 10, Windows 11, Windows Server 2016, Windows Sever 2019, Windows Sever 2022, French Windows 10, French Windows Server 2016) and add them to the customer network domain.

Example of custom decoys in customer network domain

- Add several custom Windows decoys to the customer network domain.
- On the Windows domain, configure schedule task scripts to run using the fake users, such as the one from the cache credentials lure.
- Add to each domain decoy the maximum number of IP addresses and ensure they are static IP addresses.
- On the network DNS server, configure a decoy DNS.
  - Add DNS records to each decoy IP address.
  - Set up attractive hostnames for each decoy IP address. For more information, see Deception decoy best practices on page 180.
- Deploy the SMB lure front in a domain decoy to avoid detection by tools like HoneyBuster.

Deployment best practices checklist

This checklist is an example of a deception deployment profiling and sizing. This example is based on a company with one headquarters (HQ) site and two remote sites, one of which is a manufacturing site.

Deception Items	Customer Requirements	Deployment
FortiDeceptor appliance HW/VM	VM	The VM supports VMware, Hyper-V or KVM.
HQ site installation	Yes	Deploy on the company ESXi where you have access to most of the network VLANs.
Number of remote sites	2	If the primary and remote locations are connected by FortiGate firewall, configure the VXLAN tunnel between firewalls to publish decoys over the L2 tunnel from the HQ to the remote sites. For details on setting up the VXLAN, see https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD47325&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=163742631&stateId=1%200%20163740760%27. If the firewalls are different, check with Customer Support on how to configure an L2 Tunnel.
Remote sites are office / OT network	1 remote office + 1 manufacture site	For remote office site, deploy Windows / Linux desktop decoys and deception lures like SMB, RDP and cache credentials. For remote OT site, deploy Windows / Linux and SCADA decoys.
Number of segments (VLANS) to cover	30	
Number of DC segments to cover	2	Deploy Windows / Linux server decoys.
Customer's server OS	Windows, Linux	Deploy Windows / Linux server decoys.
Critical services in the DC segments	SAP, web logistic app	Deploy ERP decoy, Windows decoy with a web app.
Number of endpoint segments to cover	25	Deploy Windows / Linux desktop decoys.
Customer's endpoint OS	Windows, MAC	Deploy deception lures such as SMB, RDP, and cache credentials for both Windows and MAC.

Deception Items	Customer Requirements	Deployment
Customer's most important asset to protect	SAP	Deploy Windows decoy with SQL that uses SAP fake data.
Attack vectors customer is facing	Phishing, PTH, lateral movement based on AD	Deploy deception lures like SMB, RDP, and cache credentials. Follow cache credentials best practice.
Customer network's IoT devices	Printer, camera, temp sensors	
Customer network's OT devices	SCADA PLC, HMI	Deploy Windows / Linux and SCADA decoys.
Customer FortiGate firewall solution	Yes	Configure Security Fabric integration for isolation mitigation response.
Customer SIEM solution	Yes	Send SYSLOG from the FDC. Configure a correlation rule to detect lateral movement based on cache credentials lure.

Network topology best practices

For effective deception, you must also understand the customer's network topology, company security risks, where his most important assets are located, and what kind of attack vectors they face or have concerns.

Several common network topologies require different deception deployment approaches.

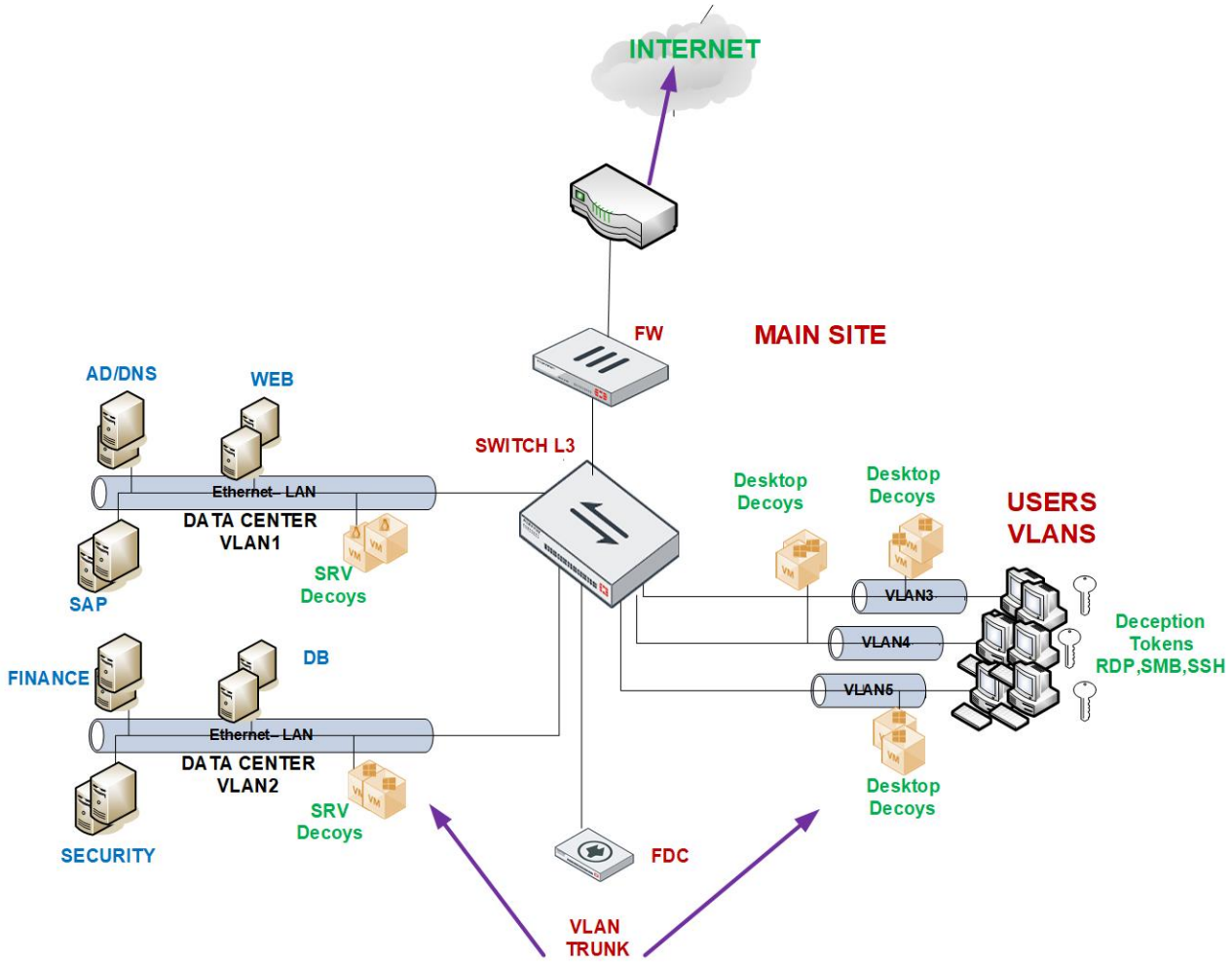
This topic provides best practices for the following scenarios:

1. Network with data center and users at the same location.
2. Network with a data center, users at the same location, and users at remote offices.
3. Network with a data center, users at the same location, users at remote offices, and remote OT sites.

Deception deployment in HQ only

A network topology without remote location is less common today. The reasoning might be that the most important assets are in HQ only and there is no need to deploy deception in remote sites.

This scenarios shows deploying deception in the main HQ only even if there are also remote locations.

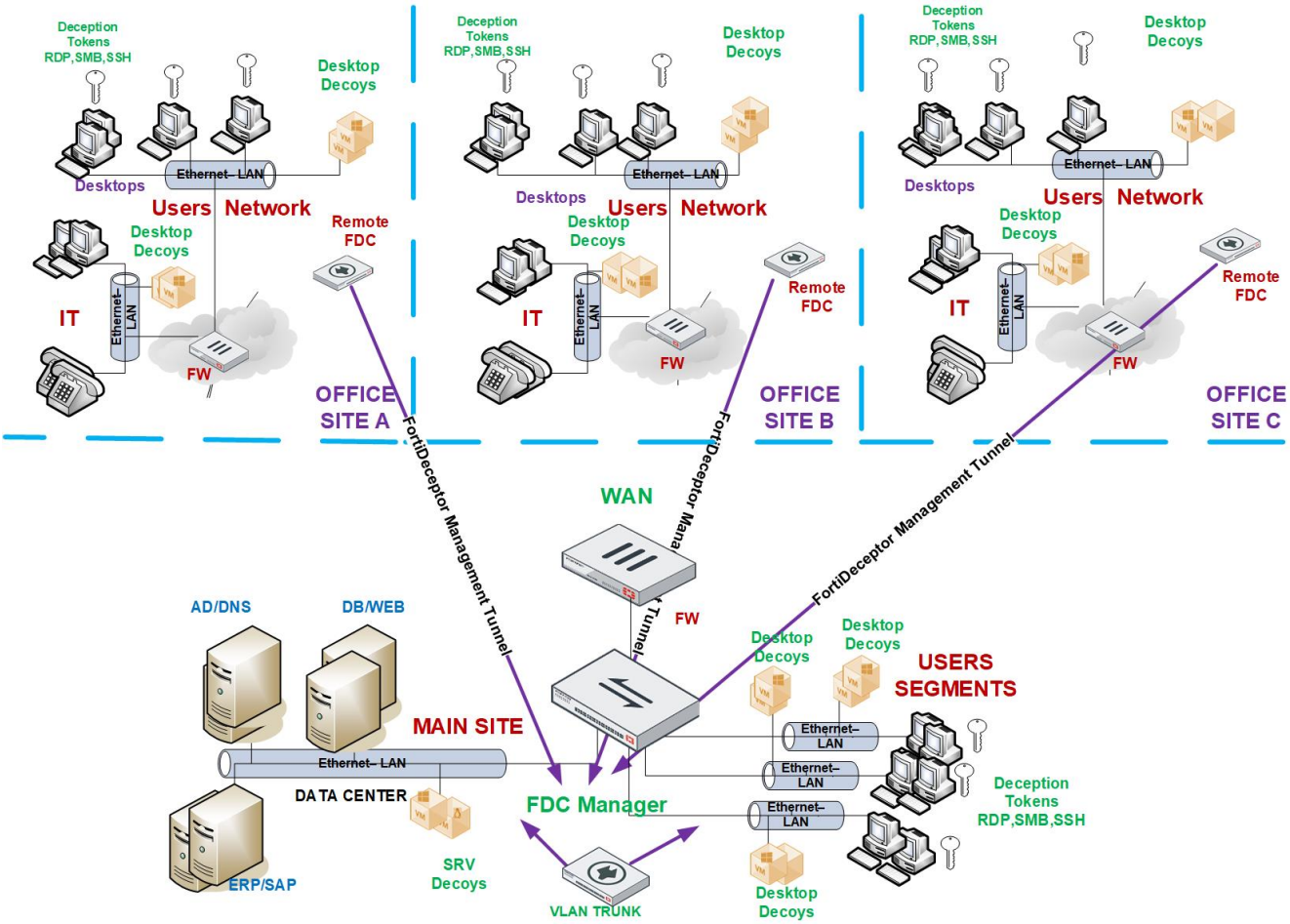


In this scenario, follow these best practice recommendations:

Deception deployment in HQ and remote offices

Network topology with remote locations is the most common enterprise network topology for installations that want to provide the same security protection across all sites.

The level of connectivity required by remote office users is broader and will lead to a data breach if the security level is not similar to the HQ security.



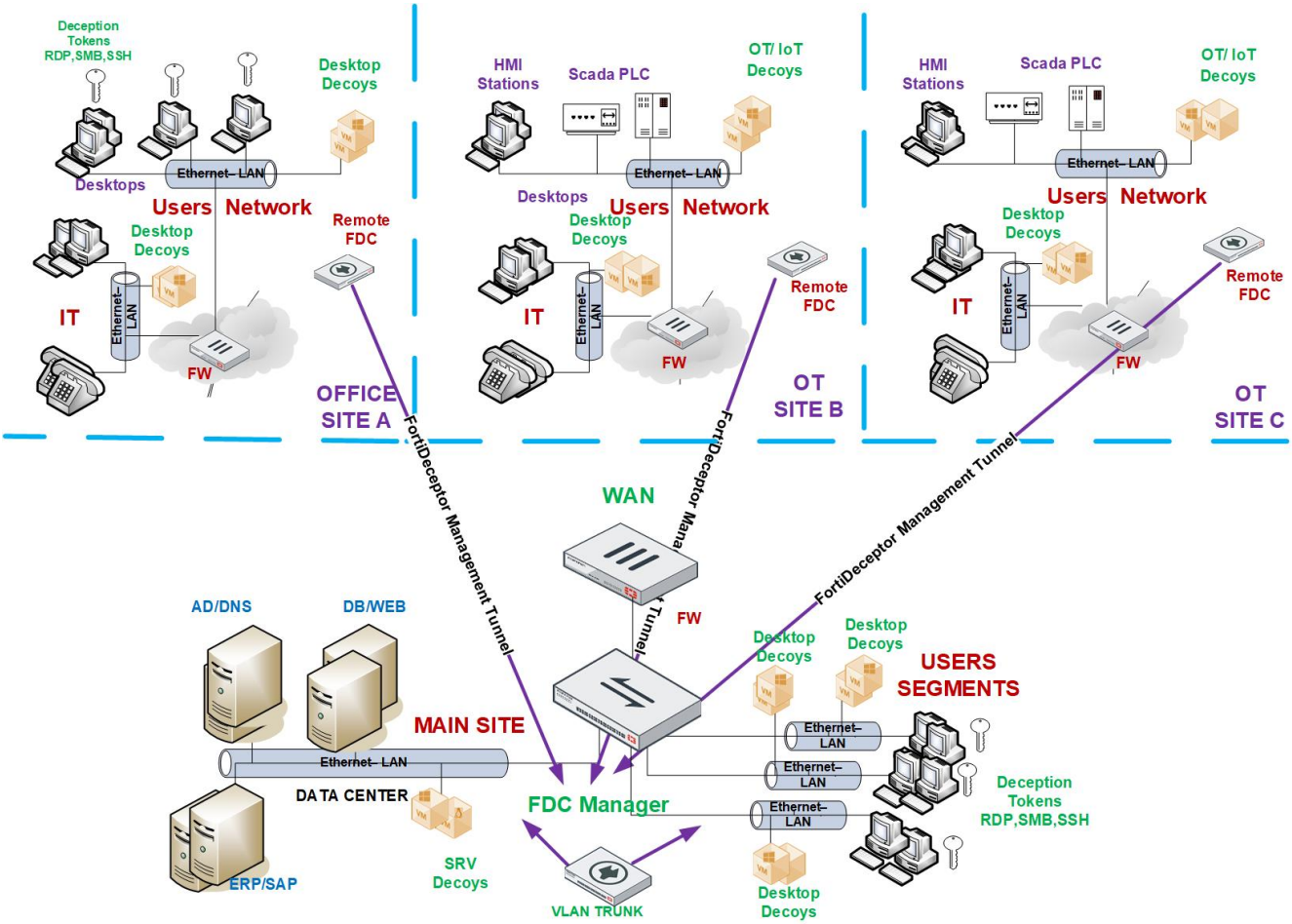
In this scenario, follow these best practice recommendations:

- Deploy a single FortiDeceptor appliance and connect it to the network via trunk to cover most of the HQ network VLANs.
- Deploy decoys following the best practice recommendation in Deception decoy best practices on page 180.
  - On data center VLANs: 5-7 decoys per VLAN.
  - On endpoint VLANs: 2-4 decoys per VLAN.
  - Deploy deception lures across all manageable endpoints even if some of them are in remote sites.
    - RDP
    - SMB
    - Cached credentials
    - HoneyDocs
    - SSH (on IT department desktops only)

- Fabric integration.
  - If you have FortiGate, consider the integration value between FortiDeceptor and FortiGate for alert mitigation by isolating the infected machine.
  - Send SYSLOG to SIEM or any logger solution in place.
  - Send SYSLOG to SOAR solution for Deception playbooks. For example, FortiSOAR has pre-built deception playbooks for FortiDeceptor.

Deception deployment in HQ, remote offices, and OT sites

Network topology with remote location (offices + OT sites) is very common for manufacturing, critical infrastructure, and energy companies. The OT site presents a security challenge due to its environmental complexity, such as legacy OSes, non-standard devices and protocols, and so on.



In this scenario, follow these best practice recommendations:

- Deploy a single FortiDeceptor appliance and connect it to the network via trunk to cover most of the HQ network VLANs.
- Deploy decoys following the best practice recommendation in Deception decoy best practices on page 180.
  - On data center VLANs: 5-7 decoys per VLAN.
  - On endpoint VLANs: 2-4 decoys per VLAN.

    - Deploy deception lures across all manageable endpoints even if some of them are in remote sites.
        - RDP
        - SMB
        - Cached credentials
        - HoneyDocs
        - SSH (on IT department desktops only)
- Fabric integration.
    - If you have FortiGate, consider the integration value between FortiDeceptor and FortiGate for alert mitigation by isolating the infected machine.
    - Send SYSLOG to SIEM or any logger solution in place.
    - Send SYSLOG to SOAR solution for Deception playbooks. For example, FortiSOAR has pre-built deception playbooks for FortiDeceptor.

Attack vectors vs deception

This section shows the best practices for attack vectors vs deception.

Compromised internal endpoint using lateral movement on page 191

Lateral movement based on AD mapping on page 193

Lateral movement based on Mimikatz / PTH on page 194

Compromised internal endpoint using lateral movement

This scenario shows a human attacker trying to compromise an internal endpoint using lateral movements.

Attack vector scenario

An attacker uses a phishing email to compromise the internal user and get access to an internal endpoint.

The attacker then explores the compromised endpoint and collect intelligence on the network before running any privileged escalation or lateral movement.

Attacker's possible first steps on the compromised endpoint:

- Use network commands to understand the network environment and the endpoint location, such as getting information on critical servers and sensitive application locations.
- Access the local / network drive to find information like sensitive files, credentials, and more. The attacker is building the lateral movement route.
- Extract / dump saved password from Windows Credential Manager, browser, or memory, whether in clear text or hashed.

Deception layer

Use SMB deception lures that generate fake network drive fronts with a file server decoy with fake files. The fake network drive configuration is hidden to avoid users from opening it and generating false alerts. Keep in mind that the

SMB lure also inserts fake credentials to the Windows credentials manager as well.

Use RDP deception lures that store saved usernames and passwords in the Windows Credential Manager that provides access to a Windows / Linux server decoy.

Use Cached credentials lures that inject saved usernames and passwords in the Windows memory to detect attacks using password dump like Mimikatz. Use a real domain user with IP restrictions.

Early breach detection

Since most users store data on the network drive, when an attacker finds that the compromised endpoint has a local disk and network drive, the attacker will likely access the fake network drive and generate alerts.

Attackers might use a tool like MIMIKATZ to extract clear-text password. An attacker engaging with a decoy using the extracted password generates alerts.

Alert details

The FortiDeceptor console presents the alert as a kill chain flow and presents a profile of the attacker. The alert data includes:

- Attacker username.
  - One of the most critical indicators that provide a quick answer regarding the attacker, attack stage, and phase.
  - A standard user means that the attacker / attack is in the early stage. Admin-level credentials means that the attacker / attack is in the privilege escalation phase or the attack was directed against high profile users from the IT department.
- Compromised IP address.
  - This is a critical indicator that points directly to the compromised host. Early detection prevents more persistent points by the attacker.
- Data that has been accessed by the attacker.
  - To see what data an attacker wants to access and steal, one way is to deploy interesting fake data that resembles your organization's real data.
  - Another way is to deploy a decoy file server with a structure that contains at least ten fake directories that resemble your organization’s real server.
  - You can monitor what data the attacker accesses or copies to assess the attacker's goal.
- Malicious binary.
  - For example, if the attacker engages with a decoy over RDP, the attacker will likely use malicious code to get more persistent and privilege access. So having malicious binary as a piece of evidence with the full binary analysis helps IOC look across the network for more compromised endpoints. You can use an IOC scanner or AV/EDR API to find the indicators across network endpoints and servers.

ECO system flow:

- Send alerts to your SIEM solution.
- Use your FortiGate Fabric integration to isolate the compromised endpoint from the network.
- Deploy more decoys on the isolated segment to keep monitoring the compromised endpoint.

Lateral movement based on AD mapping

This scenario shows a human attacker trying to compromise an internal endpoint using lateral movements based on AD mapping.

Attack vector scenario

An attacker uses a phishing email to compromise the internal user and get access to an internal endpoint.

The attacker uses the compromised user credentials to passively map the network and collect information without generating network noise.

The attacker uses the compromised user credentials to run LDAP queries against the AD to retrieve asset inventory since all users have read-only access on AD objects.

Leveraging the AD asset inventory saves the attacker from running active port scan mapping that generates network noise that can expose his malicious activity.

Attacker's toolkit for AD attack:

- PS script or LDAP query command tools to extract company endpoint and server assets.
- Analyze the hostname to find assets where the hostname reflects their role or dev / test servers that might not be protected like the rest of the network.

Deception layer

- Deploy Windows decoys and add them to the network Domain
- Add DNS A record using attractive hostnames for all domain decoys' IP address. Each decoy supports up to 24 IPs.
- Use SMB deception lures that generate a fake network drive share on the endpoint that mapped front a file server decoy with fake files. The fake network drive configuration is hidden to prevent users from opening it and generating false alerts. Keep in mind that the SMB lure also inserts fake credentials to the Windows credentials manager as well.
- Use RDP deception lures that store saved usernames and passwords in the Windows Credential Manager that provides access to a Windows / Linux server decoy.
- Use Cached credentials lures that inject saved usernames and passwords in the Windows memory to detect attacks using password dump like Mimikatz. Use a real domain user with IP restrictions.

Early breach detection

When the attacker retrieves asset inventory from the AD and starts probing the attractive servers based on their hostname or the fake network connection, these activities generate alerts.

Alert details

The FortiDeceptor console presents the alert as a kill chain flow and presents a profile of the attacker. The alert data includes:

- Attacker username.
  - One of the most critical indicators that provide a quick answer regarding the attacker, attack stage, and phase.

  - A standard user means that the attacker / attack is in the early stage. Admin-level credentials means that the attacker / attack is in the privilege escalation phase or the attack was directed against high profile users from the IT department.
- Compromised IP address.
  - This is a critical indicator that points directly to the compromised host. Early detection prevents more persistent points by the attacker.
- Malicious binary.
  - For example, if the attacker engages with a decoy over RDP, the attacker will likely use malicious code to get more persistent and privilege access. So having malicious binary as a piece of evidence with the full binary analysis helps IOC look across the network for more compromised endpoints. You can use an IOC scanner or AV/EDR API to find the indicators across network endpoints and servers.

ECO system flow:

- Send alerts to your SIEM solution.
- Use your FortiGate Fabric integration to isolate the compromised endpoint from the network. FortiDeceptor offers more fabric connectors for isolation.
- Deploy more decoys on the isolated segment to keep monitoring the compromised endpoint.

Lateral movement based on Mimikatz / PTH

This scenario shows a human attacker trying to compromise an internal endpoint using lateral movements based on Mimikatz / PTH.

Attack vector scenario

An attacker uses a phishing email to compromise the internal user and get access to an internal endpoint.

The attacker looks for any powerful user in the compromised endpoint.

The attacker / APT uses an advanced tool like Mimikatz to run several attacks to extract clear text passwords from memory or Windows Credential Manager, AD Kerberos tickets, Windows local hash, and so on.

The Mimikatz tool's goal is to get administrator-level permission and run in-depth lateral movement across the network.

Attacker's toolkit:

- Tools like Mimikatz, Meterpreter, password dump, and so on.
- Leverage services like RDP, RPC, WMI, VNC, SSH, and WINRM for lateral movement.

Deception layer

- Deploy Windows decoys and add them to the network Domain.
- Add DNS A record using attractive hostnames for all domain decoys' IP addresses. Each decoy supports up to 24 IPs.
- Use SMB deception lures that generate a fake network drive share on the endpoint that mapped front a file server decoy with fake files. The fake network drive configuration is hidden to prevent users from opening it and generating false alerts. Keep in mind that the SMB lure also inserts fake credentials to the Windows Credential Manager as well.

- Use RDP deception lures that store saved usernames and passwords in the Windows Credential Manager that provides access to a Windows / Linux server decoy.
- Use Cached credentials lures that inject saved usernames and passwords in the Windows memory to detect attacks using password dump like Mimikatz. Use a real domain user with IP restrictions.

Early breach detection

An attacker using fake credentials in the sRDP lure to engage with a decoy generates alerts.

An attacker engaging with a real asset using the fake username and password (in the cache credential lure) generate an alert on the SIEM solution. This requires a SIEM correlation rule.

Alert details

The FortiDeceptor console presents the alert as a kill chain flow and presents a profile of the attacker. The alert data includes:

- Attacker username.
  - One of the most critical indicators that provide a quick answer regarding the attacker, attack stage, and phase.
  - A standard user means that the attacker / attack is in the early stage. Admin-level credentials means that the attacker / attack is in the privilege escalation phase or the attack was directed against high profile users from the IT department.
- Compromised IP address.
  - This is a critical indicator that points directly to the compromised host. Early detection prevents more persistent points by the attacker.
- Malicious binary.
  - For example, if the attacker engages with a decoy over RDP, the attacker will likely use malicious code to get more persistent and privilege access. So having malicious binary as a piece of evidence with the full binary analysis helps IOC look across the network for more compromised endpoints. You can use an IOC scanner or AV/EDR API to find the indicators across network endpoints and servers.

ECO system flow:

- For SIEM:
  - Send alerts to your SIEM solution.
  - Create a correlation rule that creates an alert on using the fake username (cache credential lure.
- Use your FortiGate Fabric integration to isolate the compromised endpoint from the network. FortiDeceptor offers more fabric connectors for isolation.
- Deploy more decoys on the isolated segment to keep monitoring the compromised endpoint.

Deploying tokens using AD GPO logon script

FortiDeceptor generates a deception lure package based on the decoy service configuration. For example, deploying a Windows server decoy with the services RDP and SMB, and Linux desktop decoy with the services SSH and SAMBA generates a deception lure package named `FDC_TokenPKG_XXXXXXXXX` that contains the deception lure files.

The deception lure package is a zip file that has three directories containing all the relevant data and configuration for each OS.

The deception lure for each OS uses the same concept: binary files with several JSON files that provide the decoy fake access parameters for the lure.

There are two ways to assign logon scripts. The first is on the *Profile* tab of the user properties dialog in the Active Directory Users and Computers (ADUC). The second is via Group Policy Objects (GPO).

This section provides in-depth instructions on how to deploy Windows lures using the second option via AD GPO logon script.

The main idea for the GPO logon script distribution is:

- Place the deception lure package in a network directory that is accessible to all endpoints.
- Generate a batch file that runs under the logon script and runs each time the end user logs into the network domain.
- The batch file copies the deception lure package to the endpoint and executes it.
- After execution, the endpoint has the deception lure in place.

To prepare the GPO logon script:

1. Download the deception lure package from the FortiDeceptor Admin Console.
2. Unzip the downloaded file to a temporary location.
3. Open the unzipped file and access the `windows` directory.
4. Copy all the files and directories, except uninstall.bat, from the `windows` directory:
   - `windows_token.exe`
   - *Config.json*
   - *res* directory (if it is there)
   - `Honeydocs` directory (if it is there)
5. On the AD server, go to `\\%UserDNSDomain%\SysVol\domain\scripts`
   In this example, the domain is FDC.COM so the location is `\\FDC.COM\SysVol\FDC.COM\scripts`.
6. In the `scripts` directory, create a new directory and name it `MyFiles`.
7. Copy `windows_token.exe` and the `res` directory to the `MyFiles` directory.
8. Create a batch file named `Lure.bat` with the following commands. In this example, the domain is FDC.com.
   ```
   set SFolder=\\FDC.COM\SysVol\FDC.COM\scripts\MyFiles
   set DFolder=%UserProfile%
   xcopy /E /S /H /K /F /C /Y /I "%SFolder%" "%DFolder%\MyFiles"
   start /B /WAIT /MIN "windows_token" "%DFolder%\windows_token.exe" "--non-interactive"
   exit
   ```
   A similar script for token installation is:
   ```
   set SFolder=\\FDC.COM\SysVol\FDC.COM\scripts\MyFiles
   start /B /WAIT /MIN "windows_token" "%SFolder%\windows_token.exe" "--keep-files" "--non-
        interactive"
   exit
   ```
   Syntax example:
   ```
   windows_token.exe "[optional command]" "<optional parameters>"...
   ```

Command	• (blank): The default command both uninstalls previous lures (if applicable), and installs the new lures. • `uninstall`: Uninstalls all previous installed lures (if applicable) for the current user.

Parameters	`--non-interactive`: (Optional) Used with any command, this parameter prevents any user interface from being displayed while the command is being executed. `--keep-files` (Optional) Keep the installation files/directories. Otherwise, all files and directories in the current folder will be wiped out.

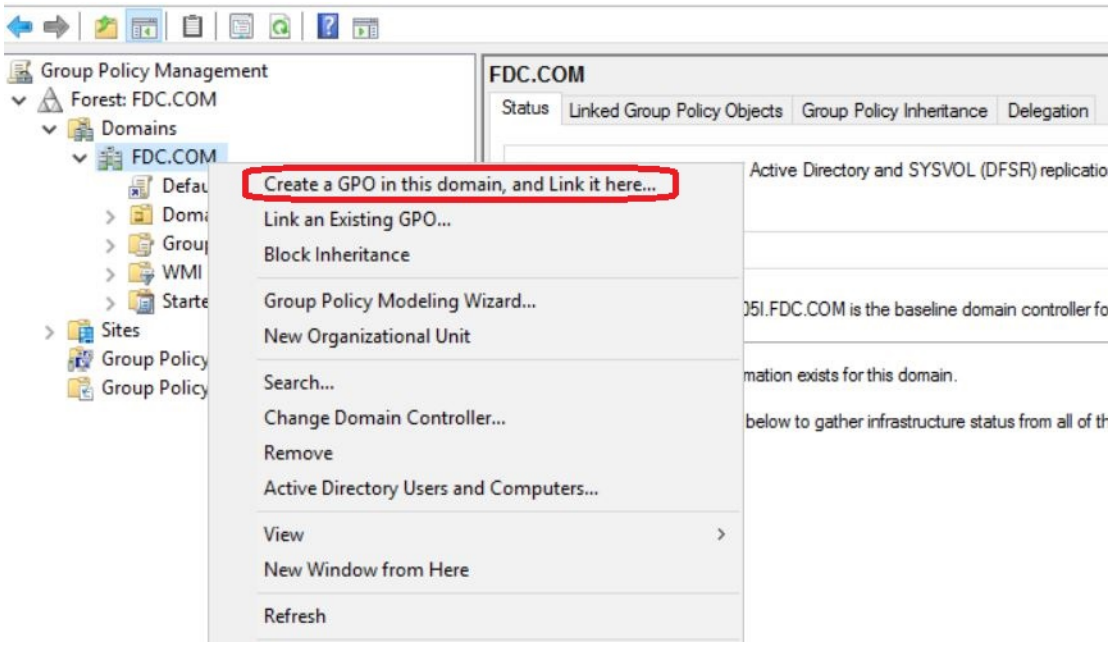
9. (Optional) *The default installation process both uninstalls previous lures (if applicable), and installs the new lures. To uninstall tokens without installation:
   a. Copy `windows_token.exe` from the windows directory to the *MyFiles\Uninstall* directory.
   b. Create a batch file named `uninstall_lure.bat` with the following commands.
   In the following example, the domain is *FDC.com*:

```
set SFolder=\\fdc.com\SYSVOL\fdc.com\scripts\MyFiles\Uninstall
start /B /WAIT /MIN "uninstall_windows_token" "%SFolder%\windows_token.exe"
"uninstall" "--non-interactive"
exit
```

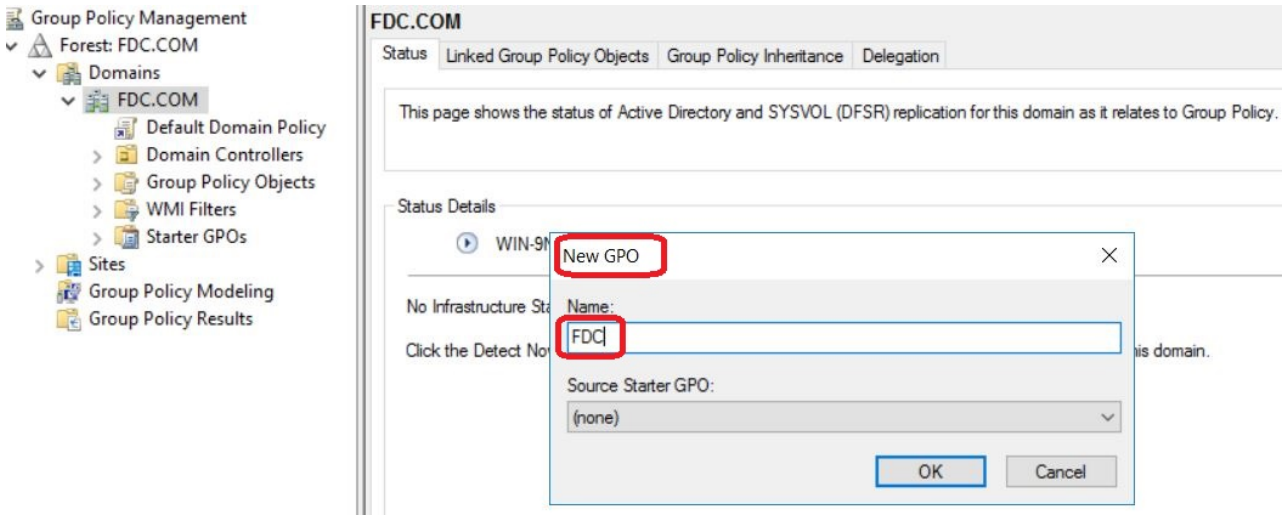
Configuring the GPO logon script

To configure the GPO logon script:

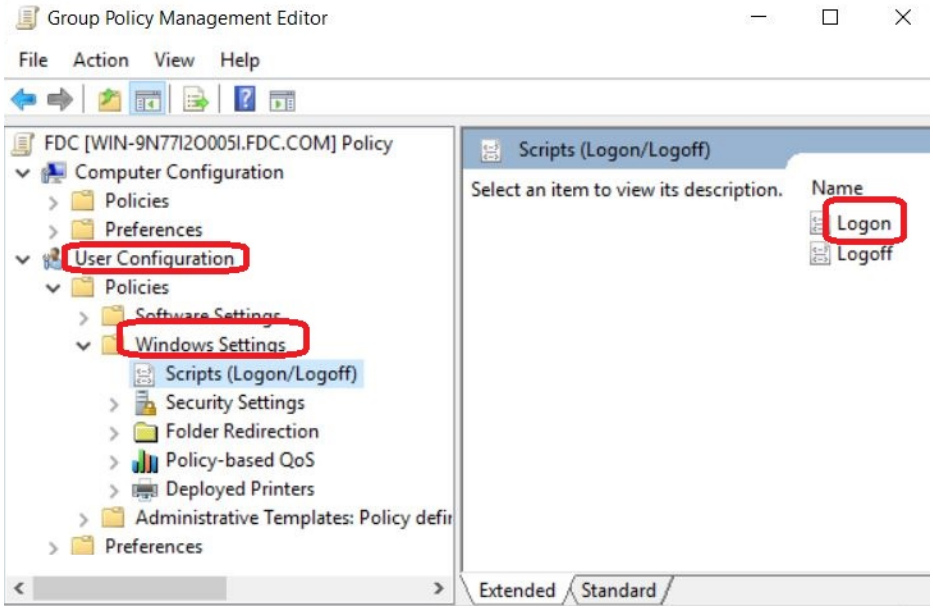
1. Log into the AD server and open the Group Policy Management tool.
   You can also open this tool using the CLI `gpmc.msc`.
2. Right-click the top-level domain object (in this example, *FDC.COM*) and select *Create a GPO in this domain, and link it here*.
   This creates a new group policy object.



3. Enter a name for the new group policy object. Do not use a name that has any association with a deception technology.

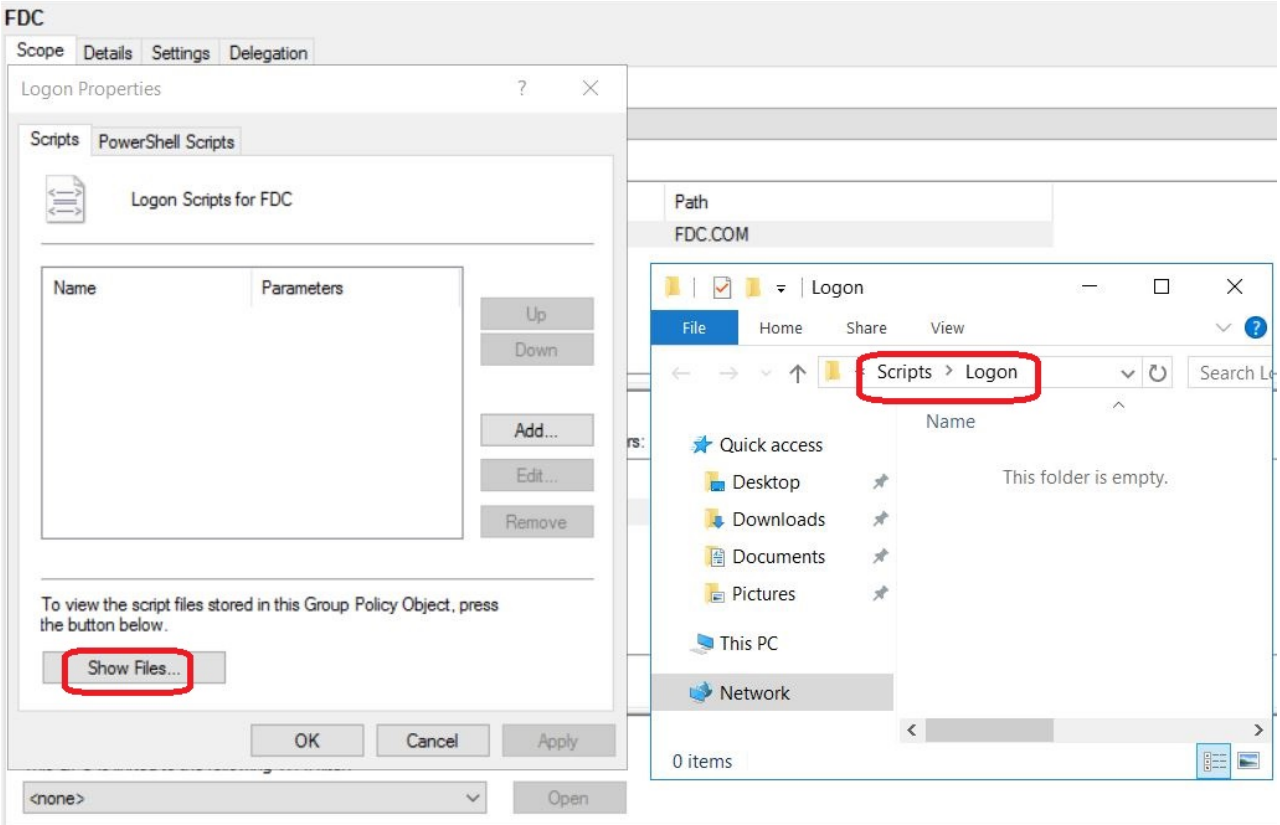


4. Right-click the new group policy object and select *Edit*.
5. Go to *User configuration* > *Policies* > *Windows Settings* > *Scripts (Logon/Logoff)*.
6. In the right pane, double click the *Logon* script to configure the Logon script properties.

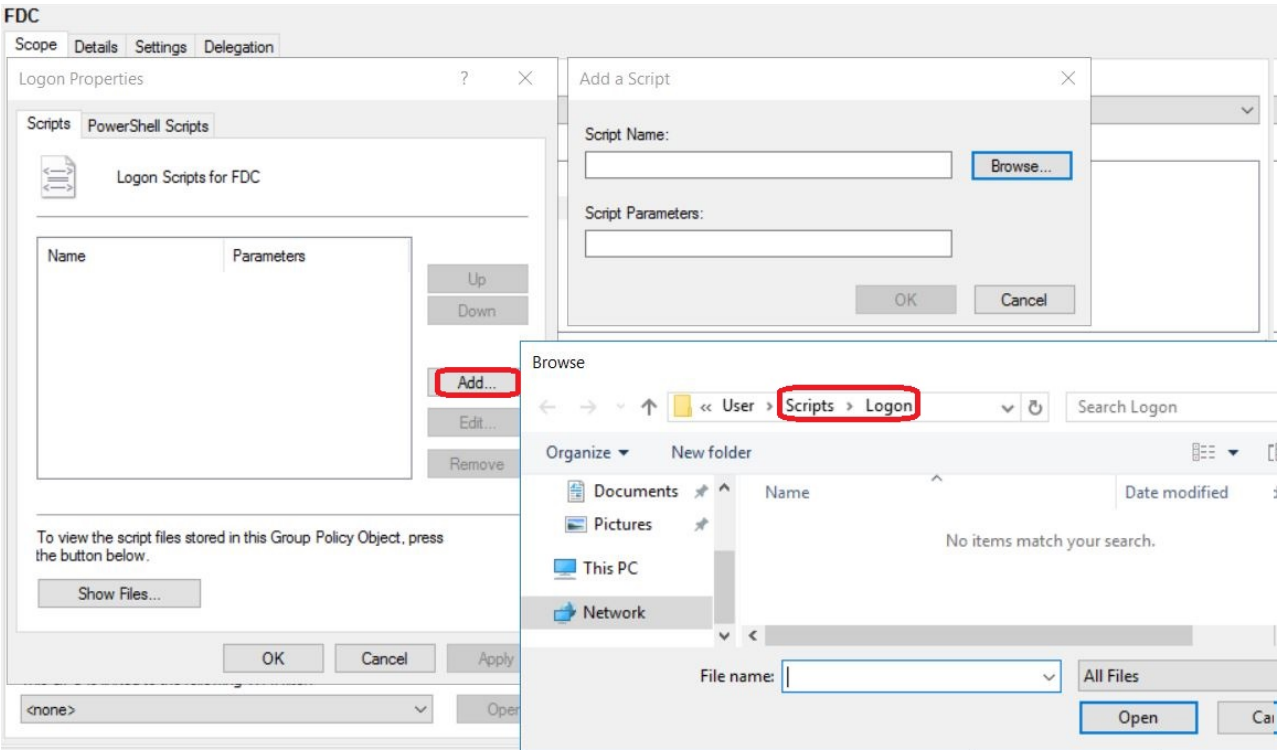


7. In the *Logon Properties* dialog box, click *Show Files*.

8. Copy the batch file `Lure.bat` that you have prepared.



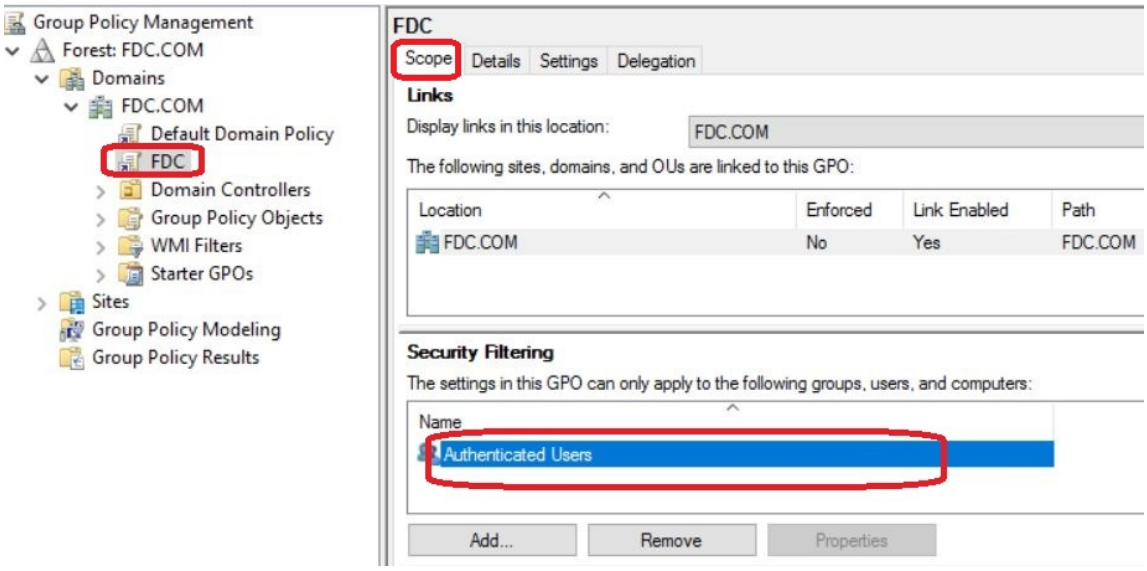
9. In the *Logon Properties* dialog box, click *Add* to open the *Add a Script*dialog box.
10. Click *Browse*, locate the `Lure.bat` batch file and add it to *Scripts (Logon/Logoff)*.



11. Click *Apply* and then click *OK* to close this window.

To enforce the group policy:

1. In the *Group Policy Management* console, select the new group policy object. In this example, *FDC.COM*.
2. In the *Scope* tab, verify that *FDC.COM* is linked.
3. In the *Security Filtering* section, add and remove the user groups to get the deception lure package through the logon script.
4. In the left pane, right-click the *FDC* group policy object and select *Enforced*.

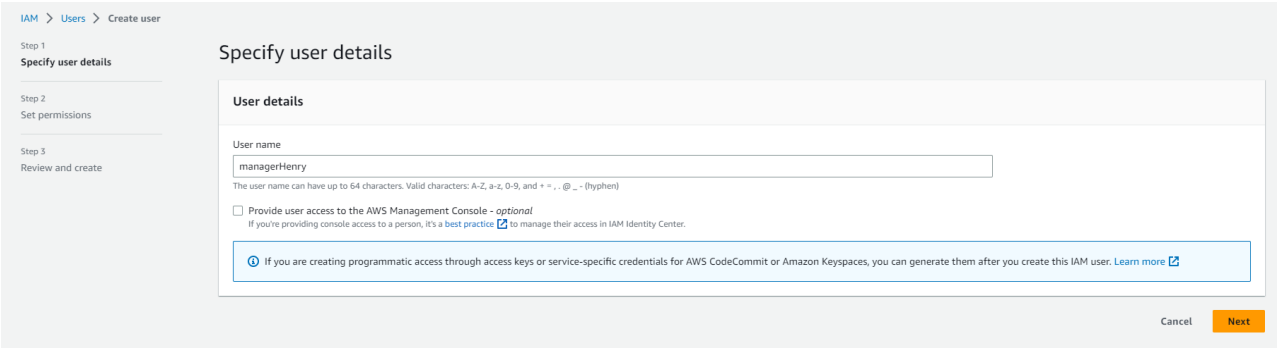


Deploying AWS deception keys

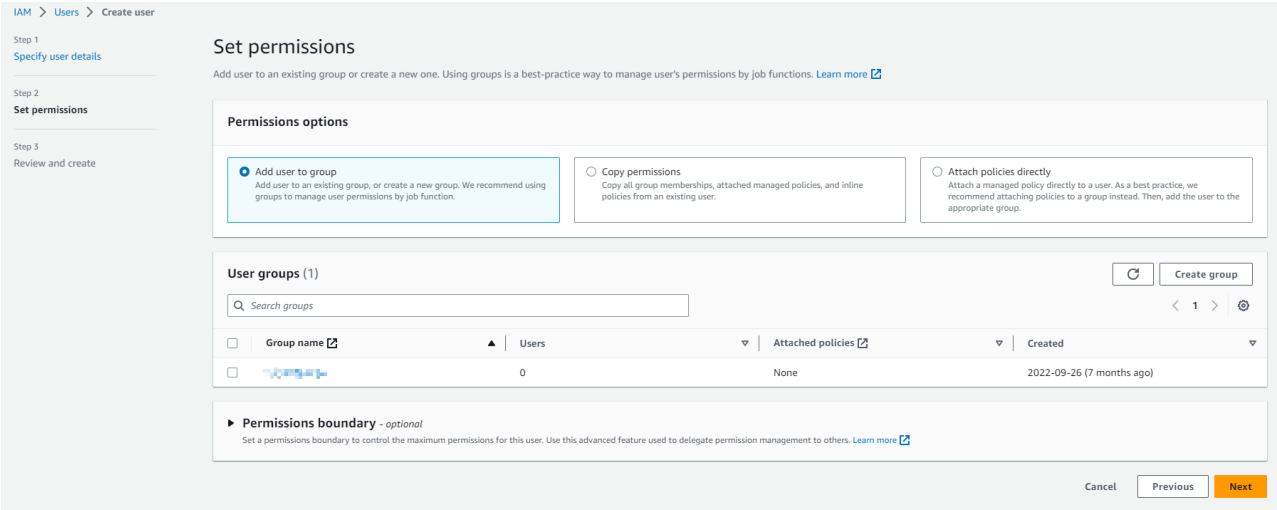
To deploy AWS deceptions keys, first create the keys in AWS, then upload them to the FortiDeceptor and create a new campaign.

To create an IAM user:

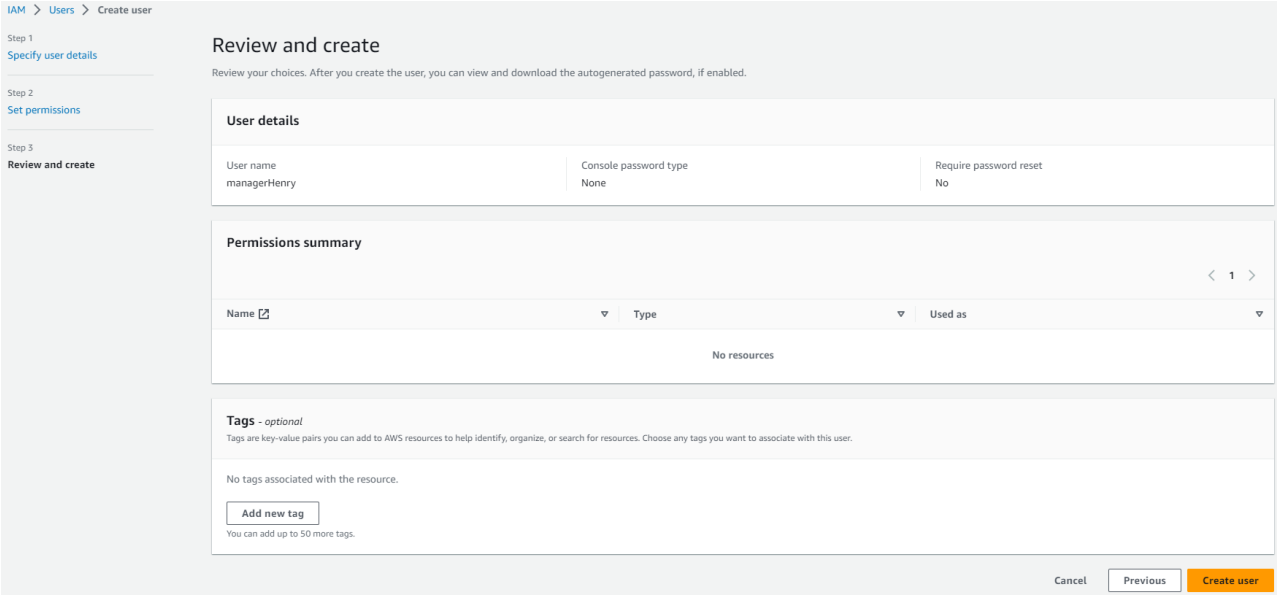
1. Log in to your AWS administrator account.
2. Go to *Access Management* > *Users* and click *Add Users*.
3. In the *User details* page, enter a *User Name* and click *Next*.



4. On the *Set Permissions* page, do not assign permissions, and click *Next*.



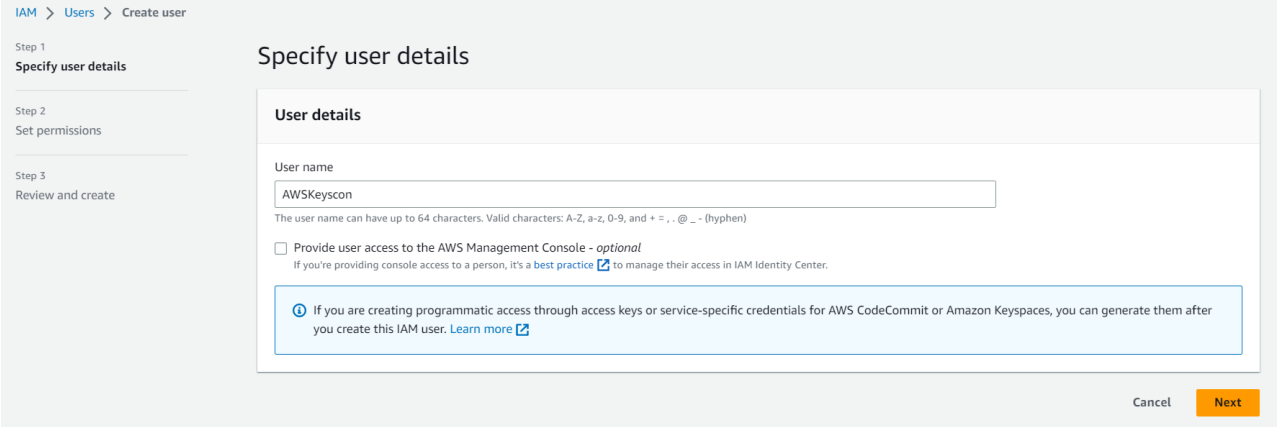
5. On the *Review and create* page, click *Create User*. The new user is created.



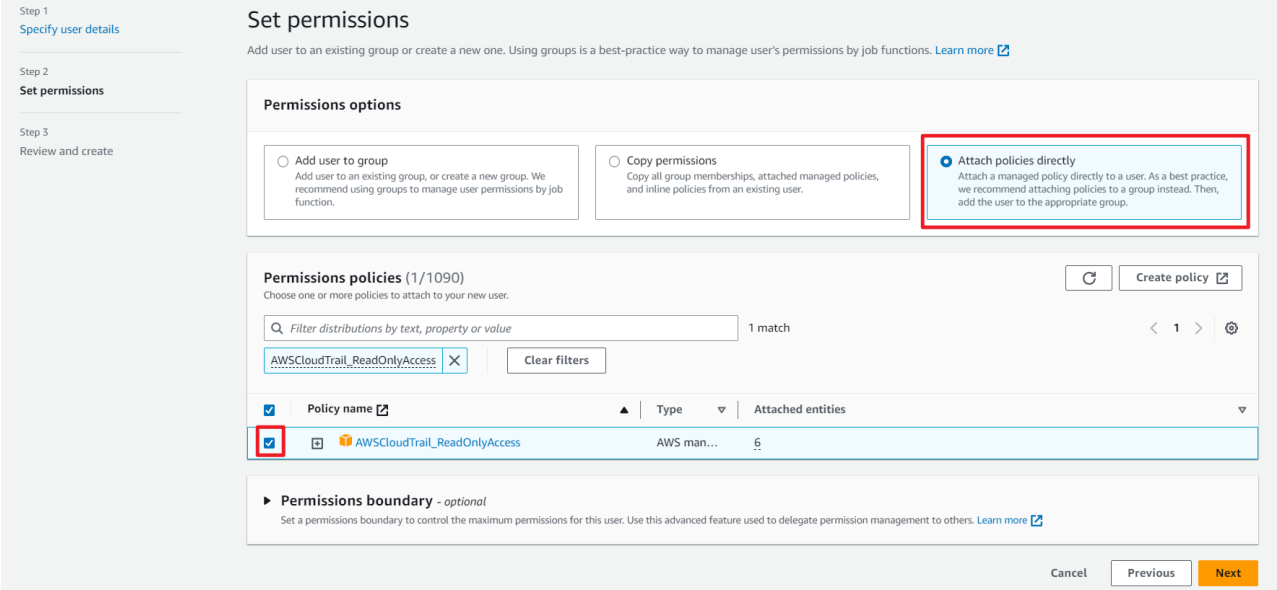
6. Create an access key for an AWS Connector user.

To create an AWS Connector user with AWSCloudTrail_ReadOnlyAccess permission:

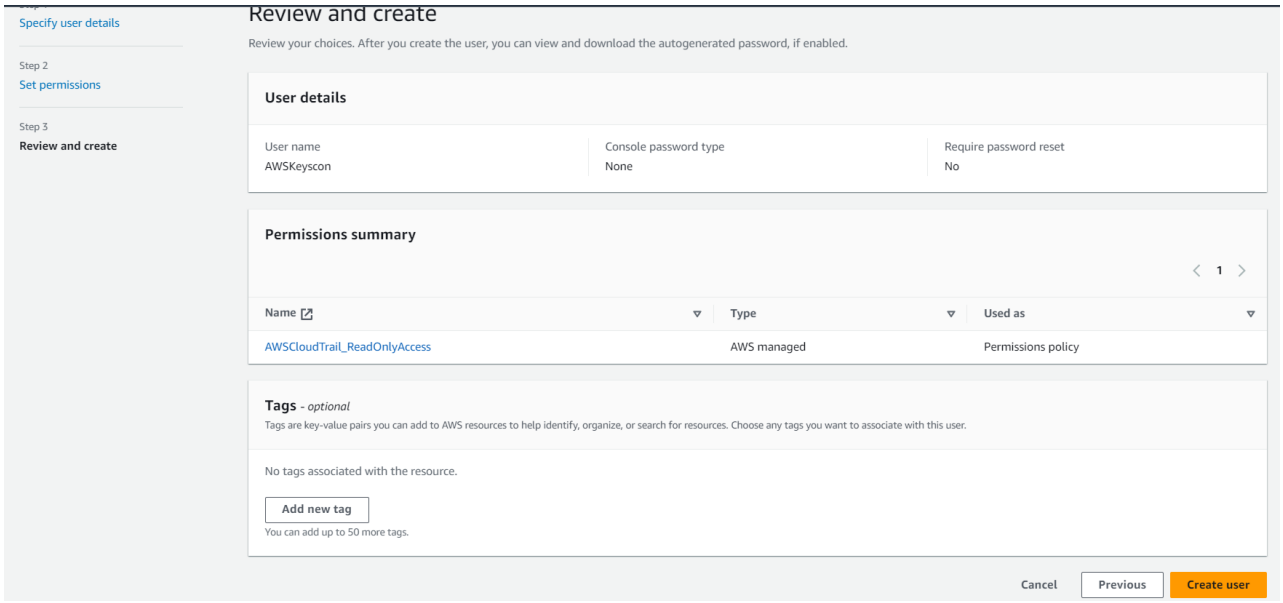
1. Create a new AWS Connector user such as *AWSKeyscon*.



2. Set the permissions to *Attach existing polices directly* and select *AWSCloudTrail_ReadOnlyAccess*.



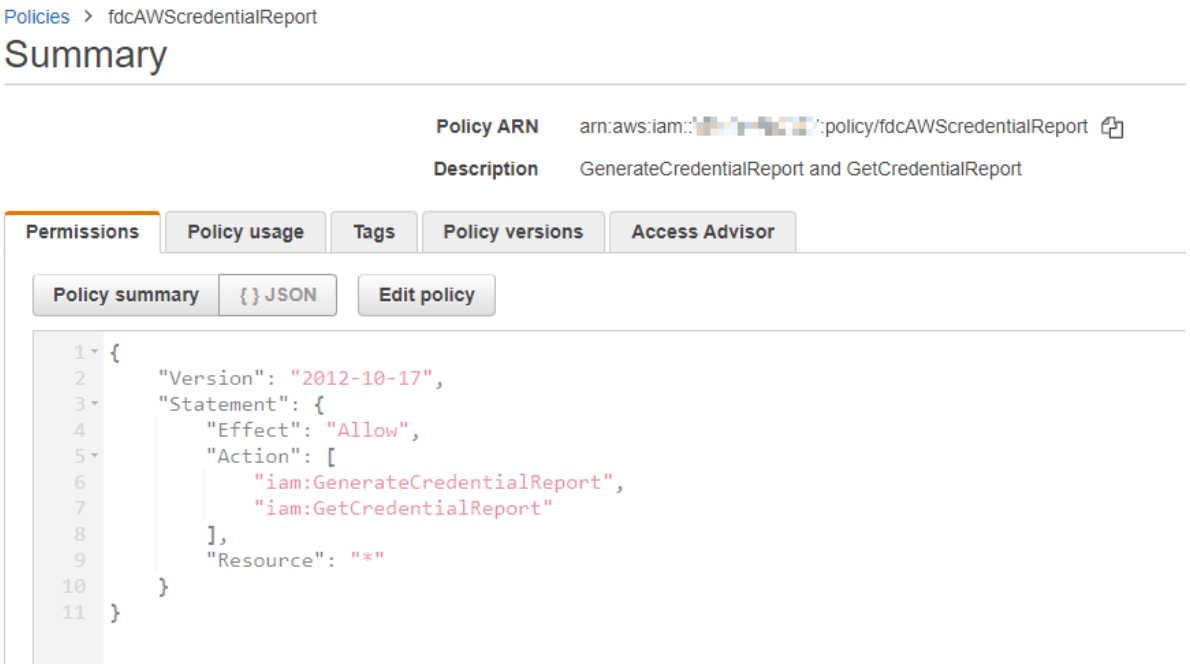
3. Review the user permissions and click *Create user*.



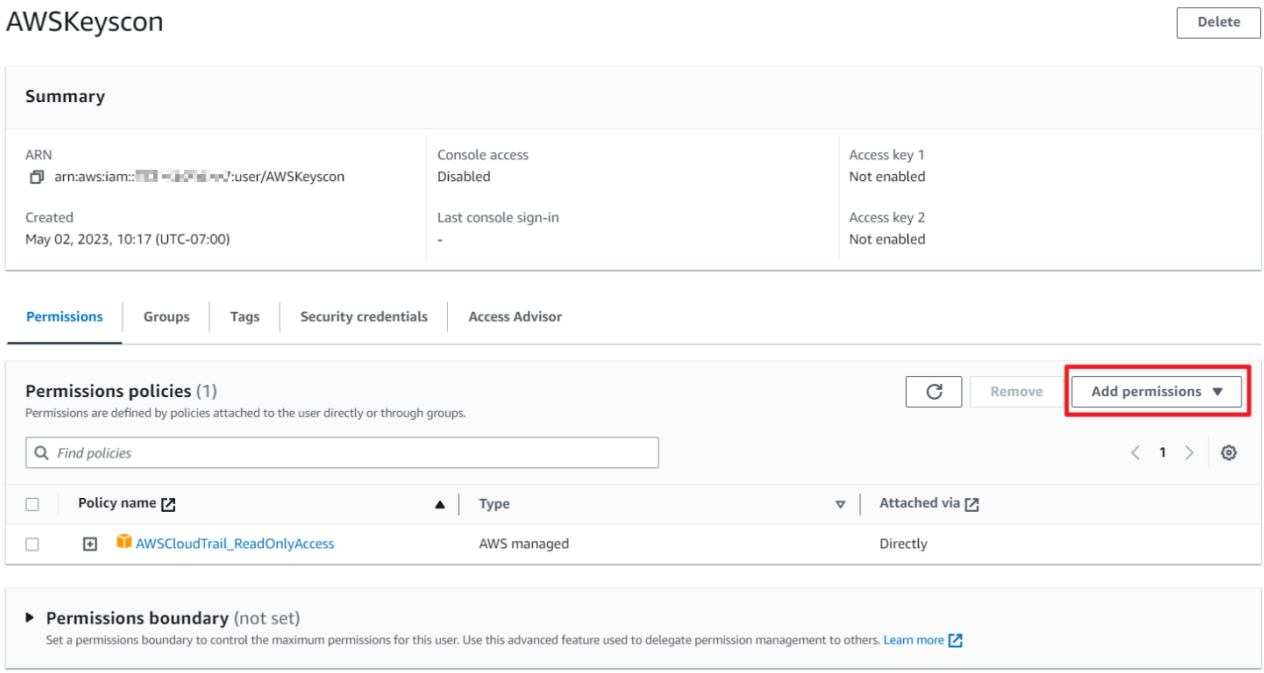
To grant an AWS connector user access to credential reports:

1. Go to *Policies* and create a custom policy such as *fdcAWScredentialReport*.
2. Click the *Permissions* tab and configure the permissions. For example:

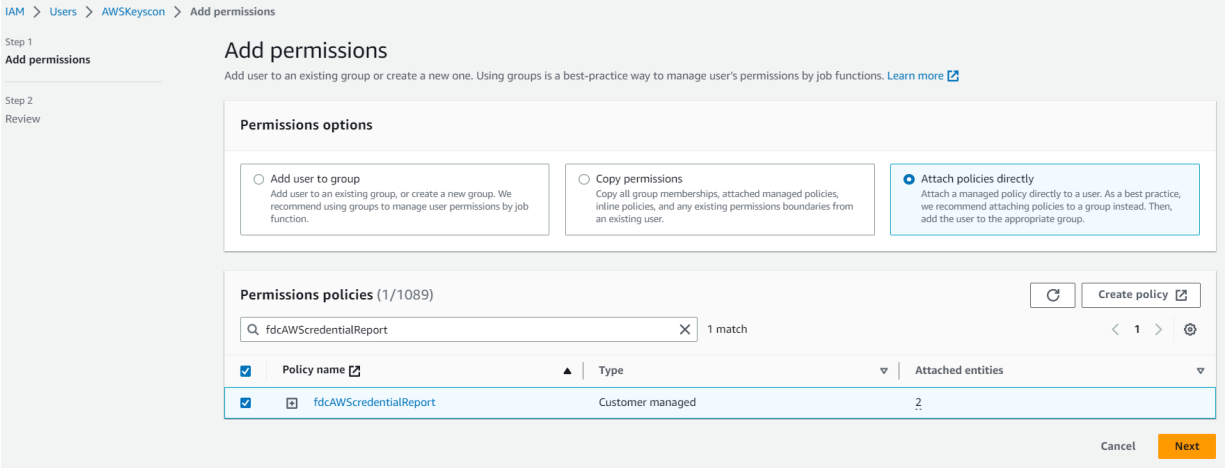
```
{
        "Version": "2012-10-17",
        "Statement": {
           "Effect": "Allow",
           "Action": [
              "iam:GenerateCredentialReport",
              "iam:GetCredentialReport"
           ],
           "Resource": "*"
        }
}
```



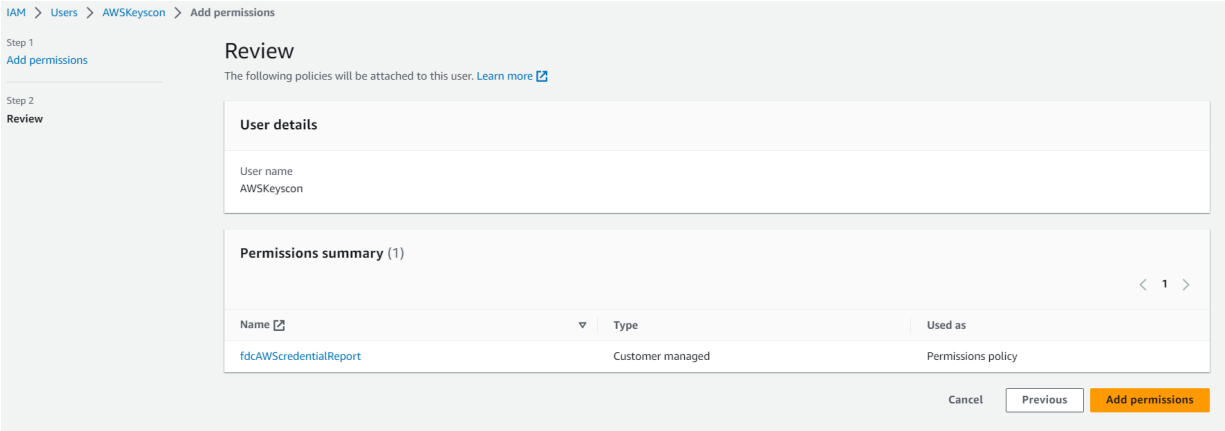
3. Go to *IAM* > *Users* and select the AWS Connector user such as *AWSKeyscon*, and then click *Add Permissions*.



4. Configure the permissions.
   a. Under *Permissions polices* add the custom policy such as `fdcAWScredentialReport`.
   b. Click *Next*.

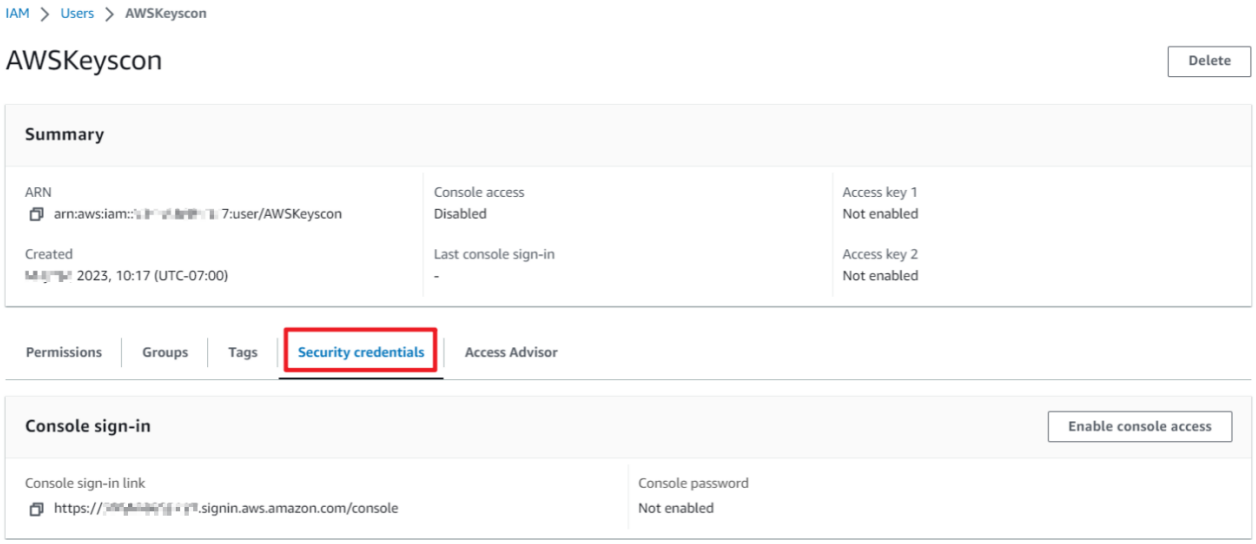


   c. Review the *User details* and *Permissions summary* and click *Add Permissions*.

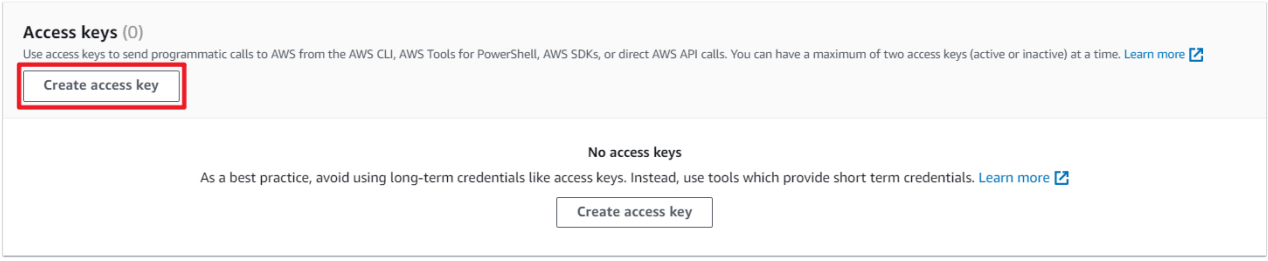


To create an access key for an AWS Connector user:

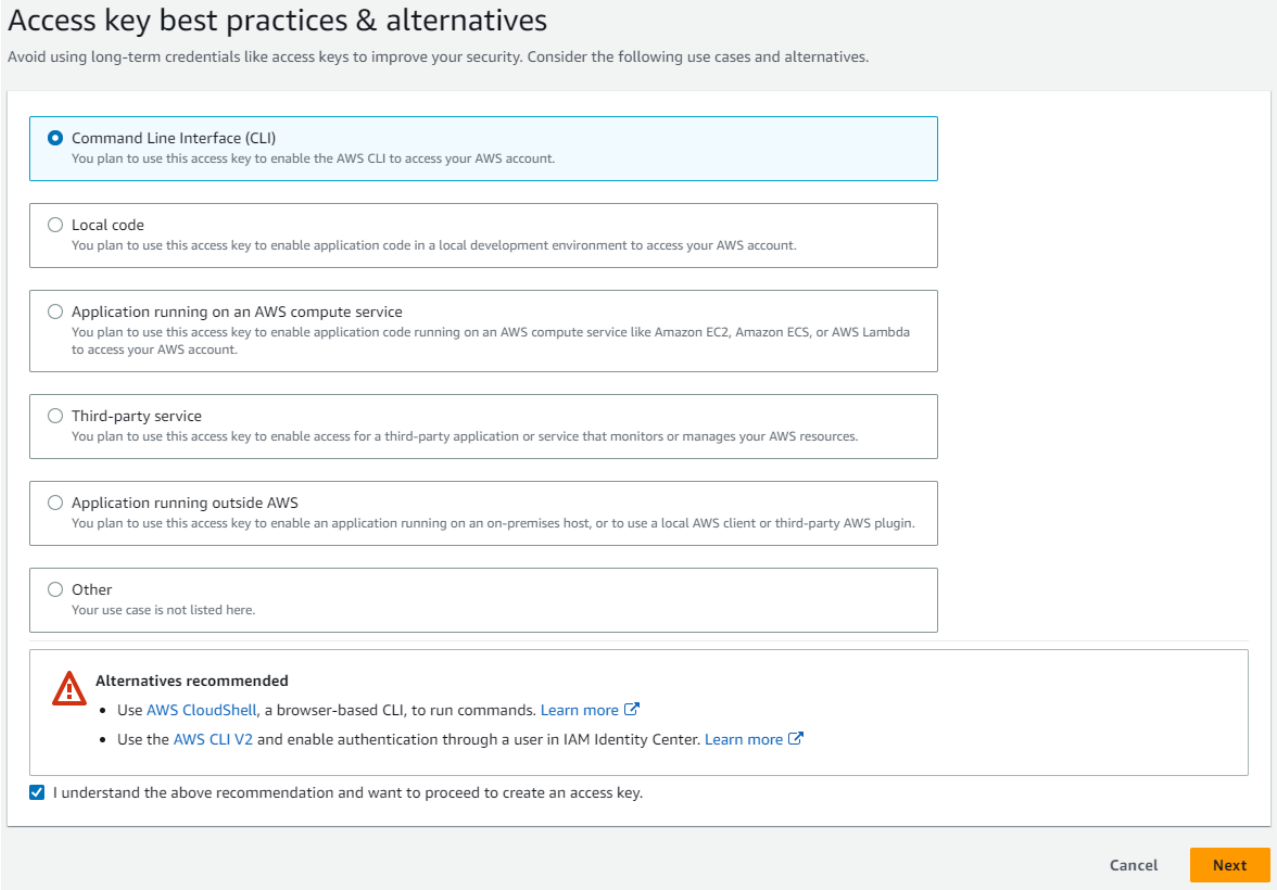
1. Go to *IAM users* and select a user such as *AWSKeyscon*, and then click the *Security credentials* tab.



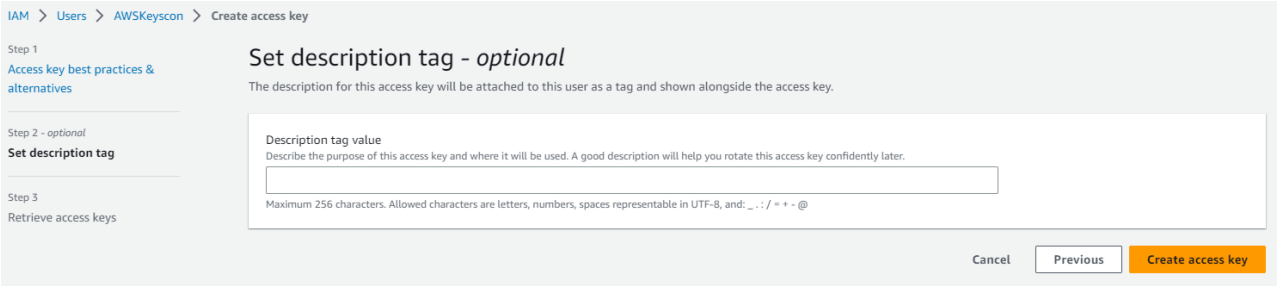
2. Under *Access keys* click *Create access key*.



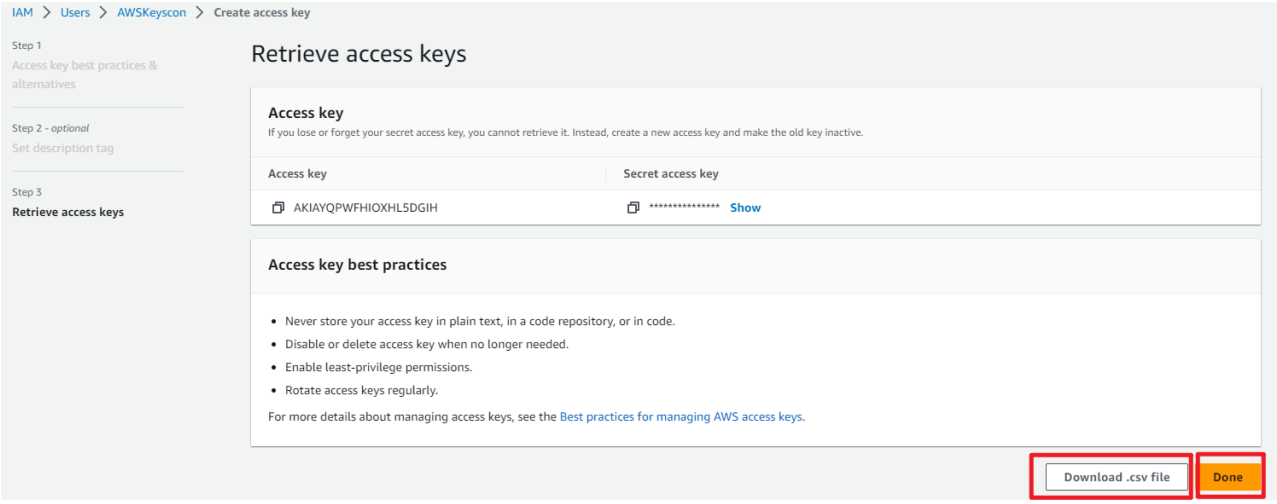
3. Under *Access key best practices & alternatives* select *Command Line Interface (CLI)* and click *Next*.



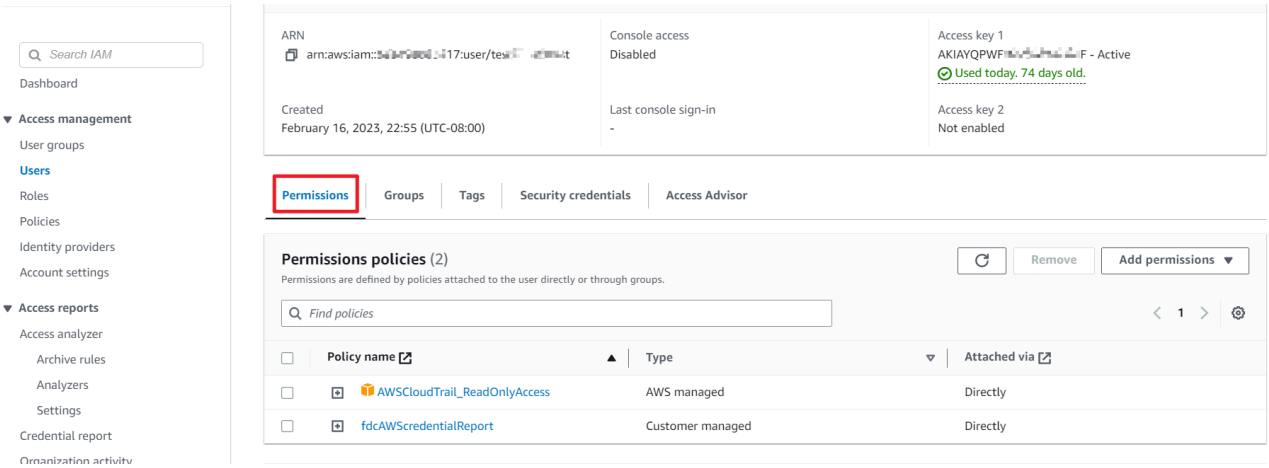
4. (Optional) Set the description tag and click *Create access key*.



5. On the *Retrieve access keys* page, click *Download .csv file* and then click *Done*.

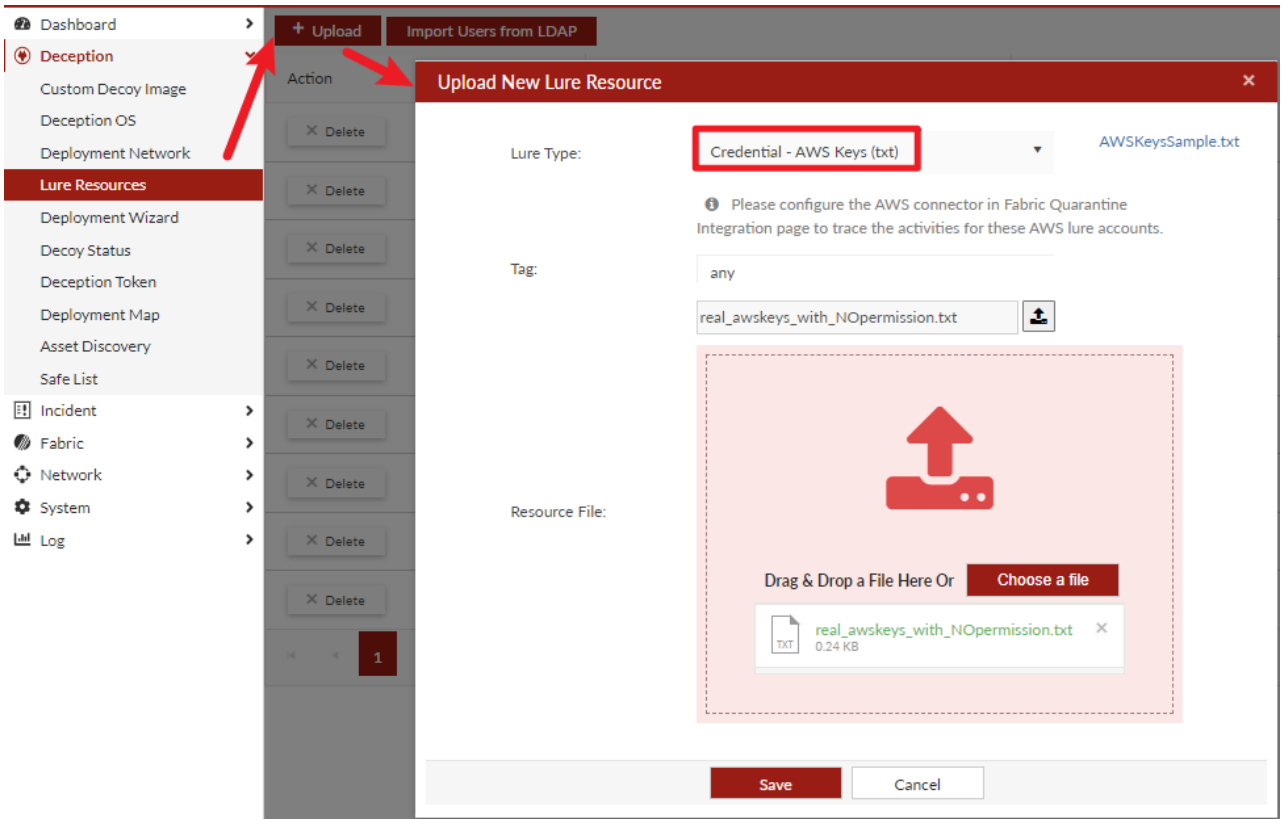


6. In the *Permissions* tab, ensure the AWS Keys Connector has the following two permissions: *AWSCloudTrail-ReadOnlyAccess* and the custom policy such as *fdcAWScredentialReport*.



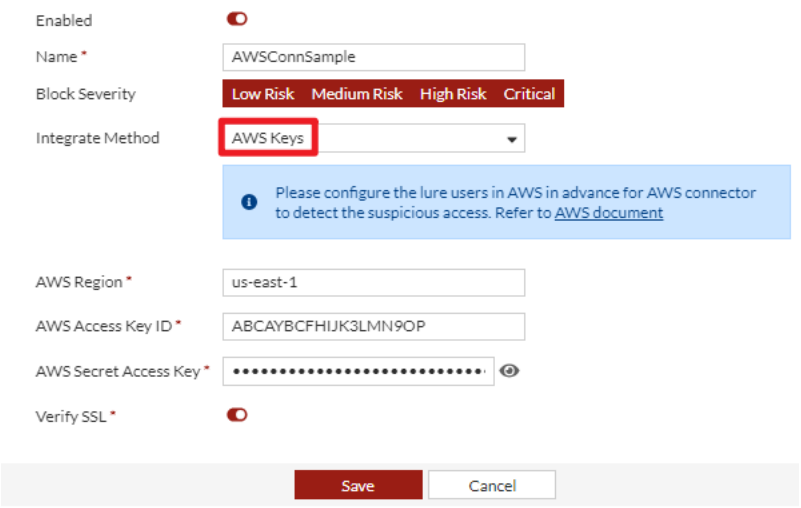
To deploy the deception keys in FortiDeceptor:

1. Log in to FortiDeceptor and go to *Deception* > *Lure Resources*.

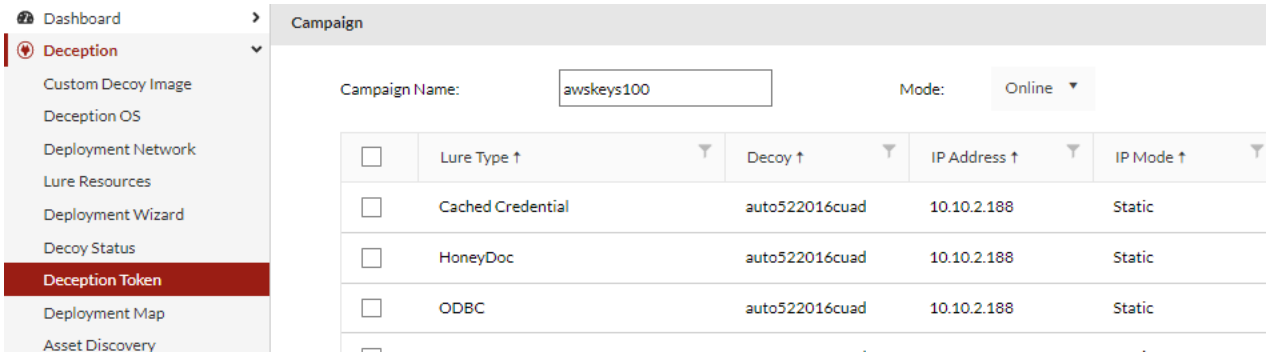


2. Go to *Fabric* > *Quarantine Integration* > *+Quarantine Integration With New Device* and configure the integration.

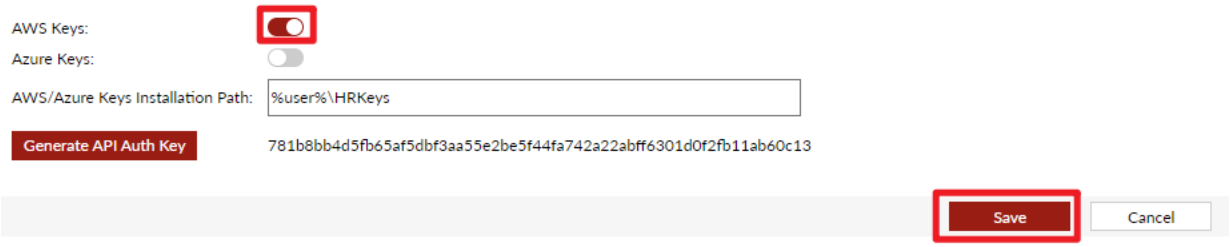
Integrate method	Select AWS Keys.
AWS Region	Enter the region for the AWS Connector user you created in the previous task.
AWS Access Key ID	Enter the access key ID for the AWS Connector user you created in the previous task.
AWS Secret Access Key	Enter the secret access key for the AWS Connector user you created in the previous task.



3. Go to *Deception* > *Deception Token* > *Token Campaign*.
4. Click + *Campaign* and select the AWS lure you unloaded in Step 2.



5. Click *Generate API Auth Key* and click *Save*.

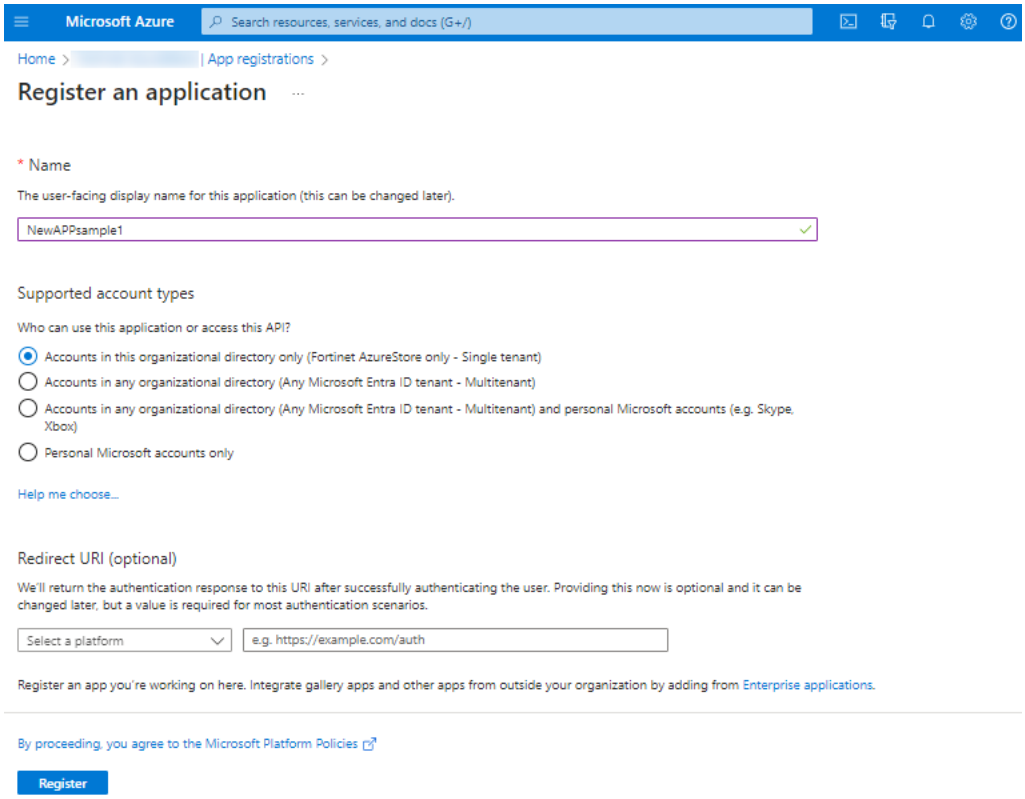


Deploying Azure deception keys

To deploy Azure deception keys, first create the keys in Azure, then upload them to the FortiDeceptor and create a new campaign.

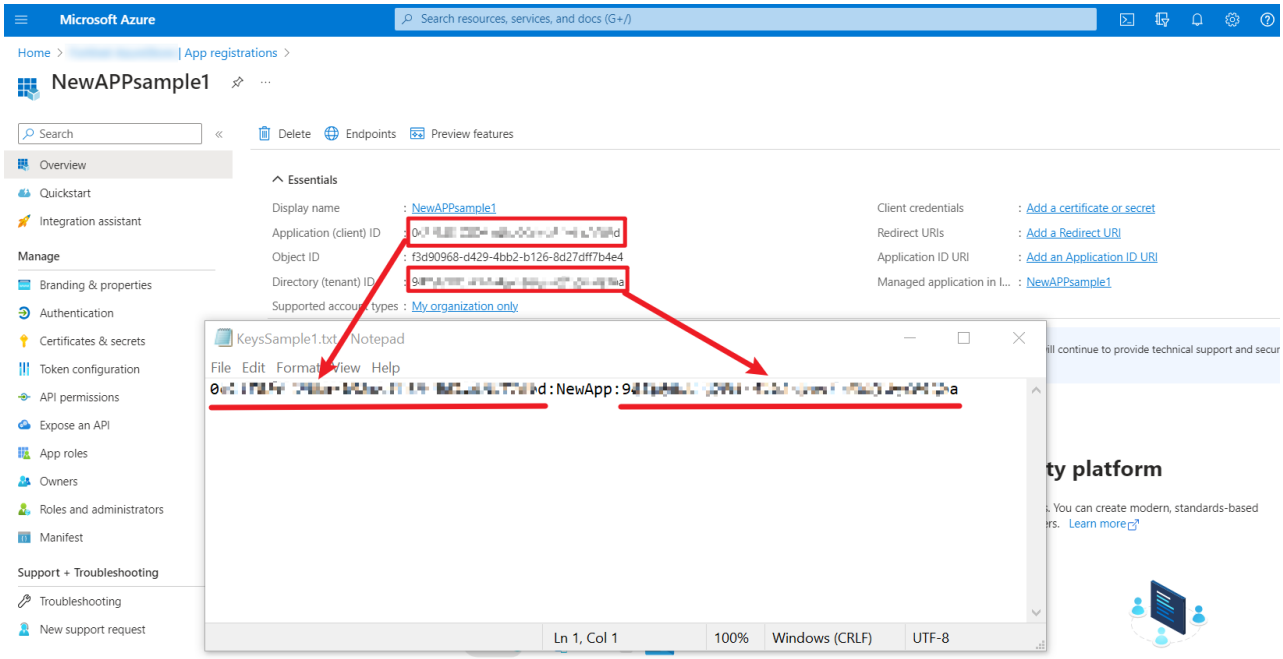
To create Azure AD application keys for Lure Resource:

1. Log in to your Azure account.
2. Go to *Azure Active Directory* > *App registrations* > *Register an application* > *Register*. Do not assign any API permissions to this application.

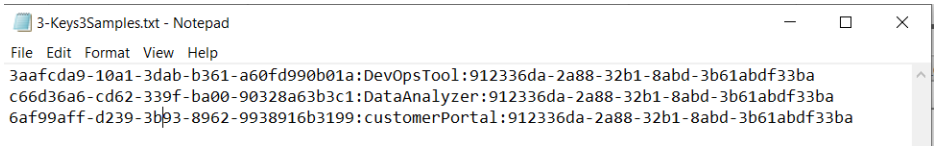


3. Go to *Azure Active Directory* > *App registrations* > *All applications*, and locate the application you created (for example, *NewAPPsample1*).

4. Copy and paste the client ID and the tenant ID into a .txt file (for example *KeysSample1.txt*).



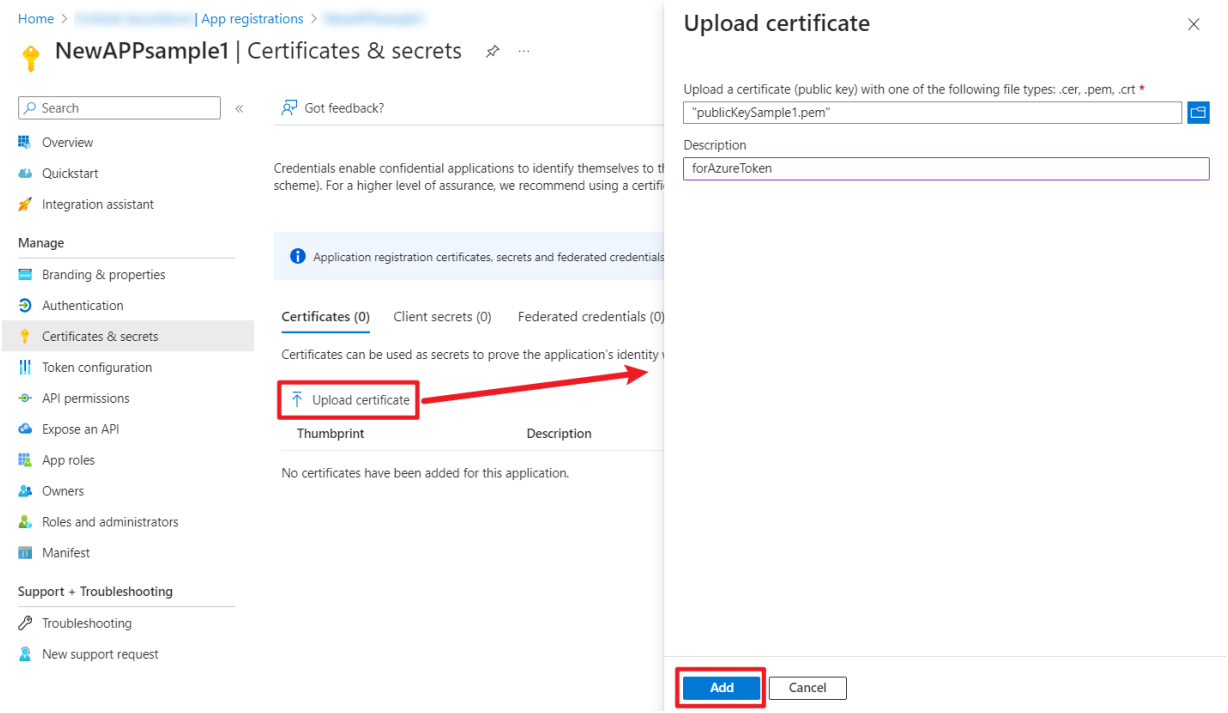
5. Input multiple applications info into one .txt file, such as *Keys3Samples.txt*



.

6. Locate the application you created (for example, NewAPPsample1). Go to *Certificate & secrets* > *Certificates*, and upload a certificate (public key).

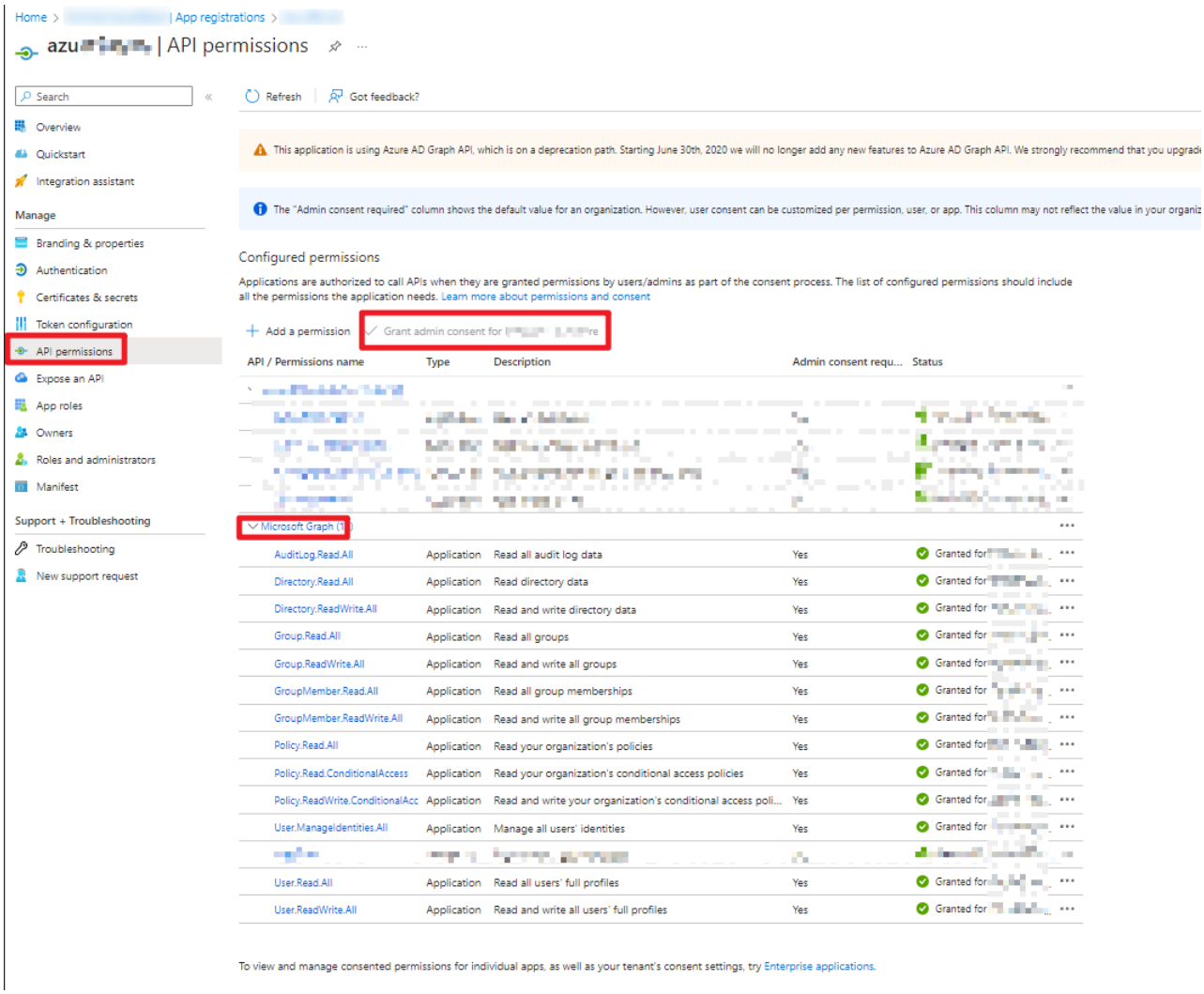
a. (Optional) Upload a public key to the deception application.



b. (Optional) Keep the certificate file that corresponds to the public key you uploaded in the previous step.

To create Azure application keys for Azure Connector:

1. Go to create an *AD application for Azure Connector*.
2. Ensure that the required permissions are granted for the registration of this application.
   For a *Microsoft Graph User*, following API/Permissions must be granted:
   - *User.Read.All*
   - *User.ReadWrite.All*
   - *GroupMember.Read.All*
   - *GroupMember.ReadWrite.All*
   - *Group.ReadWrite.All*
   - *Group.Read.All*
   - *AuditLog.Read.All*
   - *Directory.Read.All*
   - *Directory.ReadWrite.All*
   - *User.ManageIdentities.All of type Application.*



3. Create the secret, and keep the client ID and tenant ID for the Azure Connector later.

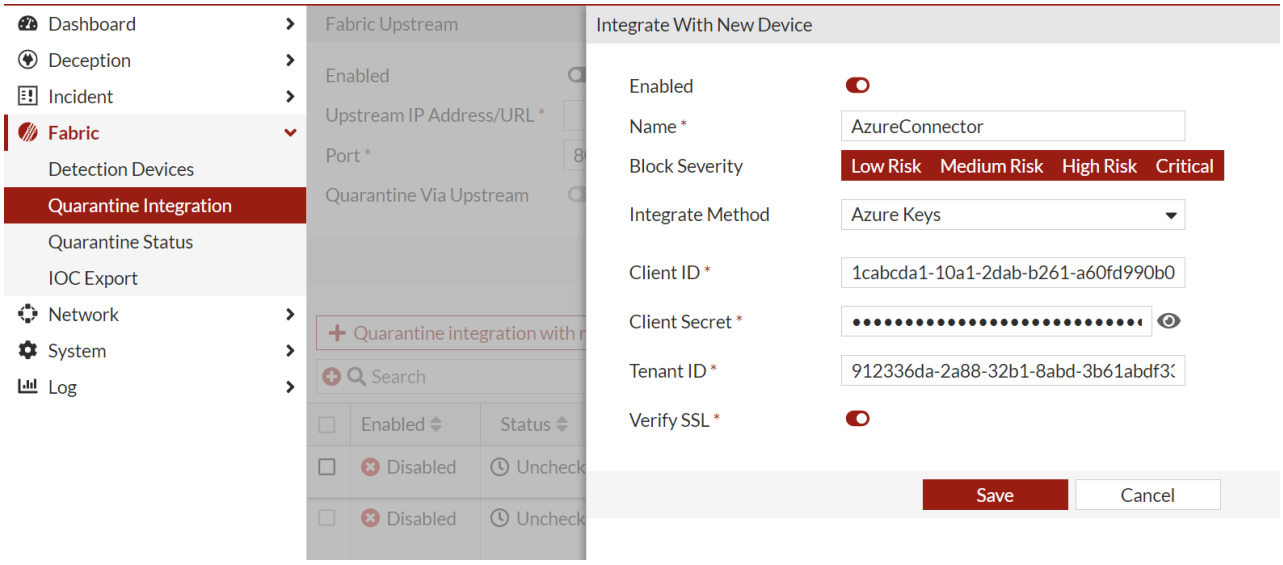
To deploy the deception keys in FortiDeceptor:

1. Log in to FortiDeceptor and go to *Deception > Lure Resources* and click *Upload*. You cannot select which Azure key is to be installed if you upload multiple keys at the same time.
2. For *Lure Type*, select *Credential - Azure Keys (txt)* and upload the text file you created in the previous task (for example, *KeysSample1.txt*) , and click *Save*.

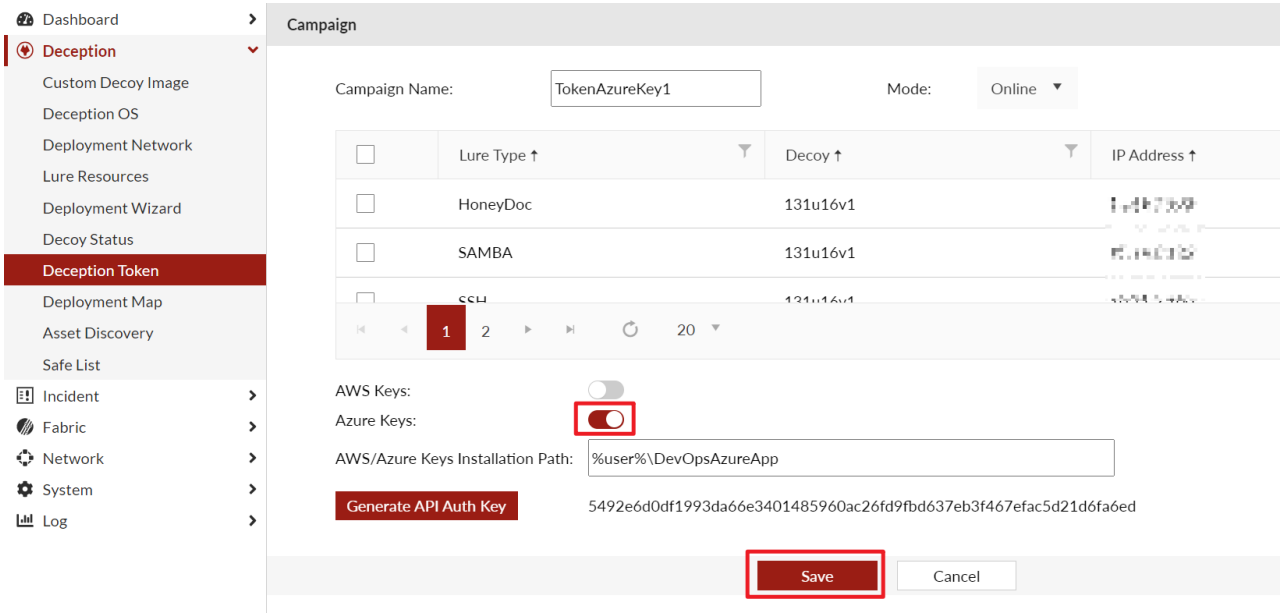
   If you kept the certificate file which includes certificate with private key, for *Lure Type*, select *Azure Certificate*, and upload the certificate file from 6.b.
3. Go to *Fabric > Quarantine Integration* .
4. Click *+Quarantine Integration With New Device* and configure the integration.

Integrate method	Select *Azure Keys*.
Client ID	Also called *Application ID;Unique ID* of the Azure Active Directory application.

Client Secret	Client Secret of the Azure Active Directory application that is used to create an authentication token required to access the API.
Tenant ID	Tenant ID provided for your Azure Active Directory.
Verify SSL	Specifies whether the SSL certificate for the server is to be verified or not. By default, this option is set as *True*.



5. Go to *Deception* > *Deception Token* > *Token Campaign*.
6. Click + *Campaign*. Enable the toggle and use the default location or customized location to create the Azure keys campaign.



7. Click *Save*.

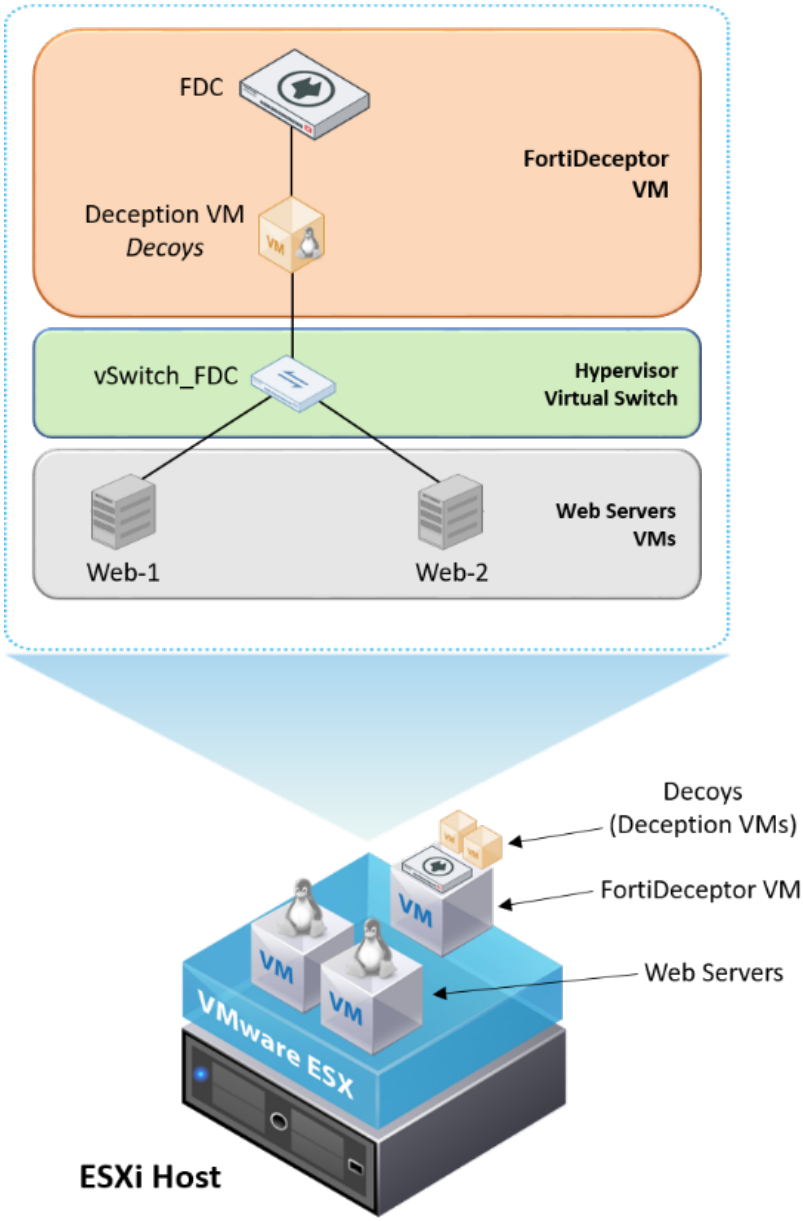
Configuring trunk ports on FortiDeceptor VM

This section describes how to configure trunk ports to extend VLANs between FortiDeceptor VM and ESXi vSwitch using a single interface.

This setup requires FortiDeceptor VM v3.1 build 0061 and vSwitch ESXi v6.7.0 build 13006603.

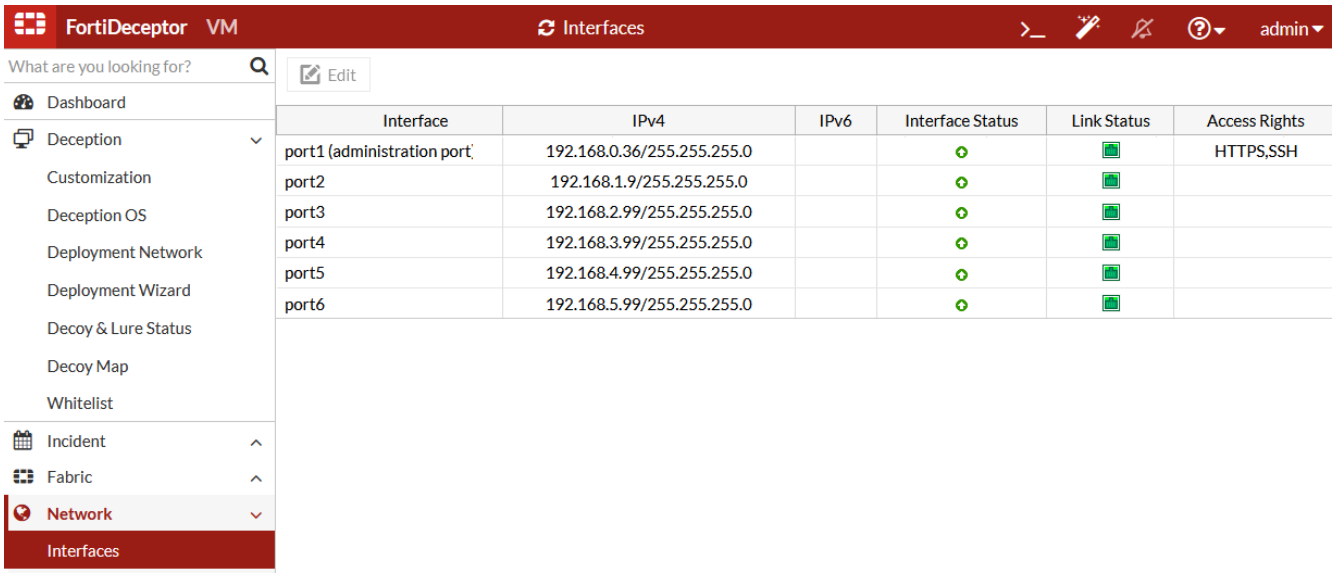
Set up a single ESXi host with the following workloads.

- 1 FortiDeceptor VM with one decoy monitoring two network segments.
- 2 web servers in different VLANs / network segments.
- 1 vSwitch dedicated to connecting the FortiDeceptor decoy to the network segments.



FortiDeceptor VM has internal network ports. Set up FortiDeceptor VM with the following.

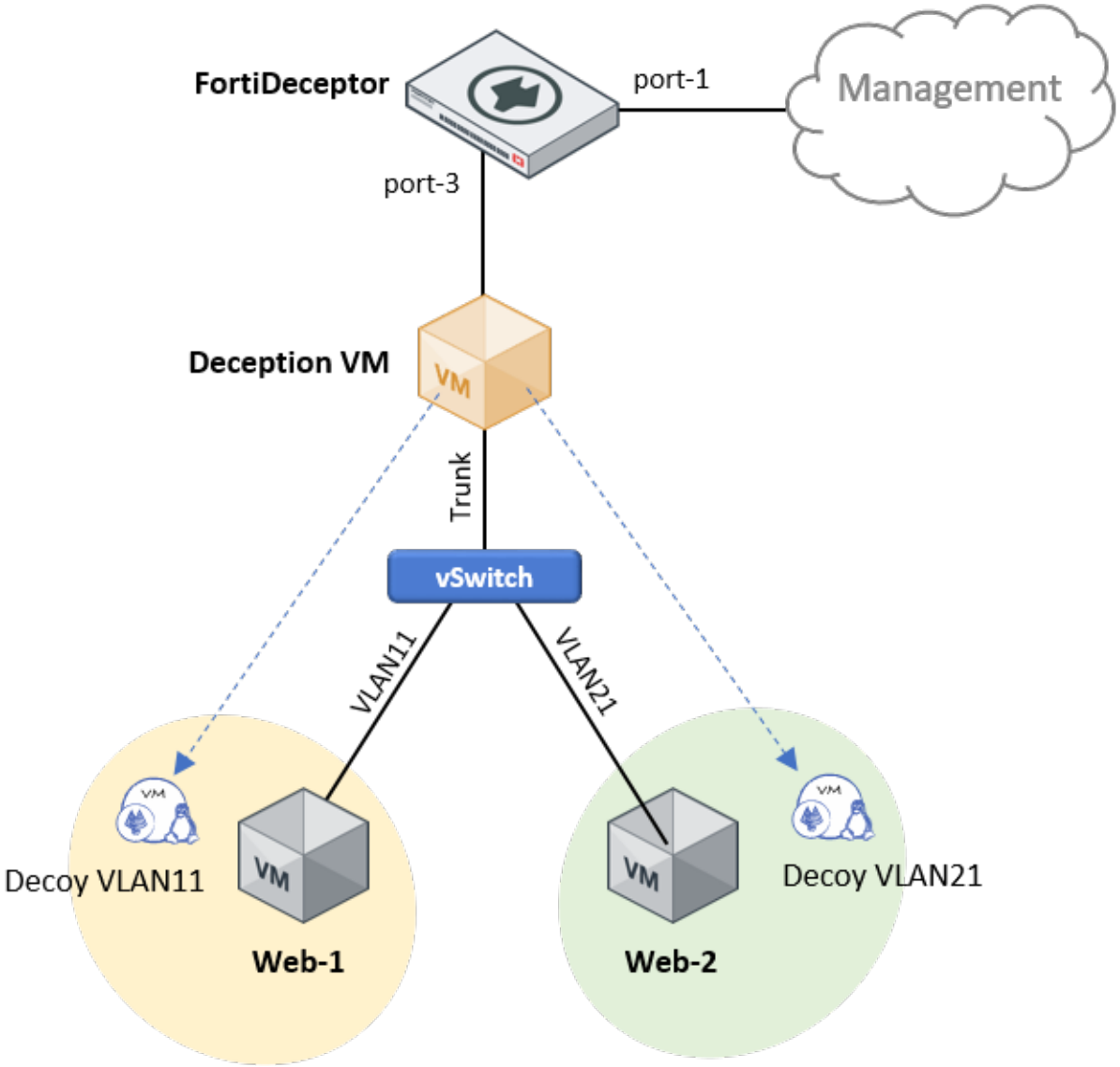
- Reserve port1 for device management.
- Use the other ports to deploy deception decoys.



Interface	IPv4	IPv6	Interface Status	Link Status	Access Rights
port1 (administration port)	192.168.0.36/255.255.255.0				HTTPS,SSH
port2	192.168.1.9/255.255.255.0				
port3	192.168.2.99/255.255.255.0				
port4	192.168.3.99/255.255.255.0				
port5	192.168.4.99/255.255.255.0				
port6	192.168.5.99/255.255.255.0				

When you initially set up FortiDeceptor, the interface configuration in *Network* > *Interfaces* is provisioned automatically. You do not need to change this section as these network settings are just for internal use. The actual deception network interfaces that connect to the monitored segments are configured under *Deception* > *Deployment Network*.

In this environment, port3 is used to deploy a Linux-based deception VM (decoy). The goal is to monitor network activity in two different VLANs where the production servers reside: WebServer-1 (192.168.11.11/24) in VLAN11 and WebServer-2 (192.168.21.21/24) in VLAN21.



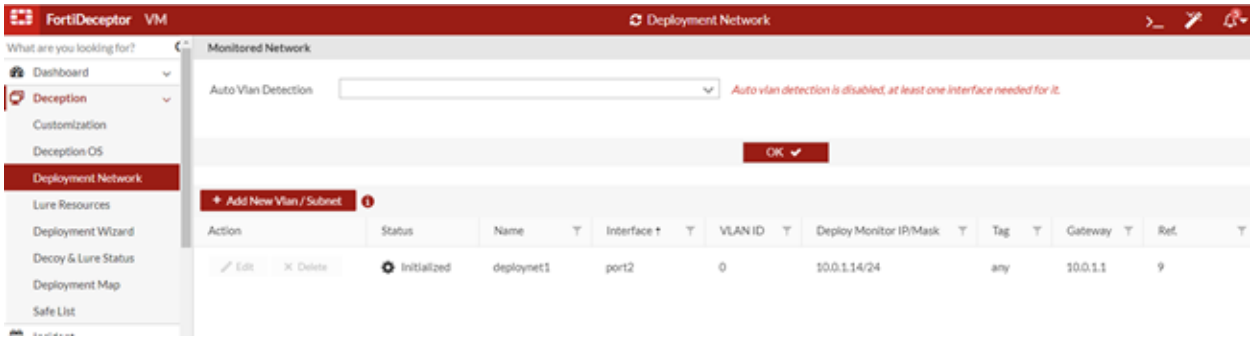
The deception VM has a single network interface to monitor two different VLANs so it is necessary to configure VLAN trunking between port3 and the ESXi vSwitch port. There is only one vSwitch to connect all the devices together using different virtual ports for each device.

Configuring FortiDeceptor

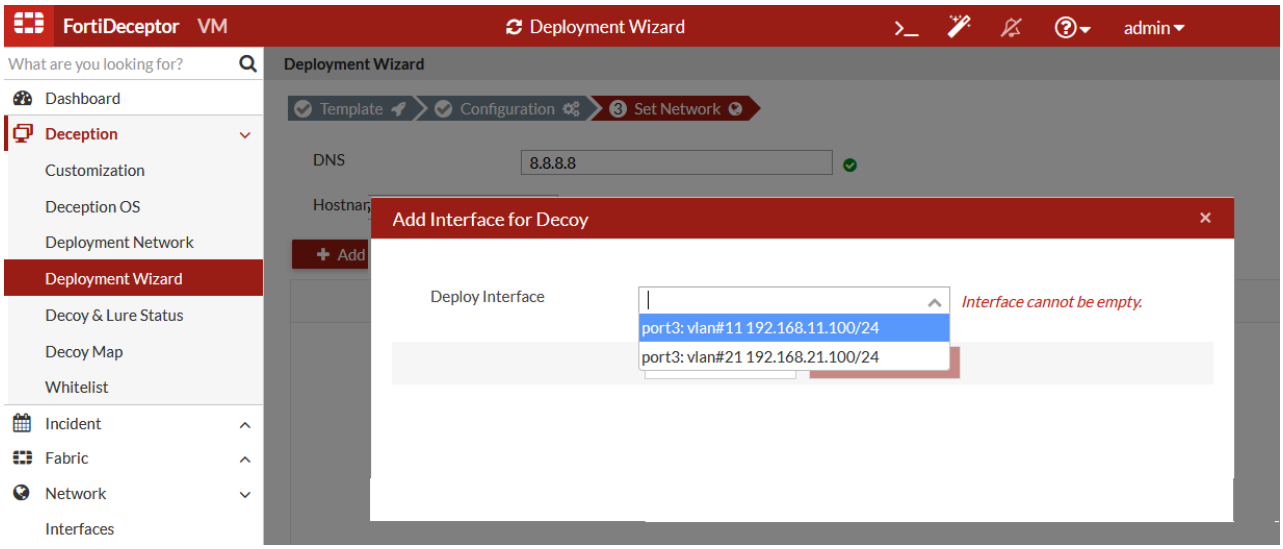
Configure FortiDeceptor to monitor the subnet networks, one for each VLAN, using the same network port3.

To configure FortiDeceptor:

1. Go to *Deception* > *Deployment Network* and click *Add New Vlan / Subnet* to add the monitored segments.

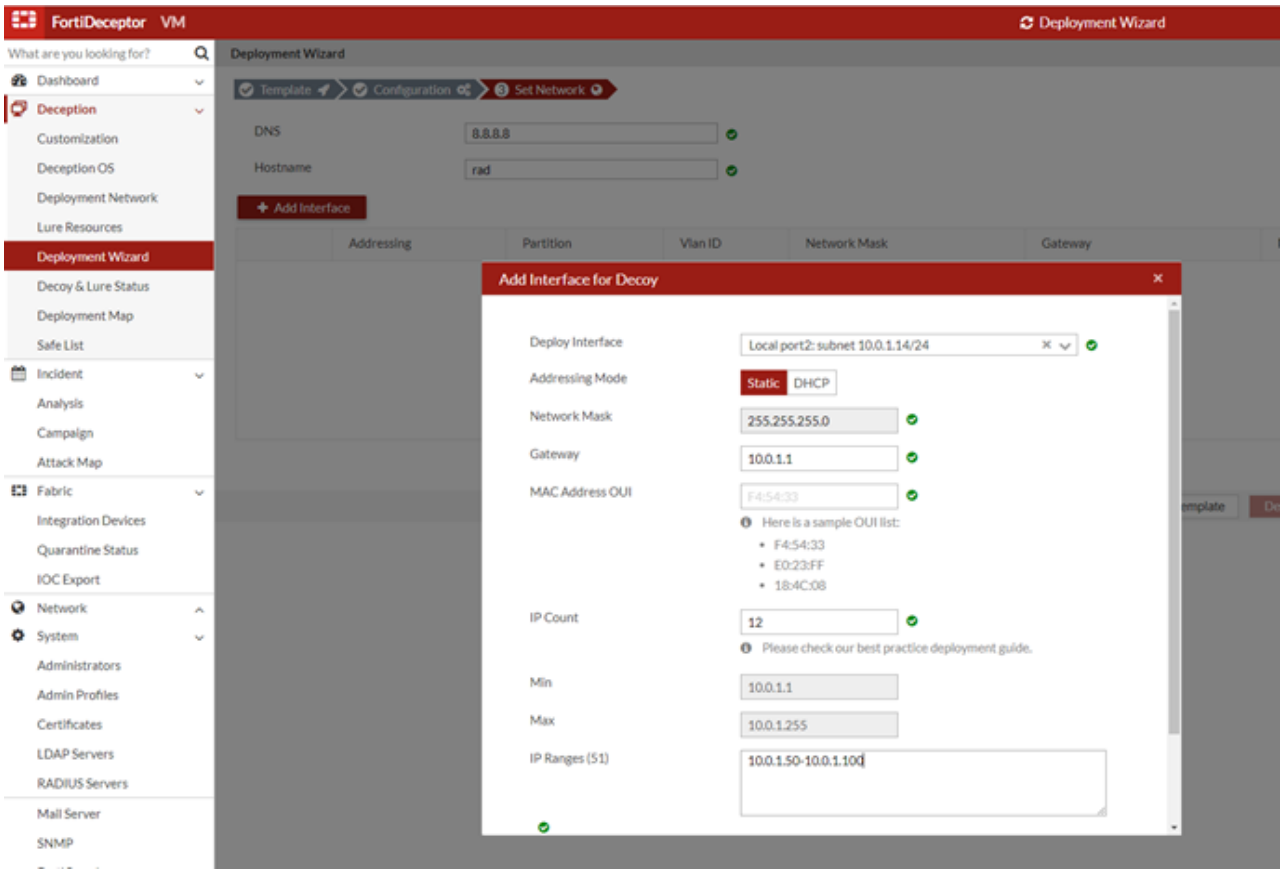


2. Use the VLAN tag for each monitored subnet so that FortiDeceptor can differentiate the traffic between them. Verify that both VLANs use port3.
3. Specify the *Deploy Network IP/Mask* that the deception VM use to monitor its decoys on each segment. Ensure these IP addresses are unique and belong to the monitored subnets.
4. Go to *Deception* > *Deployment Wizard* to deploy the actual deception VM and attach the monitored segments.

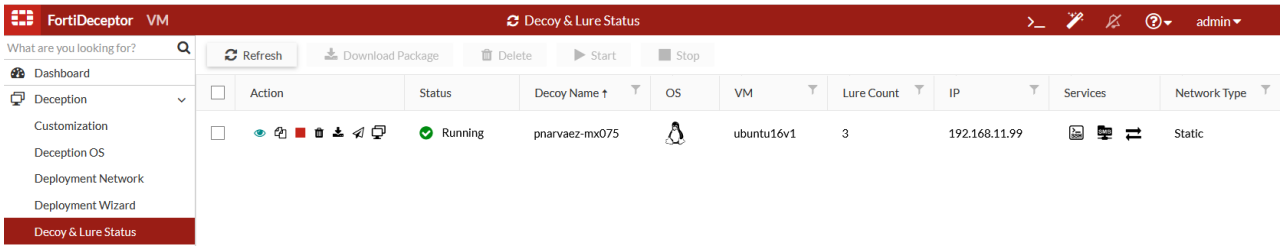


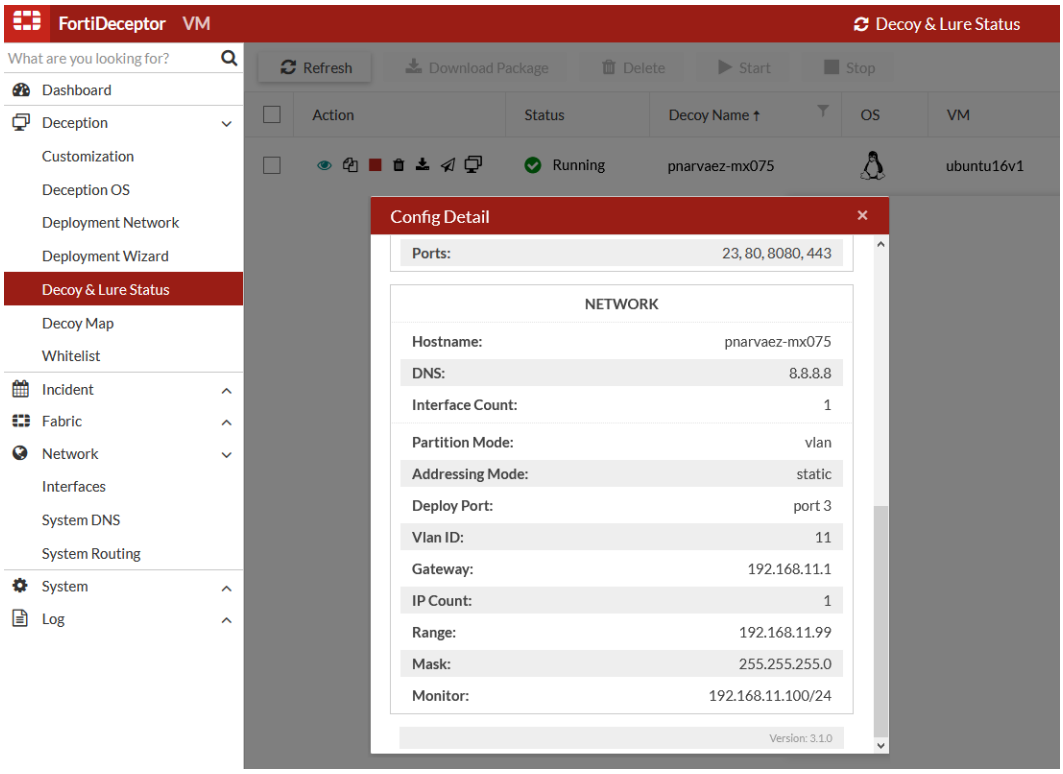
5. Specify the network settings for the decoys.
   FortiDeceptor automates the creation of deception VMs and decoy services to lure and expose attackers; so decoy services on each segment require dedicated IP addresses to interact with attackers.

If you want to use a static IP address for the decoy services, click *Static*, then specify a single IP address or IP address range in *IP Ranges*.

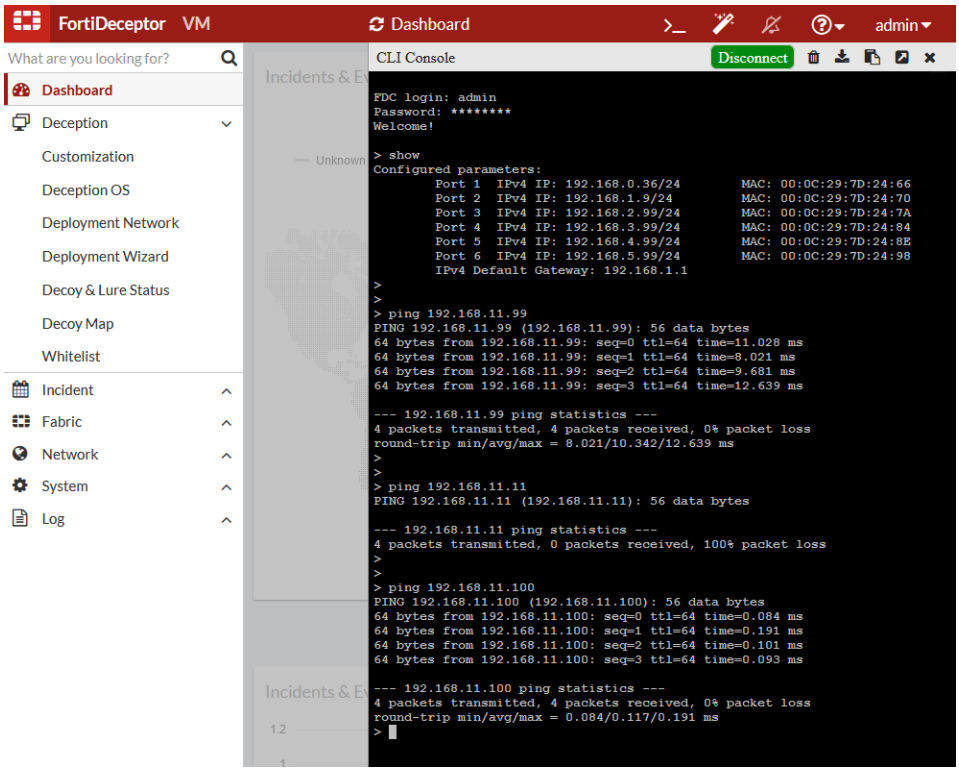


6. After completing VM deployment, go to *Decoy & Lure Status* to validate the configuration.





7. Test connectivity by pinging the decoy and the monitoring IP addresses and verify that they are reachable. The web servers are not reachable as ESXi is not configured yet.



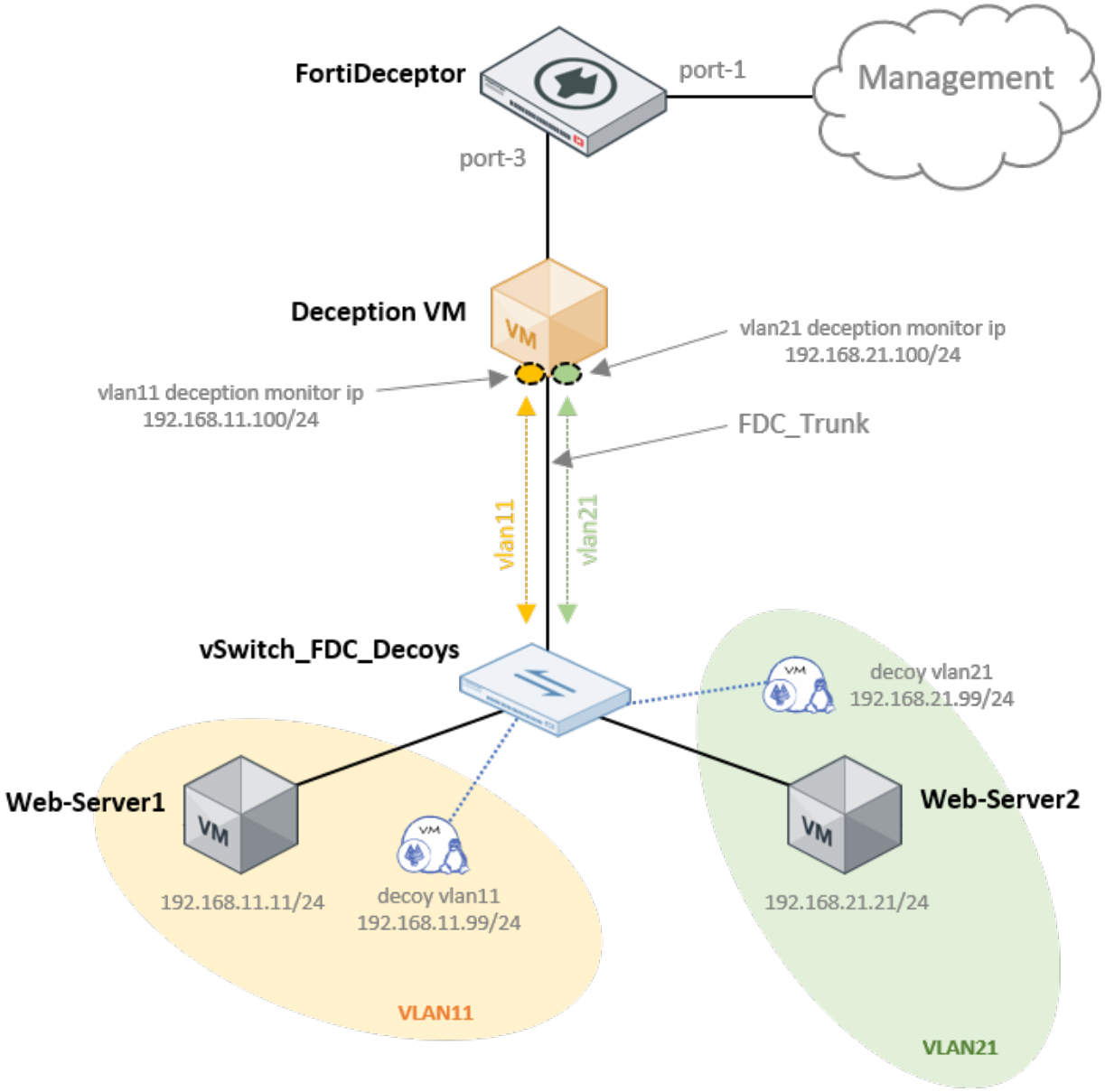
From the networking perspective, FortiDeceptor is ready to monitor both VLANs over port3. However, to activate the logical trunk interface, FortiDeceptor needs to receive VLAN trunking traffic from the vSwitch port.

If you have a physical switch connected to the ESXi host, you must configure 802.1Q on the switch port that is connected to the host uplink.

Configuring the vSwitch

To simplify configuration, we recommend using a dedicated vSwitch for the decoy and monitored segments.

The following diagram shows the vSwitch ports relationship.

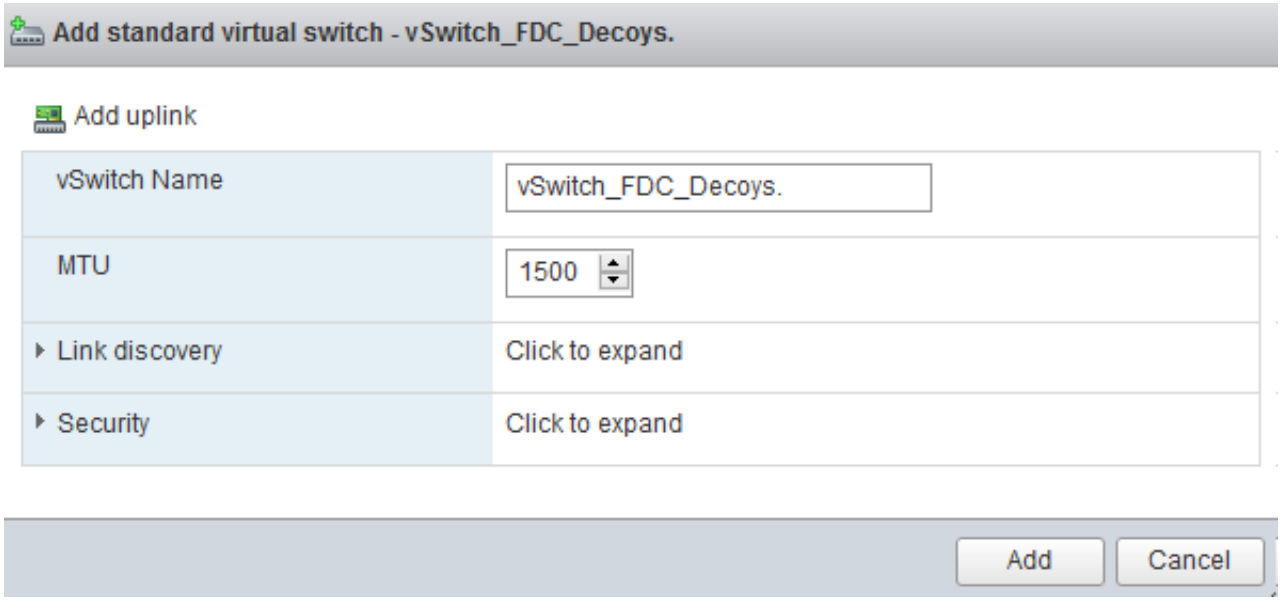


On ESXi, configure the *vSwitch_ FDC_Decoys* vSwitch to connect both VLANs to FortiDeceptor. Then configure three network port-groups:

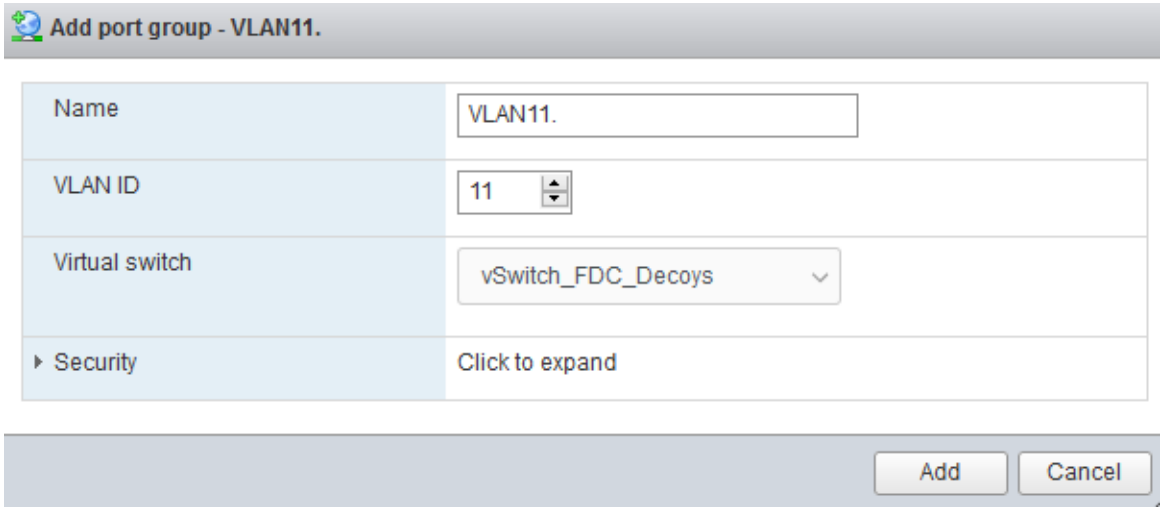
1. *FDC_Trunk* – Port-group for the actual trunk interface between FortiDeceptor and vSwitch.
2. *VLAN11* – Port-group to connect VLAN11 to vSwitch.
3. *VLAN21* – Port-group to connect VLAN21 to vSwitch.

To configure the vSwitch:

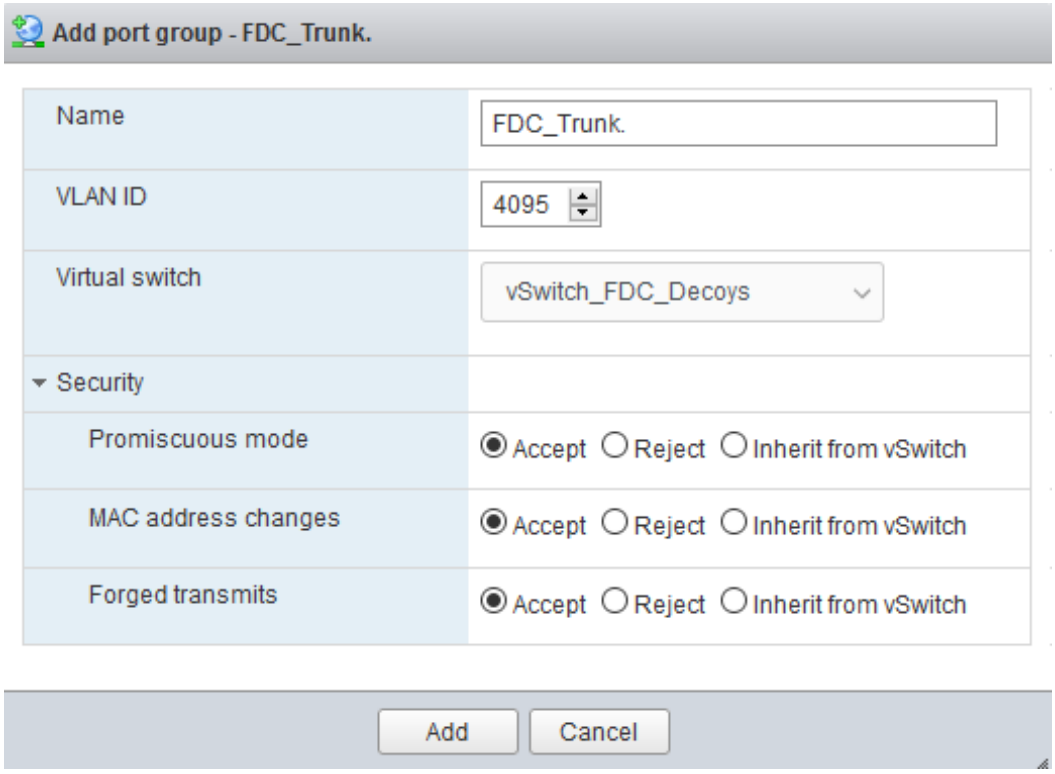
1. On the ESXi client, go to *Networking* > *Virtual Switches* and add a standard virtual switch.
   Just configure the *vSwtich Name*, remove the uplink (unless you need it), and use default values for the other options.



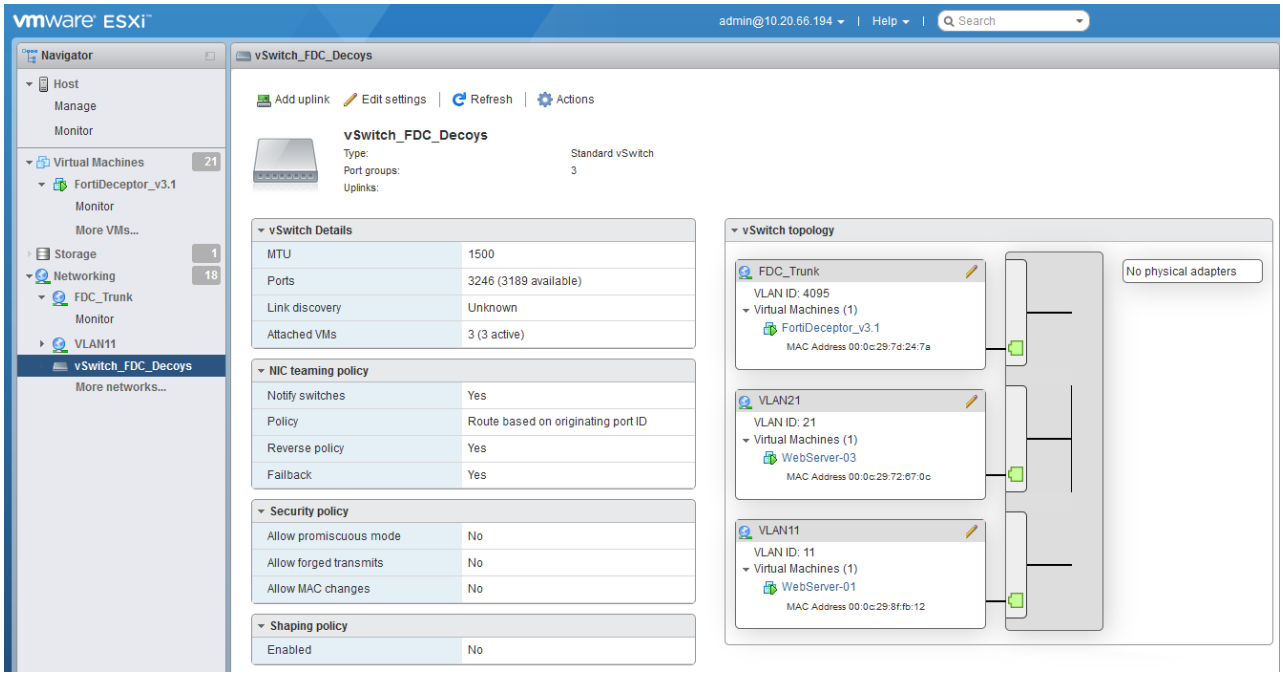
2. Go to *Networking* > *Port groups* and add the port groups.
   Port groups for VLAN11 and VLAN21 are similar. For each port group, specify a *Name*, configure the *VLAN ID*, and select the *Virtual switch*.



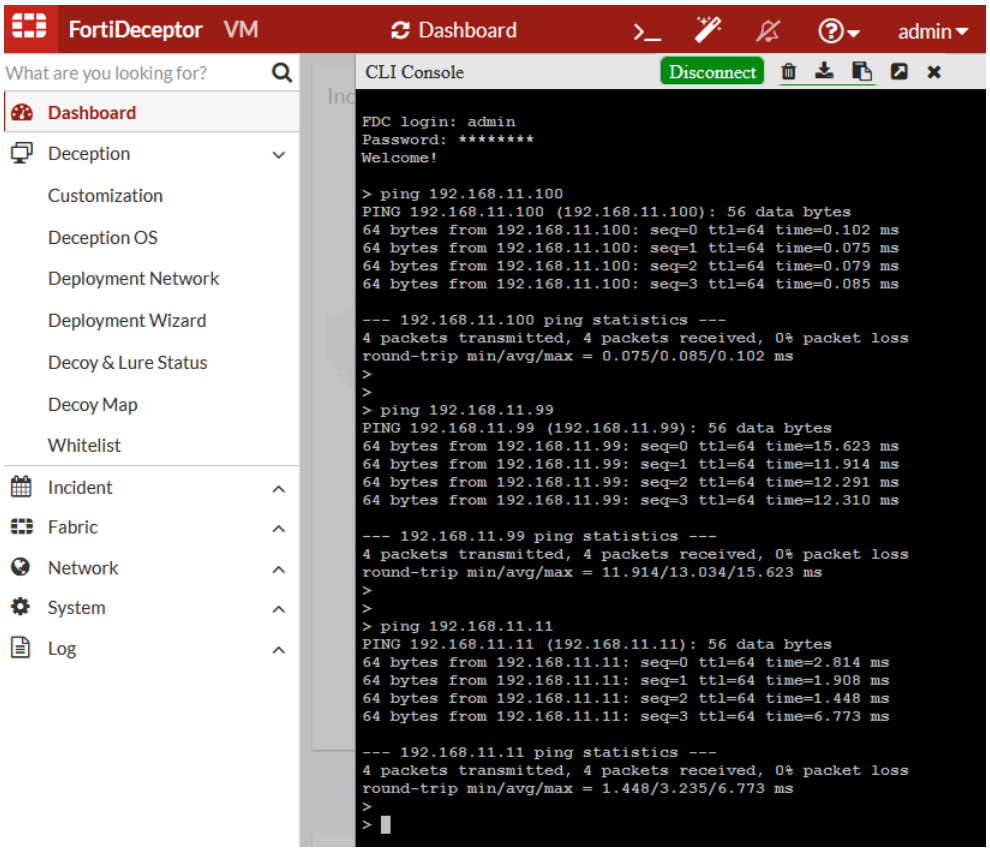
3. For the FDC Trunk port, configure a special port-group.
   On ESXi, you do not need to configure 802.1Q. You only need to set the port group to be a promiscuous interface and specify *4095* for the *VLAN ID* so the vSwitch can send and receive traffic from the VLANs configured on FortiDeceptor.
   Select the *Virtual switch* and set all *Security* options to *Accept*.



4. To verify the configuration, check the vSwitch topology and ensure all devices are connected to this switch.



5. Test connectivity from FortiDeceptor to the web servers, and from each web server to the decoys connected to the same VLAN.
   - From FortiDeceptor.



   - From web server 1.

```
fortinet@Web1:~$
fortinet@Web1:~$ ping 192.168.11.99
PING 192.168.11.99 (192.168.11.99) 56(84) bytes of data.
64 bytes from 192.168.11.99: icmp_seq=1 ttl=64 time=12.3 ms
64 bytes from 192.168.11.99: icmp_seq=2 ttl=64 time=43.2 ms
64 bytes from 192.168.11.99: icmp_seq=3 ttl=64 time=12.5 ms
64 bytes from 192.168.11.99: icmp_seq=4 ttl=64 time=12.6 ms
64 bytes from 192.168.11.99: icmp_seq=5 ttl=64 time=12.0 ms
^C
--- 192.168.11.99 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4017ms
rtt min/avg/max/mdev = 12.077/18.577/43.294/12.360 ms
fortinet@Web1:~$
fortinet@Web1:~$ ping 192.168.11.100
PING 192.168.11.100 (192.168.11.100) 56(84) bytes of data.
64 bytes from 192.168.11.100: icmp_seq=1 ttl=64 time=1.72 ms
64 bytes from 192.168.11.100: icmp_seq=2 ttl=64 time=0.894 ms
64 bytes from 192.168.11.100: icmp_seq=3 ttl=64 time=2.14 ms
64 bytes from 192.168.11.100: icmp_seq=4 ttl=64 time=1.15 ms
64 bytes from 192.168.11.100: icmp_seq=5 ttl=64 time=1.32 ms
^C
--- 192.168.11.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.894/1.448/2.146/0.440 ms
fortinet@Web1:~$
```

How to setup and use LDAP/RADIUS servers

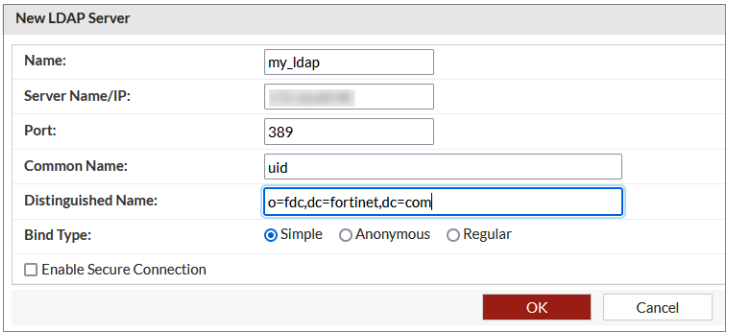
1. Set up the LDAP server

Requirements:

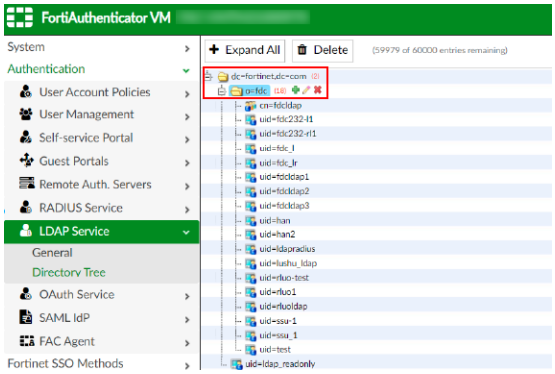
- FortiAuthenticator login credentials

To set up the LDAP server:

1. In FortiDeceptor Go to *System* > *LDAP Servers*.
2. Click *Create New*. The *New LDAP Server* window opens.
3. Configure the LDAP server settings, see LDAP Servers on page 131.



You must use the following format for the *Distinguished Name* field :*<root_node>,<subordinate_node>*. To find the names of the Root and Subordinate nodes in FortiAuthenticator, by go to *LDAP Service* > *Directory Tree*.



Setup the RADIUS server

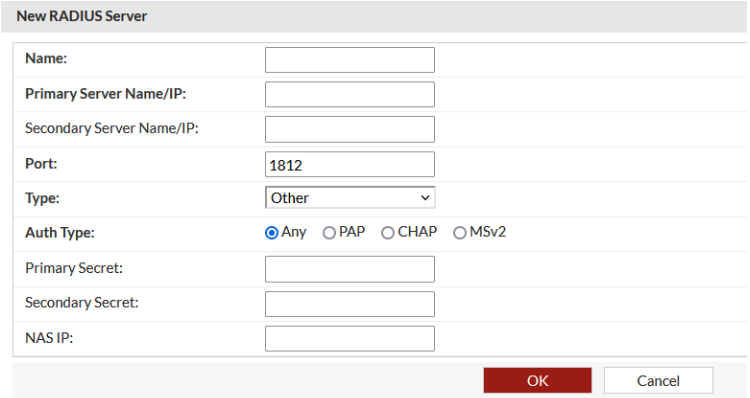
Requirements:

- FortiAuthenticator login credentials

To set up the RADIUS server in FortiDeceptor:

1. Go to *System* > *RADIUS Servers*.
2. Click *Create New*. The *New RADIUS Server* window opens.

3. Configure the RADIUS server settings. See RADIUS Servers on page 132.



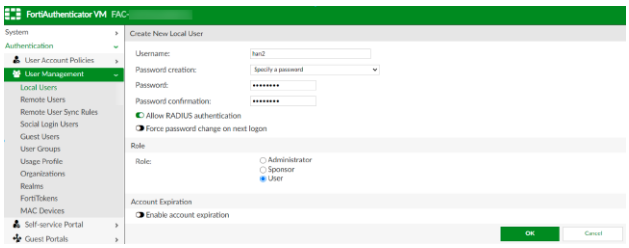
In the *Primary Secret* field enter, *fortinet*.

3. Create an account in FortiAuthenticator and enable LDAP/RADIUS

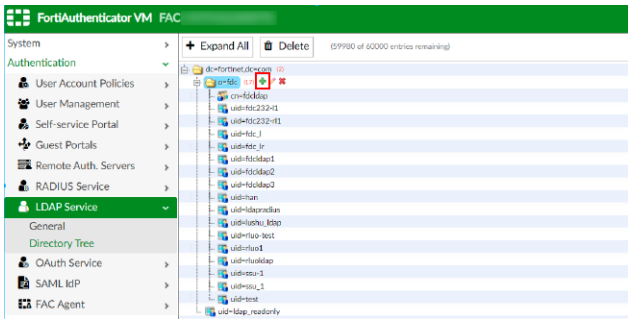
You do not need to complete this step if you already have a FortiAuthenticator account.

To enable LDAP/RADIUS:

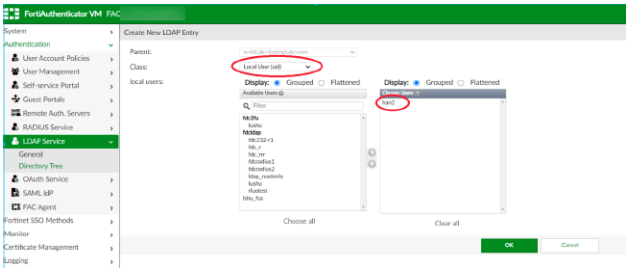
1. In FortiAuthenticator, go to *User Management* > *Local Users* and create a new account.
   a. Enable *Allow RADIUS authentication*.
   b. In the *Password* and *Password confirmation* fields, enter `fortinet`.



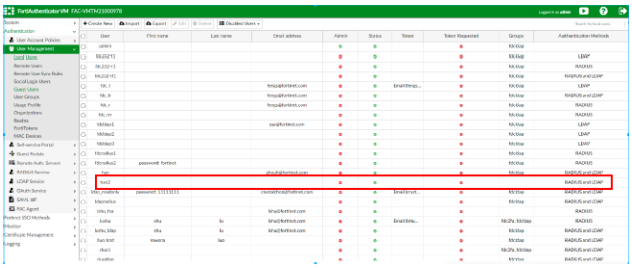
2. Go *LDAP Service* > *Directory Tree* to enable LDAP.
3. Expand the Root node, and then click the green plus symbol next to the Subordinate node. The *Create New LDAP entry* window opens.



4. From the *Class* dropdown, select *Local User (uid)*.



5. Go to *User Management* > *Local Users* to verify the RADIUS and LDAP servers are enabled. To do this, check that the *Authentication Methods* column shows *RADIUS and LDAP*.



4. Create login account using LDAP/RADIUS accounts from FortiAuthenticator

To create a login account with LDAP/RADIUS:

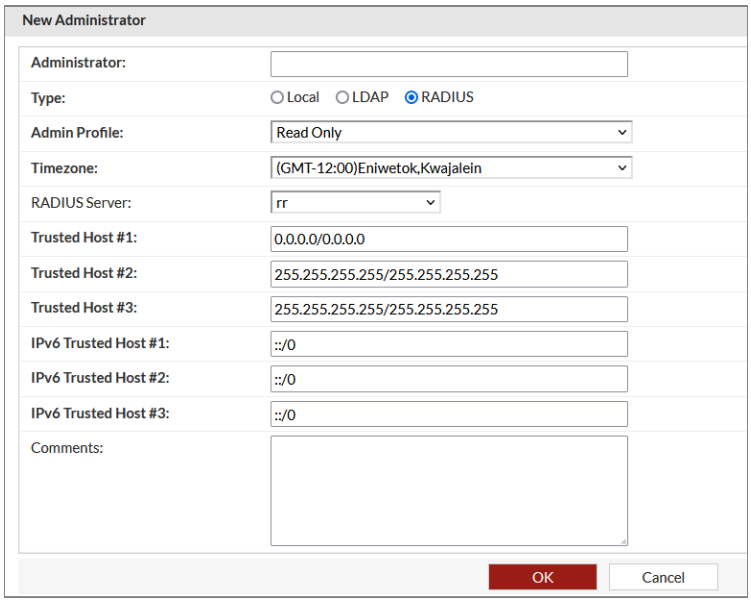
1. In FortiAuthenticator, go to *User Management* > *Local Users* and locate an account that has LDAP/RADIUS enabled. To do this, look in the *Authentication Methods* column for *RADIUS and LDAP*.
2. In FortiDeceptor, go to *System* > *Administrators* and click + *Create New* to create a new administrator. The *New Administrator* window opens.
3. Configure the administrator settings.

The values for the *Administrator*, *Type*, and *LDAP Server* fields must match the user's settings in FortiAuthenticator.

---

4. Log in to FortiDeceptor with the administrator account you created.
5. Go to *System* > *Administrators* and click + *Create New* . The *New Administrator* window opens.

6. Create a new administrator and set the *Type* to *RADIUS*.



7. Log in to FortiDeceptor with the RADIUS administrator account you created.

Appendix C - Hardening

System hardening reduces security risks by eliminating potential attack vectors and shrinking the system's attack surface. This section covers some of the actions that can be used.

Building security into FDC-OS

The FortiDeceptor operating system, FortiDeceptor hardware devices, and FortiDeceptor virtual machines (VMs) are built with security in mind, so many security features are built into the hardware and software. Fortinet maintains an ISO:9001 certified software and hardware development processes to ensure that FortiDeceptor products are developed in a secure manner.

Boot device security

The FortiDeceptor boot device in hardware devices use Fortinet’s customized bootloader which is specifically designed and implemented for the FortiDeceptor product. FortiDeceptor physical devices always boot from this boot device.

FDC-OS kernel and user processes

FortiDeceptor is a multi-process operating system with kernel and user processes. The FortiDeceptor kernel runs in a privileged hardware mode while higher-level applications run in user mode. FortiDeceptor is a closed system that does not allow the loading or execution of third-party code in the FortiDeceptor user space. All non-essential services, packages, and applications are removed.

Physical security

Install the FortiDeceptor in a physically secure location. Physical access to the FortiDeceptor can allow it to be bypassed, or other firmware could be loaded after a manual reboot.

Optionally, disable the maintainer account with CLI command set-maintainer. Note that doing this will make you unable to recover administrator access using a console connection if all of the administrator credentials are lost.

Vulnerability - monitoring PSIRT

The *FortiGuard Labs Product Security Incident Response Team* (PSIRT) continually tests and gathers information about Fortinet hardware and software products, looking for vulnerabilities and weaknesses. Any such findings are fed back to Fortinet's development teams and serious issues are described along with protective solutions. The PSIRT regulatory releases PSIRT advisories when issues are found and corrected. Advisories are listed at https://www.fortiguard.com/psirt.

Firmware

Keep the FortiDeceptor firmware up to date. The latest patch release has the most fixed bugs and vulnerabilities, and should be the most stable. Firmware is periodically updated to add new features and resolve important issues.

- Read the release notes. The known issues may include issues that affect your business.
- Do not use out of support firmware. Review the product lifecycle and plan to upgrade before the firmware expires.
- Optionally, subscribe to the Fortinet firmware RSS feed: https://pub.kb.fortinet.com/rss/firmware.xml.

Encrypted protocols

Use encrypted protocols whenever possible, for example, SNMPv3 instead of SNMP, SMTPS instead of SMTP, SSH instead of telnet and HTTPS instead of HTTP.

Strong ciphers

FortiDeceptor already sets to use higher levels of encryption and strong ciphers for communications with Fortinet fabric devices.

FortiGuard databases

Ensure that FortiGuard databases, such as Industry Security Signature, Network Alerts Signature, AntiVirus Scanner and Signatures, AI Malware Engine and ARAE Engines are updated punctually.

Trusted Hosts

Limit access to the FortiDeceptor to a management interface on a management network. Trusted hosts can also be used to specify the IP addresses or subnets that can log in to the FortiDeceptor. When authenticating to the FortiDeceptor,

implement two-factor authentication (2FA). This makes it significantly more difficult for an attacker to gain access to the FortiDeceptor.

Limit login user's access right

The features that a login user can access should be limited to the scope of that user's work to reduce possible attack vectors. The admin profile tied to the user account defines the areas on the FortiDeceptor that the user can access, and what they can do in those areas. The list of users with access should be audited regularly to ensure that it is current.

Administration access security

Secure administrative access features:

- SSH, Telnet, and SNMP are disabled by default. If required, these admin services must be explicitly enabled on each interface from the GUI or CLI.
- SSHv1 is disabled by default. SSHv2 is the default version.
- SSLv3 and TLS1.0 are disabled by default. TLSv1.1 and TLSv1.2 are the SSL versions enabled by default for HTTPS admin access.
- HTTP is disabled by default, HTTP redirect to HTTPS is enabled by default.
- The strong-crypto global setting is enabled by default and configures FortiDeceptor to use strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH/TLS/SSL functions.

Admin administrator account

All FortiDeceptor ship with a default administrator account called *admin*. By default, this account does not have a password. However, FortiDeceptor uses restricted password policy that enforce the admin account to change the password on the first user login and use a complex password. (This mechanism is enforced across all users upon their first log in.)

Maintainer account

Administrators with physical access to a FortiDeceptor appliance can use a console cable and a special administrator account called maintainer to log into the CLI. When enabled, the maintainer account can be used to log in from the console after a hard reboot. The password for the maintainer account is *bcpb* followed by the FortiDeceptor serial number. An administrator has 60-seconds to complete this login using the CLI command `admin-pwd-reset`

The only action the maintainer account has permissions to perform is to reset the passwords of `super_admin` accounts. Logging in with the maintainer account requires a hard boot of the FortiDeceptor.

FortiDeceptor generates event log messages when you log in with the maintainer account and for each password reset.

Non-factory SSL certificates

Non-factory SSL certificates should be used for the FortiDeceptor web management interface.

The default Fortinet factory self-signed certificates are provided to simplify initial installation and testing. Using these certificates leaves you vulnerable to man-in-the-middle attacks, where an attacker spoofs your certificate, compromises your connection, and steals your personal information.

Your administrator web portal should also be configured with a server certificate from a trusted CA.

Other recommended actions user can take

The following general administrative settings are recommended:

- Set the idle timeout time for login users to a low value, preferably less that ten minutes.
- In Interfaces page, limit access right for network ports.
- Replace the certificate that is offered for HTTPS access with a trusted certificate that has the FQDN or IP address of the FortiDeceptor.
- For local accounts on the FortiDeceptor, try upgrading to FortiDeceptor to V4.3.0 and later which enforces a default password policy with minimum complexity level.
- Do not use shared accounts to access the FortiDeceptor. Shared accounts are more likely to be compromised, are more difficult to maintain as password updates must be disseminated to all users, and make it impossible to audit access to the FortiDeceptor.

Appendix D - Configuration examples

This section provides configuration examples to integrate FortiDeceptor with other Fabric devices as well as third-party integrations.

This section contains the following topics:

- Configure FortiDeceptor for admin access authentication from Active Directory on page 234
- Configure a Active Directory (AD) user as FortiDeceptor administrator on page 239
- MFA (RADIUS) configuration on page 243
- Integrate with Checkpoint Firewall on page 246
- Integration with Crowdstrike on page 248
- Integrate with Cuckoo Sandbox on page 251
- Integration with FortiSIEM on page 254
- FortiSIEM Watch List on page 258
- Mitigation using windows Remote Command on page 262
- Integration with PAN devices on page 264
- Integration with Microsoft ATP on page 267
- Integration with FortiSandbox on page 269
- Integration with FortiNAC on page 272
- Integration with FortiEDR on page 277
- Integration with FortiAnalyzer on page 279
- Integration with FortiGate over Webhook on page 284
- Integrate with FortiGate 6.0.3 to 7.2.3 over REST-API on page 295
- Integrate FortiDeceptor with FortiGate over Fabric v7.2.4 on page 299
- Integrate with Cisco ISE on page 312

Configure FortiDeceptor for admin access authentication from Active Directory

To configure FortiDeceptor to authenticate from the Active Directory (AD) server, prepare and import a signed server certificate into FortiAuthenticator. Next you will configure the LDAP service and add the local user to the LDAP directory tree in FortiAuthenticator. Then you will import the server certificate and configure the LDAP server in FortiDeceptor.

FortiDeceptor admin access authentication from FortiAuthenticator

To configure FortiDeceptor admin access authentication front FortiAuthenticator using LDAP:

1. Prepare the certificate.
2. Import the signed server certificate to FortiAuthenticator.
3. Import the RootCA to FortiAuthenticator.
4. Configure the FortiAuthenticator LDAP Service.

5. Add the local user the LDAP Directory Tree.
6. Import the RootCA into FortiDeceptor.
7. Configure the LDAP server in FortiDeceptor.

1. Prepare the certificate

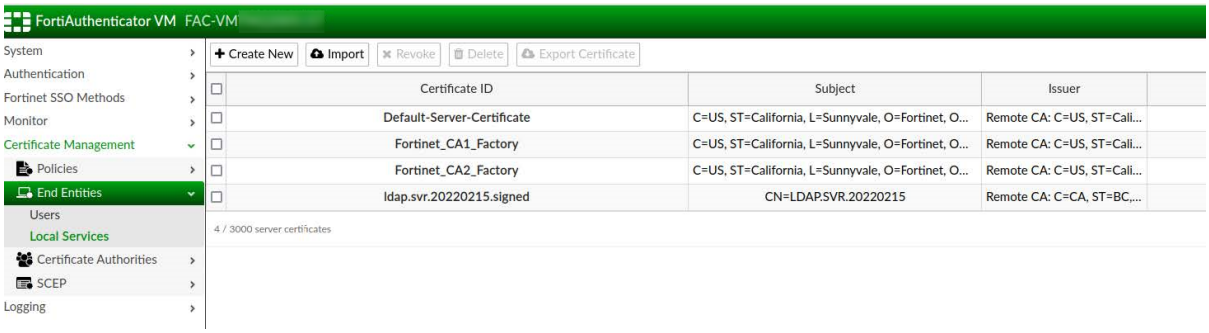
If you are not using LDAP, you can proceed directly to Step 5: Create LDAP Directory Tree.

To prepare the certificate:

1. Create a Certificate Signing Request (CSR) and private key.
2. Sign the CSR with either a public Certificate Authority (CA) or your own RootCA. For the purpose of this example, we will be using a self-created RootCA.

2. Import the signed server certificate to FortiAuthenticator

1. Log in to FortiAuthenticator.
2. Go to *Certificate Management* > *End Entities* > *Local Services* and click *Import*.



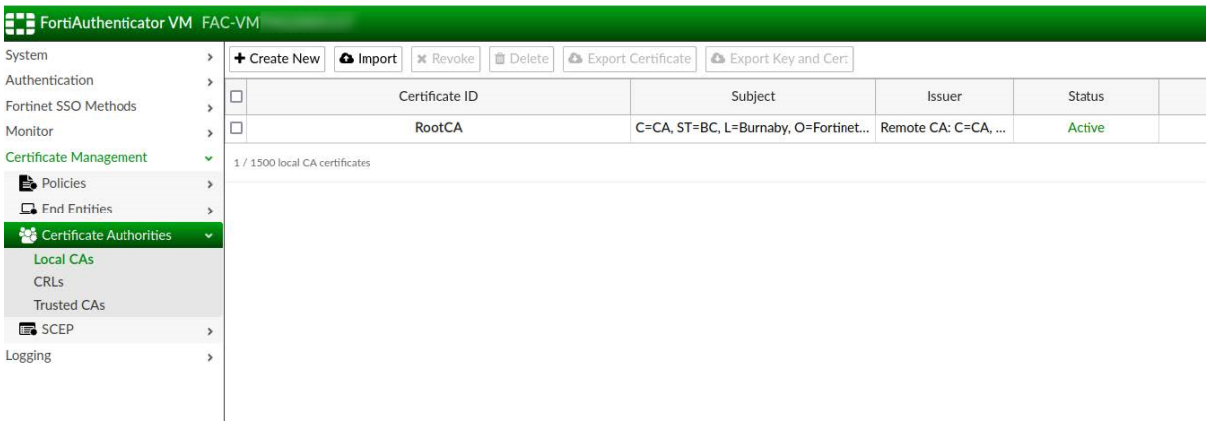
3. Select *Choose File* to locate the certificate file on your computer.
4. Select *OK* to import the certificate.

For more information, see *Certificate Management > End Entities* in the *FortiAuthenticator Administration Guide*.

3. Import the RootCA to FortiAuthenticator

1. Go to *Certificate Management* > *Certificate Authorities* > *Local CAs*.
2. Click *Create New* and configure the certificate settings.

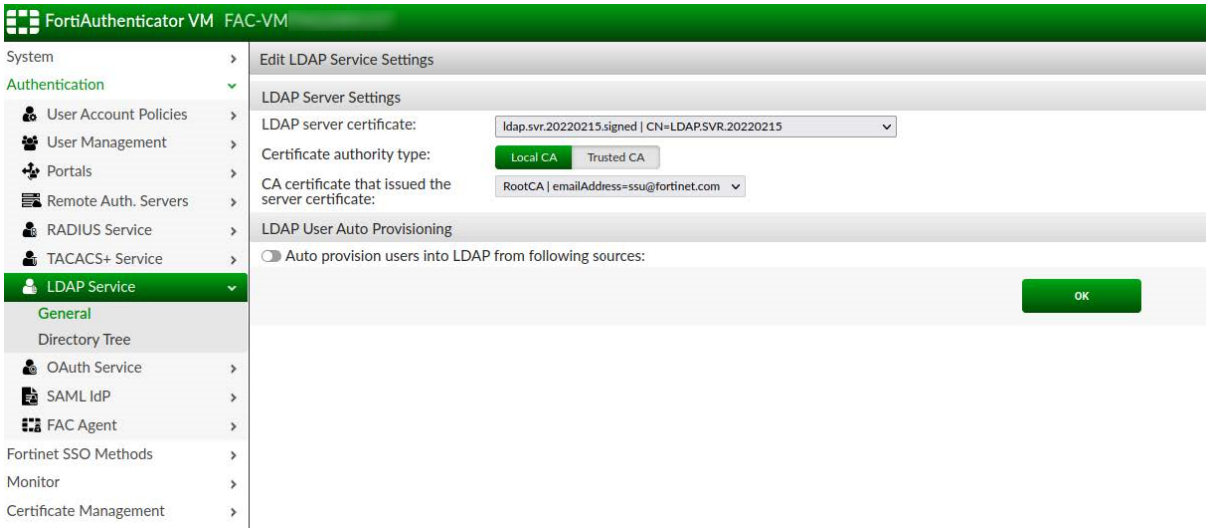
3. Click *OK* to create the new certificate.



For more information, see *Certificate Management > Certificate Authorities > Local CAs* in the *FortiAuthenticator Administration Guide*.

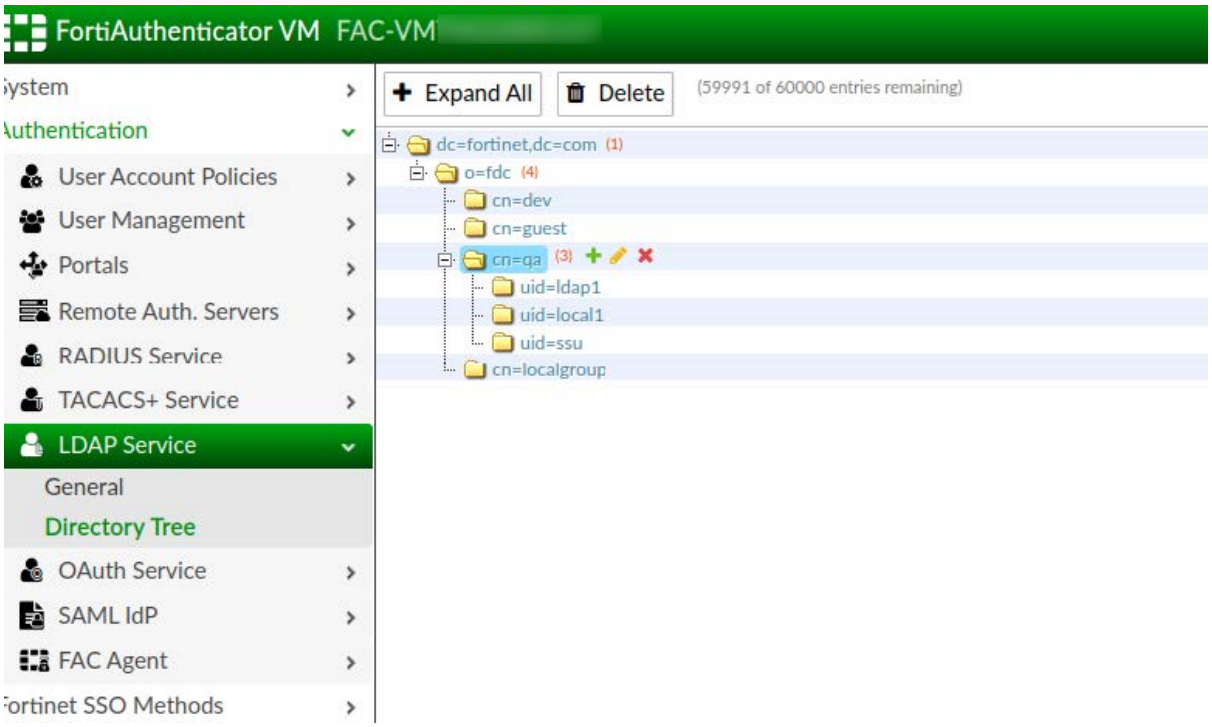
4. Configure the FortiAuthenticator LDAP Service

1. In FortiAuthenticator, go to *Authentication > LDAP Service > General*.
2. From the *LDAP server certificate* dropdown, select the server certificate you imported.
3. From the *CA certificate that issued the server certificate* dropdown, select *RootCA* and click *OK*.



5. Add the local user the LDAP Directory Tree

1. In FortiAuthenticator, from the LDAP directory tree, select the green plus (**+**) symbol next to the DN entry where you want to add the node. The *Create New LDAP Entry* window opens.



2. In the *Class* field, select the identifier to use.
3. Select the required value from the dropdown menu, or select *Create New* to create a new entry of the selected class.
4. Click *OK*.

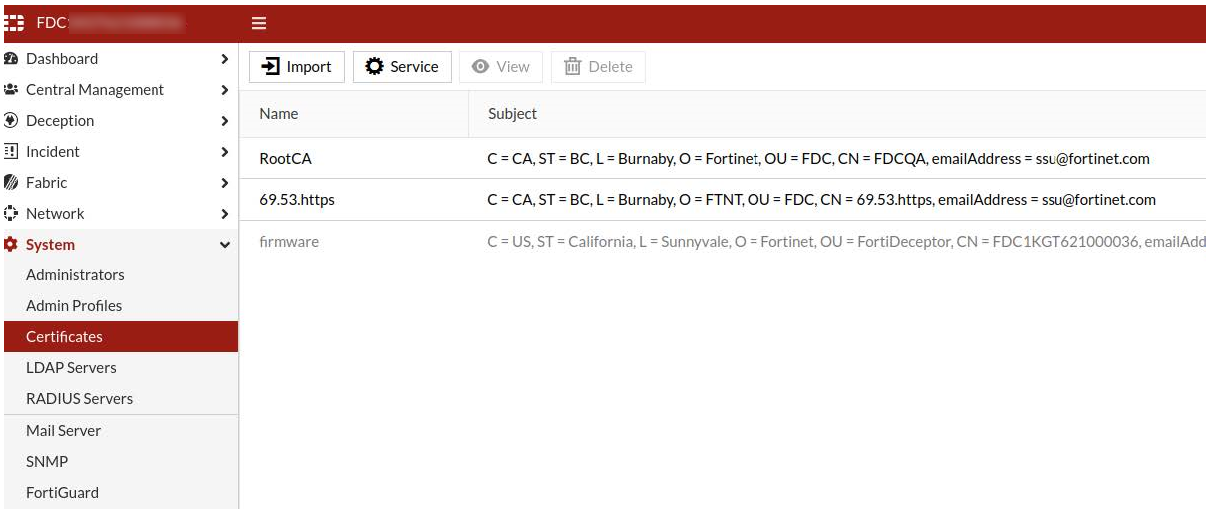
For more information, see *Creating the directory tree* in the in the *FortiAuthenticator Administration Guide*.

6. Import the RootCA into FortiDeceptor

If you are not using LDAP, proceed to Step 7. Configure the LDAP server in FortiDeceptor.

1. In FortiDeceptor, go to *System* > *Certificates* and click *Import*.
2. In the *Certificate* field, click *Browse* and upload a copy of the RootCA certificate you imported to FortiAuthenticator in Step 3 Import the RootCA to FortiAuthenticator.

3. Configure the rest of the certificate settings and click *OK*.

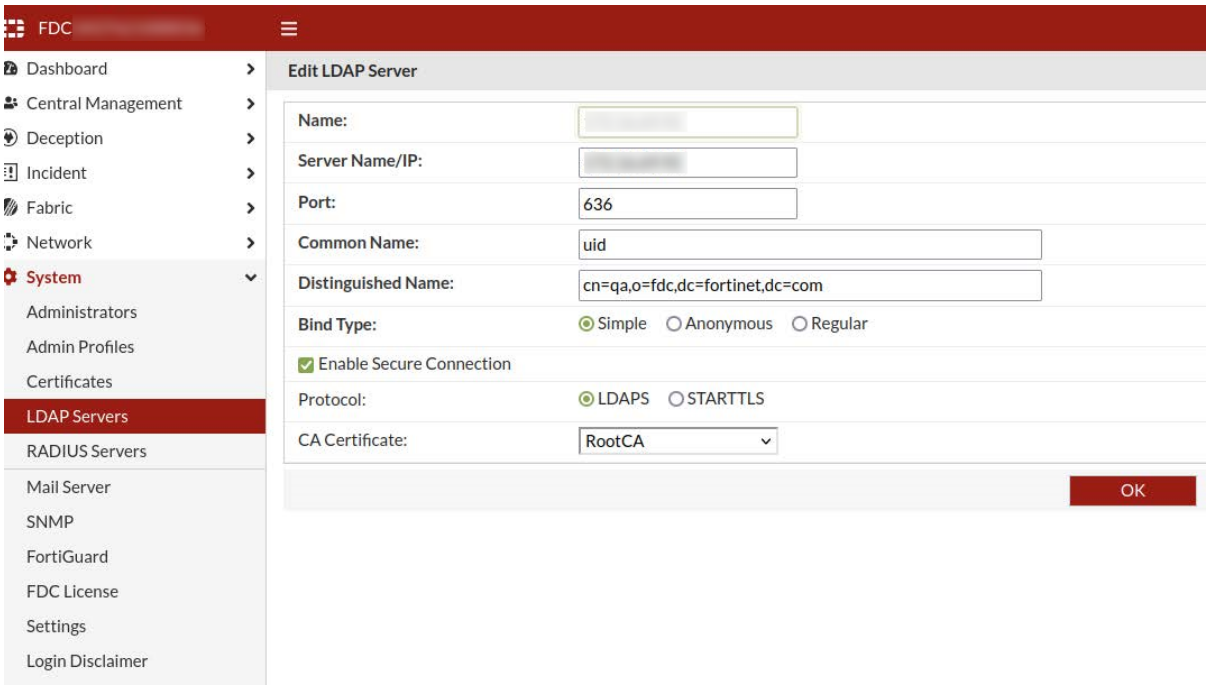


For more information, see Certificates on page 129.

7. Configure the LDAP server in FortiDeceptor

1. In FortiDeceptor, go to *System* > *LDAP servers* and click *Create New*. The *New LDAP Server* page opens.
2. Configure the LDAP settings keeping the following considerations in mind:

Common Name	The *Common Name* must match the node you created in the LDAP tree.
Enable Secure Connection	When enabled, you must select the RootCA you imported from the *CA Certificate* dropdown.



3. Click *OK*.

Configure a Active Directory (AD) user as FortiDeceptor administrator

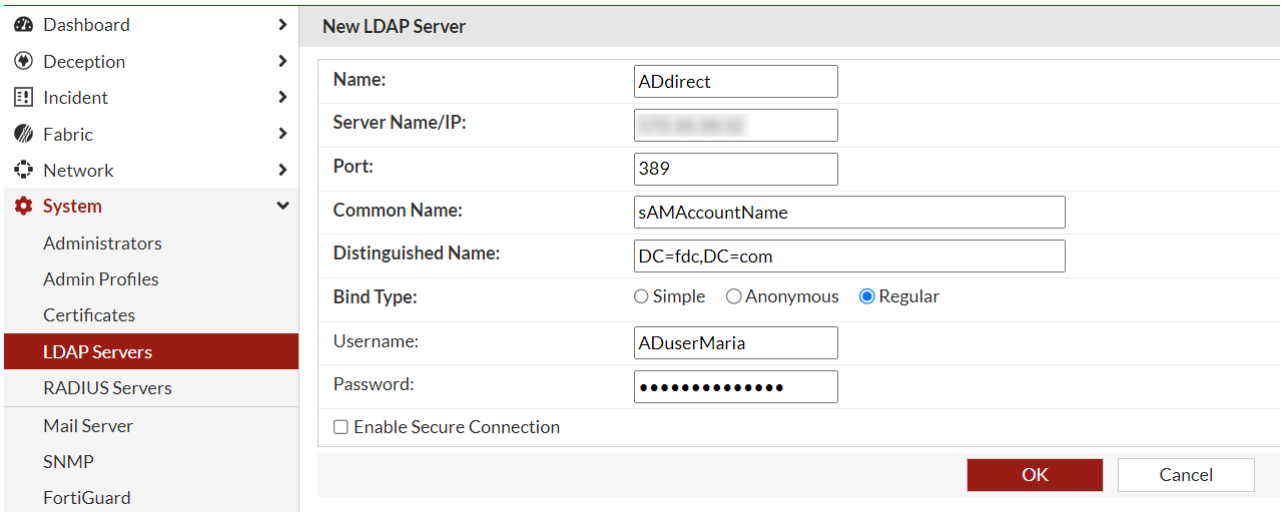
To configure an AD user as an administrator:

1. Configure the LDAP Server in FortiDeceptor.
2. Set the Active Directory user to be an administrator.

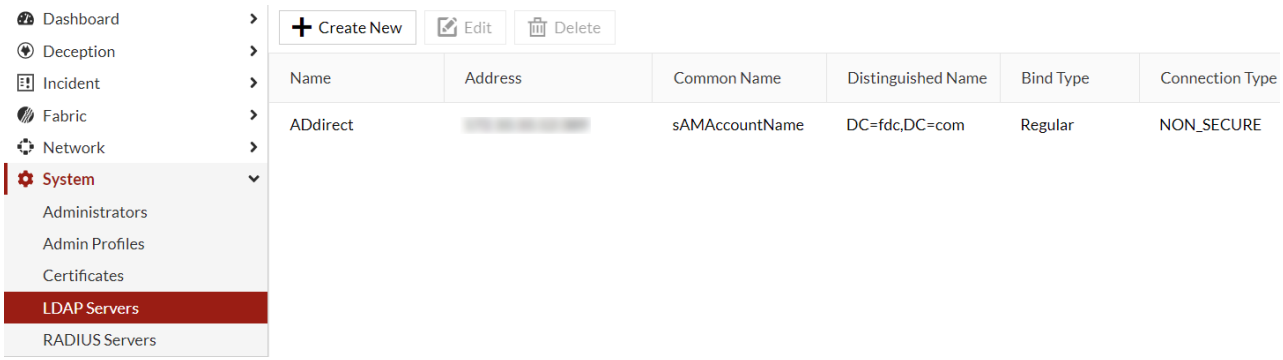
1. Configure the LDAP Server in FortiDeceptor

1. On the Active Directory server, enable LDAP signing.
2. Go to *System* > *LDAP Servers* and click *Create New*. The *New LDAP Server* page opens.
3. Configure the LDAP settings as follows:

Name	Enter a unique name for the LDAP server.
Server Name/IP	Enter the FQDN IP or address of the AD server.
Port	Enter the connection port of the LDAP server.
Common Name	Enter the name of the user identifier field on the LDAP server. In this example, *sAMAccountName*.
Distinguished Name	Enter the LDAP node where the user account entries can be found. In this example, *DC=fdc,DC=com*.
Bind Type	Select the binding type: • *Simple*: Bind using a simple password authentication without a search. • *Anonymous*: Bind using anonymous user search. • *Regular*: Bind using username/password and then search. Use simple authentication if the user records all fall under one distinguished name (DN). If the users are under more than one DN, use the anonymous or regular type, which can search the entire LDAP database for the required username. If the LDAP server requires authentication to perform searches, use the regular type and provide the *Username* and *Password*.
Username	Enter the LDAP server domain username.
Password	Enter the LDAP server domain password.
Enable Secure Connection	Enable or disable secure connection to the LDAP server.



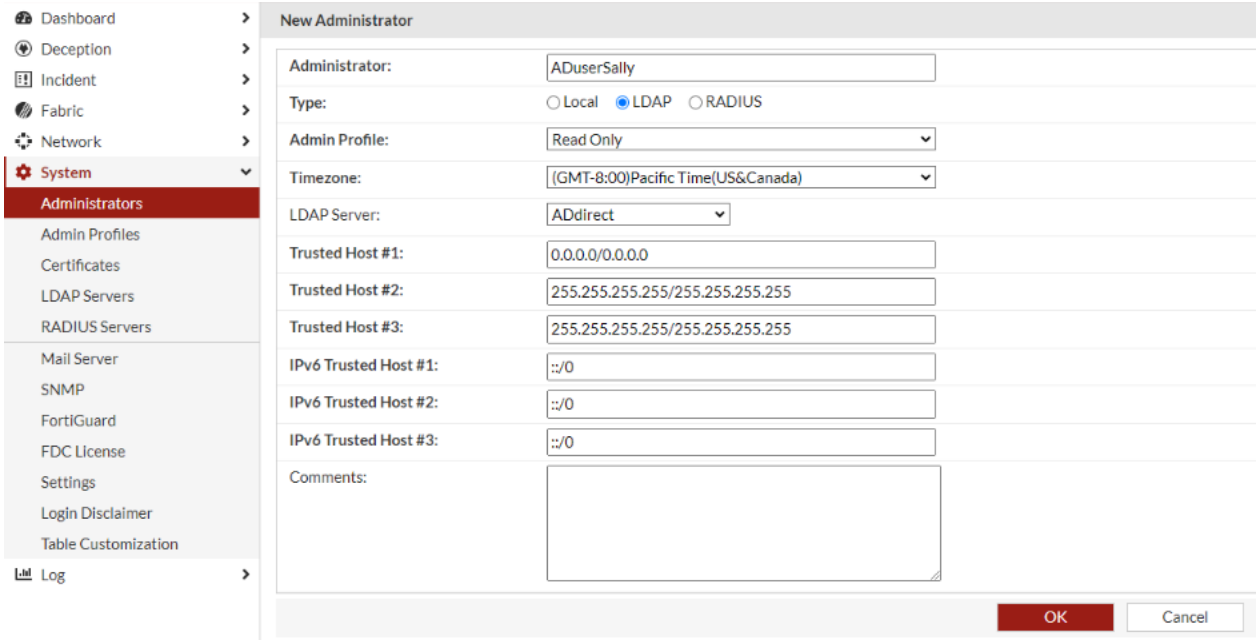
4. Click *OK*.



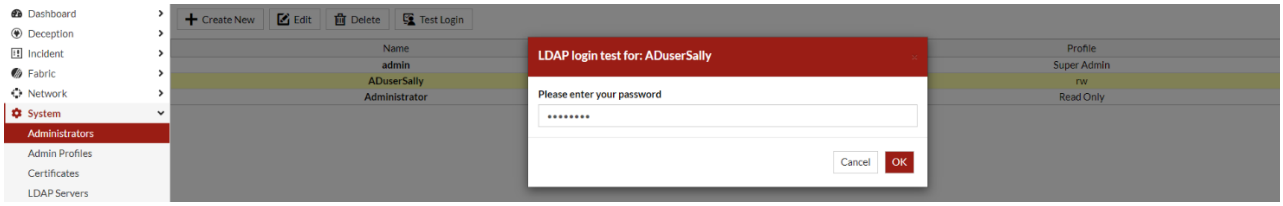
2. Set the Active Directory user to be an administrator

1. Go to *System* > *Administrators* and click *Create New*. The *New Administrator* page opens.
2. Configure the administrator settings keeping the following considerations in mind:

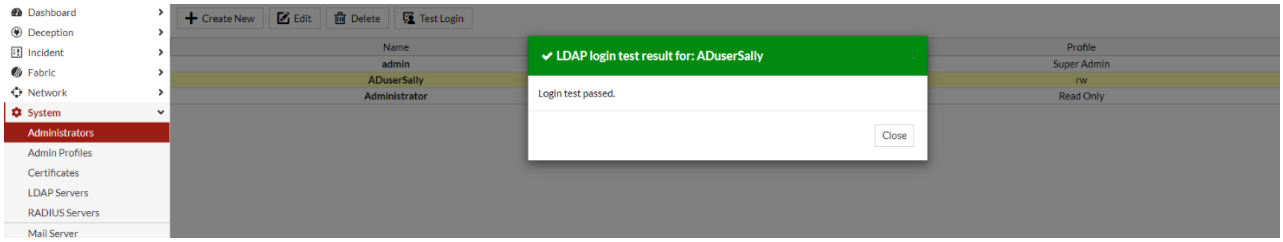
Type	Select *LDAP*.
LDAP Server	Select the LDAP server you created in Step 1.



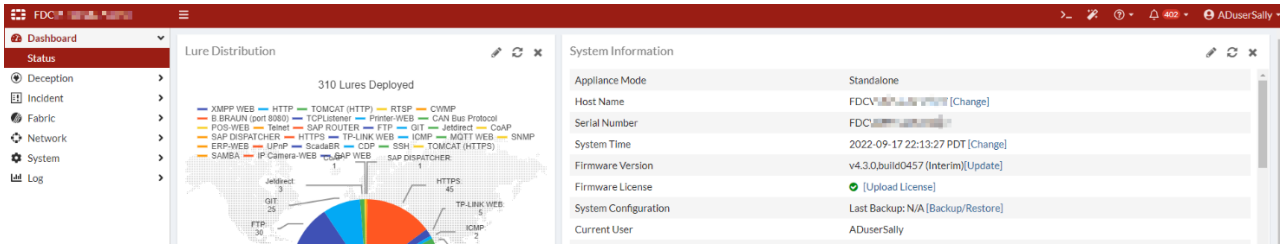
3. Click *OK*.
4. (Optional)To test the user credentials, select the user you created, and click *Test Login*.



Enter the password and click *OK*.



Use the Active Directory user account you created to log in to FortiDeceptor.



Import network users from the Active Director server for Decoy lure configuration

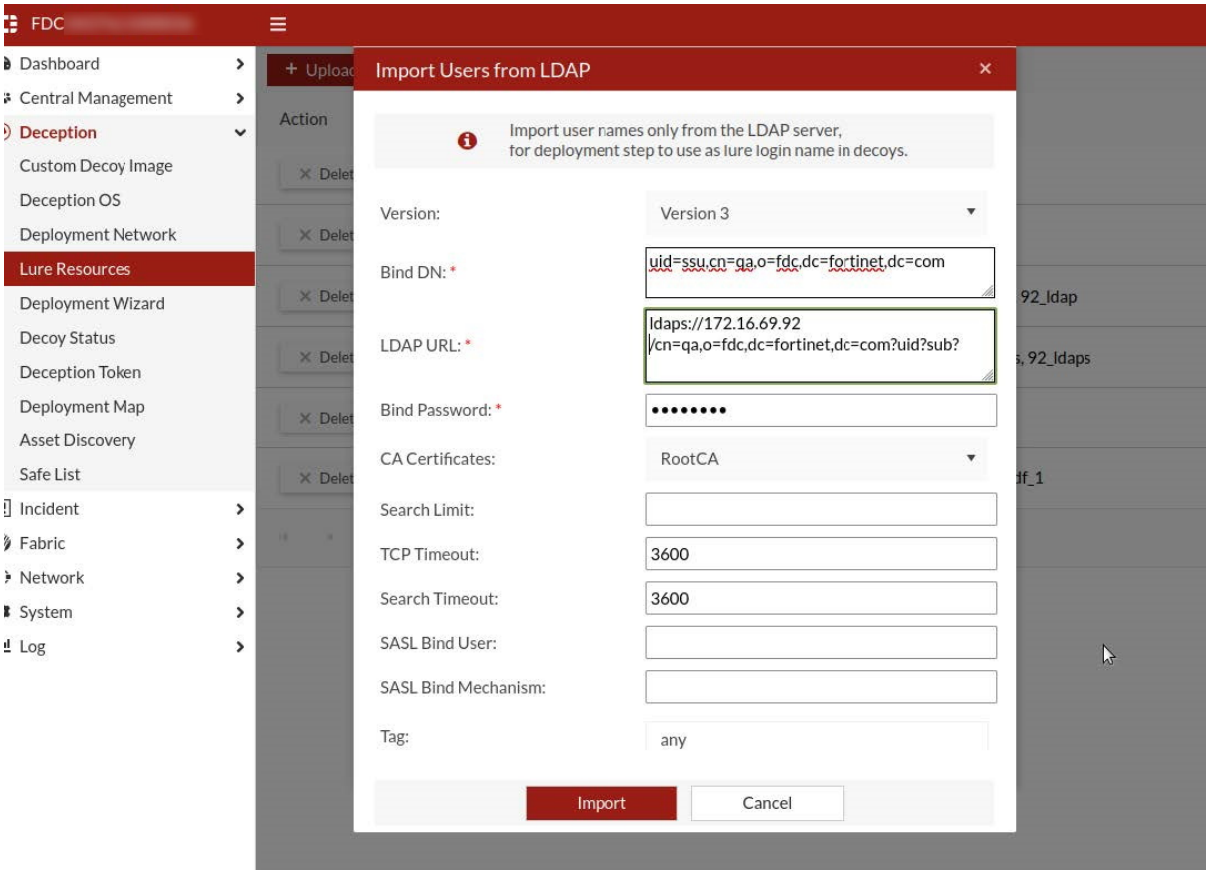
To Import the lure user from the Active Directory server:

1. In FortiDeceptor, go to *Deception > Lure Resources* and click *Import Users from LDAP*. The *Import Users from LDAP* dialog opens.
2. Configure the import and click *Import*. For more information, see Lure Resources on page 69.

Bind DN	Username used to connect to the LDAP service on the specified LDAP Server. For example: `uid=ssu.cn=qa.o=fdc.dc=fortinet.dc=com`

LDAP URL	Enter the LDAP URL using the following format:
	`[protocol///]host[:port][/basedn[?attribute,...][?scope][?filter]]`
	For example:
	`ldap://<ip_address>/cn=qa,o=fdc,dc=fortinet,dc=com?uid?sub?`

Bind Password	Enter the Bind DN's password.
CA Certificates	Select *RootCA*.



MFA (RADIUS) configuration

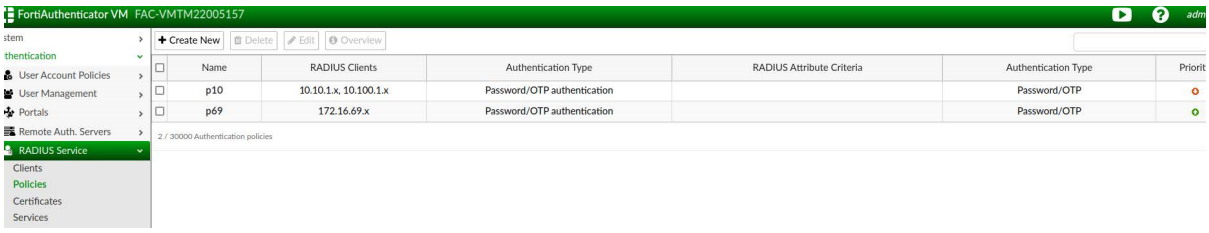
To integrate the RADIUS service with FortiDeceptor:

1. Configure FortiAuthenticator on the RADIUS server side.
2. Configure the RADIUS user on FortiDeceptor.

1. Configure FortiAuthenticator on the RADIUS server side

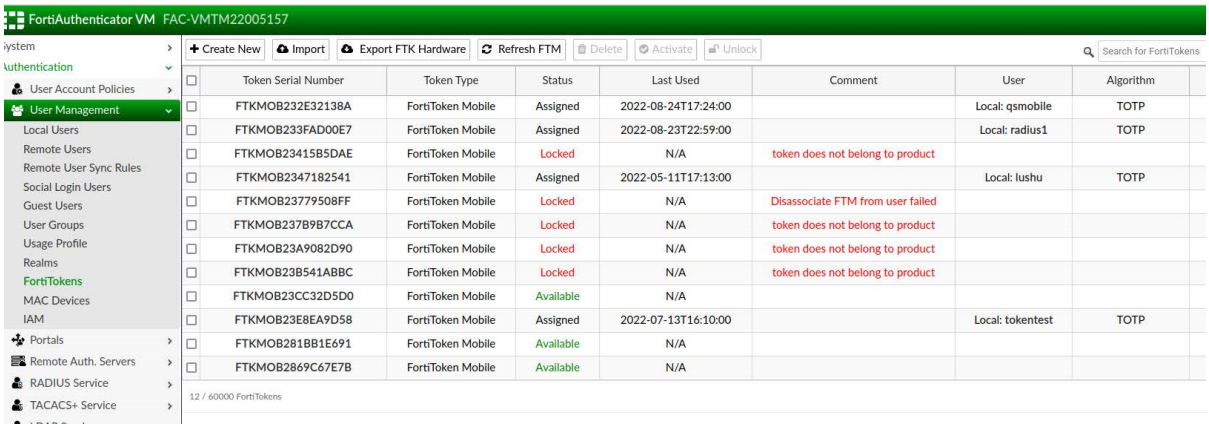
1. Add the radius clients for remote RADIUS service access.
   a. In FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients*, and click *Create New*. The *Create New Authentication Client* window opens.
   b. Configure the client service settings. For information, see *Clients > To configure a RADIUS client* in the *FortiAuthenticator Administration Guide*.
   c. Click *OK*.

2. Create a radius policy for the radius client you created.
   a. Go to *Authentication* > *RADIUS Service* > *Policies*, and click *Create New*. The *RADIUS Policy Creation Wizard* opens.

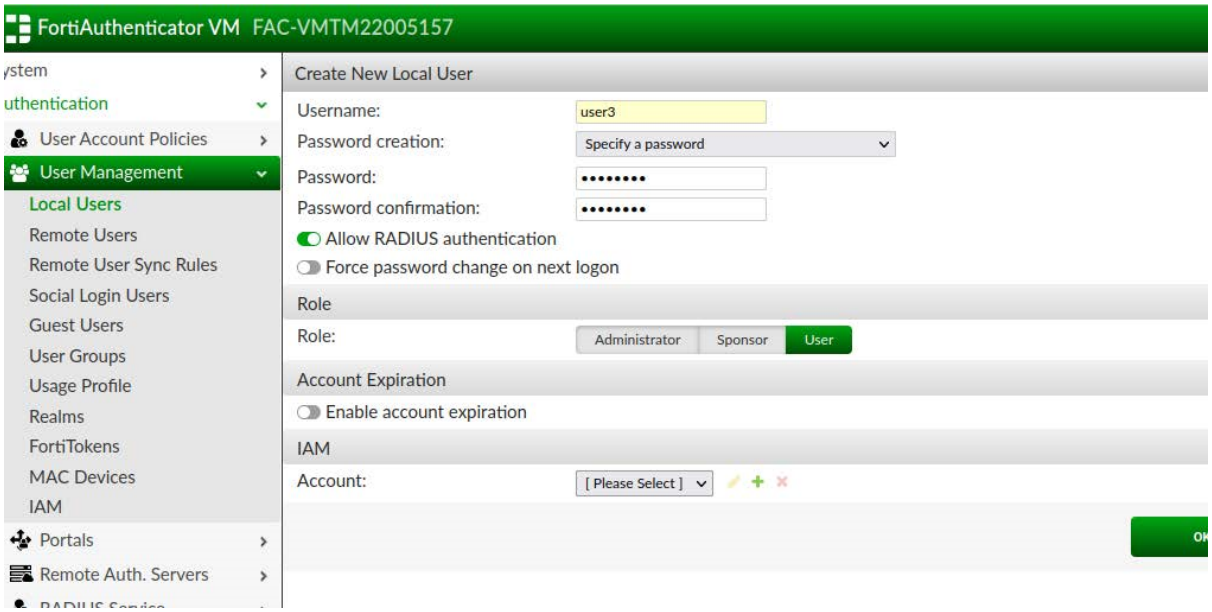


   b. Follow the steps in the wizard to configure the policy. For information, see *Policies > To configure a RADIUS policy* in the *FortiAuthenticator Administration Guide*.
   c. Click *OK*.

3. (Optional) Create or import a FortiToken.
   a. In FortiAuthenticator, go to *Authentication* > *User Management* > *FortiTokens* and click *Create New*.

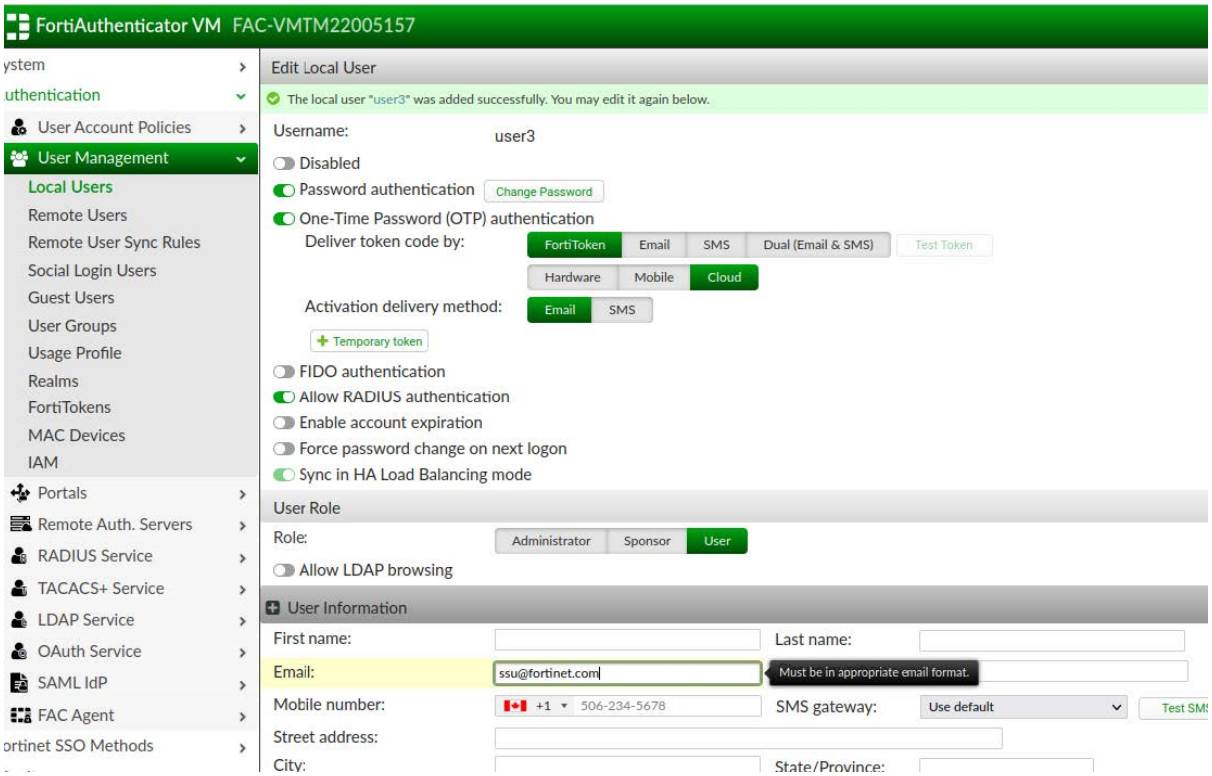


4. Create a local user.
   a. Go to *Authentication* > *Local Users* and click *Create New*.
   b. Configure the user settings and click *OK*.



c. After the user is created, enable OTP with FortiToken for this local user.

One-Time Password (OTP authentication	Enable.
Deliver token by	FortiToken

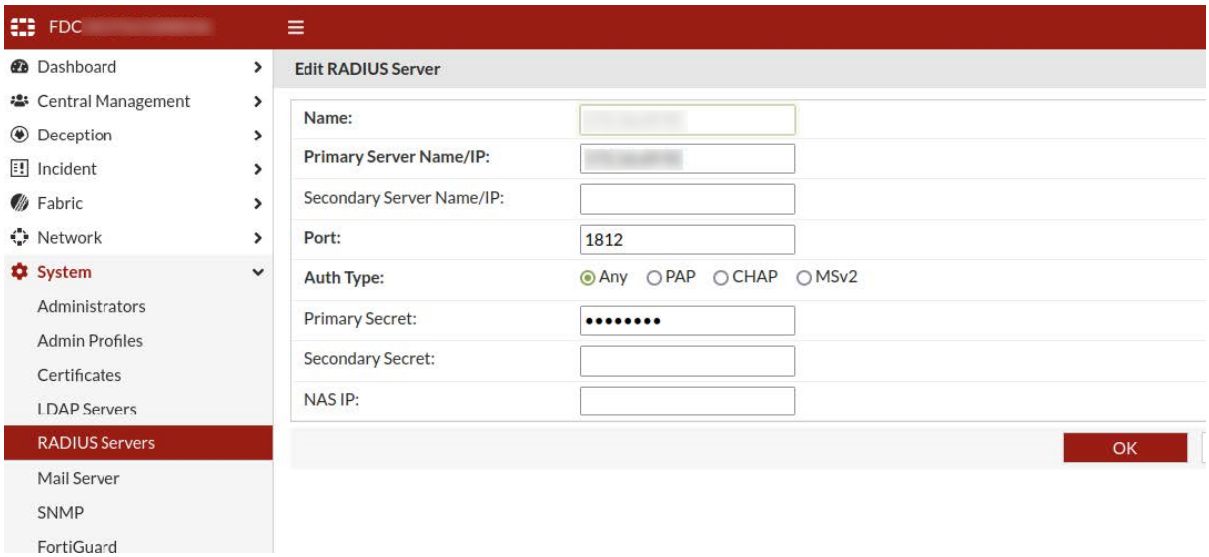


5. Activate the FortiToken for this user via an email link.

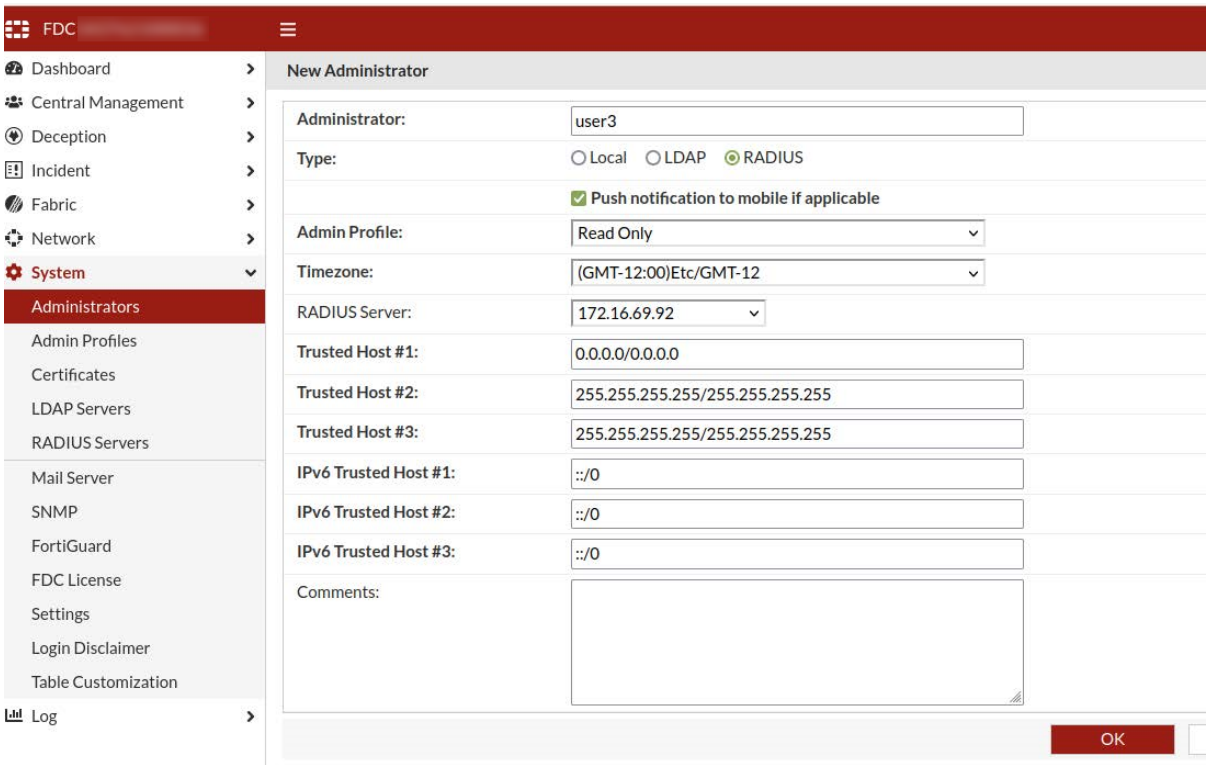
2. Configure the RADIUS user on FortiDeceptor

1. Add the RADIUS server.
   a. In FortiDeceptor, go to *System* > *RADIUS*.
   b. Configure the server settings and click *OK*.

We recommend enabling *Push notification to mobile of applicable* to allow users to authorize the login with a mobile device.



2. Add the local user you created in FortiAuthenticator.
   a. Go to *System* > *Administrators* and click *Create New*.
   b. Configure the *Administrator* settings and click *OK*.



   c. Click *Test Login* to verify the credentials.

Integrate with Checkpoint Firewall

All the configurations for CheckPoint Firewall are done with the SmartConsole.

1. Configure the REST API permissions.

1. Open the SmartConsole and go to *Management API* and click *Advanced Settings* > *All IP addresses*.
2. Click *Publish*.
3. Use SSH to log in to the manager server, then type `api restart`.
4. Create a domain object named `.quarantine.com`.
5. Create a network group object named `fdc-block-ip`.
6. Add the domain object named `.quarantine.com` to the network group object named `fdc-block-ip`.
7. Create a new policy rule.
   a. Create a new policy rule named `quarantine`.
   b. Set the policy *Source* to *fdc-block-ip*.
   c. Set `Destination` to *Any*.

   d. Set *Action* to *Inline Layer* > *New Layer*. Give the layer a name such as `Cleanup Rule` and click *OK*.

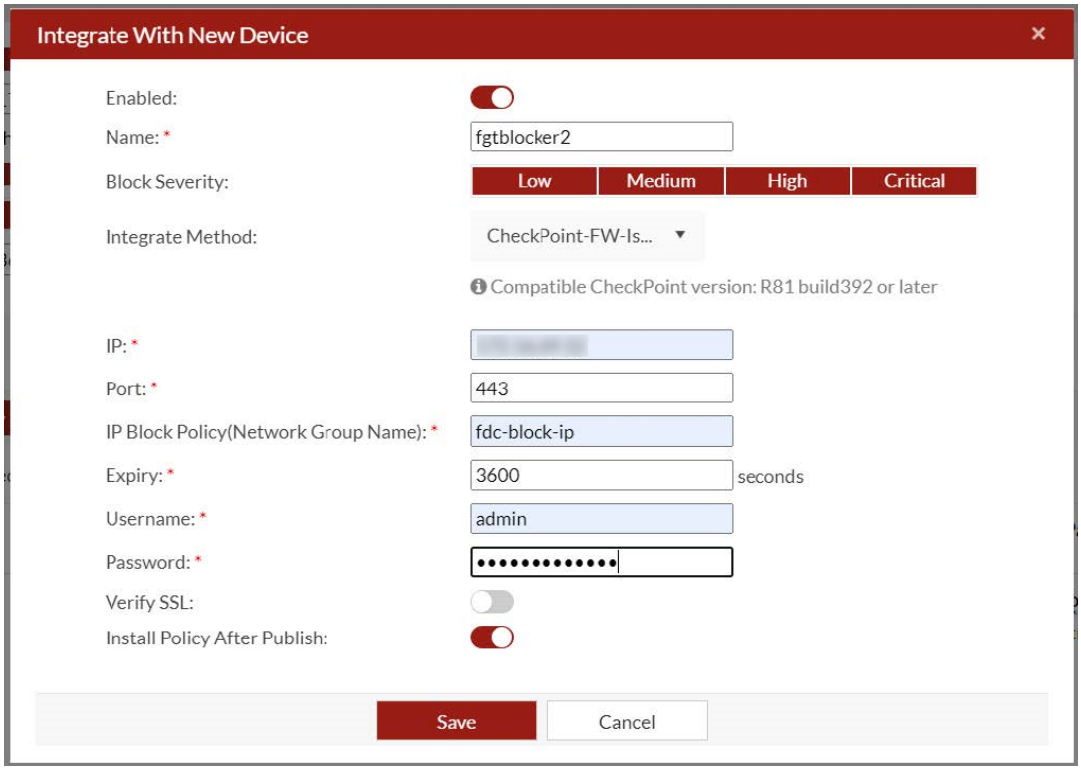
   e. Set *Action* to *Drop*.
   f. You can use the default settings for the other fields.
8. (Optional) Make the CheckPoint Fire Wall pingable.
   a. Log in to the SmartConsole.
   b. Go to *Global Properties* and enable *Accept ICMP requests*.
   c. Install the policy.

2. Configure FortiDeceptor

1. On FortiDeceptor go to *Fabric* > *Quarantine Integration*, and click +*Quarantine Integration with New Device*.
2. Configure the new device based on the following recommendations and click *Save*.

Integrate Method	Select *CheckPoint-FW-Isolation*.

IP Block Policy (network Group Name)	Enter the group object name you created (`fdc-block-ip`).
Username	Enter the Username for the management account in CheckPoint Fire Wall. You can create new admin with API permissions or use `Admin`.
Password	Enter the Password for the management account in CheckPoint Fire Wall.
Verify SSL	Disable.
Install Policy After Publish	Enable.



Integration with Crowdstrike

1 Configure CrowdStrike

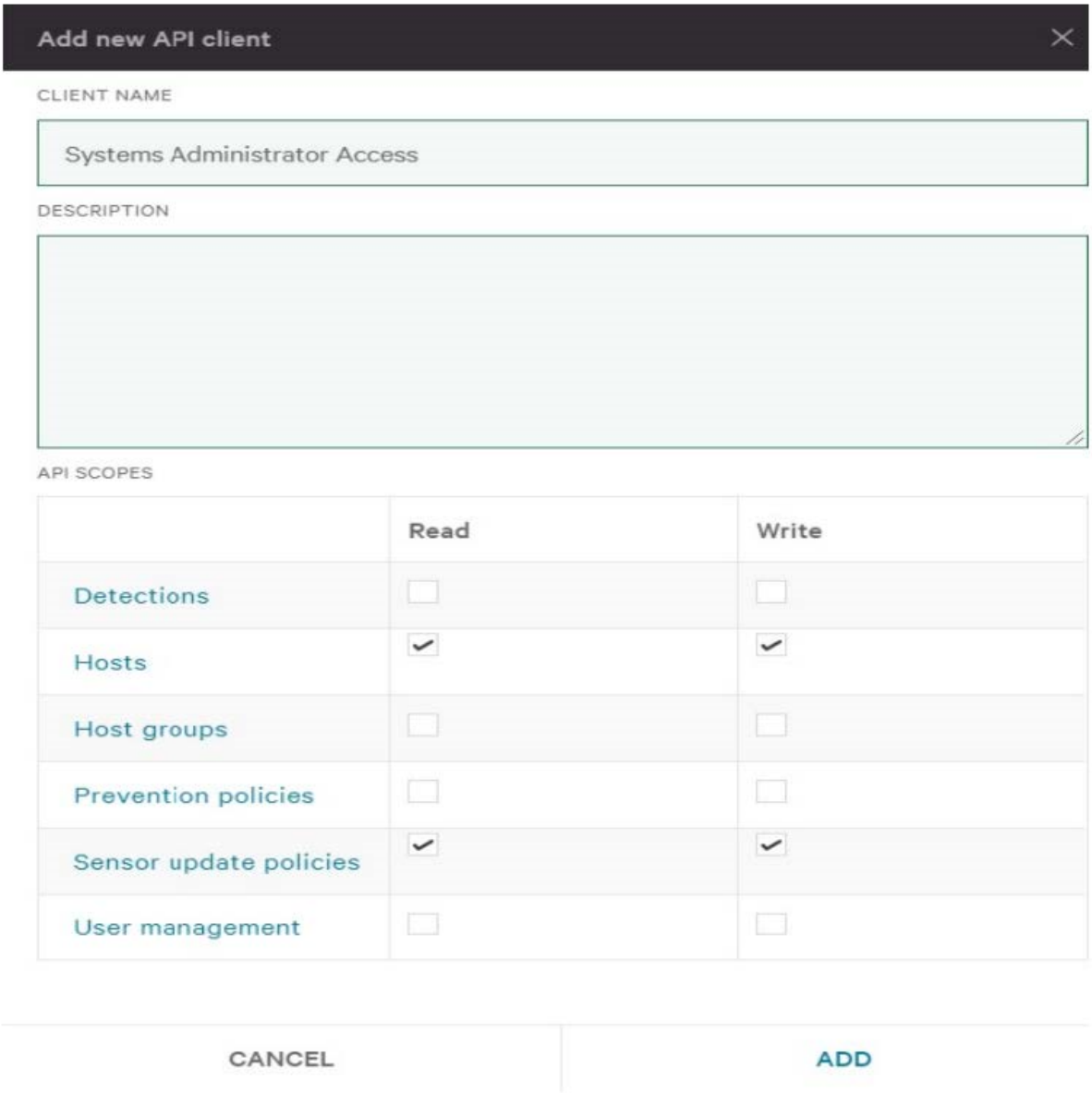
OAuth2 will be used for authentication of the incoming REST API requests.

1.1 REST API Permission

To define a CrowdStrike API client, you must be designated as the Falcon Administrator role to view, create, or modify API clients or keys. Secrets are only shown when a new API Client is created or when it is reset.

1.2 Create client ID and client secret

1. Log in to the Falcon UI.
2. Go to *Support > API Clients and Keys* to view existing clients, add new API clients, or view the audit log.
3. Click *Add new API Client*. You will be prompted to provide a descriptive name and select the appropriate API scopes.
4. Click *Save*. You will be presented with the *Client ID* and *Client Secret*. The secret will only be shown once and should be stored in a secure place. If the *Client Secret* is lost, a reset must be performed and any applications relying on the Client Secret will need to be updated with the new credentials.

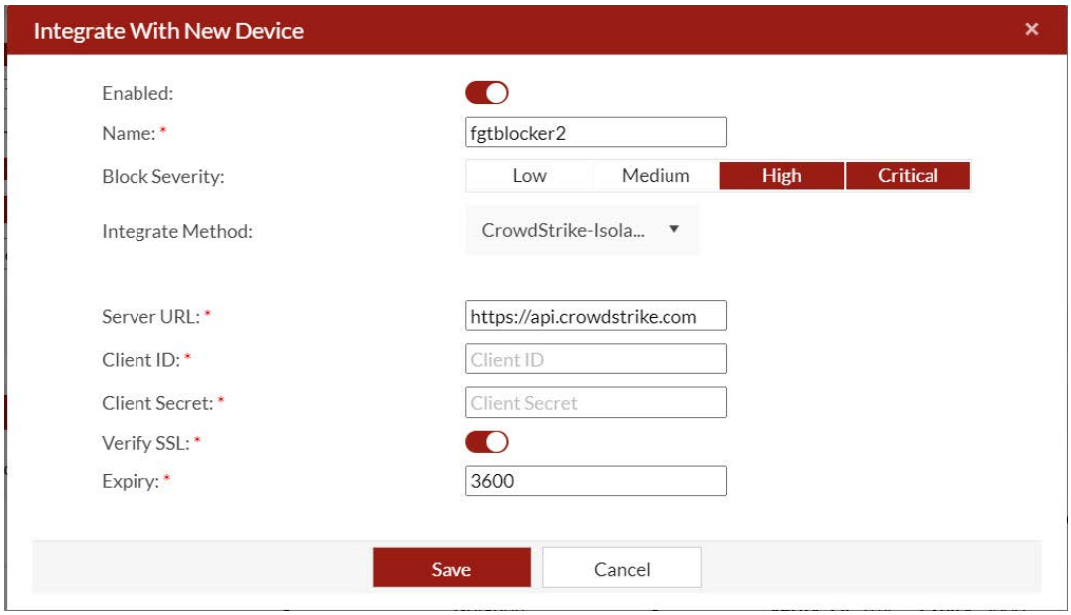


2. Configure FortiDeceptor

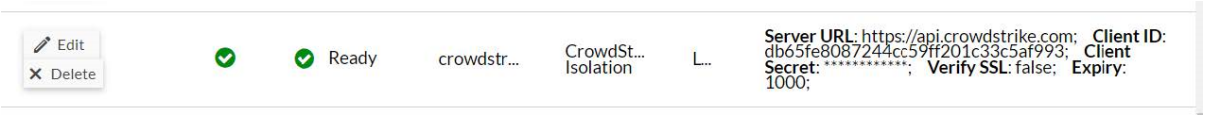
1. In FortiDeceptor, go to *Fabric* > *Quarantine Integration*.
2. Click + *Quarantine Integration with new device*. The *Integrate With New Device* window opens.
3. Configure the integration settings.

Name	Enter the Quarantine Integration name.
Integrate Method	Select *CrowdStrike-Isolation* from the dropdown list.

Server URL	Set the server URL
Client ID	Enter the Client ID.
Client Secret	Enter the Client Secret.



4. Click *Save*.
5. Confirm the status is *Ready*.



Integrate with Cuckoo Sandbox

1. Configure Cuckoo Sandbox

For information about installing Cuckoo Sandbox, please see the product documentation.

1.1 Start Cuckoo Sandbox

Before starting Cuckoo Sandbox, ensure the guest machine (for example, Win 7 running in VirtualBox) has started. To start Cuckoo, use the command `cuckoo_venv`.

In this example, cuckoo is installed in the Python virtual environment. In this case, you will need to activate the virtual environment first.

1.2 Start cuckoo API server

To start the Cuckoo API server, use the following command:

```
cuckoo api --host 172.16.69.243 --port 1337
```

```
(cuckoo_venv) [redacted]:~/cuckoo_venv$ cuckoo api --host
172.16.69.243 --port 1337
```

To access to the API, the `api_token` can be found in `<cwd>/conf/cuckoo.cfg`.

Troubleshooting:

If you see the following attribute error when requesting the API:

```
AttributeError: 'Request' object has no attribute 'is_xhr'
```

```
(cuckoo_venv) [redacted]:~/cuckoo_venv$ cuckoo api --host 172.16.69.243 --port 1337
/home/[redacted]/cuckoo_venv/lib/python2.7/site-packages/sflock/decode/office.py:12: CryptographyDeprecationWarning: Python
on core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends import default_backend
2022-01-28 17:36:23,151 [werkzeug] INFO:  * Running on http://172.16.69.243:1337/ (Press CTRL+C to quit)
[2022-01-28 17:38:36,553] ERROR in app: Exception on /tasks/list [GET]
Traceback (most recent call last):
  File "/home/[redacted]/cuckoo_venv/lib/python2.7/site-packages/flask/app.py", line 1982, in wsgi_app
    response = self.full_dispatch_request()
  File "/home/[redacted]/cuckoo_venv/lib/python2.7/site-packages/flask/app.py", line 1614, in full_dispatch_request
    rv = self.handle_user_exception(e)
  File "/home/[redacted]/cuckoo_venv/lib/python2.7/site-packages/flask/app.py", line 1517, in handle_user_exception
    reraise(exc_type, exc_value, tb)
  File "/home/[redacted]/cuckoo_venv/lib/python2.7/site-packages/flask/app.py", line 1612, in full_dispatch_request
    rv = self.dispatch_request()
  File "/home/[redacted]/cuckoo_venv/lib/python2.7/site-packages/flask/app.py", line 1598, in dispatch_request
    return self.view_functions[rule.endpoint](**req.view_args)
  File "/home/[redacted]/cuckoo_venv/lib/python2.7/site-packages/cuckoo/apps/api.py", line 256, in tasks_list
    return jsonify(response)
  File "/home/[redacted]/cuckoo_venv/lib/python2.7/site-packages/flask/json.py", line 251, in jsonify
    if current_app.config['JSONIFY_PRETTYPRINT_REGULAR'] and not request.is_xhr:
  File "/home/[redacted]/cuckoo_venv/lib/python2.7/site-packages/werkzeug/local.py", line 347, in __getattr__
    return getattr(self._get_current_object(), name)
AttributeError: 'Request' object has no attribute 'is_xhr'
2022-01-28 17:38:36,596 [werkzeug] INFO: 172.16.197.161 - - [28/Jan/2022 17:38:36] "GET /tasks/list HTTP/1.1" 500 -
```

Open `/flask/app.py` and set `JSONIFY_PRETTYPRINT_REGULAR` to `False`.

```
    'JSON_SORT_KEYS':                          True,
    'JSONIFY_PRETTYPRINT_REGULAR':             False,
    'JSONIFY_MIMETYPE':                        'application/json',
```

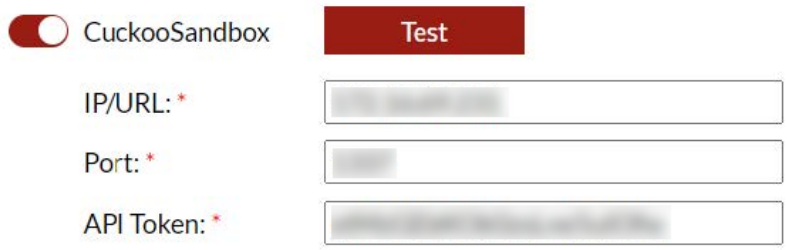
The request`.is_xhr property` was deprecated since Werkzeug 0.13 and removed in Werkzeug 1.0.0. As a result, this error will occur when using Flask <= 0.12.4 and Werkzeug >=1.0.0 because Flask uses this property in the source before the 1.0.0 version.

2. Configure FortiDeceptor to integrate with Cuckoo Sandbox

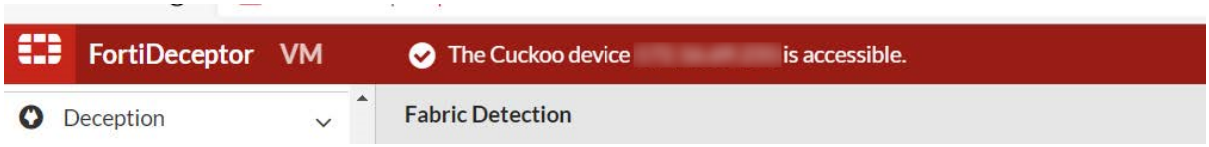
1. In FortiDeceptor go to *Fabric* > *Detection Devices*.
2. Enable *Cuckoo Sandbox*.

3. Configure Cuckoo Sandbox.

IP/URL	Set the IP the based on the command in step 1.2 Start cuckoo API server.
Port	Set the Port the based on the command in step 1.2 Start cuckoo API server.
API Token	API token information can be found on `<cwd>/conf/cuckoo.cfg`.

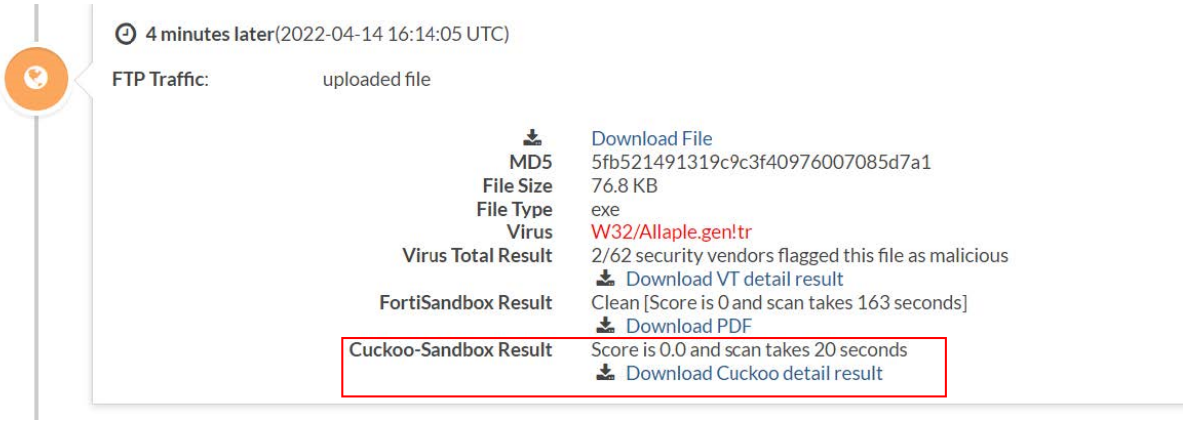


4. Click *Test*. You should see *The Cuckoo device <IP> is accessible*".

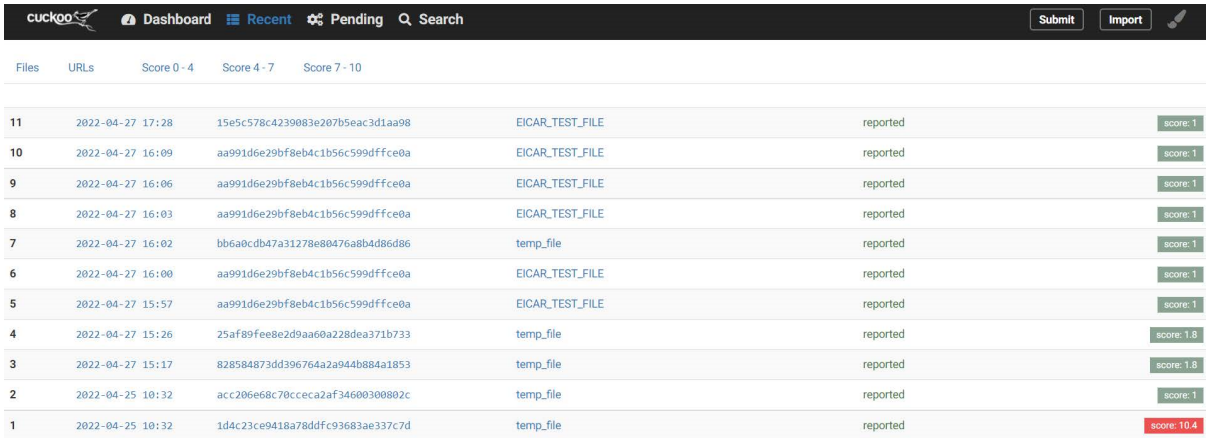


3. Verify the detection result from Cuckoo Sandbox

1. Copy a file from any endpoint to the decoy using SMB/FTP protocol and verify that the file is captured and analyzed by the Cuckoo sandbox.
2. To verify the result in FortiDeceptor:
   a. Go to *Incident* > *Analysis*.
   b. Expand the incident and verify *Cuckoo-Sandbox Result* is displayed.



3. To verify the result in Cuckoo Sandbox, go to *WebUI* > *Recent*. Open the Cuckoo report to verify result.



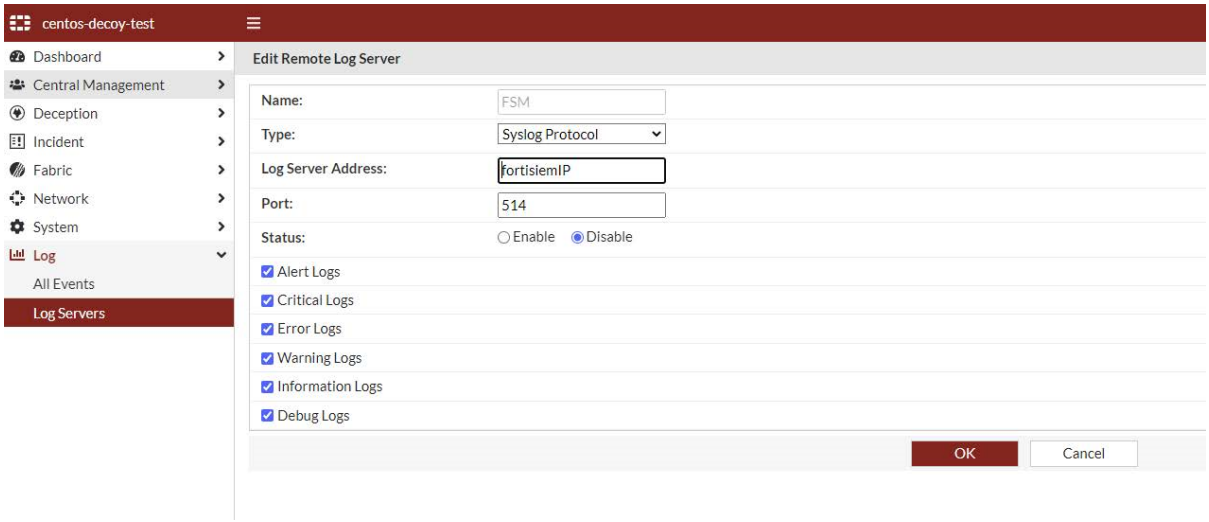
Integration with FortiSIEM

To integrate FortiDeceptor with FortiSIEM:

1. Configure FortiSIEM as a remote log server in FortiDeceptor
2. Change the discovered FortiDeceptor status from Pending to Approved
3. Check the logs and generate reports in FortiSIEM

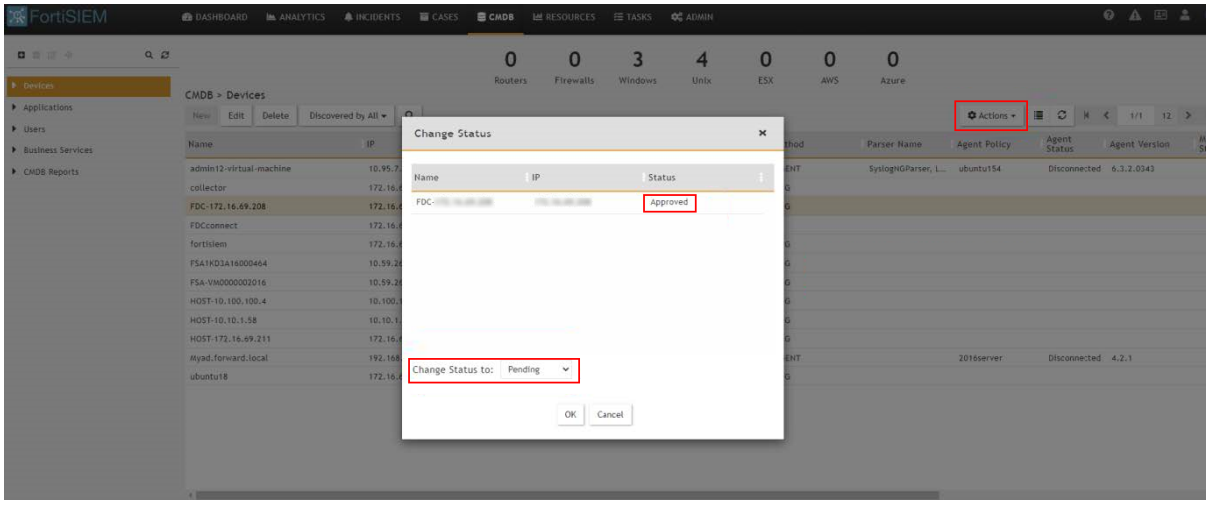
1. Configure FortiSIEM as a remote log server in FortiDeceptor

1. In FortiDeceptor, go to *Log* > *Log Servers*.
2. Click *Create new*. The *New Remote Log Server* window opens.
3. Configure the *Log Server Address* for FortiSIEM and click *OK*. For more information, see Log Servers on page 150.



2. Change the discovered FortiDeceptor status from Pending to Approved

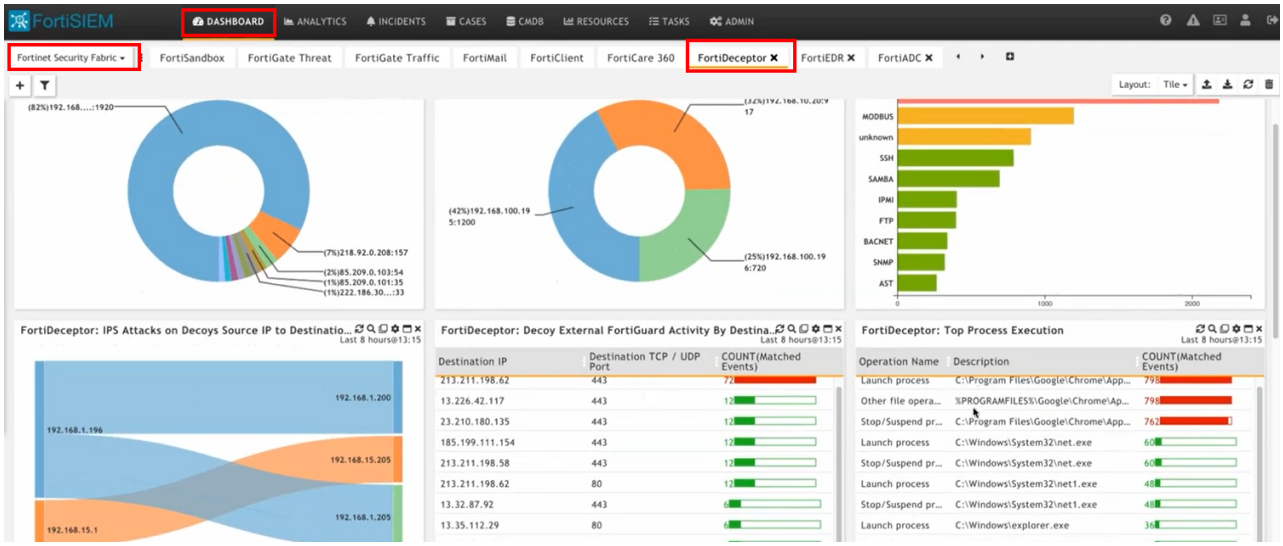
1. In FortiSIEM go to *Devices* and select the FortiDeceptor device from the list.
2. Click the *Actions* dropdown and change the status from *Pending* to *Approved*.



3. Check the logs and generate reports in FortiSIEM

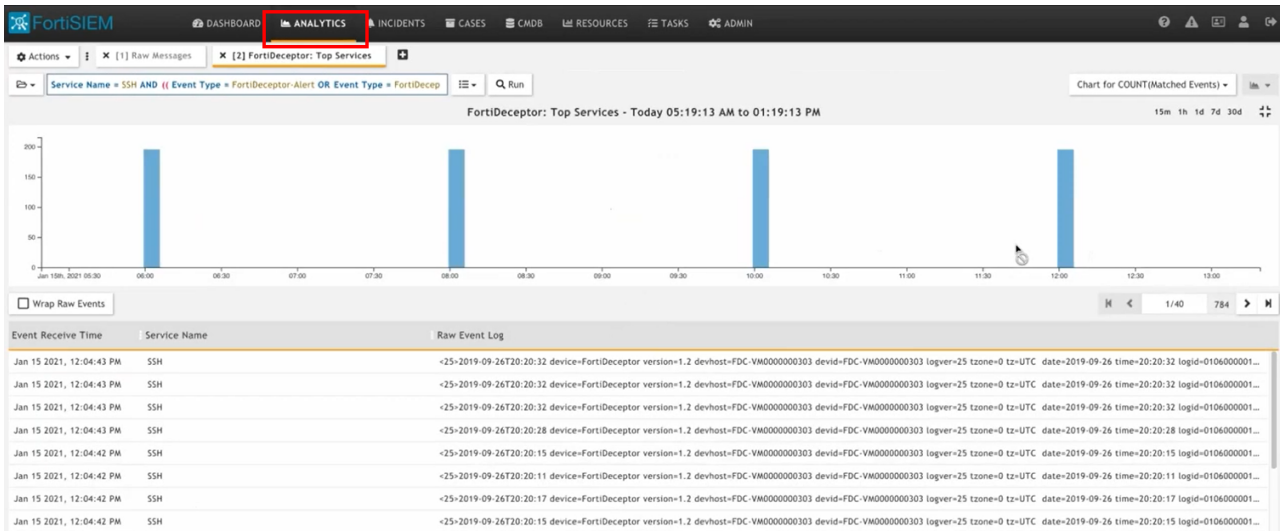
To see how FortiSIEM and FortiDeceptor integrations improve cyberthreat detection and increase visibility of potential attacks, watch this short video *FortiSIEM Demo: FortiSIEM and FortiDeceptor Integrations*

1. In FortiSIEM click the *DASHOBARD* tab, the *Fortinet Security Fabric* dashboard, and click the FortiDeceptor dashboard. The information received from FortiDeceptor is displayed. You can click on any widget to drill down on the information.

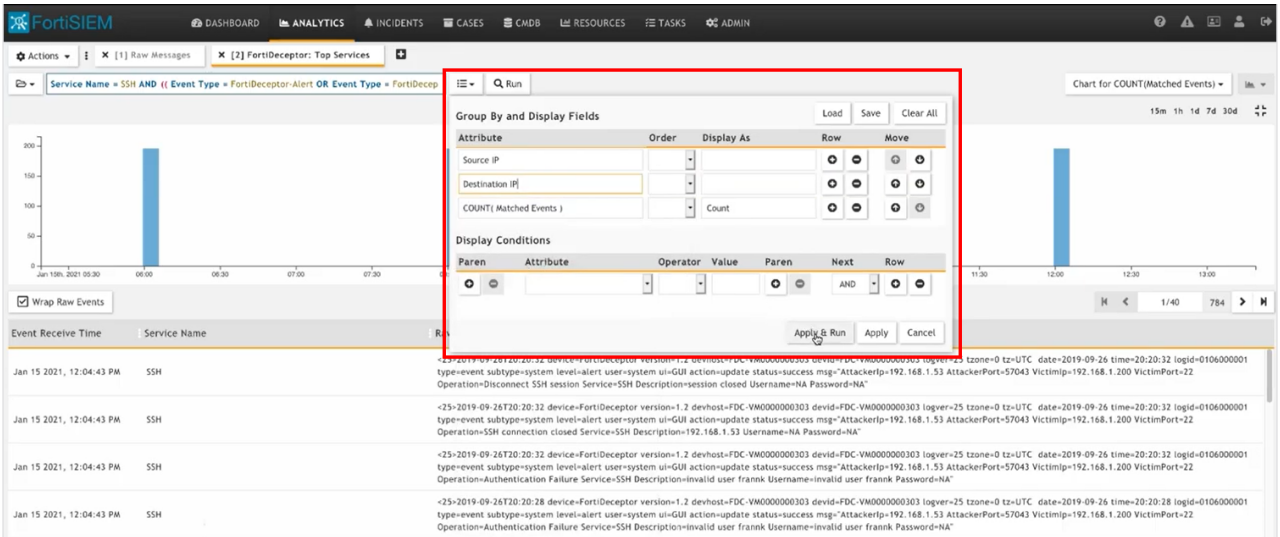


2. In the *Top Services* widget click *SSH*.

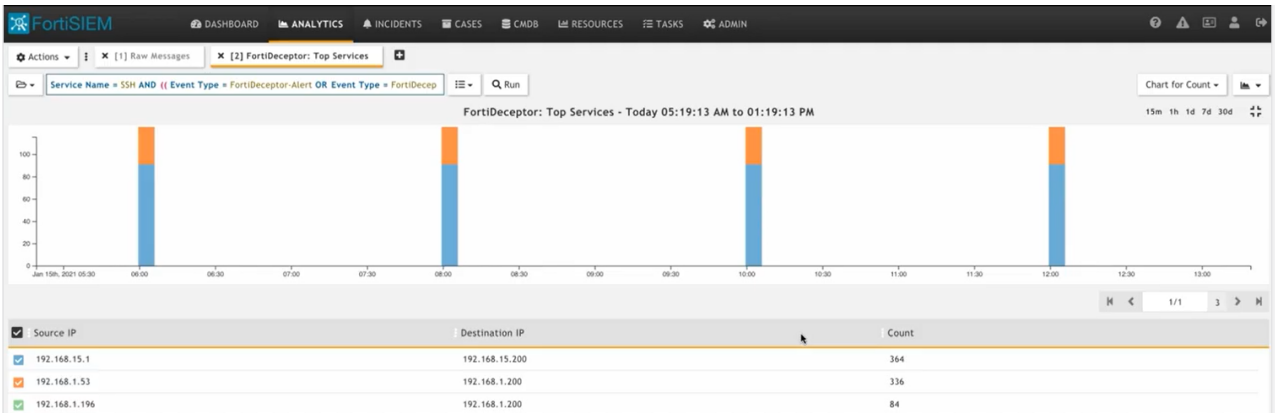
The events and the raw logs are displayed in the *ANALYTICS* tab.



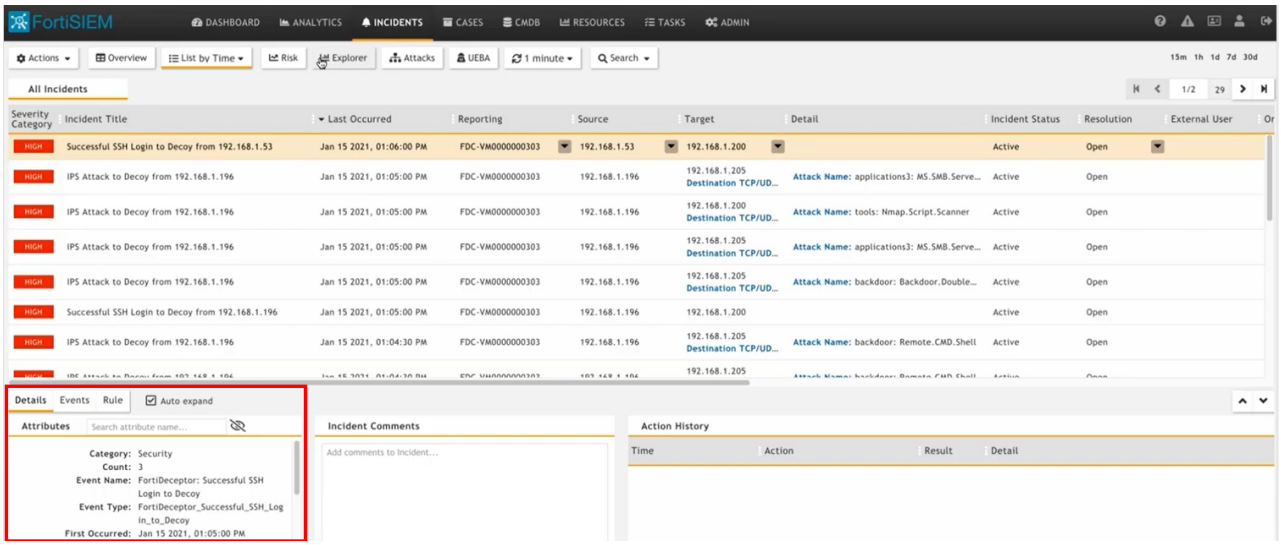
3. Use a *Group By and the Display Fields* template to view the Source IP and Destination IP.



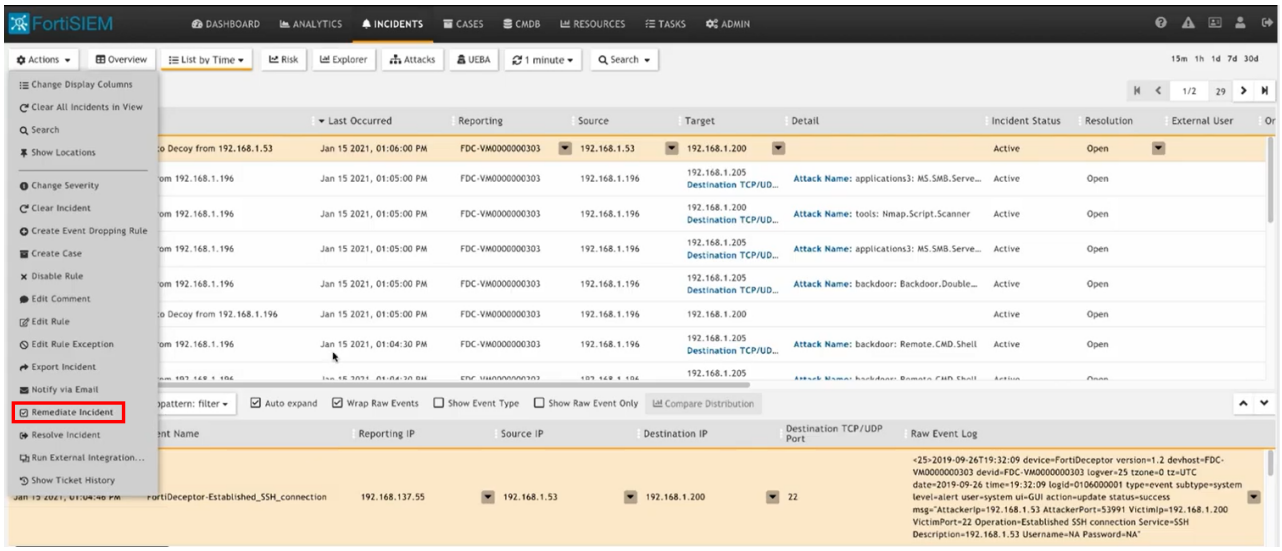
The Source and Destination IPs are displayed.



4. Click the *Incidents* tab. Select and incident in the list and the click the *Details*, *Events*, and *Rule* tab to view more information about the incident.



5. Click the *Actions* menu and select *Remediable Incident* to block the IP address.



FortiSIEM Watch List

Deception Tokens are part of the FortiDeceptor platform and are included in the product license at no additional cost.

FortiDeceptorTokens:

- Are an agentless technology.
- Deceive threat actors by adding breadcrumbs to real endpoints and servers so the actor engages with network decoys instead of real assets.
- Are normally distributed within real endpoints and server assets to expand the attack surface.

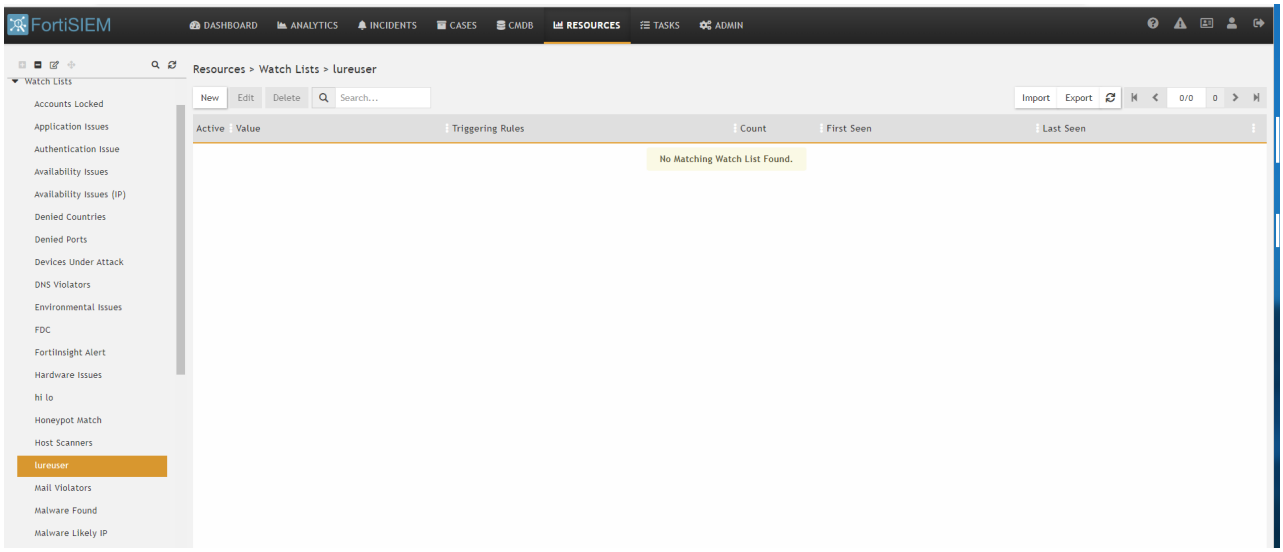
FortiDeceptor generates a deception token package based on the decoy service configuration. The FortiDeceptor and FortiSIEM integration for the Watch List detects when a threat actor attempts to use the fake credentials from the token package to access a real asset (as opposed to a decoy). FortiDeceptor cannot detect this type of access because the asset is not a decoy. When integrated, both the FortiDeceptor and FortiSIEM GUI will display an alert for this type of access.

To integrate FortiDeceptor with FortiSIEM:

1. Configure FortiSIEM.
2. Configure the Watch List in FortiDeceptor.
3. Test the integration.
4. Check the incidents on FortiSIEM.
5. View the incidents on FortiDeceptor.

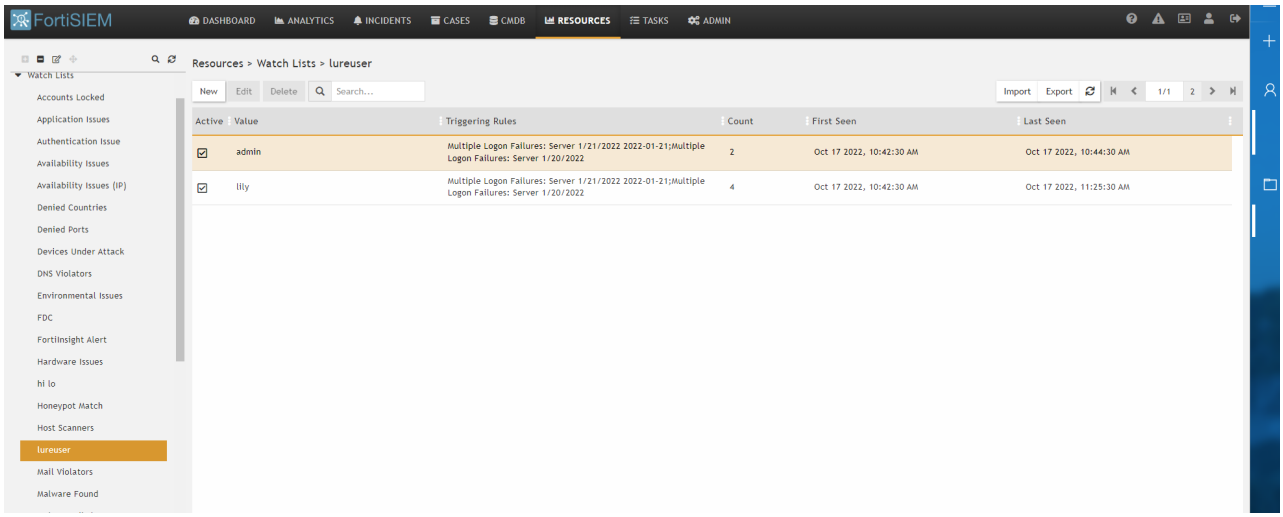
1. Configure FortiSIEM

1. In FortiSIEM go to *Watch Lists* and click *New* to create a new watch list or edit an existing Watch List. For more information, see *Managing Resources* > *Watch List* > *Creating a Watch List* in the *FortiSIEM User Guide*.



2. Go to *Resources* and define the Watch List rules. For information, see *Managing Resources* > *Watch List* > *Using a Watch List* > *Adding a Watch List to a Rule* in the *FortiSIEM User Guide*.

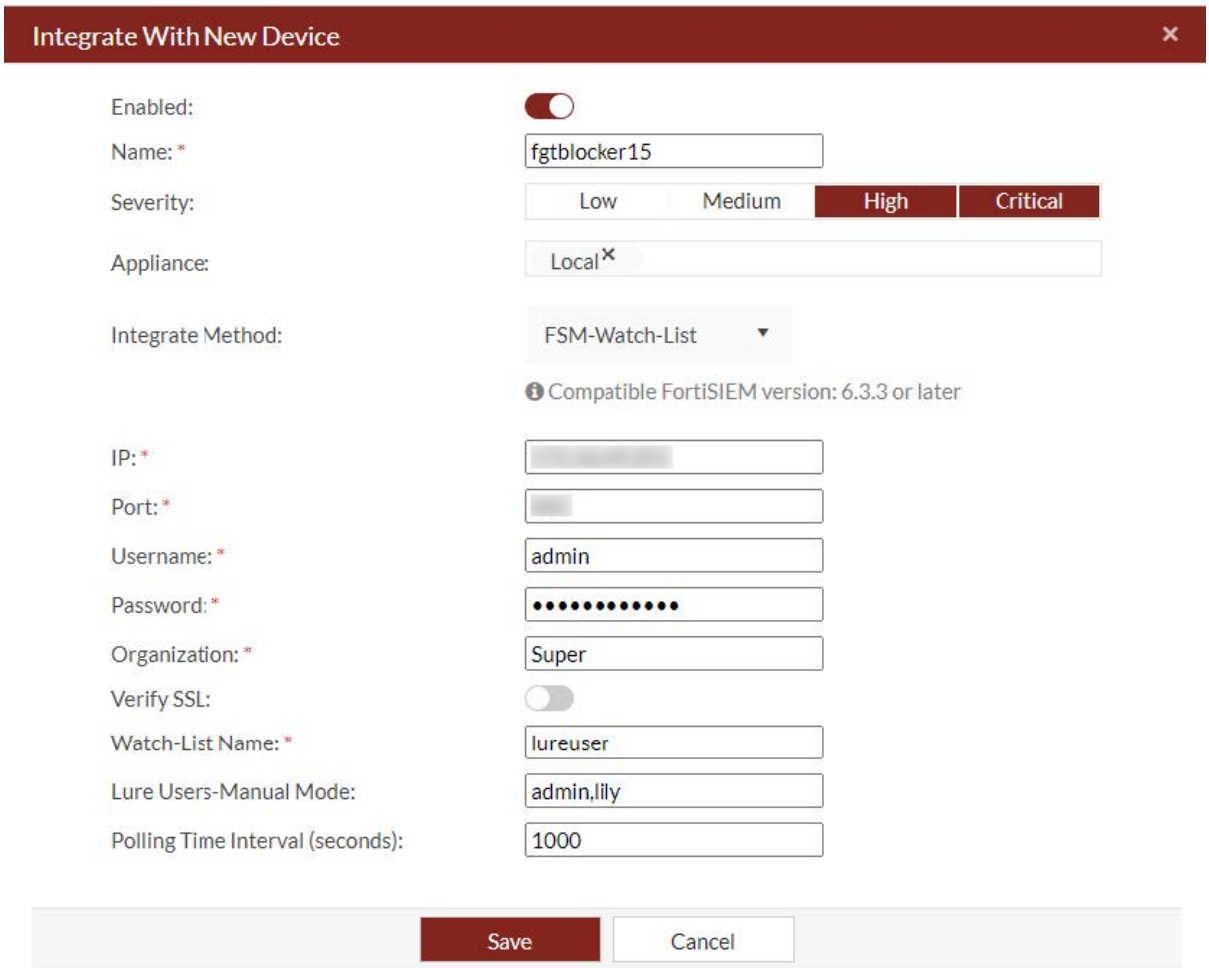
In the image below, the usernames (face credential tokens) are generated automatically by FortiDeceptor during the integration.



2. Configure the Watch List in FortiDeceptor

1. In FortiDeceptor, go to *Fabric* > *Quarantine Integration* and click *Quarantine Integration With New Device*.
2. From the *Integrate Method* dropdown, select *FSM Watch-List*.
3. Configure the integration settings.

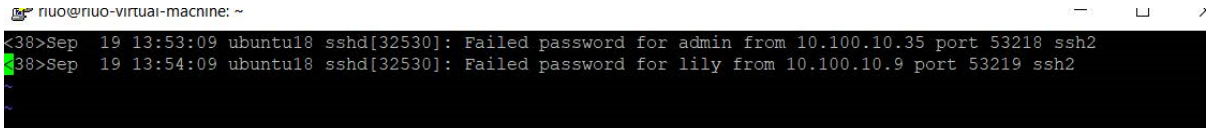
IP	Enter the IP for the FortiSIEM device.
Port	Enter the Port number for the FortiSIEM device.
Username	Enter the username for the FortiSIEM device.
Password	Enter the password for the FortiSIEM device.
Watch-List Name	Enter the name of the Watch List you created in Step 1 Configure FortiSIEM.
Lure Users-Manual Mode	This option allow you to add more usernames manually to the FortiSIEM watch list in addition to the one that FortiDeceptor generates automatically based on the deception token package. Please enter the Lure Users you created and separate multiple users with a comma.



4. Click *Save*.

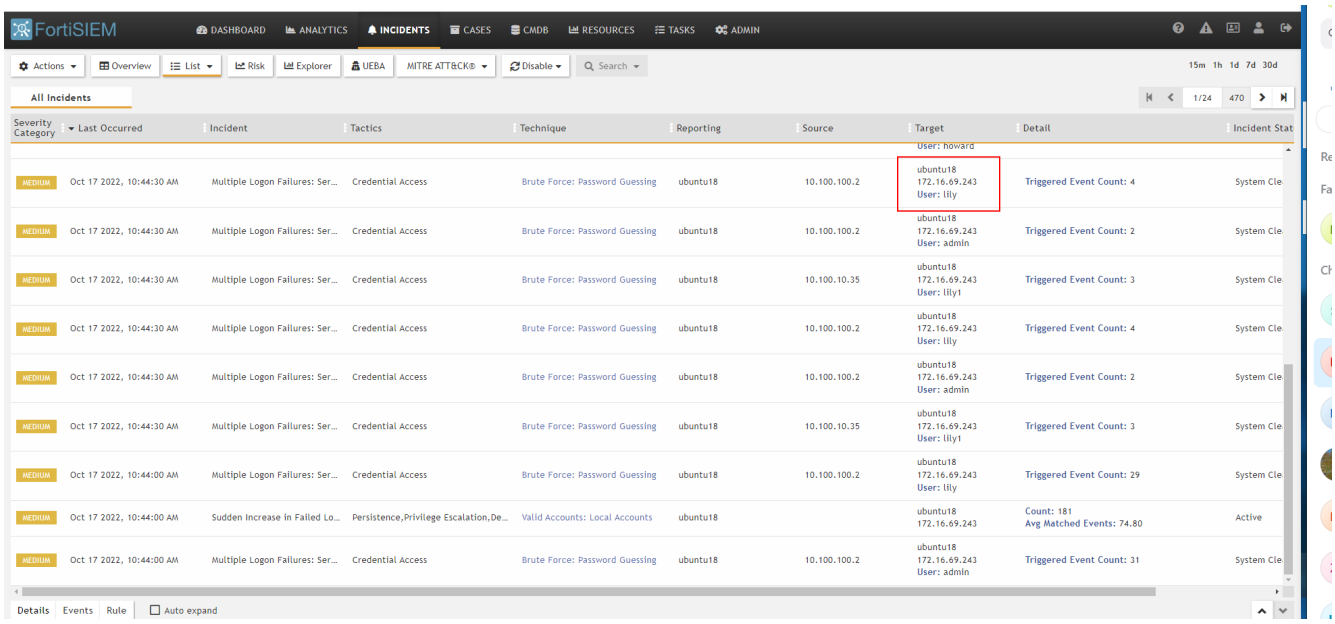
3. Test the integration

To test the integration, use one of the fake credentials to access a real asset. Verify that FortiSIEM can detect fake credentials when used to access an asset that is not a decoy.



4. Check the incidents on FortiSIEM

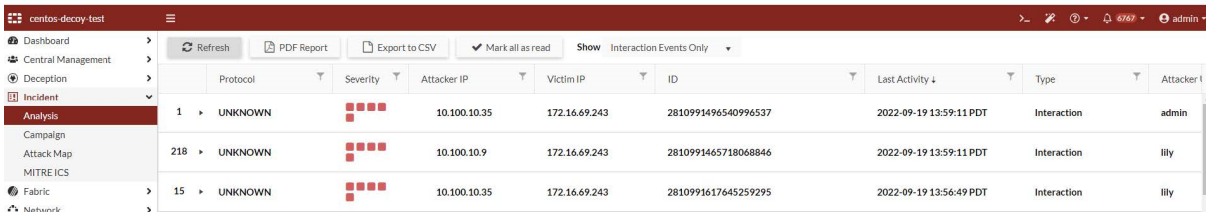
In FortiSIEM, go to *Incidents* to verify the incidents you triggered are reported. For information, see *FortiSIEM Manager > FortiSIEM Manager Incidents > FortiSIEM Manager Incidents - List View* in the *FortiSIEM User Guide*.



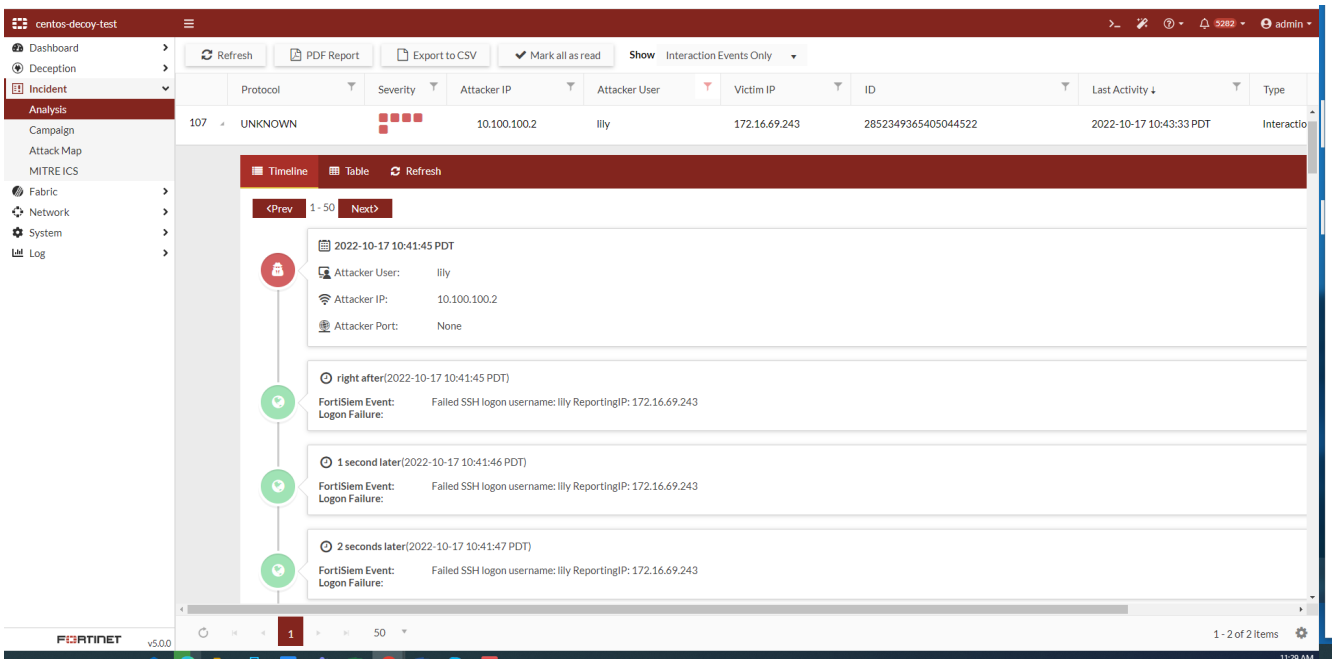
5. View the incidents on FortiDeceptor

In FortiDeceptor, go to *Incident > Analysis* to view the incidents you triggered.

Incidents captured by FortiSIEM are recorded as *UNKNOWN* in the *Protocol* column.



Click the arrow to expand the alert. You will see the incident was captured by FortiSIEM.



Mitigation using windows Remote Command

1. Configure the endpoint

1.1 Verify the endpoint domains and permissions.

FortiDeceptor will use the administrator account of the AD domain to access Windows endpoints. Please ensure the Windows endpoints are connected to the AD domain and the administrator account of AD domain can access the endpoints.

The administrator can also be a domain local admin with permission to disable the endpoint network interfaces.

1.2 Open the Windows SMB port

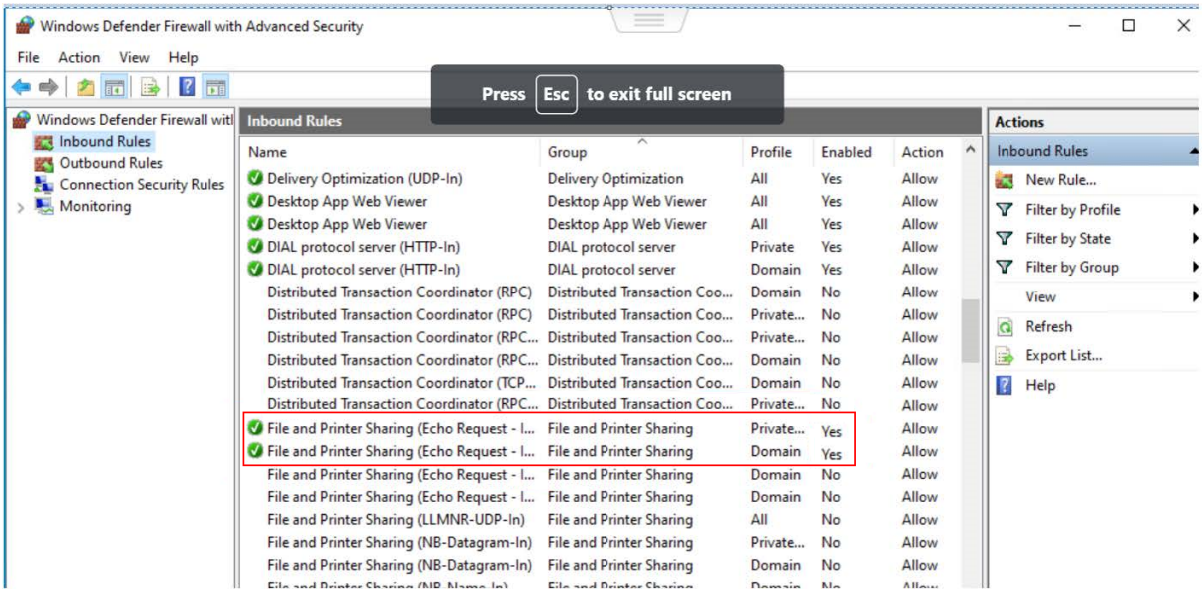
By default, Windows blocks the SMB port 445. To open the port run the following command in PowerShell:

```
Set-NetFirewallRule -Name FPS-SMB-In-TCP -Enabled True
```

1.3 Enable SMB

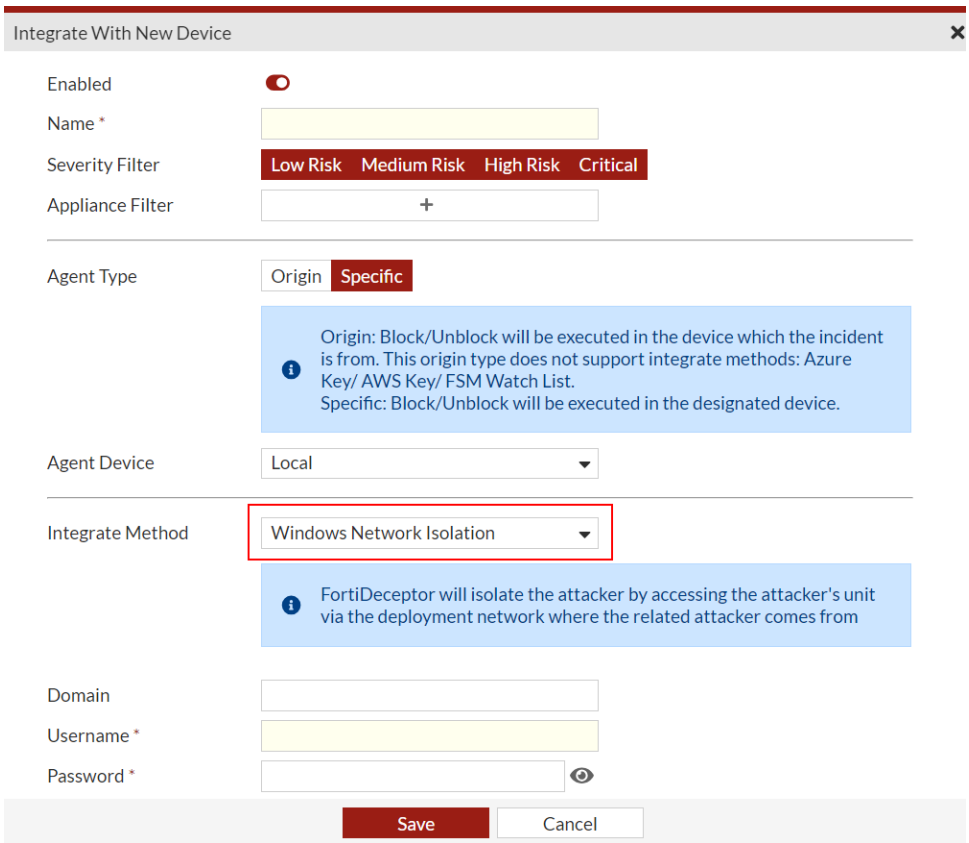
If the Firewall is enabled by the A/D GPO, you will need to add the FortiDeceptor management IP to the exclusion list.

1. Type `wf. msc` in the Windows search box.
2. Click *Inbound Rules* in the navigation pane.
3. Scroll down to *File and Printer Sharing (Echo Request - ICMPv4-In)*.
4. Enable the options in both *Private* and *Domain* profile

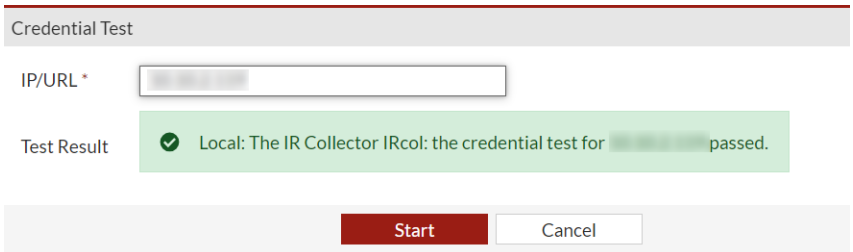


2. Configure FortiDeceptor

1. In FortiDeceptor, go to *Fabric* > *Quarantine Integration* and click + *Quarantine Integration with new device*.
2. Configure the integration settings ensuring the user has sufficient privileges to manage NICs.



3. (Optional) Click *Credentials Test* and then click *Start* to test the connection.



Integration with PAN devices

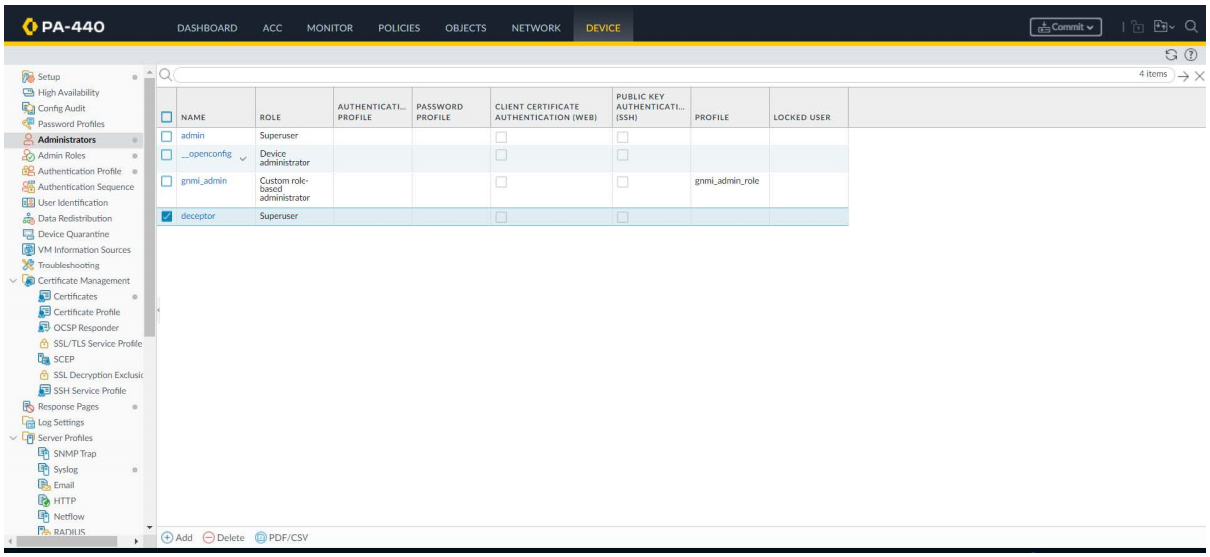
To integrate FortiDeceptor with PAN devices:

1. Configure PAN.
2. Configure the PAN device on FortiDeceptor.
3. Check the PAN status on FortiDeceptor.

4. Verify the policy has been added on PAN.
5. Attack a decoy and check the quarantine status in FortiDeceptor.

1. Configure PAN

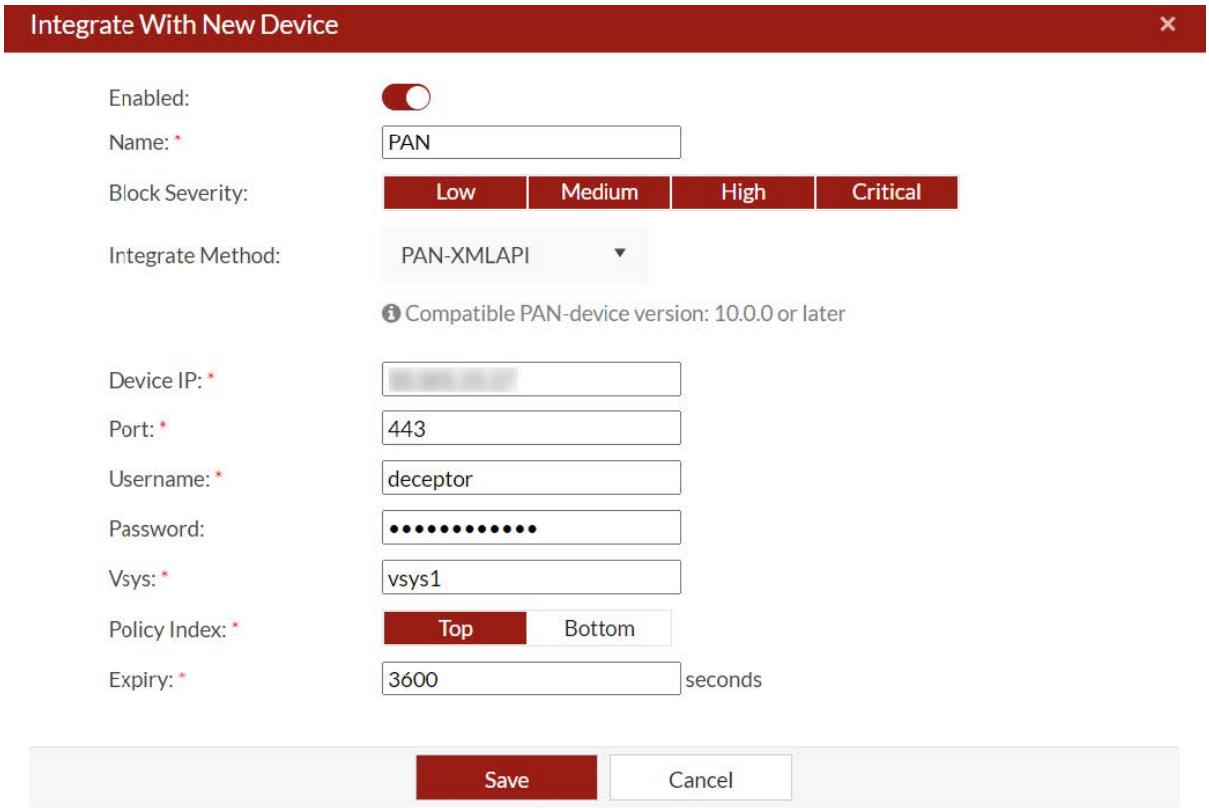
Create an administrator on the PAN device. For information, see the PAN-OS Administrator's Guide.



2. Configure the PAN device on FortiDeceptor

1. In FortiDeceptor, go to *Fabric* > *Quarantine Integration* and click + *Quarantine Integration with new device*.
2. Configure the integration settings and click *Save*.

Enabled	Enable
Name	Enter a name for the integration.
Integration Method	Select *PAN-XMLAPI*.
Device IP	Enter the IP for the PAN device.
Port	Enter the port number for the PAN device.
Username	Enter the username for the PAN device.
Password	Enter the password the PAN device.
Vsys	The virtual system (Vsys) which is configured on the PAN device.
Policy Index	Select *Top* or *Bottom*.
Expiry	Default blocking time in seconds. Default is 3600 seconds.

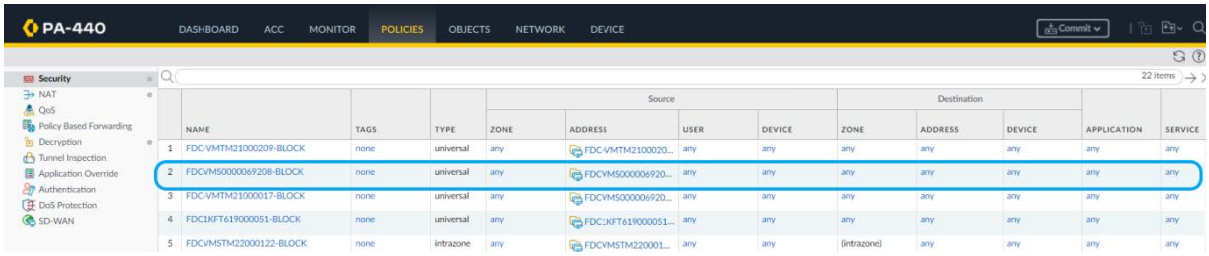


3. Check the PAN status on FortiDeceptor

In FortiDeceptor, click *Quarantine Integration* and verify the PAN device status is *Ready*.

4. Verify the policy has been added on PAN

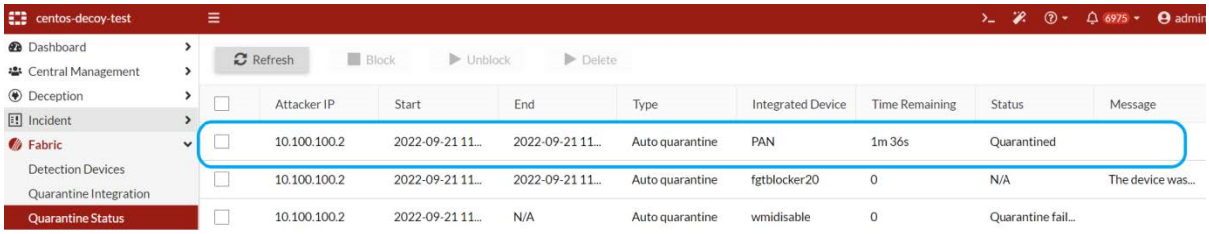
For more information about PAN polices, see the PAN-OS Administrator's Guide.



5. Attack a decoy and check the quarantine status in FortiDeceptor

To check quarantine status in FortiDeceptor:

1. Go to *Fabric* > *Quarantine Status*.
2. Search for the PAN device in the *Integrated Device* column.



Integration with Microsoft ATP

1. Configure Azure

1.1 Configure the permissions

For the Application registration stage, you must have a Global administrator role in your Azure Active Directory (Azure AD) tenant.

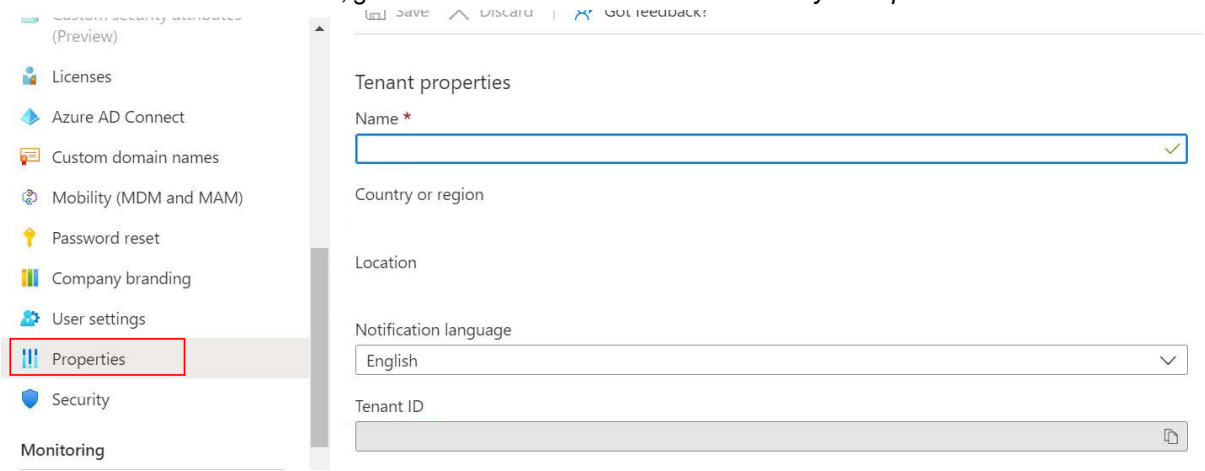
1.2 Create an App in Microsoft

For information about creating an App in the Azure Active Directory, see Microsoft Defender for Endpoint API - Hello World.

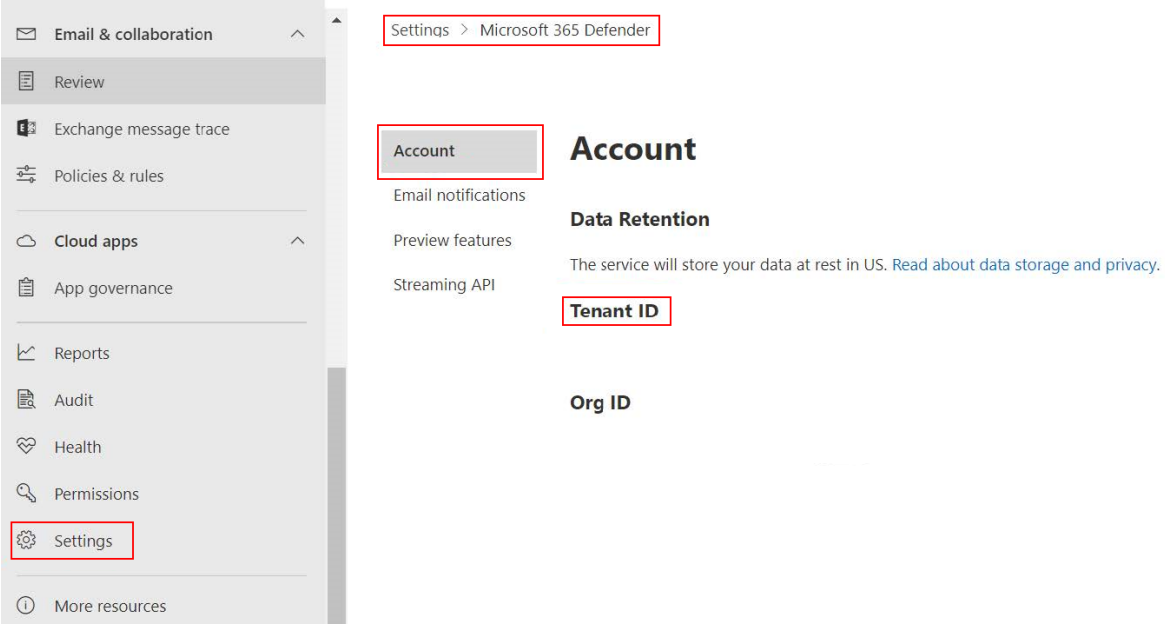
2. Onboard devices on Microsoft 365 Defender

2.1 Verify the tenant IDs are identical

1. Login to Microsoft 365 Defender (https://security.microsoft.com/) with your Azure account.
2. Ensure the Tenant IDs in Azure and Microsoft 365 Defender are identical.
   - To view the Tenant ID in Azure, go to *Azure Home* > *Azure Active Directory* > *Properties*.



   - To view the Tenant ID in Microsoft 365 Defender, go to *Settings* > *Microsoft 365 Defender* > *Account*.



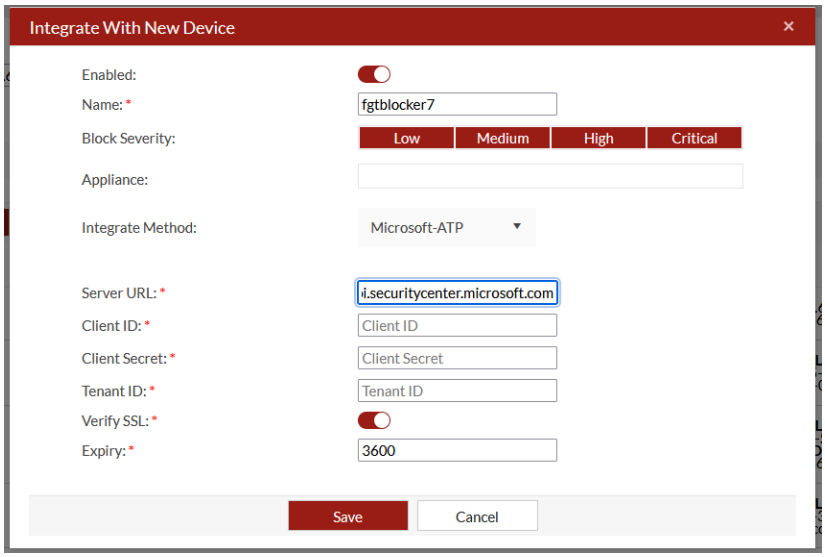
2.1 Onboard devices in Defender

1. In Microsoft Defender, go to *Settings* > *Endpoints* > *Device management* > *Onboarding* .
2. Onboard the endpoints you want to manage.

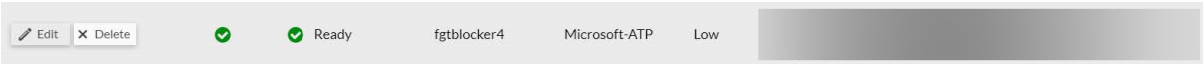
3. Configure FortiDeceptor

1. In FortiDeceptor, go to *Fabric* > *Quarantine Integration* and click *Quarantine Integration With New Device*.
2. Configure the integration settings and click *Save*.

Integrate Method	Select *Microsoft-ATP*.
Server URL	Enter the URL of API: `https://api.securitycenter.microsoft.com`.
Client ID	Enter the Azure Client ID.
Client Secret	Enter the Azure Client Secret.
Tenant ID	Enter the Azure Tenant ID.



3. Verify the device status is *Ready*



Integration with FortiSandbox

FortiSandbox is an anti-virus engine. When integrated, FortiDeceptor submits malware to FortiSandbox and retrieves the scanning result.

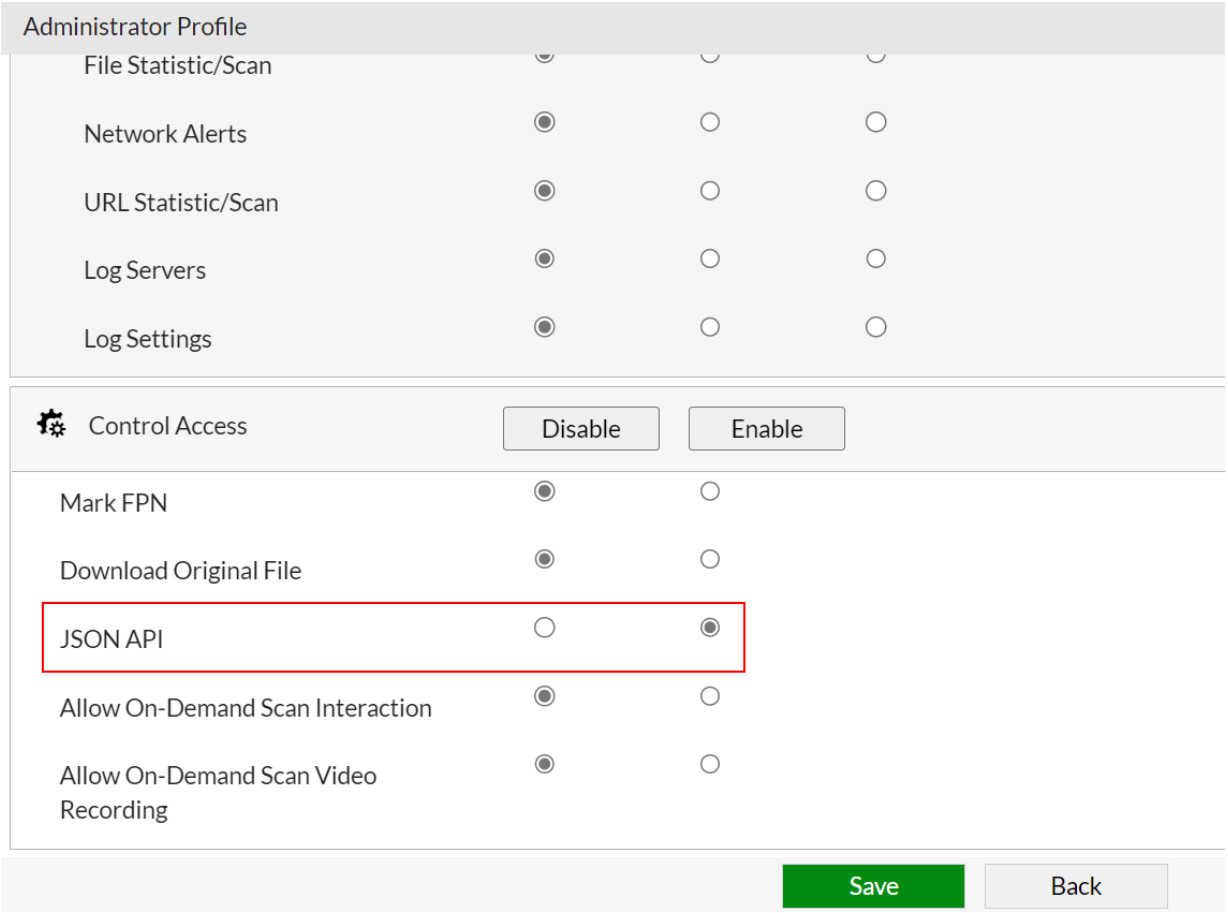
To integrate FortiDeceptor with FortiSandbox:

1. Create a new user role in FortiSandbox.
2. Integrate FortiDeceptor with FortiSandbox.
3. Verify the scanning results in FortiDeceptor and FortiSandbox.

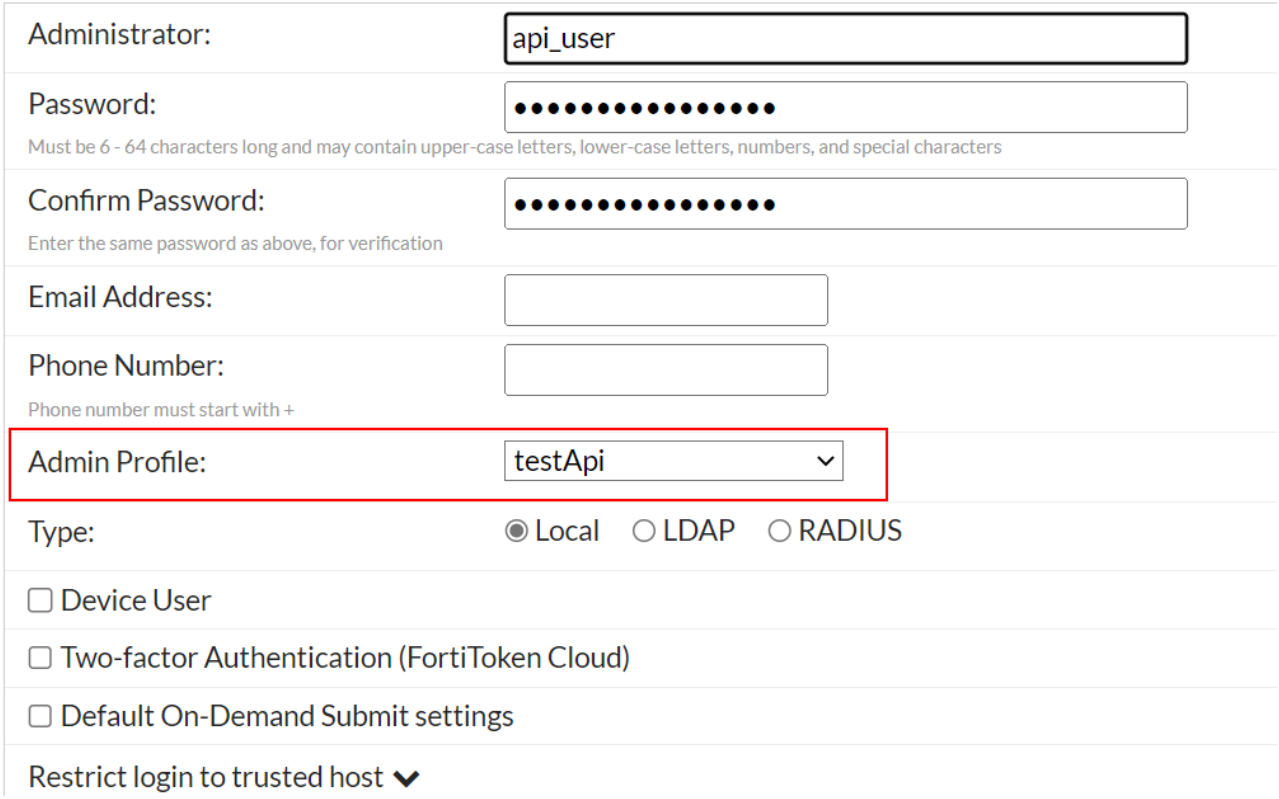
1. Create a new user role in FortiSandbox

Create a new user role whose with privileges to access JSON API.

1. Create an Admin Profile with JSON API privileges. For information, see *Admin Profiles* in the *FortiSandbox Administration Guide*.
   a. Go to *System* > *Admin Profiles* and click *Create New*.
   b. Give the profile a descriptive *Name* such as `testApi`.
   c. Under *Control Access*, select *JSON API*. Configure the other settings as required and click *Save*.

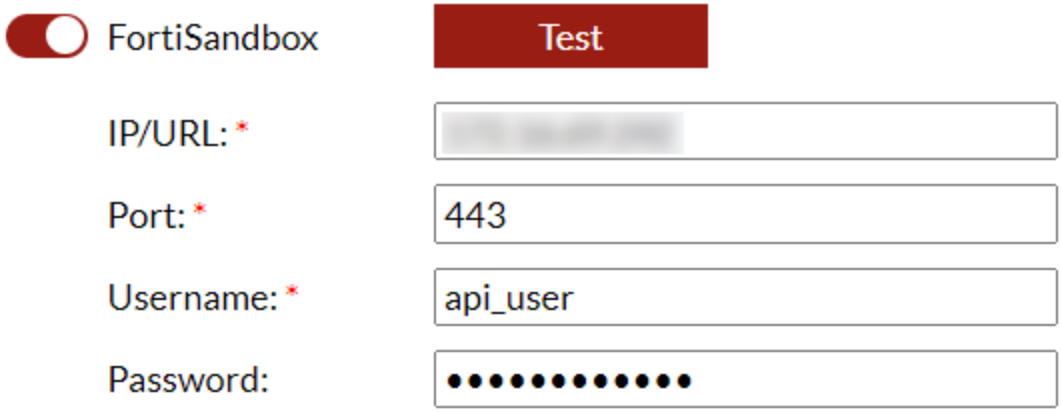


2. Create a new administrator with the profile you just created. For information see *Administrators* in the *FortiSandbox Administration Guide*.
   a. Go to *System* > *Administrators*, click *Create New*.
   b. Set administrator name and password.
   c. From the *Admin Profile* dropdown, select the profile you just created and click *OK*.



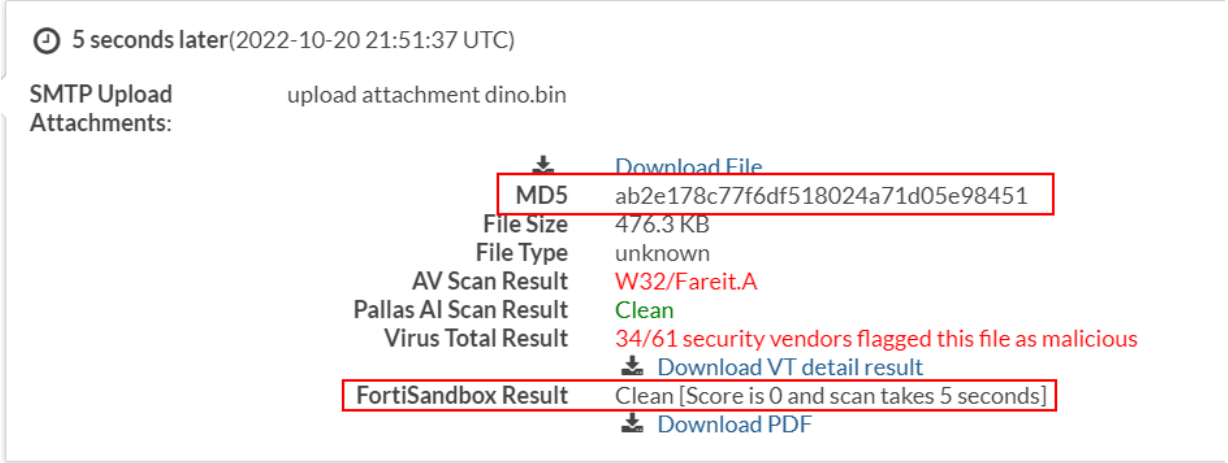
2. Integrate FortiDeceptor with FortiSandbox

1. Configure a user on FortiSandbox to use for access from FortiDeceptor.
2. In FortiDeceptor, go to *Fabric* > *Detection Device*. The *Fabric Detection* dialog opens.
3. Enable *FortiSandbox*.
4. Configure the device settings and click *Save*.

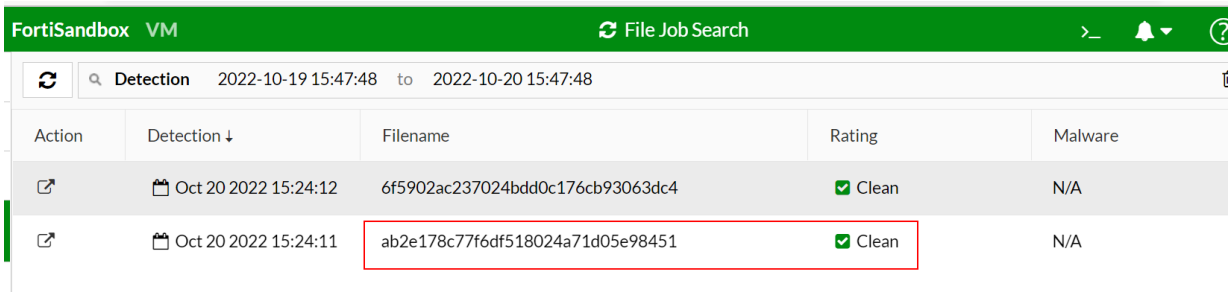


3. Verify the scanning results in FortiDeceptor and FortiSandbox

1. Send a SMB/FTP put attack to the decoy from the endpoint.
2. To verify the results in FortiDeceptor:
   a. Go to *Incident* > *Analysis*.
   b. Expand the incident and a make a note of the filename in the *MD5* field and the *FortiSandbox Result*.



3. To verify the results in FortiSandbox:
   a. Go to *Scan Job* > *File Job Search*.
   b. Search for the filename and verify the *Rating* is the same as the *FortiSandbox Result* in FortiDeceptor.



Integration with FortiNAC

This topic assumes FortiNAC has been set up properly as a NAC solution. We have provided an example on how to configure the integration for testing purposes.

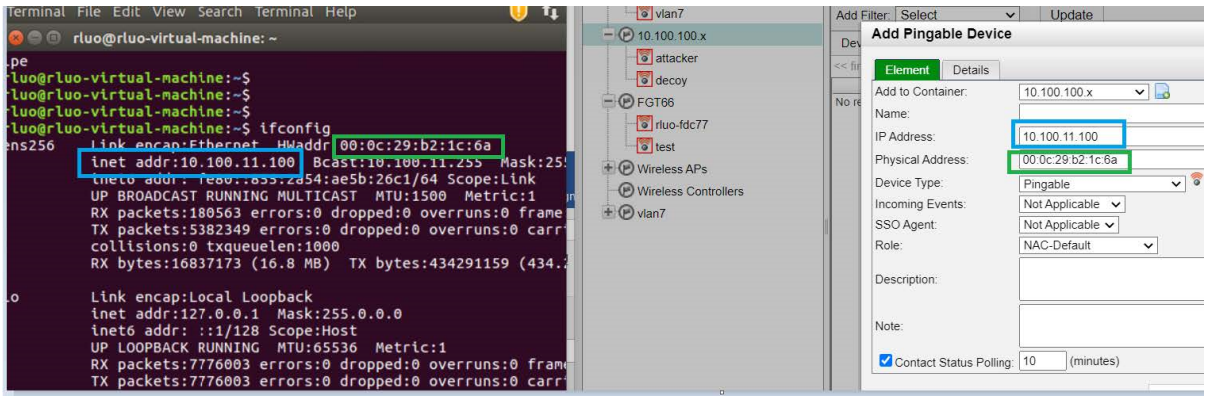
To integrate FortiDeceptor with FortiNAC:

1. Configure the attack host on FortiNAC.
2. Convert the pingable device to a host.
3. Verify the host was added successfully.
4. Generate an API token on FortiNAC.
5. Configure the integration with FortiNAC (Gen-Webhook).
6. Configure the integration with FortiNAC (FNAC-WEBHOOK).

1. Configure the attack host on FortiNAC

1. On FortiNAC, go to *Network* > *Inventory*.
2. Select the *Container* icon.
3. Right-click a container and select *Add Pingable Device* or right-click a pingable device in the *Devices* tab and select *Modify*.
4. From the drop-down menu select the *Container* where this device will be stored. You can use the icon next to the *Container* field to add a new container.
5. Configure the pingable device.

IP Address	Enter the IP address of the endpoint.
Physical Address	Enter the address of hardware endpoint.



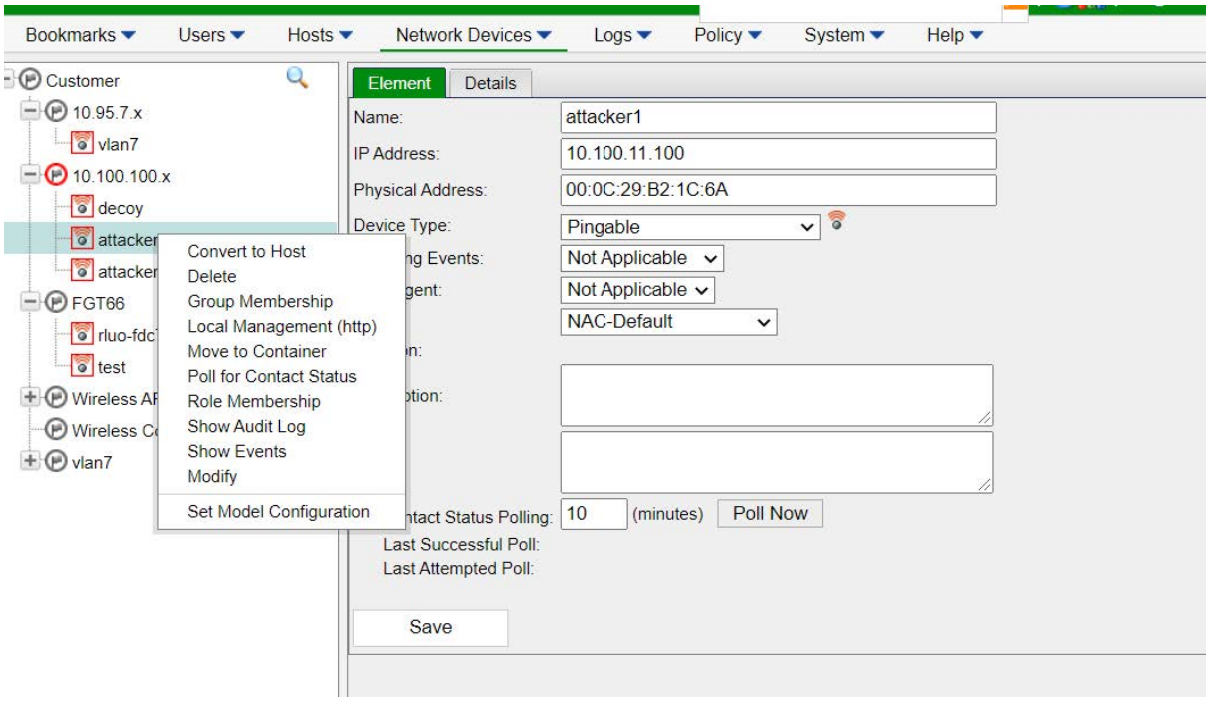
6. Click *OK*.

For information about adding and modifying pingable devices in FortiNAC, see Add or modify a pingable device in the *FortiNAC Administration Guide*.

2. Convert the pingable device to a host

1. In FortiNAC, click *Network* > *Inventory*.
2. Expand the *Container* where the device is located.
3. Select the device to be converted.

4. Right-click a device and select *Convert To Host*. This option converts the non-SNMP devices selected to hosts.

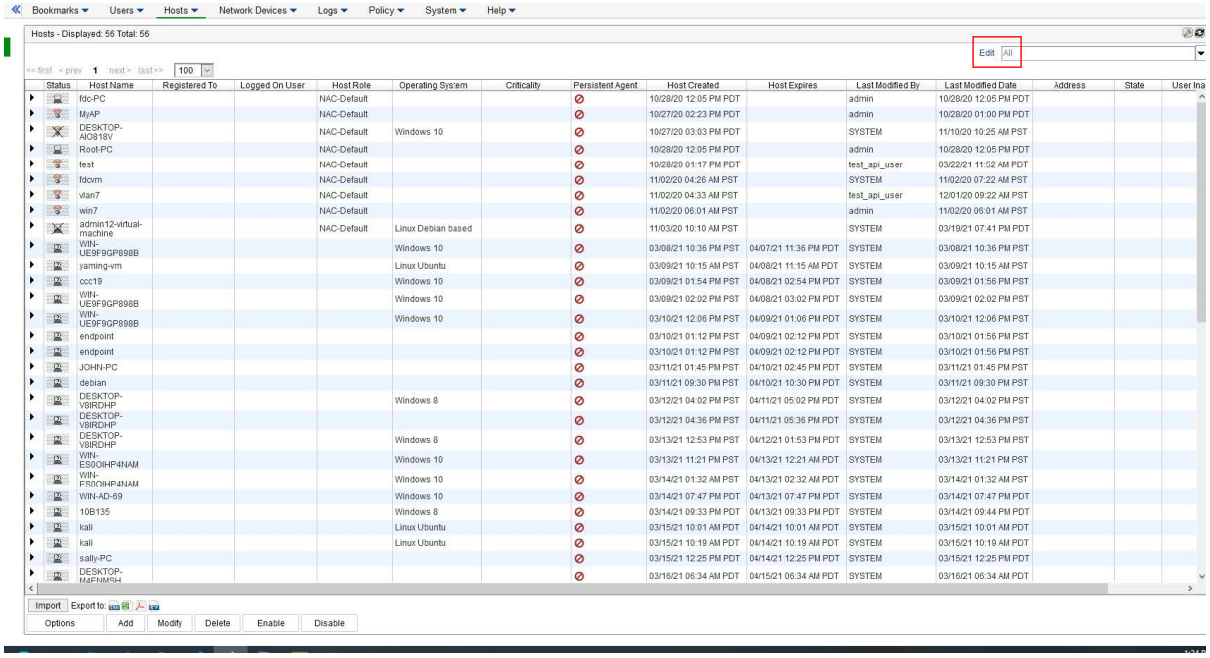


5. Click *Yes* on the confirmation window.
6. *Select and verify that the pingable devices now display.*

For more information, see Convert all pingables to hosts in the *FortiNAC Administration Guide*.

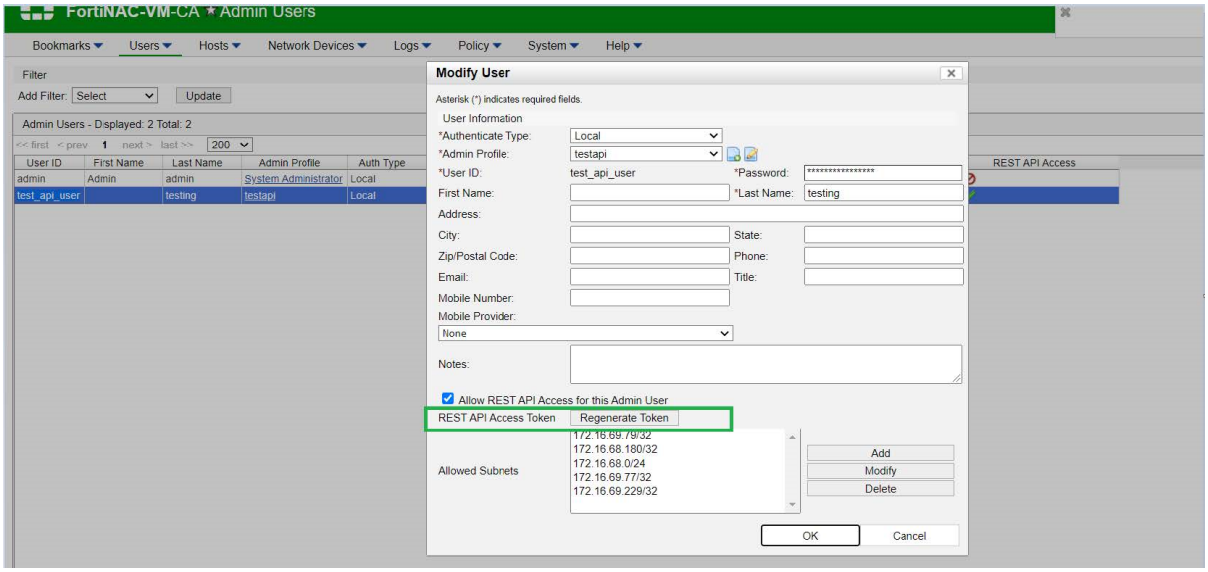
3. Verify the host was added successfully

Go to the *Hosts* tab, and check the status. For information, see Host Summary in the *FortiNAC Administration Guide*.



4. Generate an API token on FortiNAC

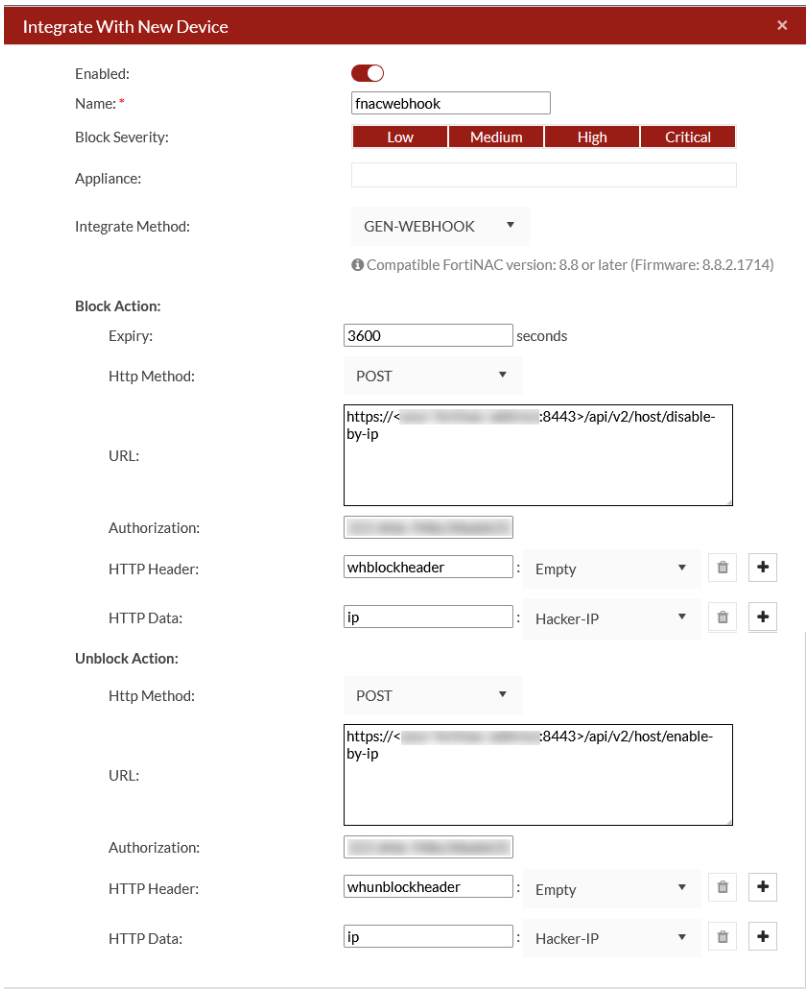
1. In FortiNAC go to the *Users* tab.
2. Select a user from the list. The *Modify User* page opens.
3. Next to *REST API Access Token*, click *Regenerate Token*.



5. Configure the integration with FortiNAC (Gen-Webhook)

1. In FortiDeceptor, go to *Fabric* > *Quarantine Integration* and click *Quarantine Integration With New Device*.
2. Configure the integration settings and click *Save*.

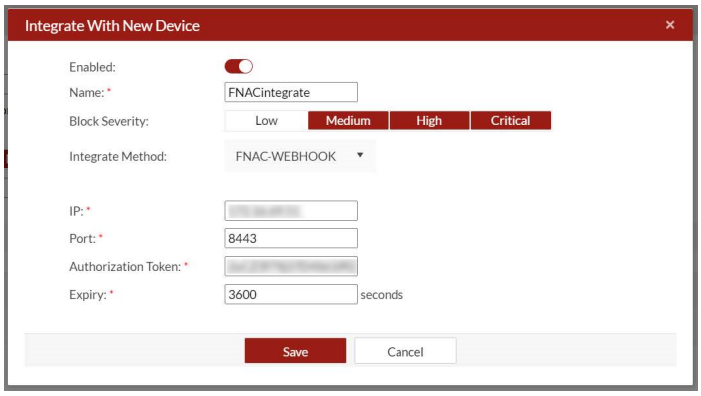
Integrate Method	Select *GEN-WEBHOOK*.
Block Action	
Http Method	POST
URL	https://<your-fortinac-address:8443>/api/v2/host/disable-by-ip
Authorization	Enter the API access token you generated in step 4
HTTP Header	blockheader
HTTP Data	ip
Unblock Action	
HTTP Method	POST
URL	https://<your-fortinac-address:8443>/api/v2/host/enable-by-ip



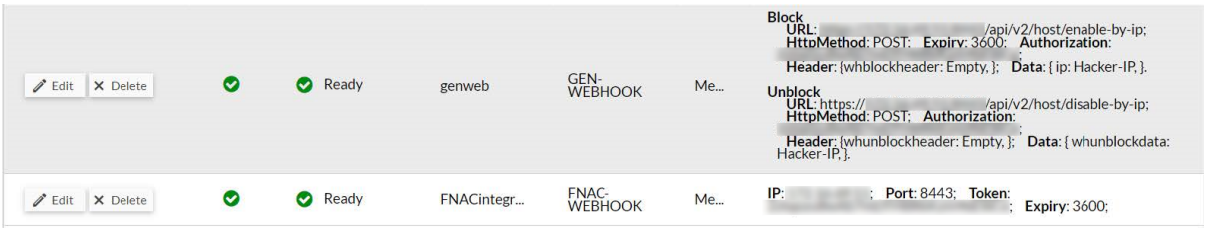
6. Configure the integration with FortiNAC (FNAC-WEBHOOK)

1. In FortiDeceptor, go to *Fabric* > *Quarantine Integration* and click *Quarantine Integration With New Device*.
2. Configure the integration settings and click *Save*.

IP	Enter the FortiNAC address.
PORT	8443
Authorization Token	Enter the API access token you generated in Step 4.
Expiry	1-3600 (default is 3600).



3. Verify the device status is *Ready*.



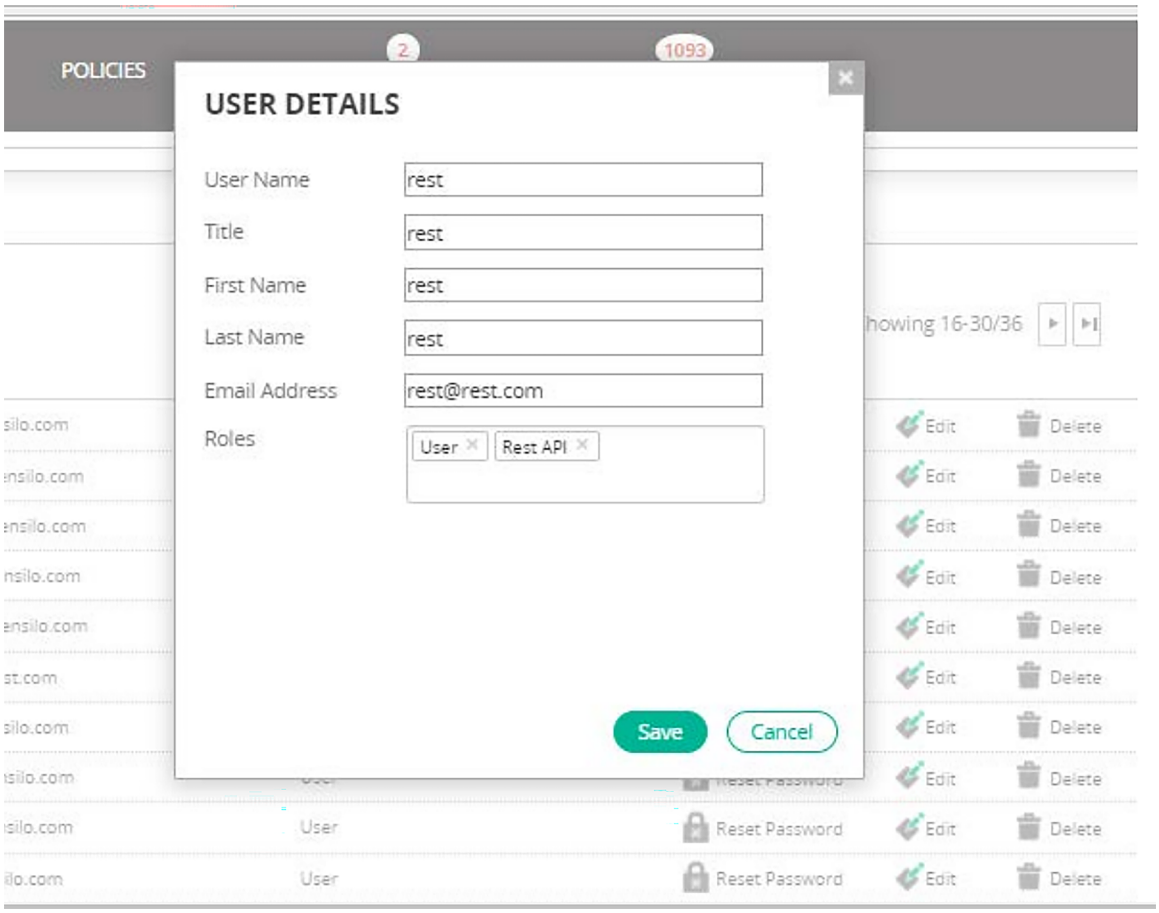
Integration with FortiEDR

To integrate FortiDeceptor with FortiEDR:

1. Configure FortiEDR.
2. Configuration on FortiDeceptor.

1. Configure FortiEDR

FortiDeceptor performs API calls using basic authentication by supplying a username and password. The user performing the calls must have the relevant REST API role defined in FortiEDR.

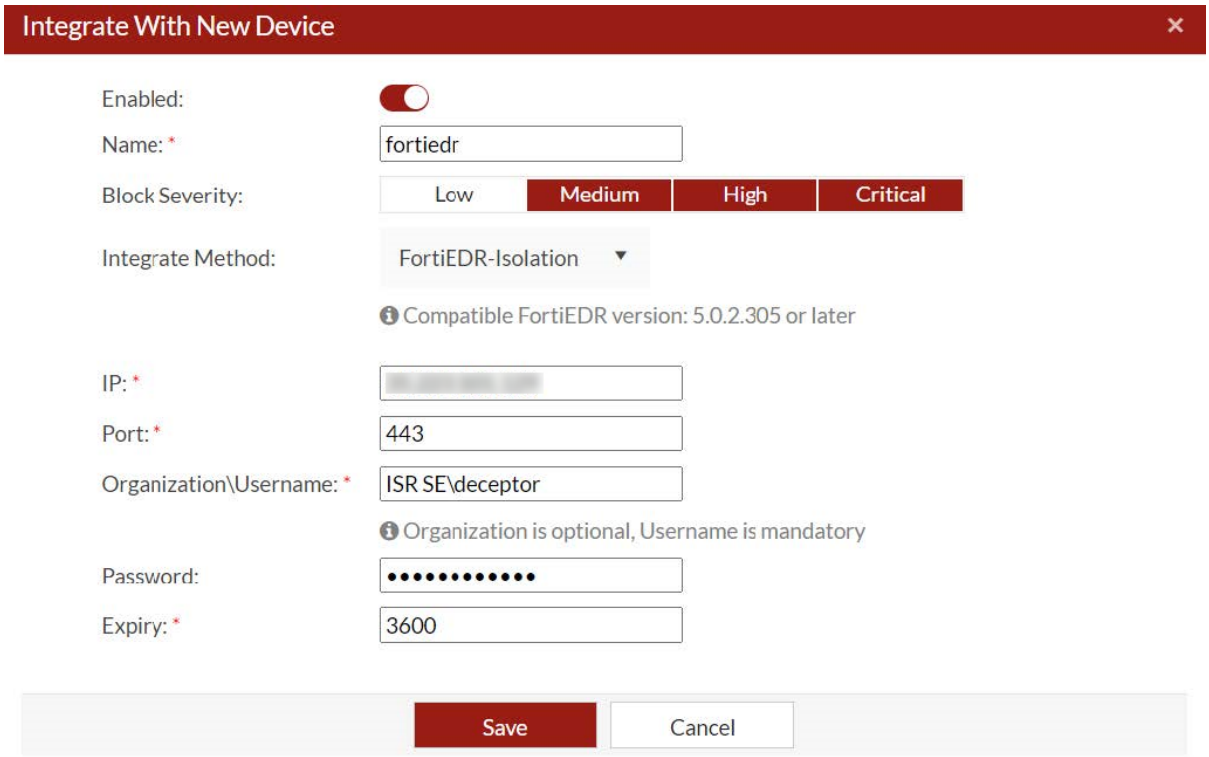


A user attempting to perform API calls without the REST API role sees a *401 Unauthorized Access* error code. The *Admin* role does not provide access to the REST API layer, and does not contain the REST API role.

2. Configuration on FortiDeceptor

1. In FortiDeceptor, go to *Fabric* > *Quarantine Integration* and click *Quarantine Integration With New Device*.
2. Configure the integration settings and click *Save*.

Integrate Method	Select *FortiEDR-Isolation*.
IP	Enter the IP address of the FortiEDR.
Organization\Username	Separate the organization and username with a backslash (\) if organization is applicable.
Password	Enter the password for the FortiEDR username.



Integration with FortiAnalyzer

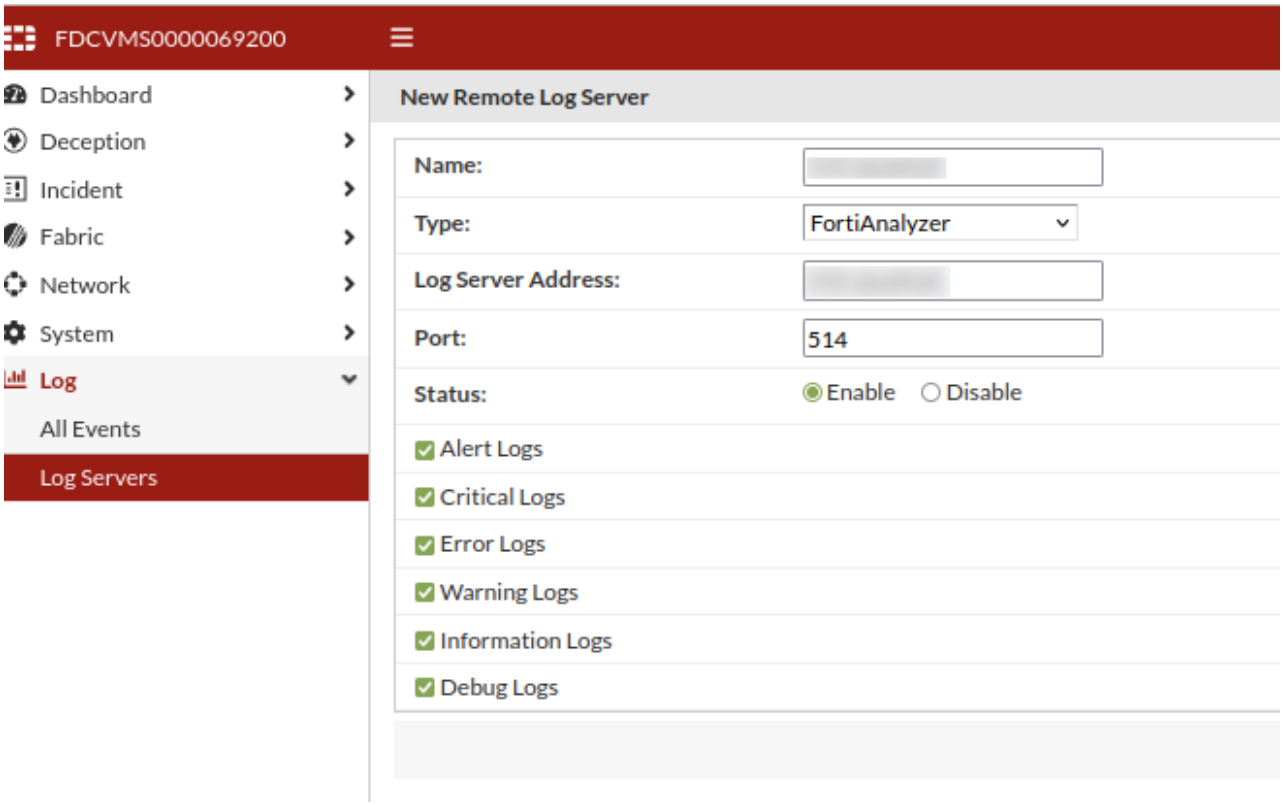
The steps in this topic assume the FortiDeceptor device has never to been connected to and has not been authorized by FortiAnalyzer.

To integrate FortiDeceptor with FortiAnalyzer:

1. Configure the Log Servers in FortiDeceptor.
2. Authorize FortiDeceptor in FortiAnalyzer.
3. Create the FortiDeceptor security report in FortiAnalyzer.

1. Configure the Log Servers in FortiDeceptor

1. In FortiDeceptor, go to *Log* > *Log Servers* and click *Create New*. The *New Remote Log Server* window opens.
2. Set the *Type* to *FortiAnalyzer* and enter the *Log Server Address*.

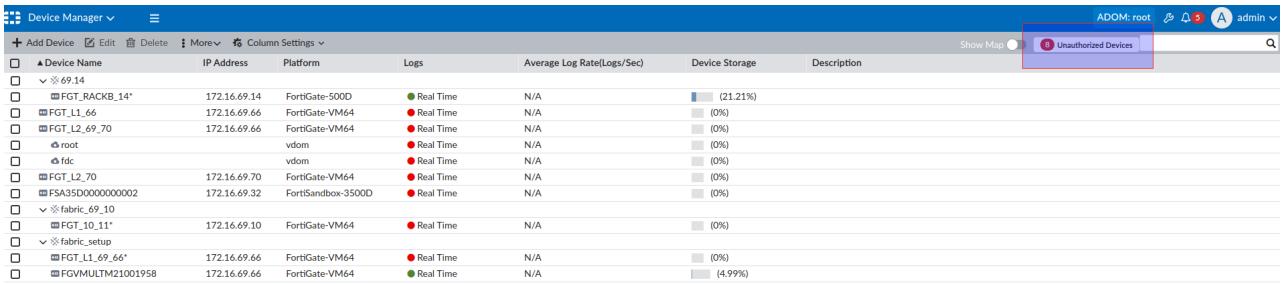


3. Configure the additional log server settings as required and click *OK*.

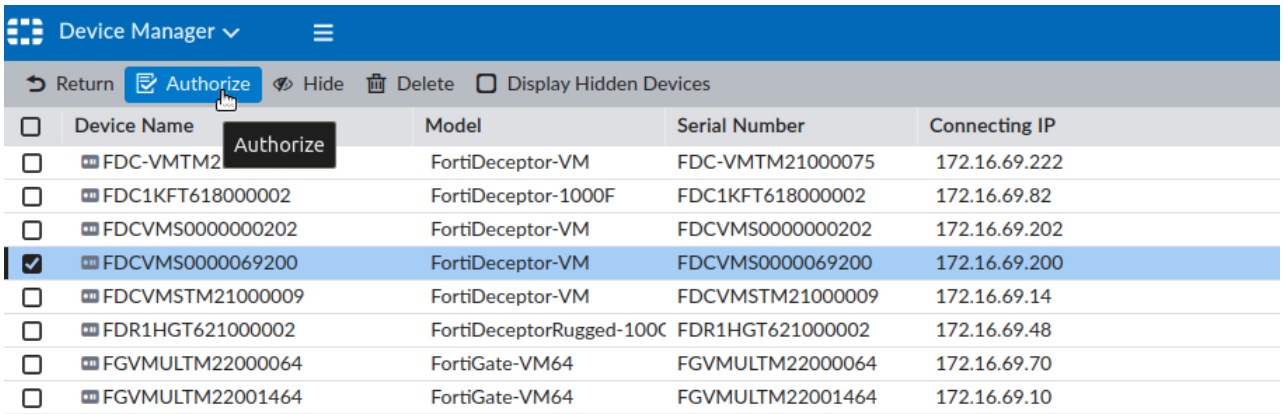
2. Authorize FortiDeceptor in FortiAnalyzer

Allow a minimum of five minutes before attempting to authorize FortiDeceptor in FortiAnalyzer.

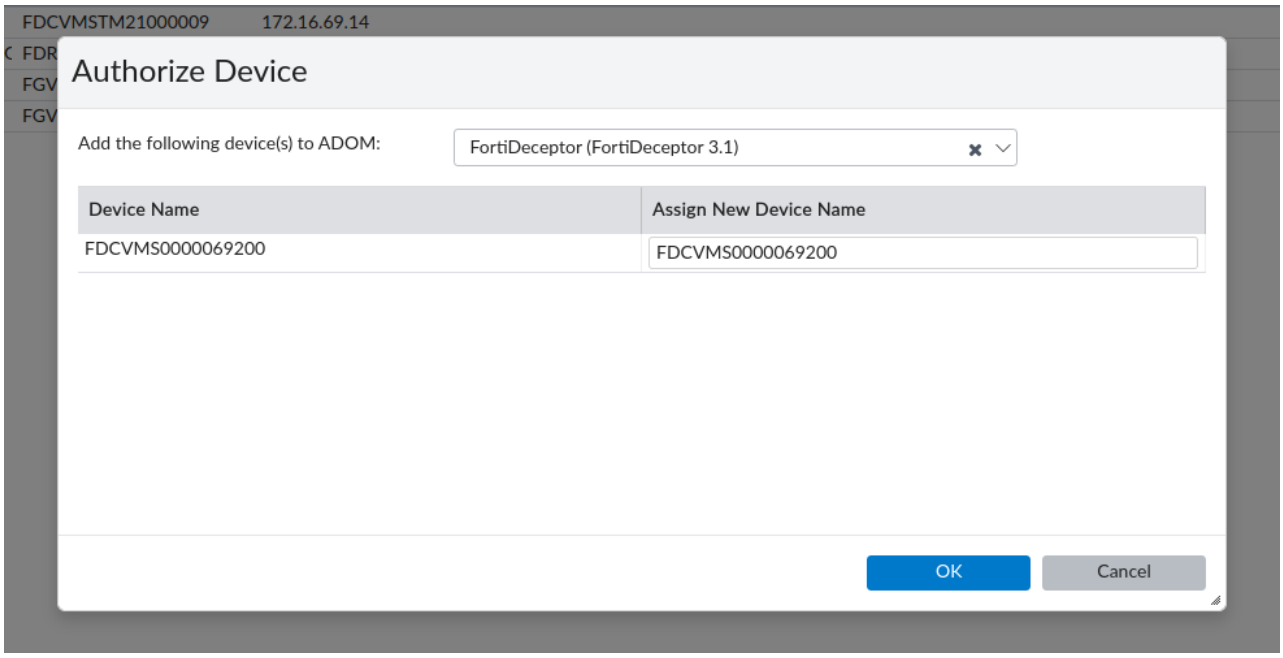
1. In FortiAnalyzer, go to *Device Manager*.
2. Search for FortiDeceptor in the *Unauthorized Devices* list. It may take up to half an hour for the device to appear in the list.



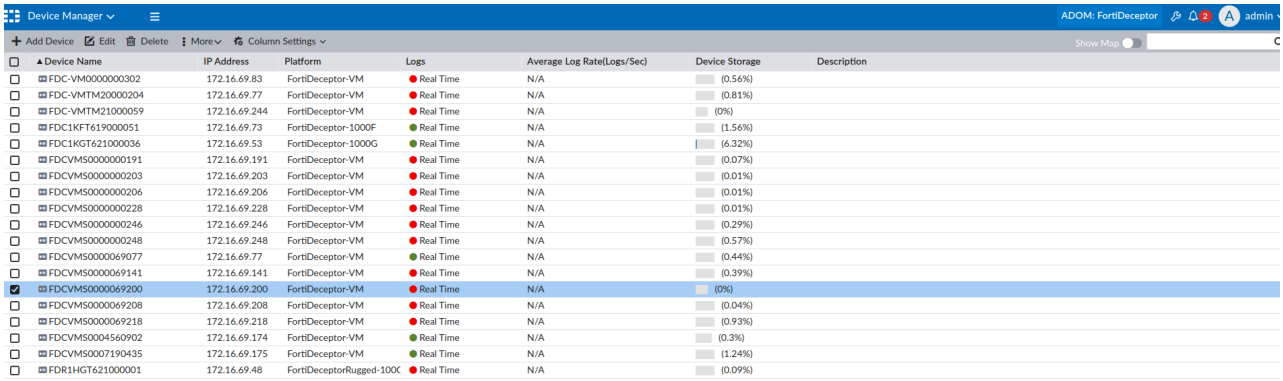
3. Select the device and click *Authorize*. The *Authorize Device* dialog opens.



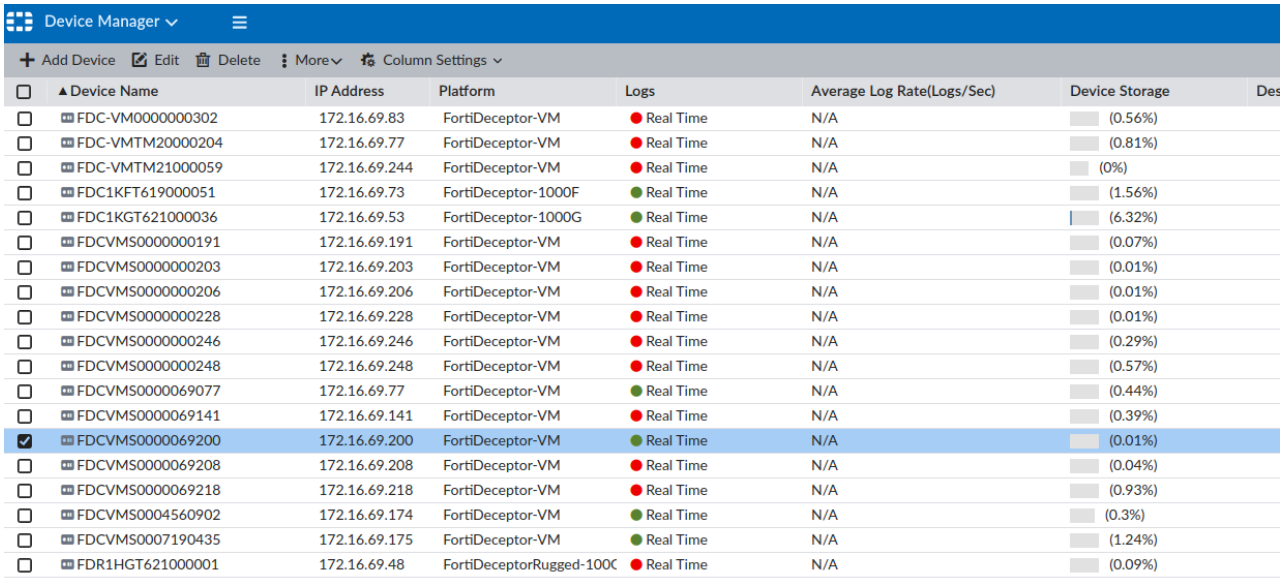
4. From the *Add the following device(s) to ADOM list*, select the ADOM you want to add the device to.



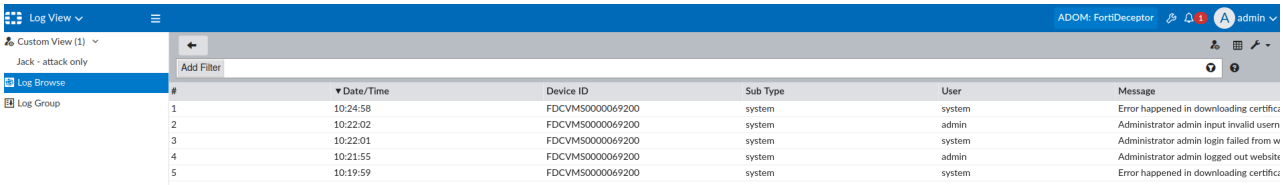
5. Go to the ADOM's *Device Manager* and verify the FortiDeceptor is added.



6. In the *Logs* column, the status will display a red dot until FortiDeceptor generates syslogs. A green dot indicates the device is connected and functioning properly.



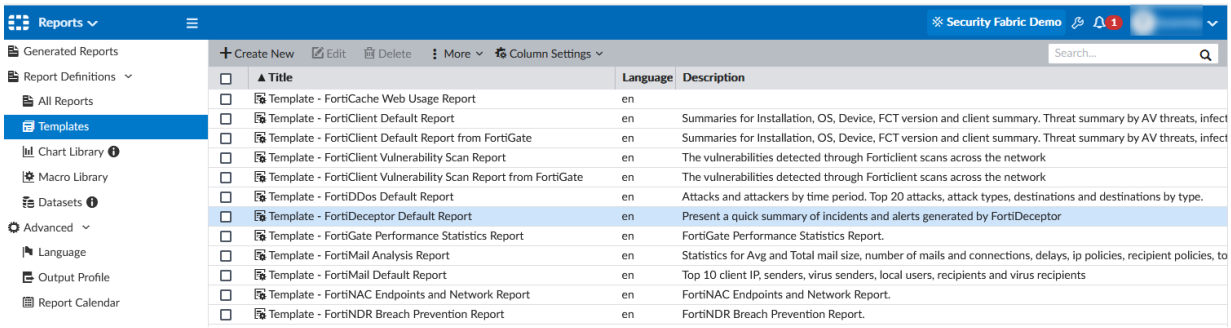
7. Go to *Log View* and select this FortiDeceptor to view the logs.



3. Create the FortiDeceptor security report in FortiAnalyzer

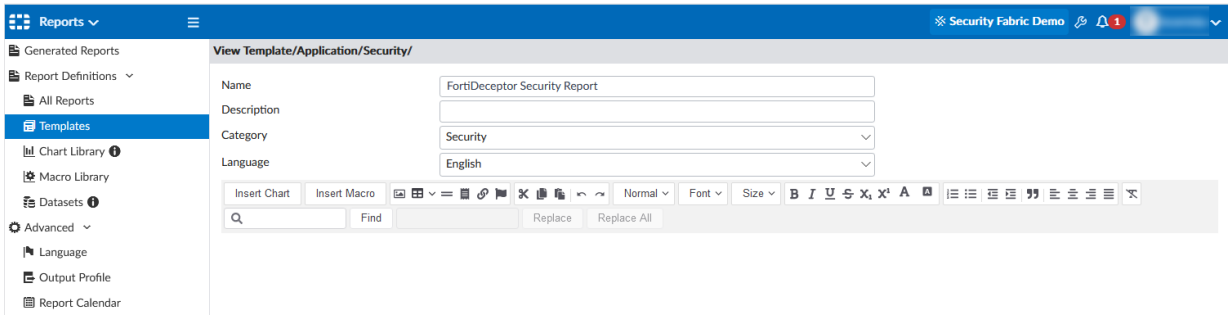
1. In FortiAnalyzer, create the report template:
   a. Open the *Reports* module.
   b. Go to the *Reports* > *Report Definitions* > *Templates*.

c. In the template list, select *FortiDeceptor Default Report*.



d. In the toolbar, click *Create New*.

e. Give the template a descriptive *Name* such as `FortiDeceptor Security Report` and from the *Category* dropdown, select *Security*.



f. Configure the rest of the template settings as required and click *OK*. For information, see *Creating report templates* in the *FortiAnalyzer Administration Guide*.

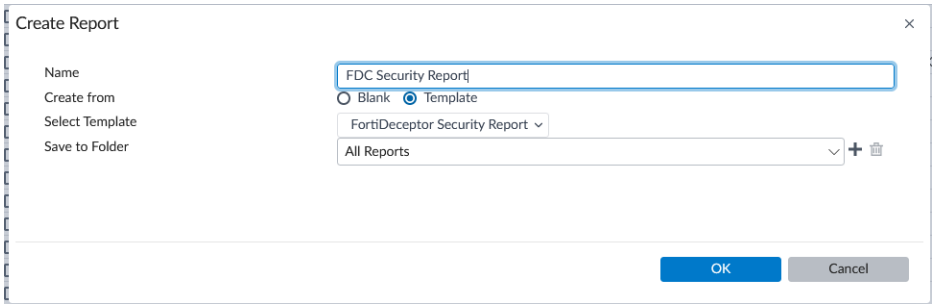
2. Create the report:

a. Go to the *Reports* > *Report Definitions*.

b. In the toolbar, click *Report* > *Create New*.

c. Give the report a distinctive *Name*.

d. Next to *Create From*, select *Template* and from the *Select Template* dropdown, select the FortiDeceptor template you created.



e. Select the folder to save the report and click *OK*.

For more information about creating reports in FortiAnalyzer see *Reports* in the *FortiAnalyzer Administration Guide*.

Integration with FortiGate over Webhook

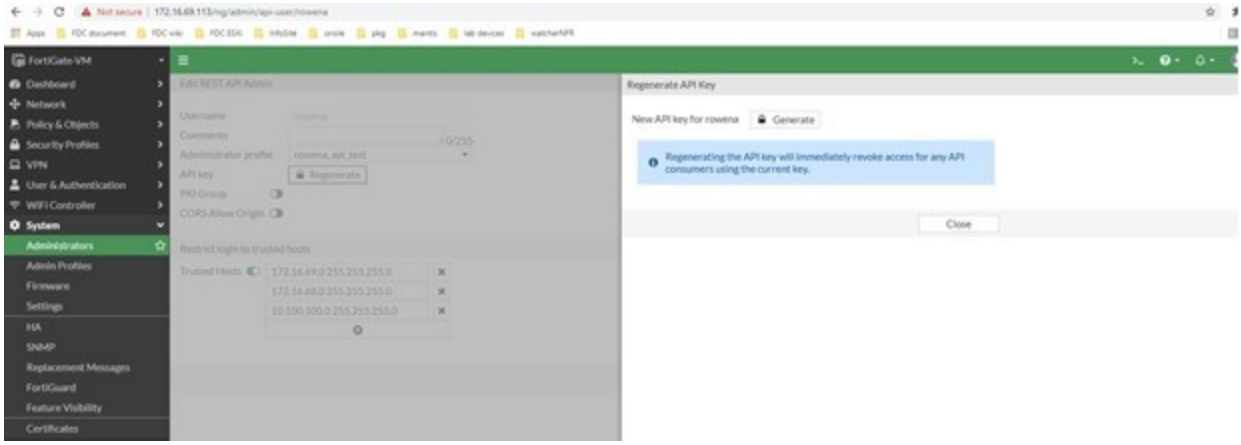
This topic describes how to integrate FortiDeceptor with FortiGate versions 6.4 and 7.0. The GUI may vary depending the version of FortiGate/FortiOS you are using. For more information about Automation Stitches, select the version of *FortiGate / FortiOS Administration Guide* you are using in the Fortinet Document Library.

To integrate FortiDeceptor with FortiGate over Webhook:

1. Configure the API key on FortiGate.
2. Configure Webhook on FortiGate 6.4.x .
3. Configure Webhook on FortiGate 7.0.x .
4. Configure FortiDeceptor to integrate with FortiGate over Webhook.

1. Configure the API key on FortiGate

1. In FortiGate, go to *System* > *Administrators* and select a user.
2. Next to *API Key*, click *Regenerate*, then copy the API key.



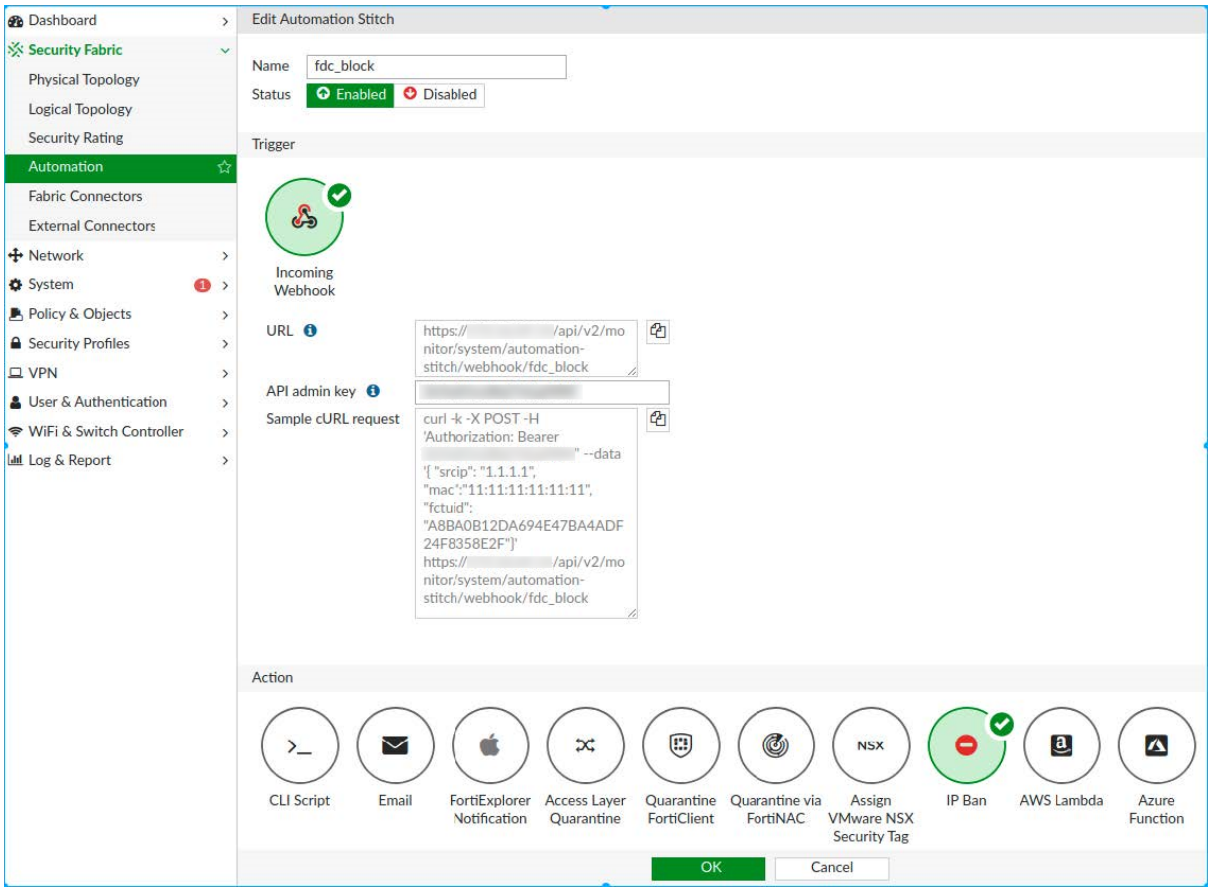
2. Configure Webhook on FortiGate 6.4.x

For information about creating and editing webhooks in FortiGate, see *Automation webhook stitches* in the *FortiGate / FortiOS 6.4.0 Administration Guide*.

2.1 Configure the incoming webhook for block action

1. Go to *Security Fabric* > *Automation*.
2. Create a new Automation Stitch
   a. In the toolbar, click *Create New*.
   b. Under *Trigger* click *Incoming Webhook*.
   c. Under *Action*, click *IP Ban*.
   d. In the *API admin key* field, enter the API key you recorded in Step 1. Configure the API key on FortiGate . A Sample cURL request is created.

e. Copy the *Sample cURL request*.



3. Execute the request:

a. Edit the sample cURL you recorded in the previous step.

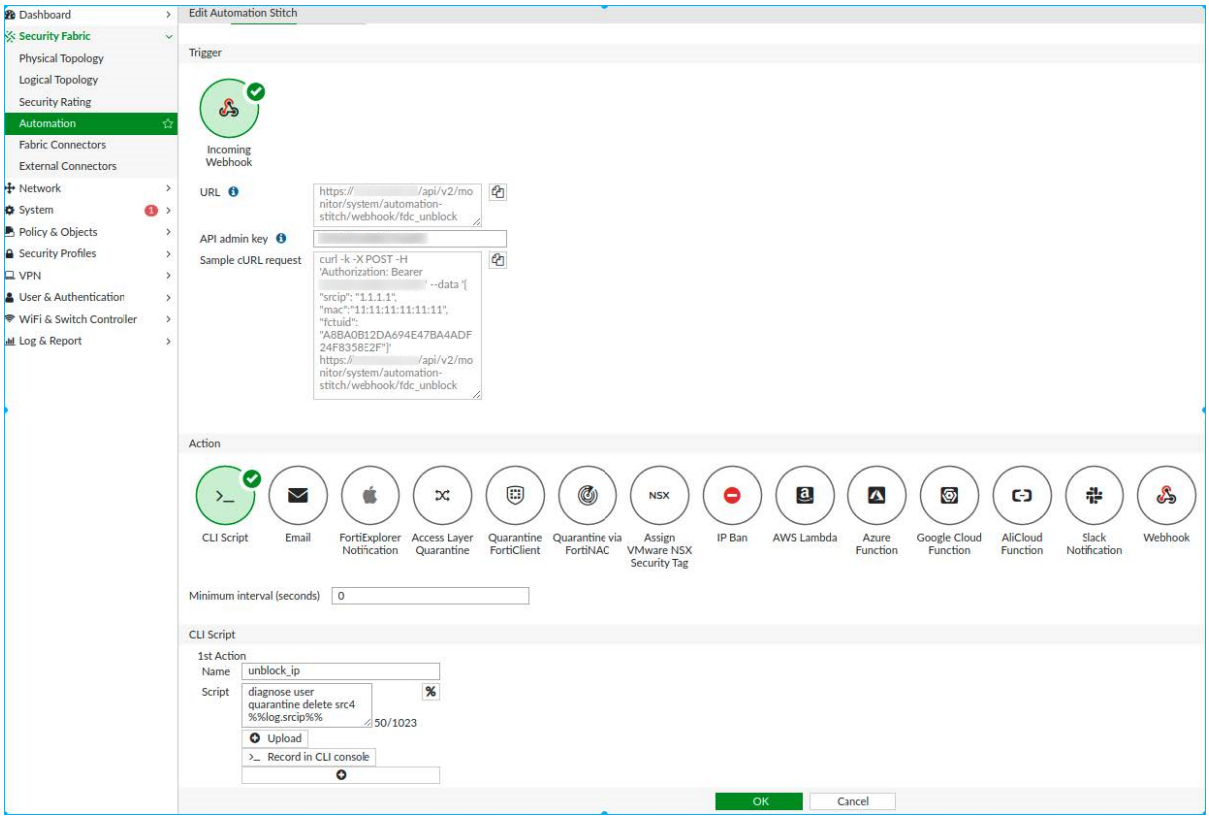
b. Edit parameters to the data field (“`srcip`”, "`mac`" and "`fctuid`"), and then execute the request.

```
root@pc:~# curl -k -X POST -H 'Authorization: Bearer cfgtct1mmx3fQxr4khb994p7swdfmk' --
     data '{ "mac":"0c:0a:00:0c:ce:b0", "fctuid": "0000BB0B0ABD0D00B0D0A0B0E0F0B00B"}'
     https://172.16.116.226/api/v2/monitor/system/automation-
     stitch/webhook/Incoming%20Webhook%20Quarantine
{
   "http_method":"POST",
   "status":"success",
   "http_status":200,
   "serial":"FGT00E0Q00000000",
   "version":"v6.4.0",
   "build":1545
```

Encode the spaces in the automation-stitch name with `%20`. For example, `Incoming%20Webhook%20Quarantine`

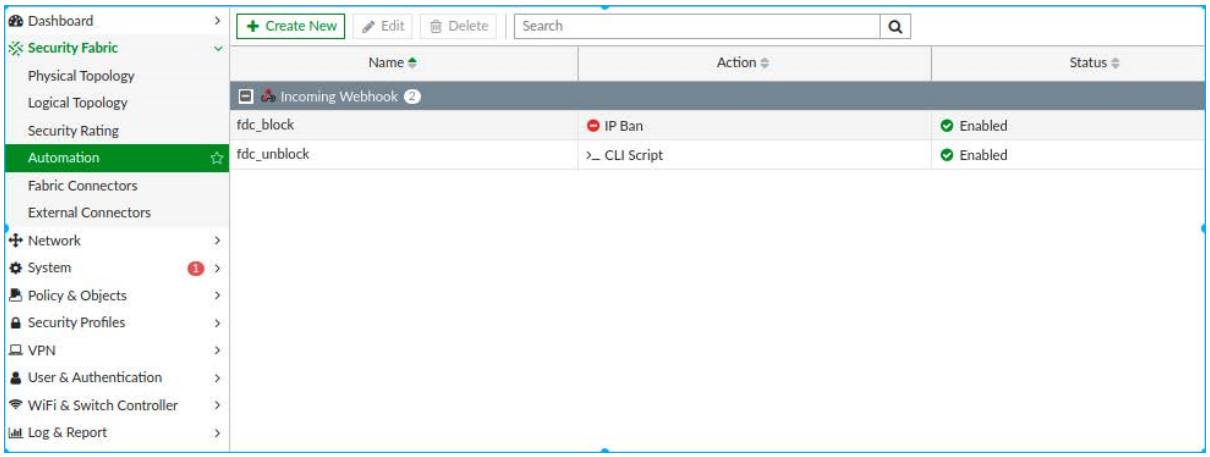
2.2 Configure the incoming webhook for unblock action

1. Go to *Security Fabric* > *Automation*.
2. Create a new Automation Stitch
   a. In the toolbar, click *Create New*.
   b. Under *Trigger* click *Incoming Webhook*.
   c. Under *Action*, click *CLI Script*.
   d. Under CLI Script, in the *Script* field enter the following command: `diagnose user quarantine delete src4 %%log.srcip%%`
   e. In the *API admin key* field, enter the API key you recorded in the previous Step 1. Configure the API key on FortiGate . A Sample cURL request is created.



2.3 Review the configuration on FortiGate side

In FortiGate, go to *Security Fabric* > *Automation* and verify the *Status* for the block and unblock webhooks are *Enabled*.

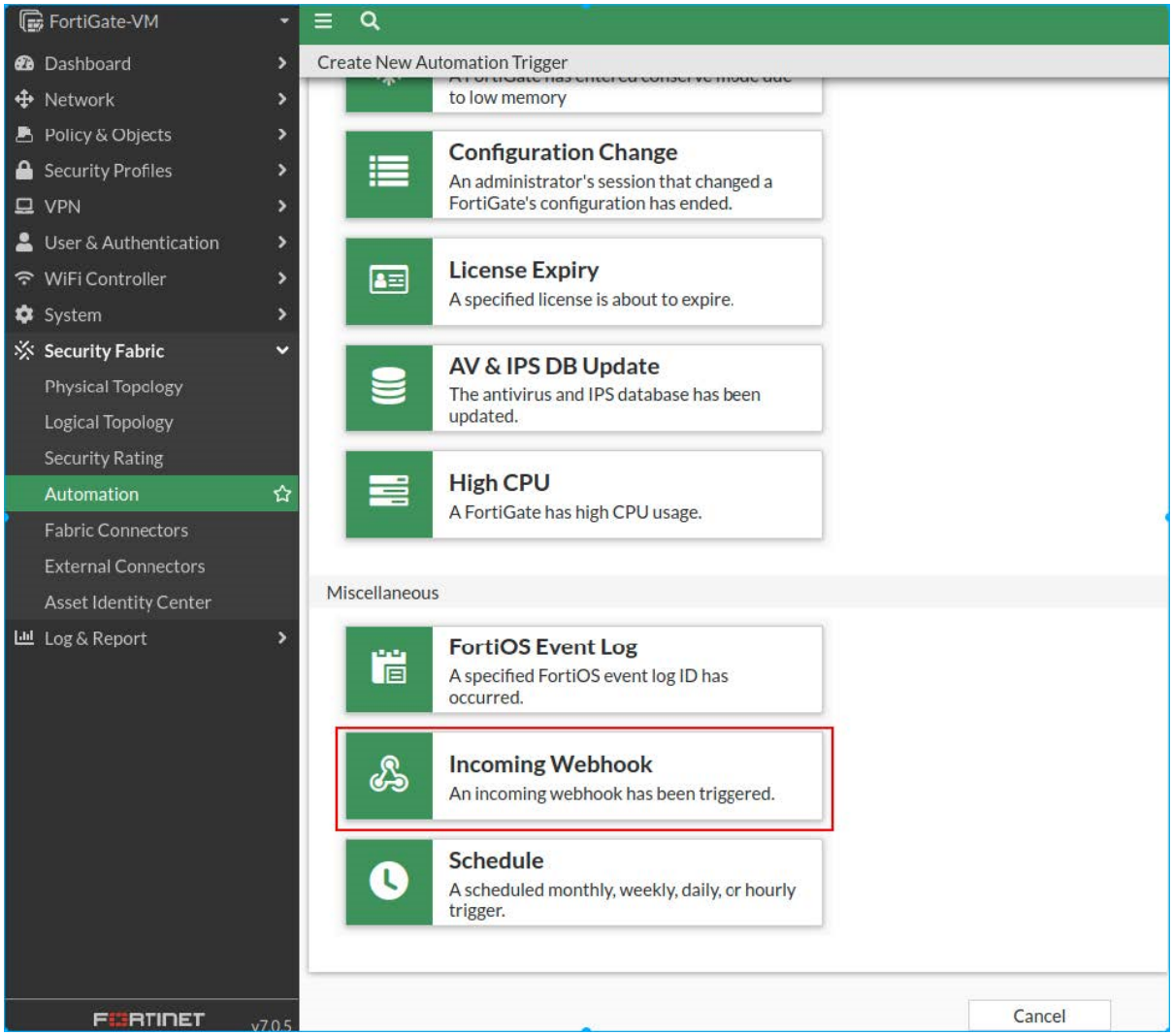


3. Configure Webhook on FortiGate 7.0.x

3.1 Configure the incoming webhook for block automation

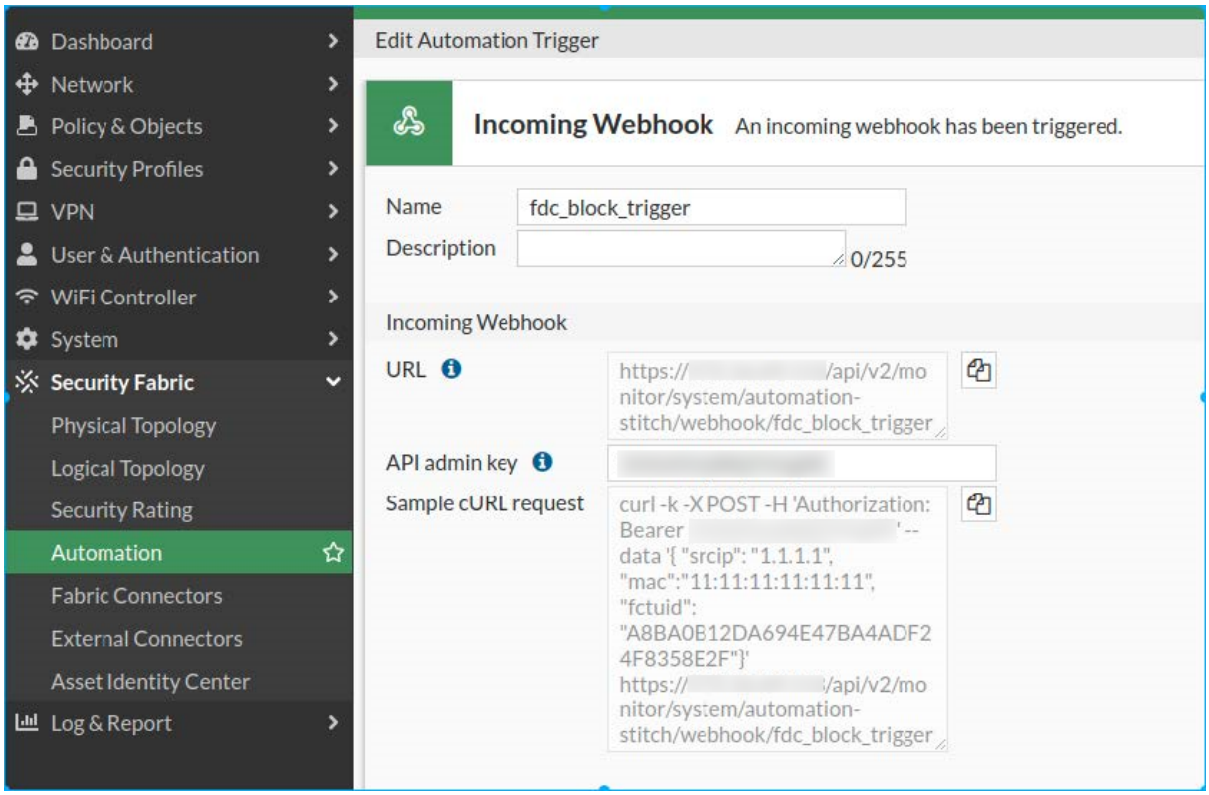
1. Go to *Security Fabric* > *Automation*.
2. In the banner, click *Trigger* > *Create New*. The *Create New Automation Trigger* page opens.

3. Click *Incoming Webhook*. The *Create New Automation Trigger* dialog opens.



4. Give the trigger a descriptive name such as `fdc_block_trigger` and click *OK*.

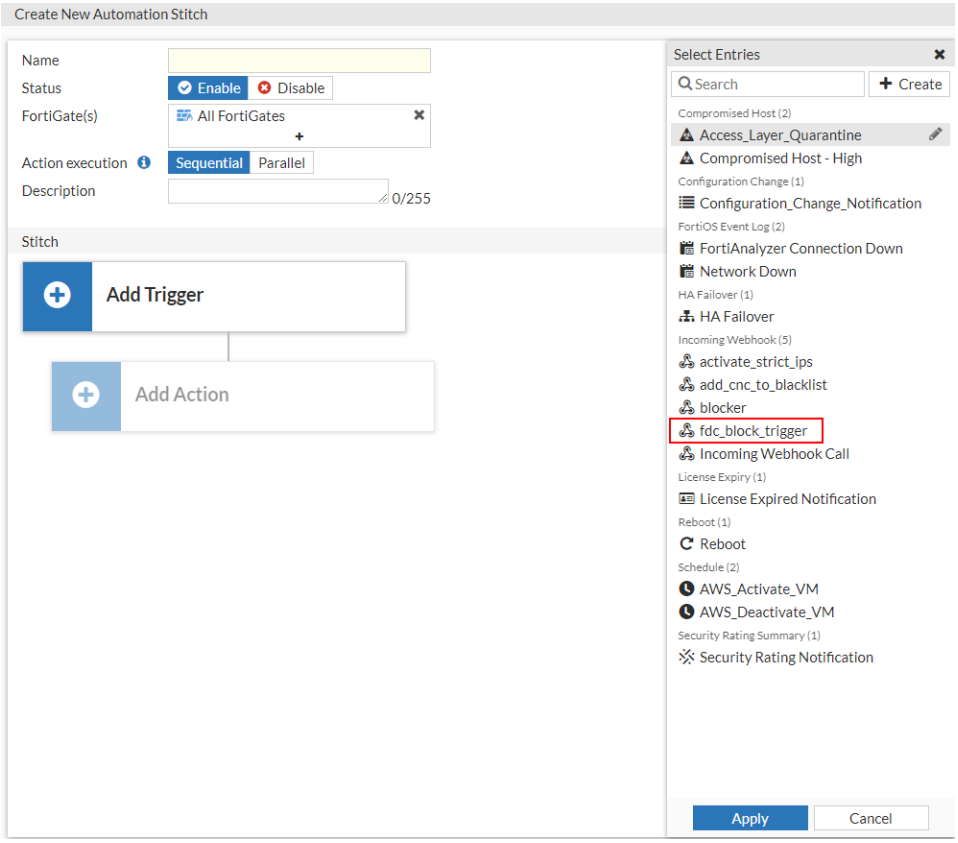
5. Enter the *API admin key* and click *OK*.



3.2 Create block stitch with the block trigger

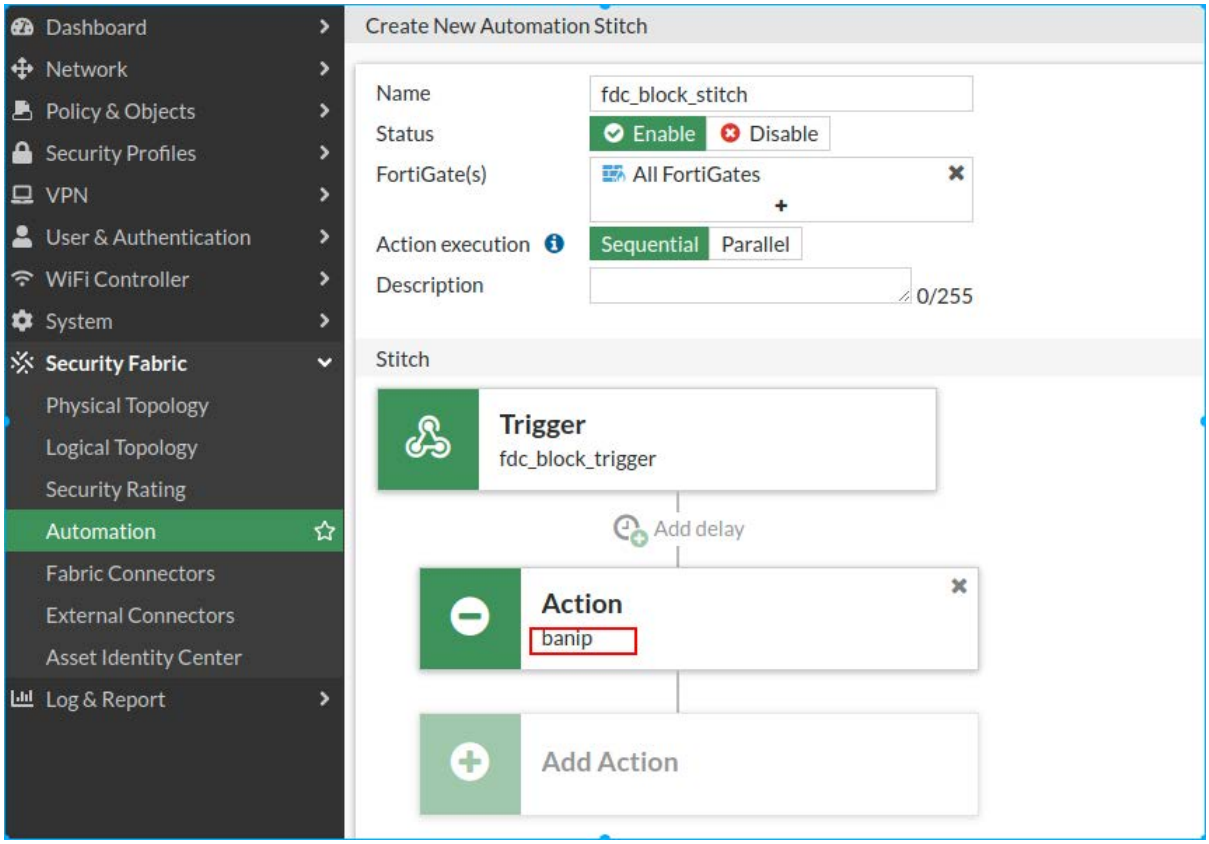
1. Go to *Security Fabric* > *Automation*.
2. In the banner, click *Stitch* > *Create New*. The *Create New Automation Stitch* page opens.
3. Click *Add Trigger*. The *Select Entries* pane opens.

4. Select the `fdc_block_trigger` you created and click *Apply*.



5. Click *Add Action*. The *Select Entries* pane opens.
6. Click *Create*. The *Create New Automation Trigger* windows opens.
7. Click *IP Ban*. Enter a *Name* such as `banip` and click *OK*.

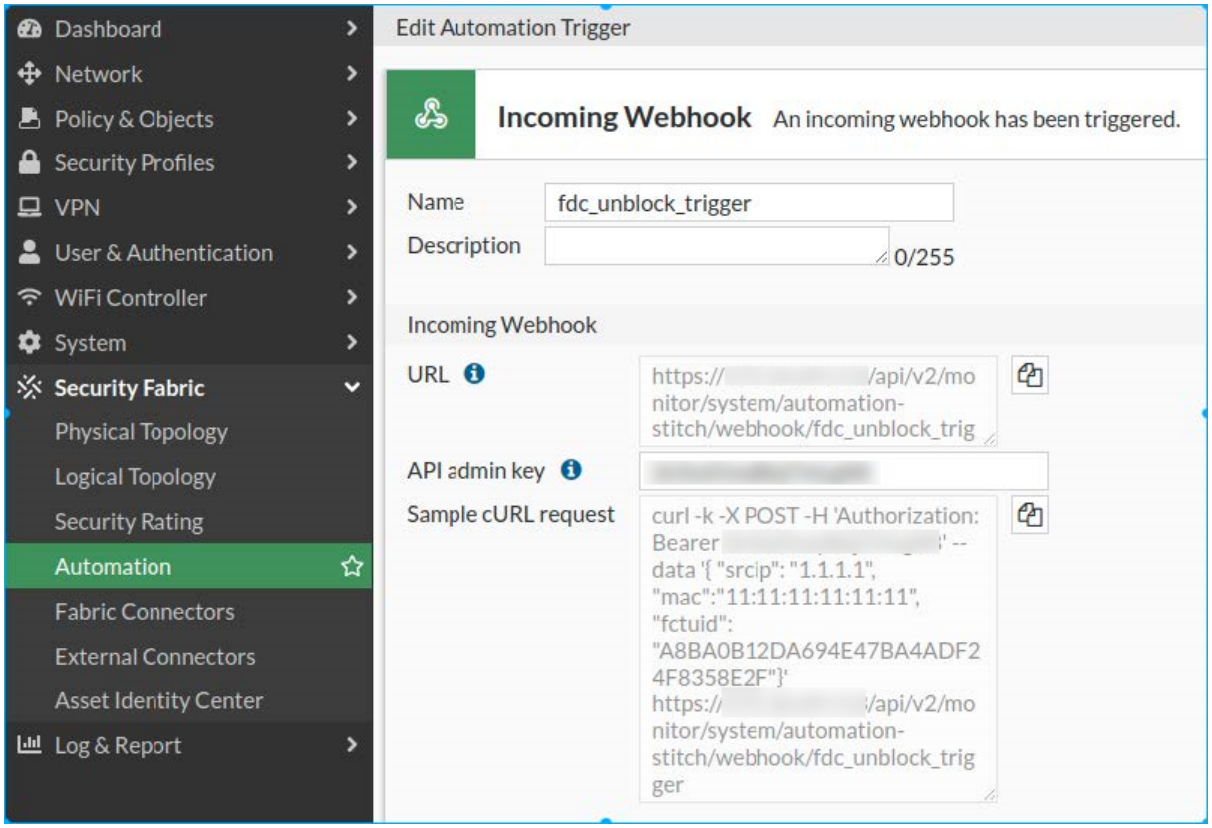
8. Select the action you created (`banip`), click *Apply* and click *OK*.



3.3 Configure the incoming webhook for unblock automation

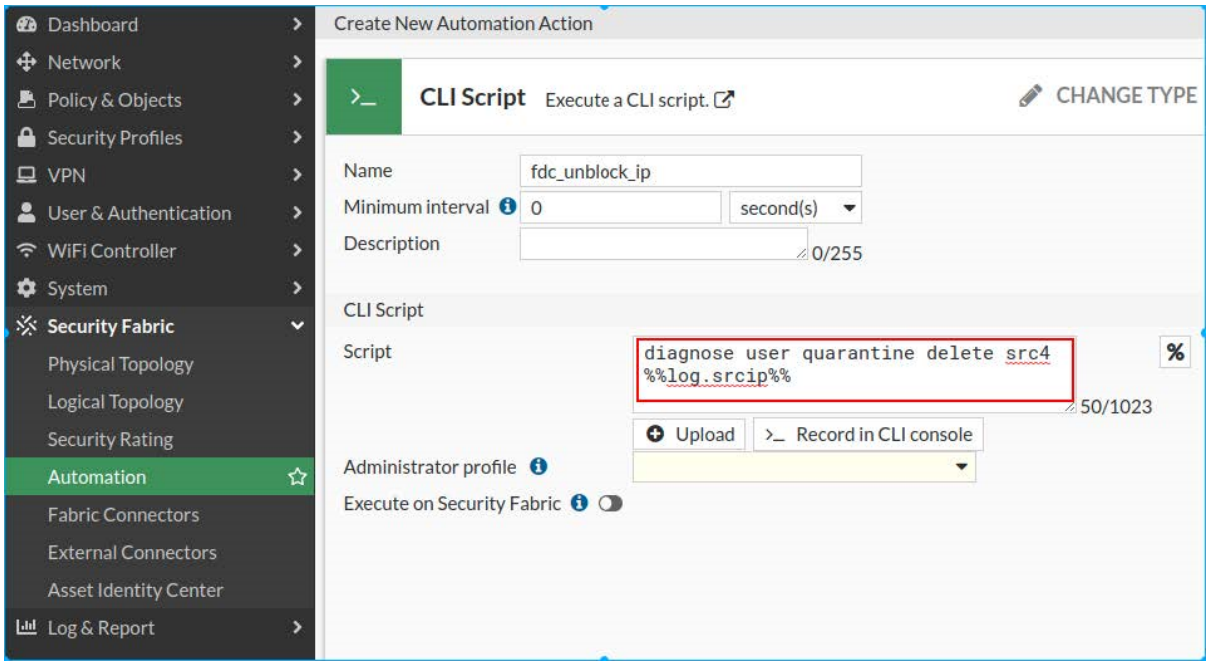
1. Go to *Security Fabric* > *Automation*.
2. In the banner, click *Trigger* > *Create New*. The *Create New Automation Trigger* page opens.
3. Click *Incoming Webhook*. The *Create New Automation Trigger* dialog opens.
4. Give the Trigger a descriptive name such as `fdc_unblock_trigger` and click *OK*.

5. Enter the *API admin key* and click *OK*.



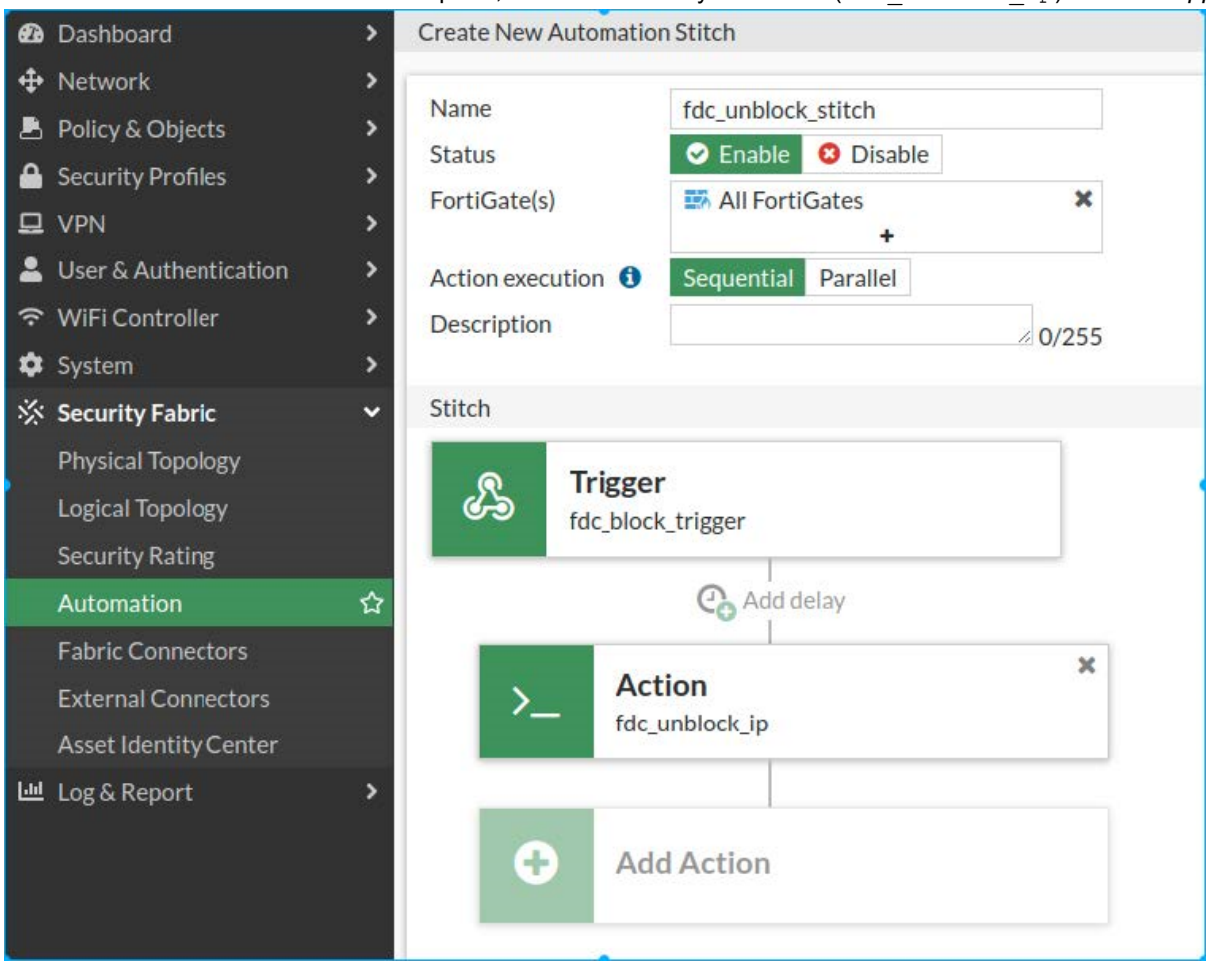
3.4 Create unblock action with CLI script

1. Go to *Security Fabric* > *Automation*.
2. In the banner, click *Stitch* > *Create New*. The *Create New Automation Stitch* page opens.
3. Click *Add Trigger*. The *Select Entries* pane opens.
4. Select the `fdc_unblock_trigger` you created and click *Apply*.
5. Click *Add Action*. The *Select Entries* pane opens.
6. Click *Create*. The *Create New Automation Trigger* windows opens.
7. In the *Search* field enter `CLI` and click the *CLI Script* tile. The *Create New Automation Action* opens.
8. Click *IP Ban*. Enter a *Name* such as `fdc_unblock_ip` .
9. In the *Script* field enter the following command: `diagnose user quarantine delete src4 %%log.srcip%%`.


Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Physical Topology
Logical Topology
Security Rating
Automation
Fabric Connectors
External Connectors
Asset Identity Center
Log & Report
Create New Automation Action
CLI Script
Execute a CLI script.
CHANGE TYPE
Name
fdc_unblock_ip
Minimum interval
0
second(s)
Description
0/255
CLI Script
Script
diagnose user quarantine delete src4
%%log.srcip%%
50/1023
Upload
Record in CLI console
Administrator profile
Execute on Security Fabric

10. Click *OK*.

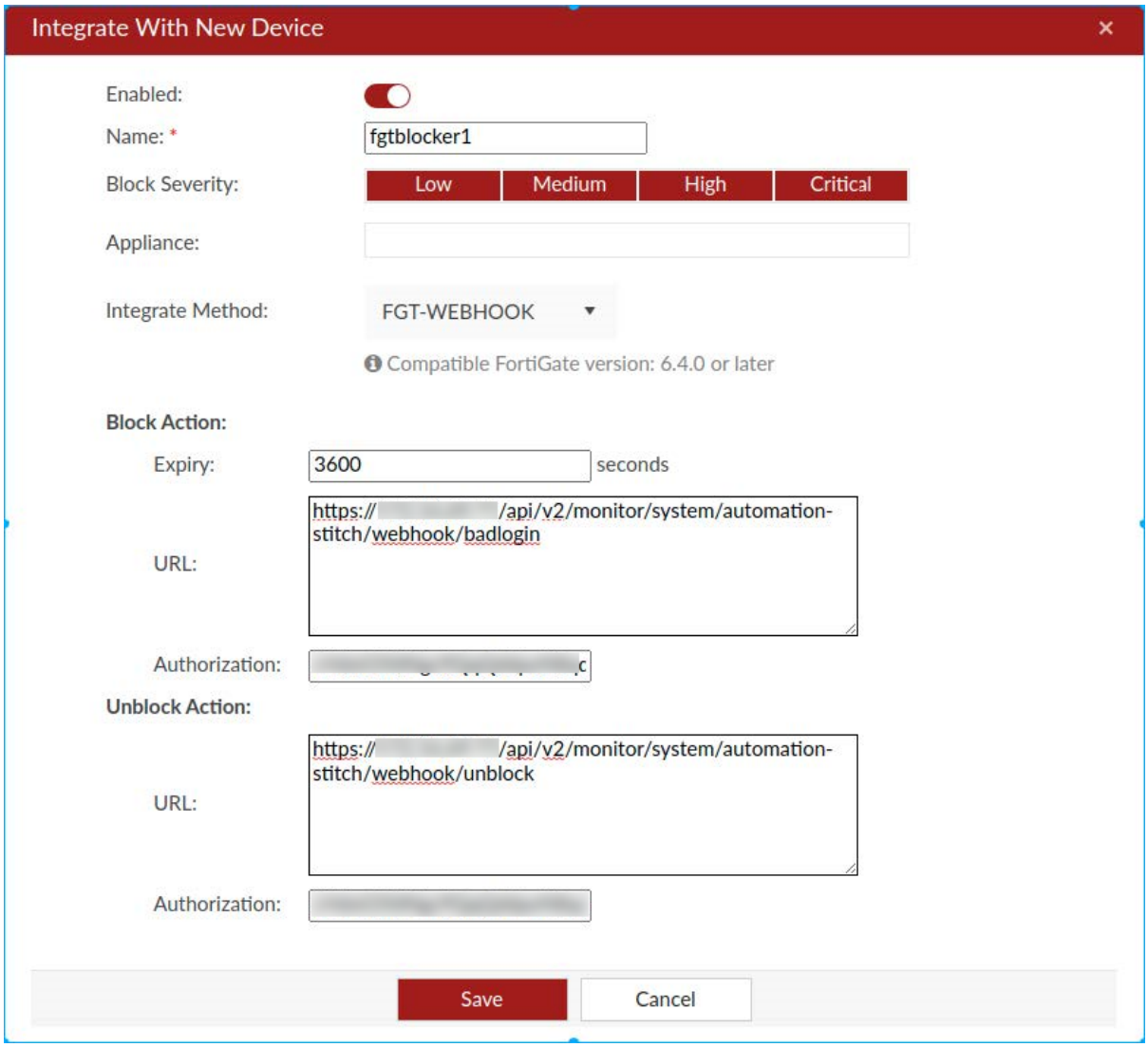
11. Click *Add Action*. From the *Add Entries* pane, select the Action you created (`fdc_unblock_ip`) and click *Apply*.



4. Configure FortiDeceptor to integrate with FortiGate over Webhook

1. In FortiDeceptor, go to *Fabric* > *Quarantine Integration* and click *Quarantine Integration With New Device*.
2. Configure the integration settings and click *Save*.

Integrate Method	Select *FGT-WEBHOOK*.
Block Action	
URL	Enter the webhook URL from FortiGate.
Authorization	Enter the API key from FortiGate.
Unblock Action	
URL	Enter the webhook URL from FortiGate.
Authorization	Enter the API key from FortiGate.



3. Ensure the integration *Status* is *Ready*.

Integrate with FortiGate 6.0.3 to 7.2.3 over REST-API

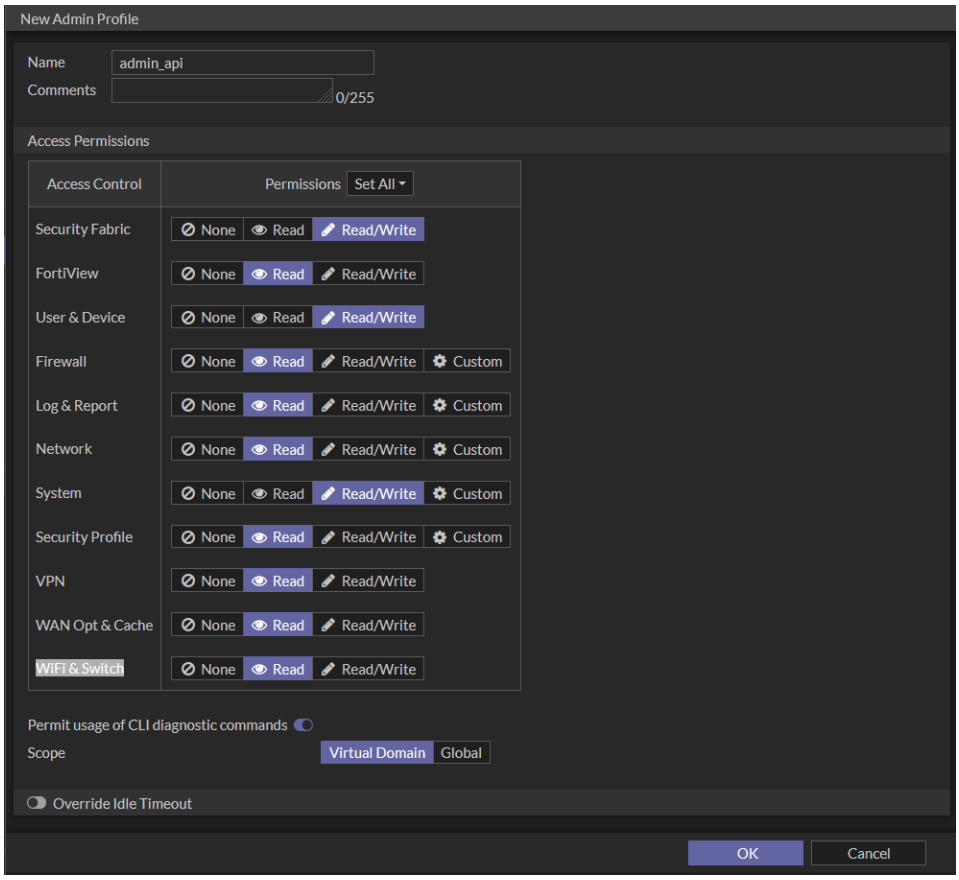
The following instructions are based on FortiGate 6.0.3 to 7.2.3 and FortiDeceptor 4.3.0. For information about the versions of FortiGate and FortiDeceptor you are using, select the version in the Fortinet Document Library.

1. Configure FortiGate

1.1 Configure a new profile with minimum permissions for REST API integration

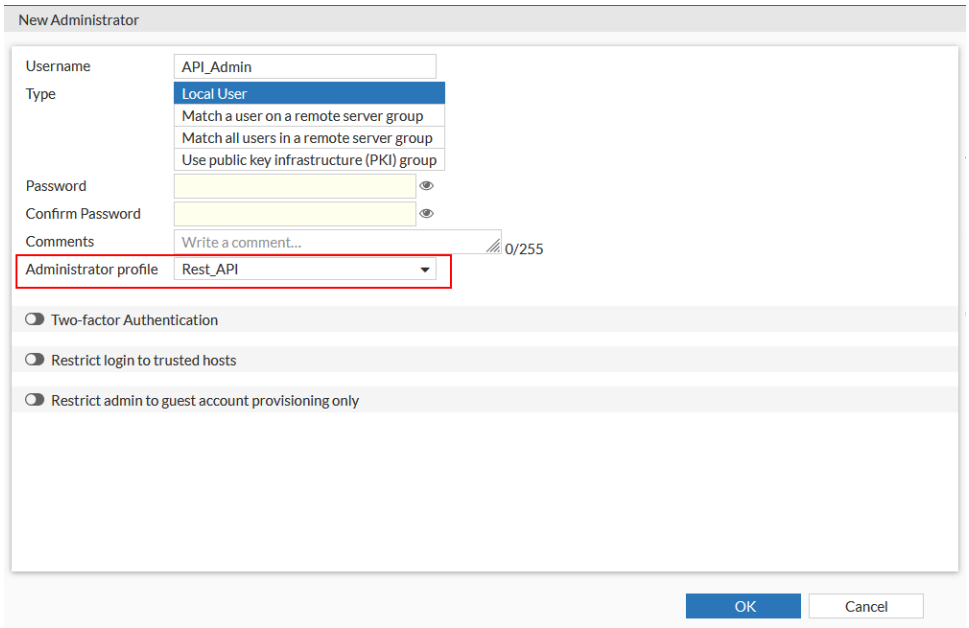
1. On FortiGate, go to *System* > *Admin Profiles* and click *Create New*.
2. Configure the profile *Access Permissions*. The following are the minimum required permissions.

Access Control	Permissions
Security Fabric	Read/Write
FortiView	Read
User & Device	Read/Write
Firewall	Read
Log & Report	Read
Network	Read
System	Read/Write
Security Profile	Read
VPN	Read
WAN Opt & Cache	Read
WiFi & Switch	Read



1.2 Create a new administrator

1. On FortiGate, go to *System* > *Administrators*.
2. Click *Create New* > *Administrator*.
3. Enter a *Username* and *Password* for the administrator.
4. From the *Administrator profile* dropdown, select the profile you created in step 1.1 Create the administrator profile in FortiGate.

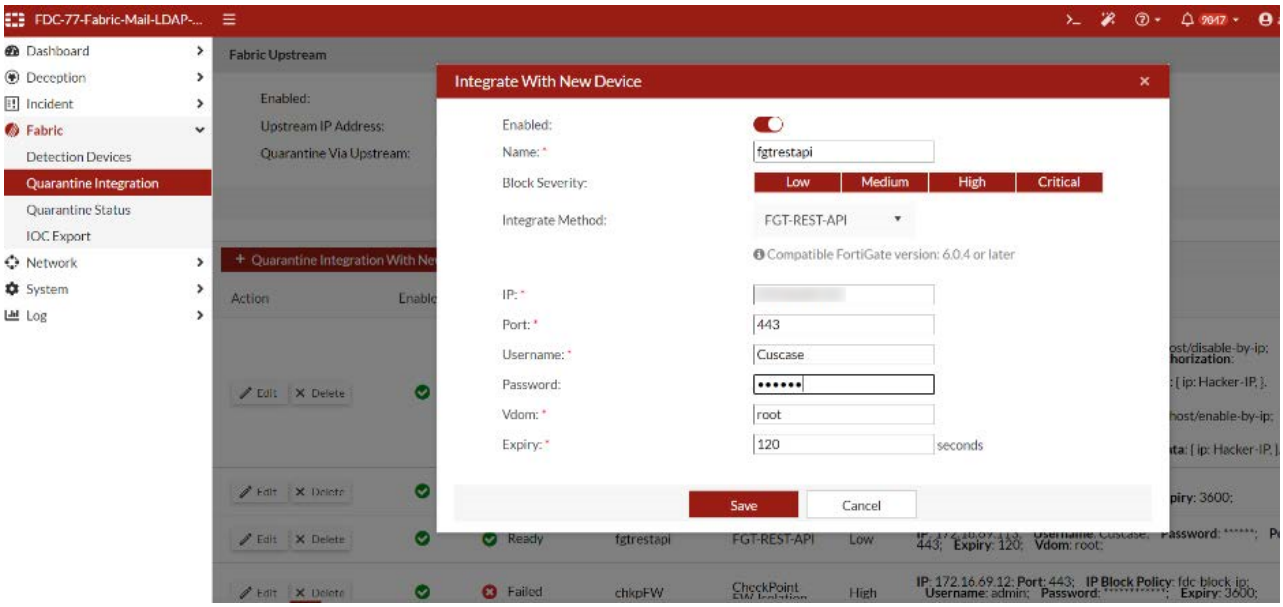


5. Click *OK*.

2. Configure FortiDeceptor to integrate with FortiGate

1. In FortiDeceptor, go to *Fabric* > *Quarantine Integration* and click *Quarantine Integration With New Device*.
2. Configure the integration settings and click *OK*.

Enabled	Enable the integration.
Name	Enter a name for the integration.
Integrate Method	Select *FGT-REST-API*.
IP	Enter the IP address of the FortiGate.
Port	Enter the Port for the FortiGate.
Username	Enter the username for the admin you just created.
Password	Enter the password for the admin you just created.
Vdom	Enter the VDOM the FortiGate belongs to.



3. Verify the integration *Status* is *Ready*.

3. Test the integration

1. Send an attack against a decoy.
2. On FortiDeceptor, check the quarantine status.
3. On FortiGate, go to *Dashboard* > *Users Device* and expand the *Quarantine* widget to check quarantine status.
4. (Optional) Check the quarantine status on FortiDeceptor after it has expired.
   - On FortiDeceptor, go to *Fabric* > *Quarantine Status* to check the status.
5. (Optional) Check the quarantine status on FortiGate after it has expired.
   - On FortiGate, go to *Dashboard* > *Users Device* and expand the *Quarantine* widget to check quarantine status.

Integrate FortiDeceptor with FortiGate over Fabric v7.2.4

This topic describes how to integrate FortiDeceptor with FortiGate over Fabric in FortiOS versions 7.2.4 .

FortiGate 7.2.1 has a bug which prevents adding and displaying the FortiDeceptor information widgets in the dashboard.

Integrate FortiDeceptor with FortiGate over Fabric:

1. Configure the Fabric Connector on FortiGate.
2. Configure the upstream FortiDeceptor.

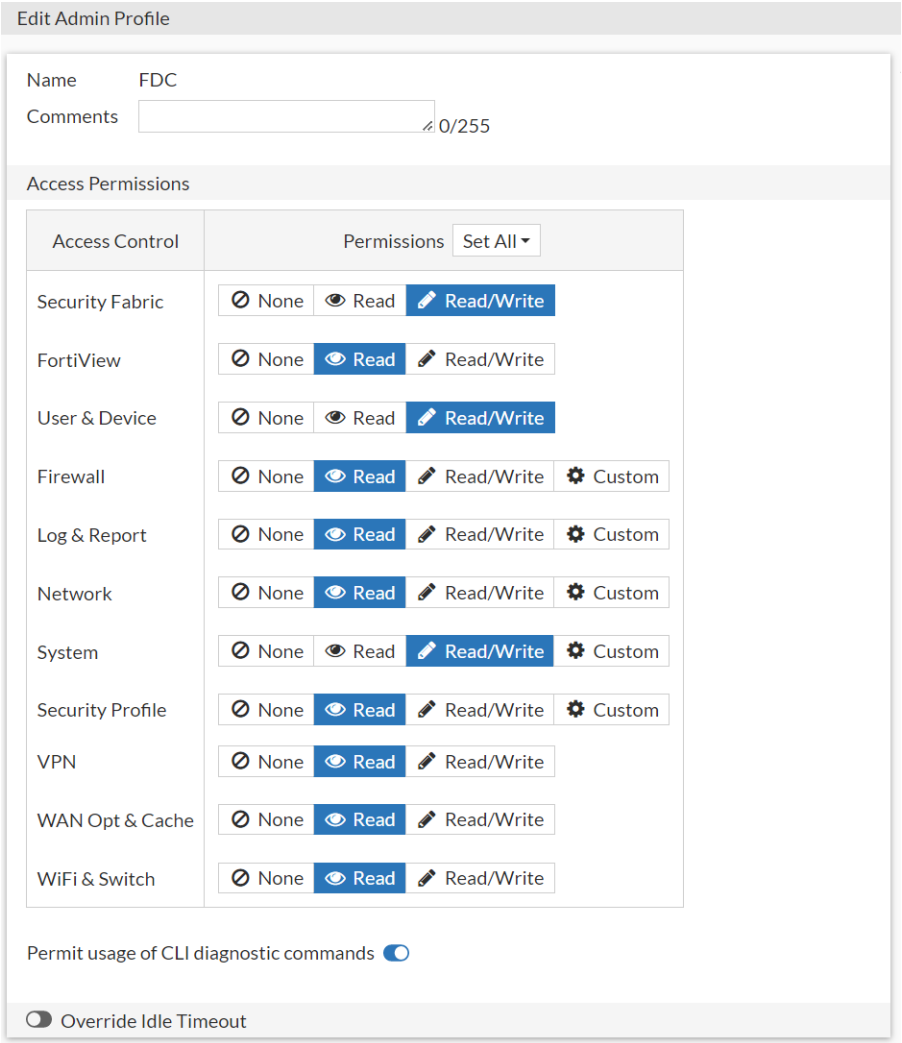
3. Authorize FortiDeceptor on FortiGate.
4. Configure the automation on FortiGate.
5. Create a stitch for manual block on FortiGate.
6. Create a stitch for manual unblock.
7. Check the quarantine status in FortiDeceptor.
8. Check quarantine status on FortiGate.

1. Configure the Fabric Connector on FortiGate

1.1 Create the administrator profile in FortiGate

1. In FortiGate, go to *System* > *Admin Profiles*.
2. Select *prof_admin* or *super_admin* and click *Create New*. The *New Admin Profile* page opens.
3. Configure the profile *Access Permissions*. The following are the minimum required permissions.

Access Control	Permissions
Security Fabric	Read/Write
FortiView	Read
User & Device	Read/Write
Firewall	Read
Log & Report	Read
Network	Read
System	Read/Write
Security Profile	Read
VPN	Read
WAN Opt & Cache	Read
WiFi & Switch	Read



4. Click *OK*.

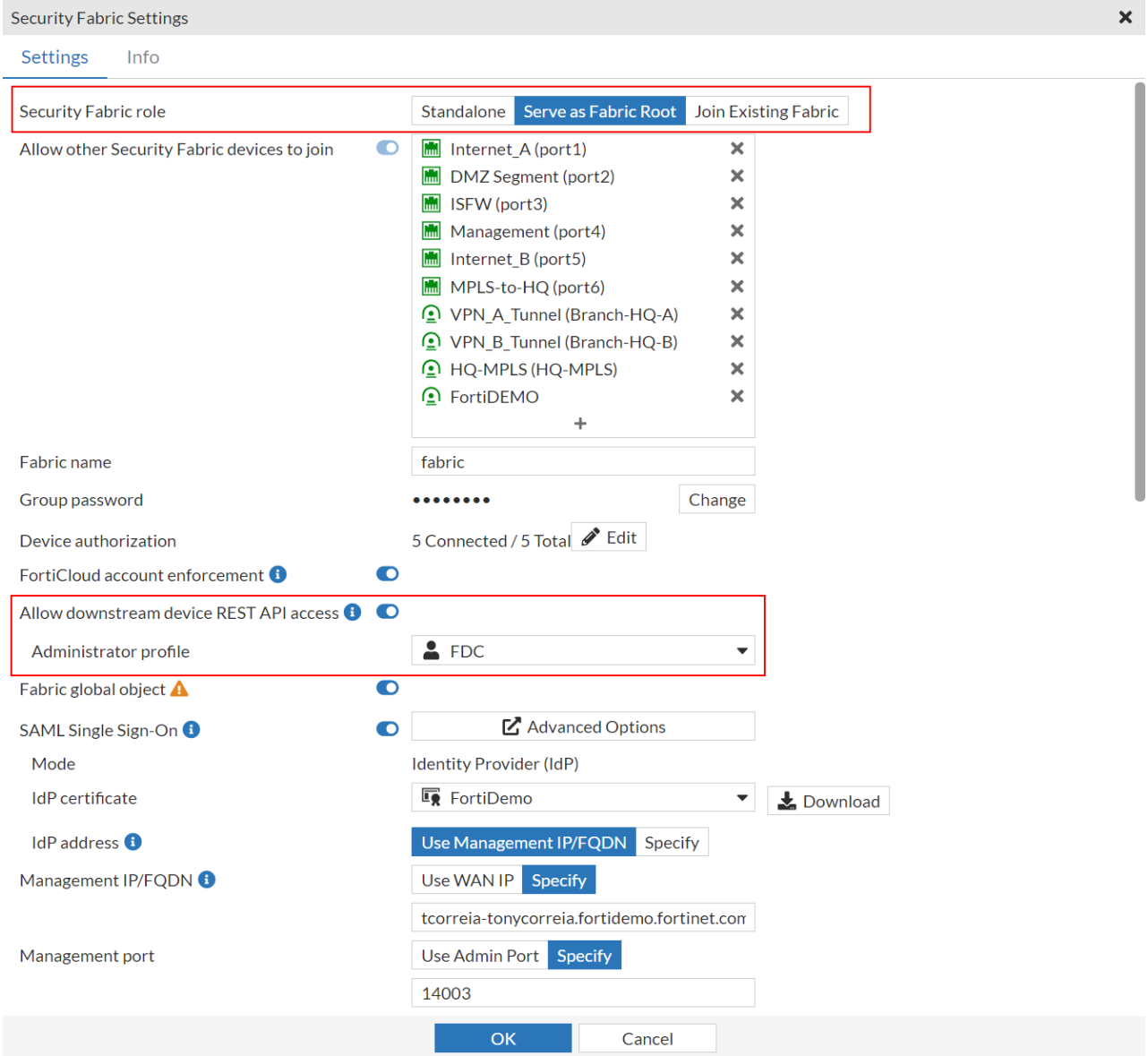
1.2 Configure the Fabric Connector using the FortiGate profile

Enable the Security Fabric. For more information, see Configuring the root FortiGate and downstream FortiGates.

1. Go to *Security Fabric* > *Fabric Connectors*.
2. Click the *Security Fabric Setup* tile and click *Edit*. The *Security Fabric Settings* window opens.

3. Configure the following settings and click *OK*.

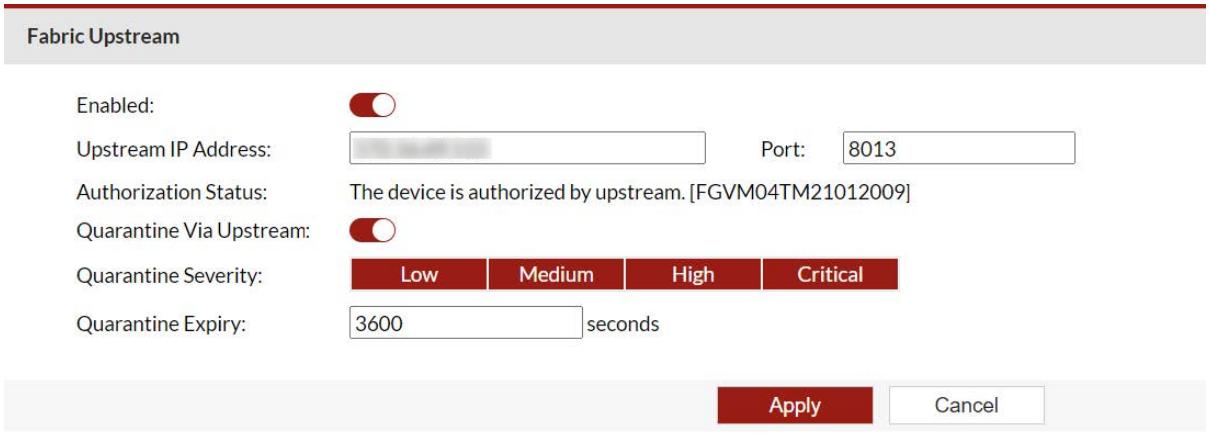
Security Fabric role	Select *Serve as Fabric Root*.
Allow downstream device REST API access	Enable. Enabling *Allow downstream device REST API access* is mandatory.
Administrator profile	Select the profile you create in Step 1.1 Create the administrator profile in FortiGate.



2. Configure the upstream FortiDeceptor

1. In FortiDeceptor, go to *Fabric* > *Quarantine Integration*.
2. Configure the *Fabric Upstream* settings and click *Apply*.

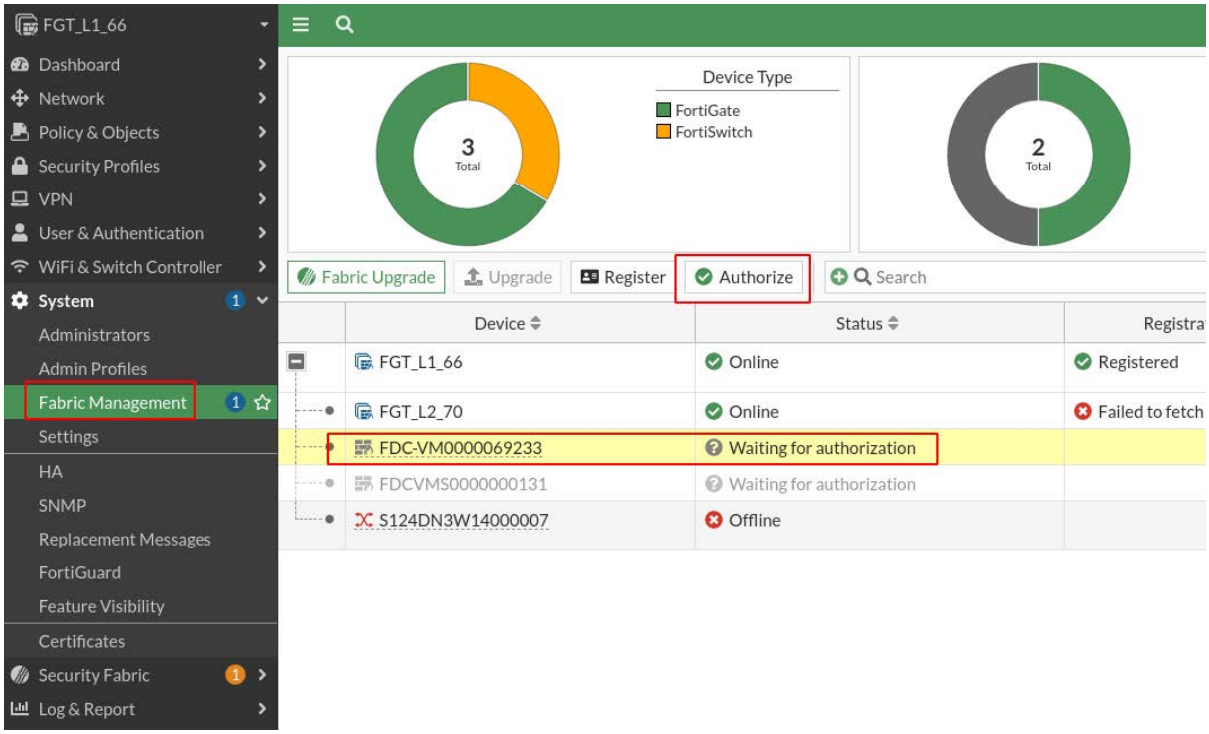
Enabled	Enable.
Upstream IP address	Enter the IP of the upstream FortiGate
Quarantine Via Upstream	Enable.



3. Authorize FortiDeceptor on FortiGate

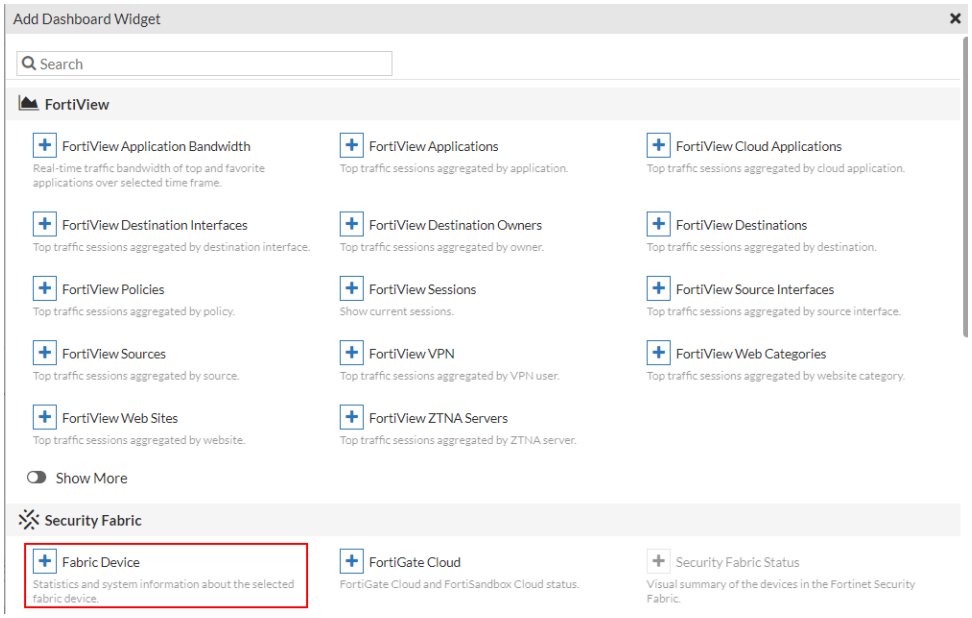
3.1 Update the device status

1. Go to *System* > *Fabric Management*.
2. Select the FortiDeceptor with a status of *Waiting for authorization* and click "*Authorize*.

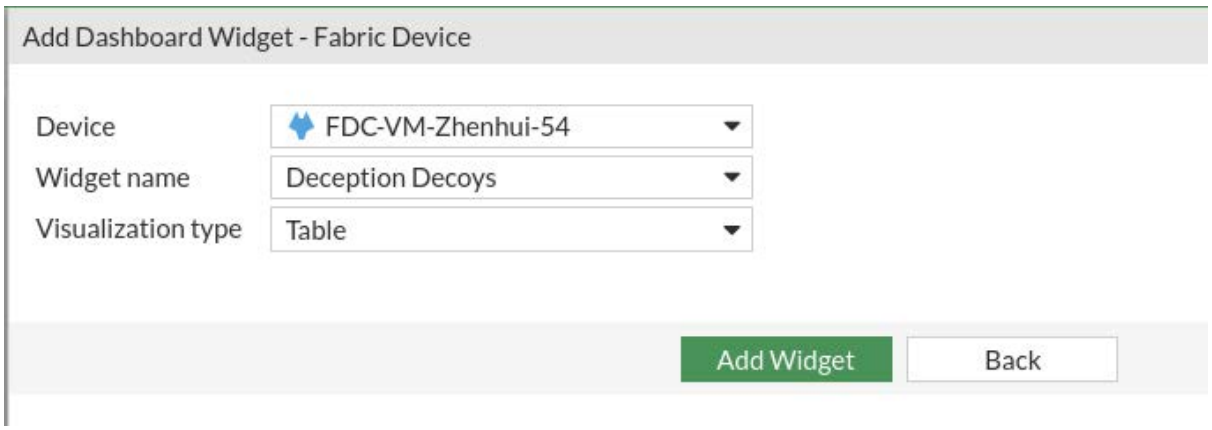


3.2 Add the fabric device widget in FortiGate Dashboard

1. Go to *Dashboard* > *Status* and click *Add Widget*. The *Add Dashboard Widget* menu opens.
2. Under *Security Fabric*, click *Fabric Device*.



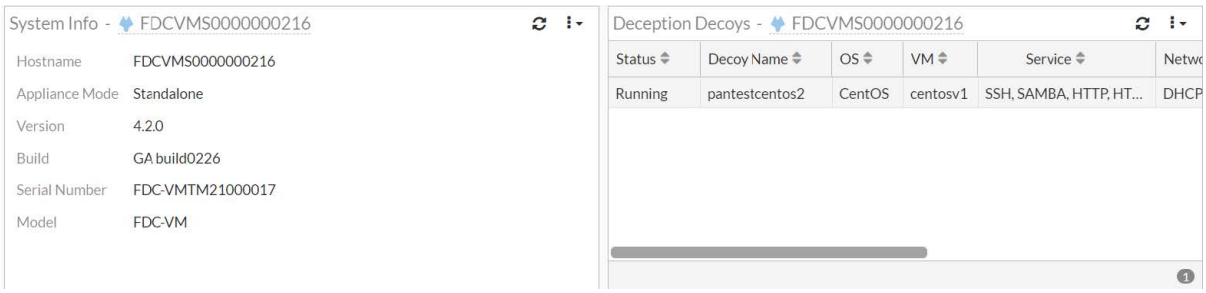
3. From the *Device* dropdown, select the FortiDeceptor.



4. Configure the other settings and click *Add Widget*.

3.3 Monitor the FortiDeceptor widgets on FortiGate

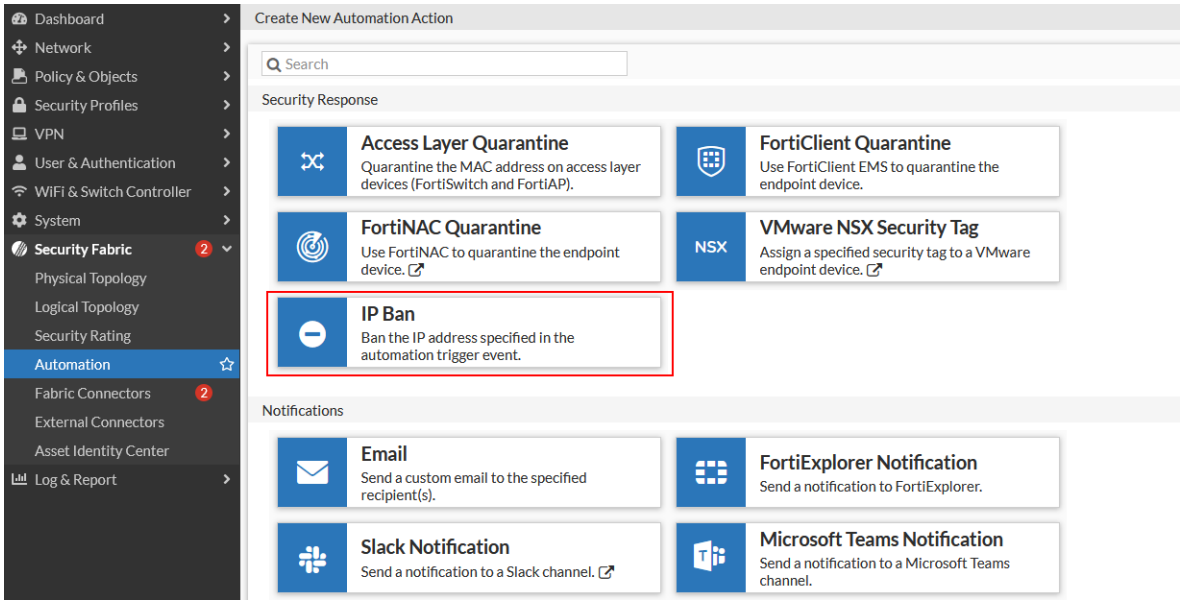
Use the FortiDeceptor Fabric Device widget to monitor FortiDeceptor System Information and Deception Decoys information.



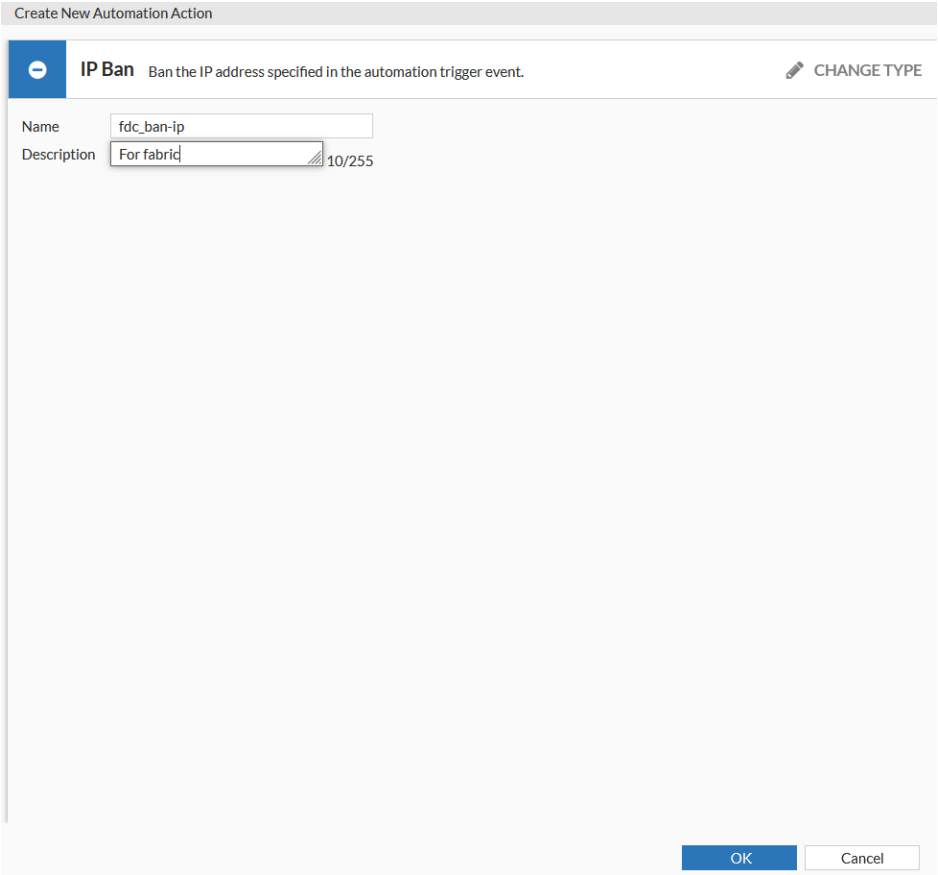
4. Configure the automation on FortiGate

4.1 Create Stitch for automated quarantine on FortiGate side

1. Go to *Security Fabric >Automation*.
2. In the banner click *Action*.
3. Click *Create New* and then click *IP Ban*. The *Create New Automation Action* page opens.



4. Enter a descriptive name *Name* such as `fdc_ban-ip` and a *Description* such as `For fabric` and click *OK*.

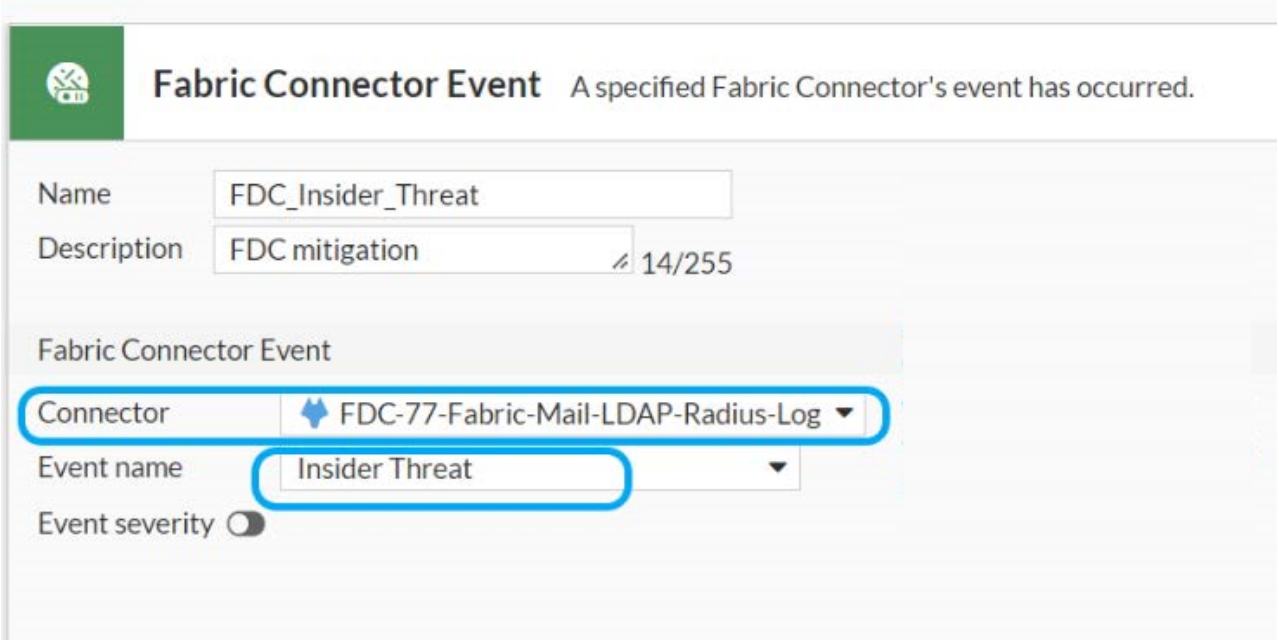


4.2. Create a trigger for automated quarantine

1. In FortiGate go to *Fabric* > *Automation*.
2. In the banner, click *Trigger*.
3. Click *Create New* and then click the *Fabric Connector Event* tile.

4. Configure the following settings, and click *OK*.

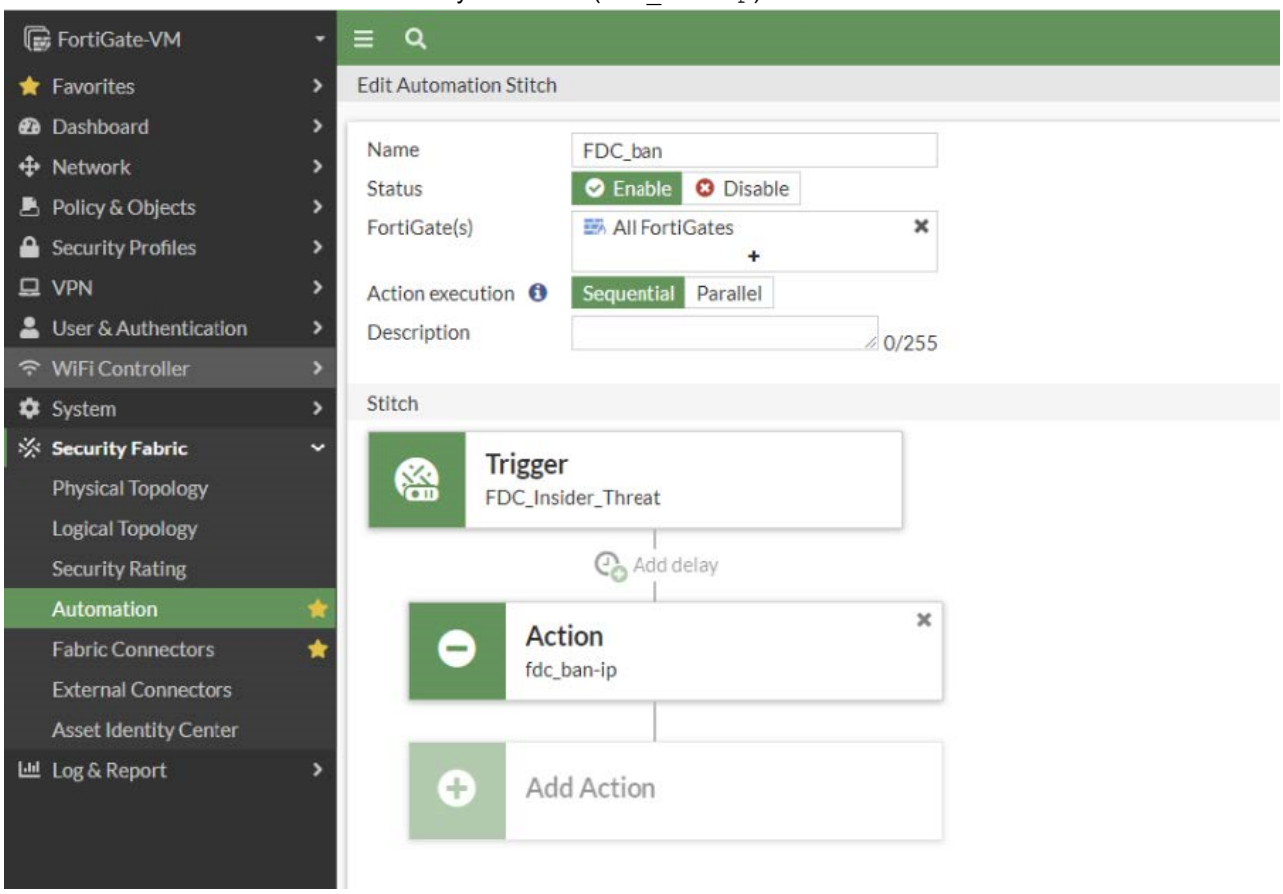
Name	Give the connector a descriptive name such as `FDC_Insider_Threat`.
Description	Enter a description such as `FDC mitigation`.
Connector	Select the upstream FortiDeceptor device.
Event name	Select *Insider Threat*.



4.3 Create a stitch for automated quarantine

1. In FortiGate go to *Security Fabric* > *Automation*.
2. In the banner, click *Stitch* and then click *Create New*.
3. Give the Stitch a descriptive name such as `FDC_ban`.
4. Click the *Trigger* tile and select the trigger you created in Step 4.2. Create Trigger for automated quarantine (`FDC_Insider_Threat`).

5. Click the *Action* tile and select the Action you created (`fdc_ban-ip`).

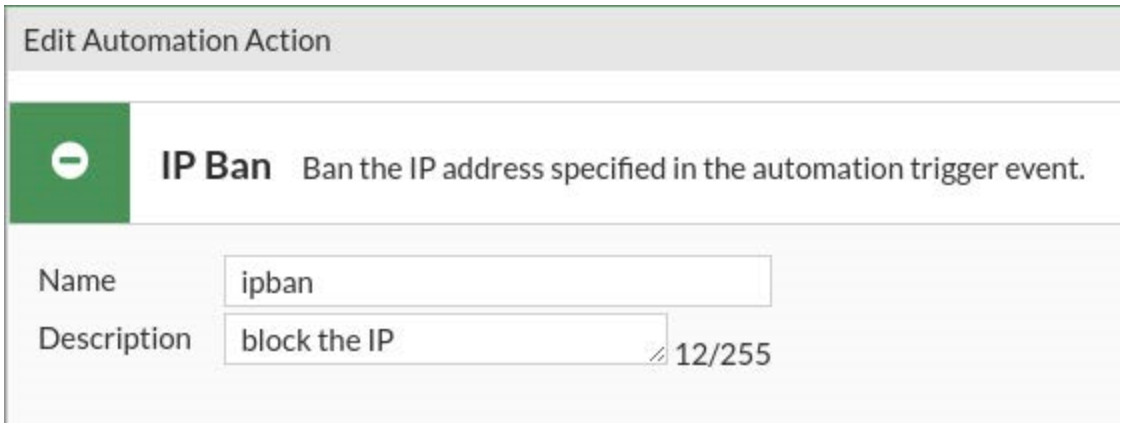


5. Create a stitch for manual block on FortiGate

5.1 Create an Action for manual block

1. In FortiGate go to *Security Fabric* > *Automation*.
2. In the banner, click *Action*.
3. Click *Create New* and then click the *IP Ban* tile.

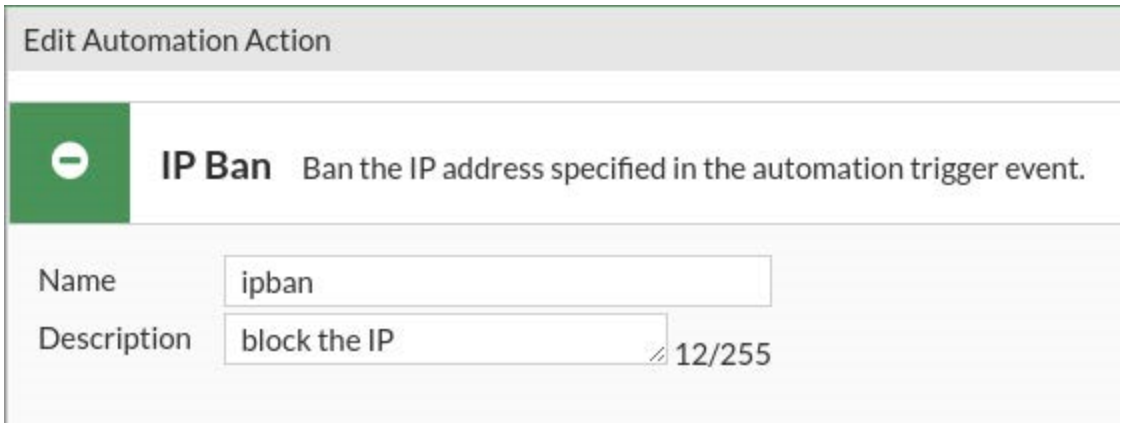
4. Give the Action a descriptive *Name* such as `ipban` and enter a *Description* such as `block the IP` and click *OK*.



5.2 Create a trigger for manual block

1. In FortiGate, go to *Security Fabric* > *Automation*.
2. In the banner, click *Trigger*;
3. Click *Create New* and then click the *Fabric Connector Event* tile.
4. Configure the following settings and click *OK*.

Name	Enter a descriptive name such as `manual-ban`.
Connector	Select the downstream FortiDeceptor device.
Event Name	Select *Notify Ban*.



5.3 Create a stitch for manual block

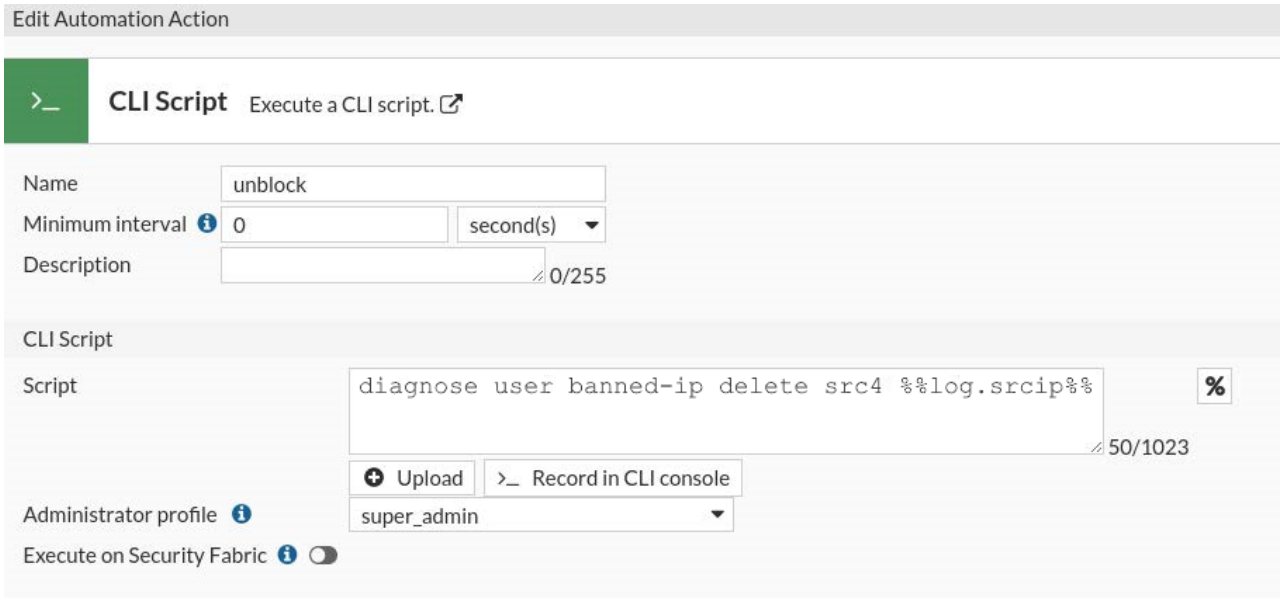
1. Go to *Security Fabric* > *Automation*.
2. In the banner, click *Stitch*, and then click *Create New*.
3. Give the *Stitch* a descriptive name such as `FDC_Manual_Block`.
4. Click the *Trigger* tile and select the trigger you created in 5.2 Create Trigger for manual block (`manual-ban`).
5. Click the *Action* tile and select the Action you created in Step 5.1 Create Action for manual block (`ipban`)

6. Create a stitch for manual unblock

6.1 Create an Action for manual unblock

1. In FortiGate go to *Security Fabric* > *Automation*.
2. In the banner, click *Action*.
3. Click *Create New* and then scroll down and click the *CLI Script* tile.
4. Give the action an descriptive *Name* such as `unblock`.
5. In the *CLI Script* > *Script* field enter the following command and click *OK*.

```
diagnose user banned-ip delete src4 %%log.srcip%%
```



6.2 Create a trigger for manual unblock

1. In FortiGate, go to *Security Fabric* > *Automation*.
2. In the banner, click *Trigger*
3. Click *Create New*, then configure the following settings and click *OK*.

Name	Give the trigger a descriptive name such as `Trigger-unban`.
Connector	Select the downstream FortiDeceptor device.
Event name	Select *Notify Unban*.

6.3 Create a stitch for manual unblock

1. Go to *Security Fabric* > *Automation*.
2. In the banner, click *Stitch*, and then click *Create New*.
3. Give the *Stitch* a descriptive name such as `FDC_Manual_Unblock`.
4. Click the *Trigger* tile and select the trigger you created in 6.2 Create Trigger for manual unblock (`unblock`) .

5. Click the *Action* tile and select the Action you created in Step 6.1 Create Action for manual unblock (`Trigger-ban`).

7. Check the quarantine status in FortiDeceptor

1. In FortiDeceptor, go to *Fabric* > *Quarantine Status*.
2. For *Type* > *Auto quarantine*, verify the *Status* is *Quarantined*.
3. (Optional) Trigger a manual block.
   a. Select a device with *Type* > *Manual quarantine*.
   b. In the toolbar, click *Block*.

8. Check quarantine status on FortiGate

To view the quarantine status with the FortiGate GUI:

Go to *Dashboard* > *Users & Devices* and expand the *Quarantine* widget.

To view quarantine status with FortiGate CLI:

Run the following command:

```
diagnose user quarantine list
```

To view the debug log for quarantine with the FortiGate CLI:

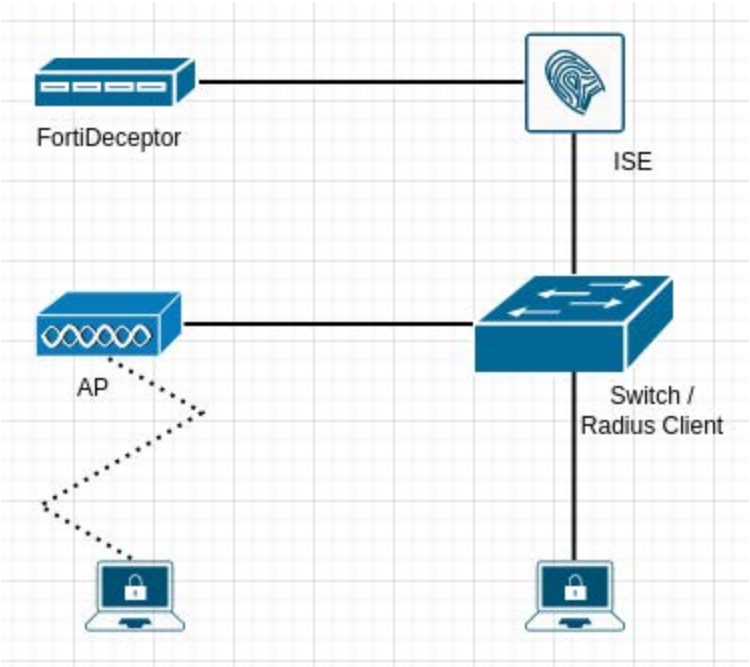
Run the following command:

```
diagnose debug en
```

Integrate with Cisco ISE

Topology

This topic assumes Cisco ISE has been set up properly as a NAC solution, to work with a switch which has CoA enabled.



To integrate FortiDeceptor with Cisco ISE:

1. Configure Cisco ISE.
2. Configure the Authorization Policy.
3. Check the configuration
4. Configure FortiDeceptor.
5. Quarantine the endpoint.
6. Un-quarantine the endpoint.

1. Configure Cisco ISE

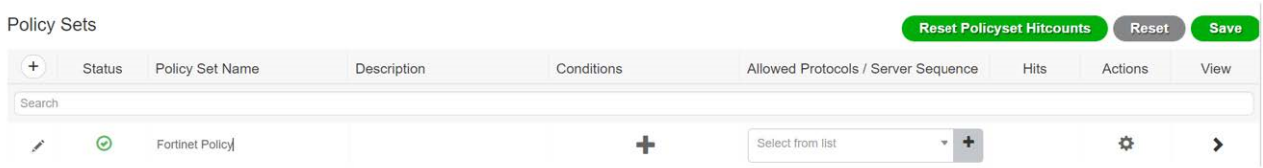
1.1 Configure the ERS on Cisco ISE

Please refer to the Cisco developer documentation on how to enable the ERS interface and configure the ERS admin account on Cisco ISE. This ERS admin account must be enabled with REST API and will be used by FortiDeceptor to communicate with Cisco ISE to quarantine and un-quarantine the attackers by IP.

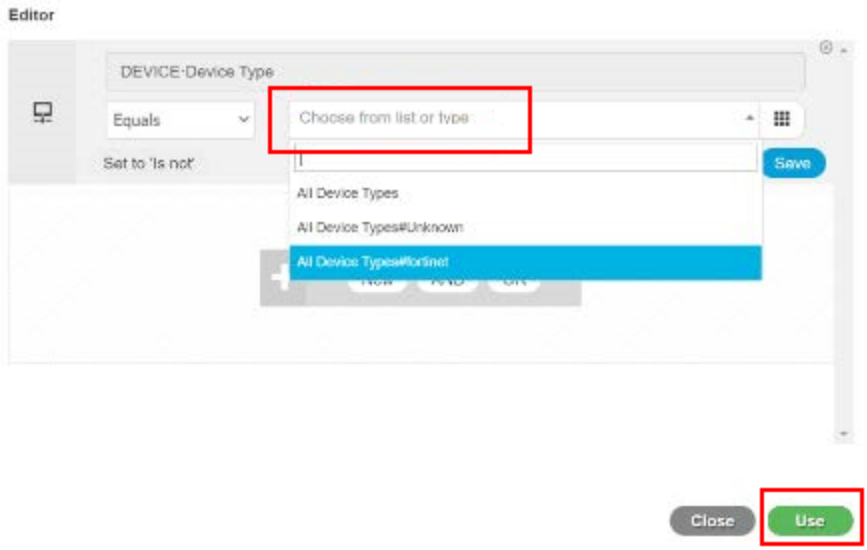
1.2 Create a new policy in Cisco ISE

1. In Cisco ISE, go to *Policy* > *Policy Sets*.
2. Click the **+** button, and type a name in the *Policy Set Name* field such as `Fortinet Policy`.

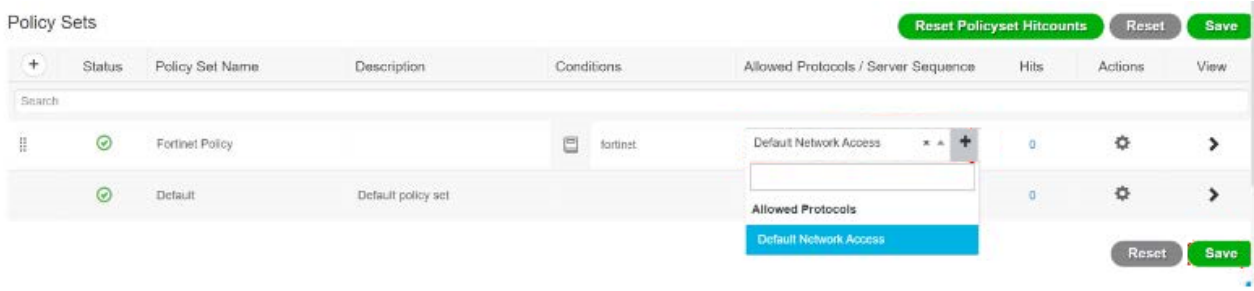
3. In the *Conditions* column, click **+**.



4. In *Conditions Studio*, click *Click to add an attribute*.
5. In the *Editor* pop-up window, type `device type`.
6. In the *Attribute* box, click *Choose from list or type* and select *All Device Types*.
7. Click *Use*.

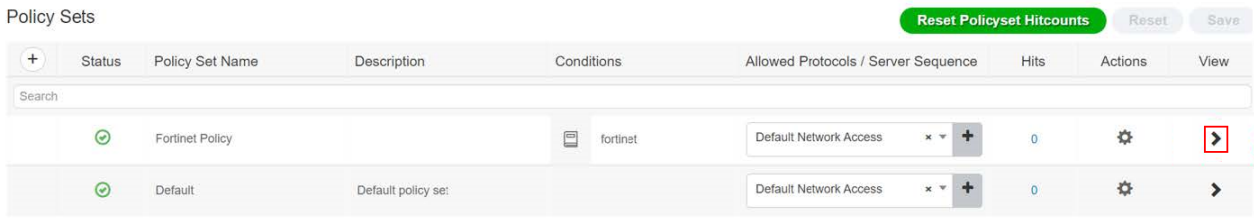


The new policy will look like the image below.

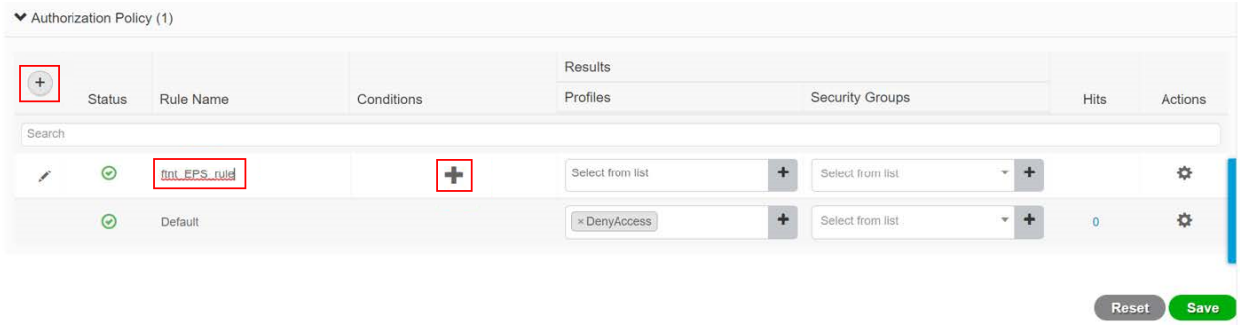


2. Configure the Authorization Policy

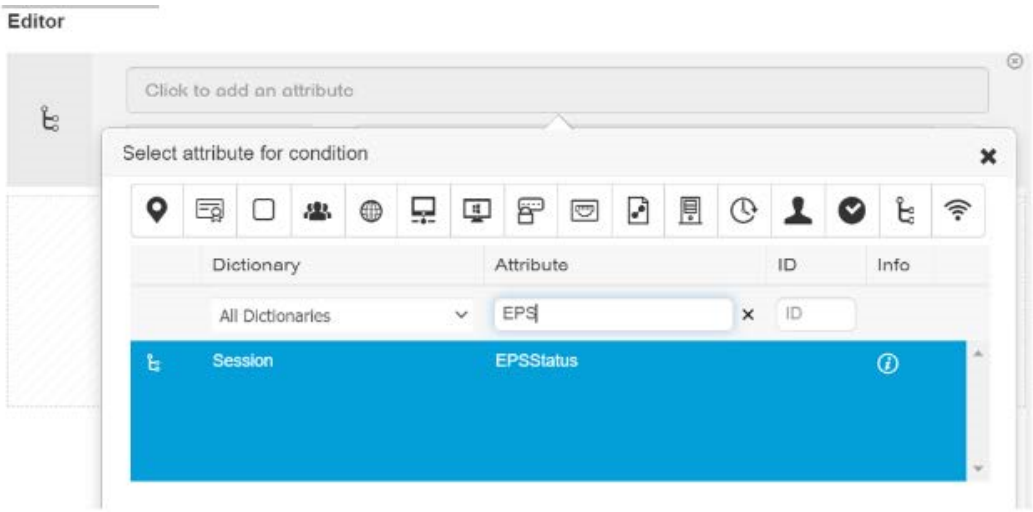
1. In the *View* column, click on the arrow **>**.



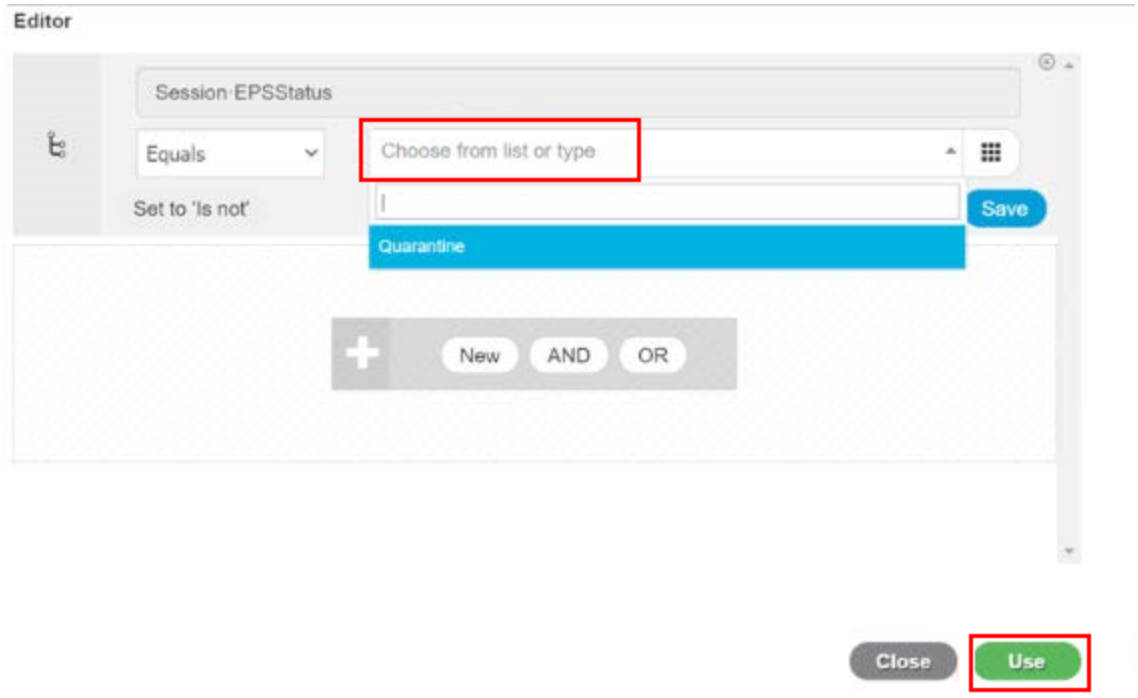
2. Click **+** to the left side of the *Status* column. A new authorization is generated.
3. In the *Rule Name* column, enter a name such as `ftnt_EPS_rule`.



4. In the *Conditions* column, click **+**.
5. In *Conditions Studio*, in the *Editor*, click *Click to add an attribute*.
6. in the *Attribute* box, type `EPS` and select *EPSStatus*.



7. Click *Choose from list or type* and select *Quarantine* from the dropdown list.

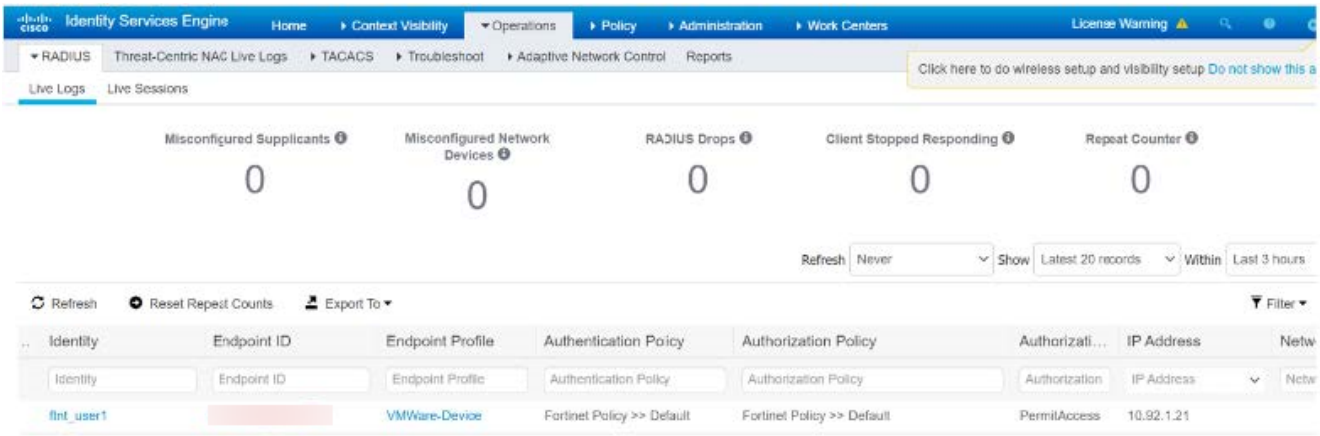


8. Click *Use*.

3 Check the configuration

If each network component is configured properly, the endpoint will be authenticated successfully. In Windows 10, use the Command Prompt of Windows 10, to verify the IP address is acquired and the DHCP server is pingable.

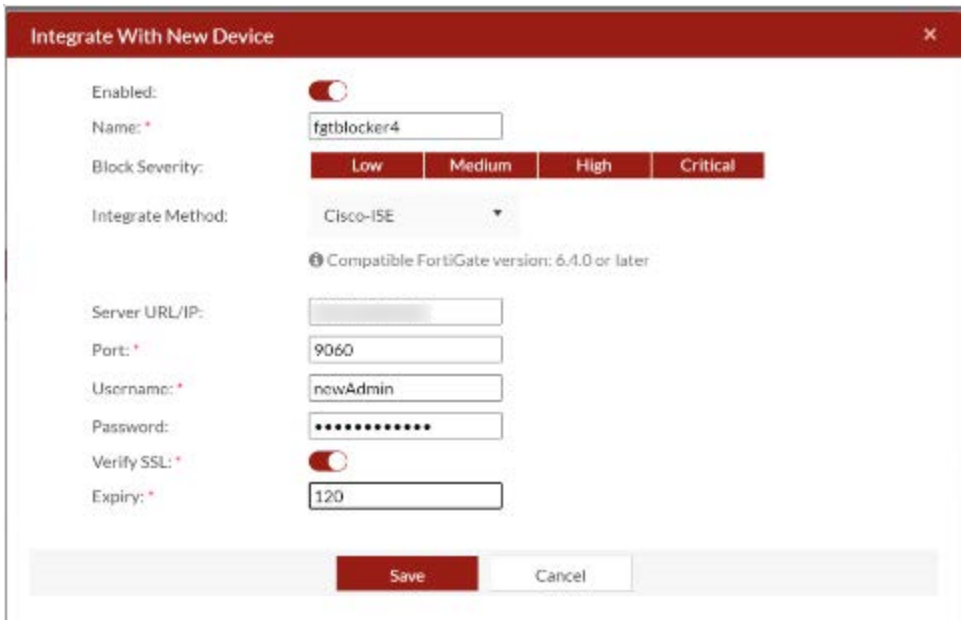
In Cisco ISE go to *Operations* > *RADIUS* > *Live Logs*. The endpoint should be displayed.



4. Configure FortiDeceptor

1. In FortiDeceptor, go to *Fabric* > *Quarantine Integration* and click *Quarantine Integration With New Device*.
2. Configure the integration settings and click *Save*.

Enabled	Enable
Name	Enter a descriptive name for the integrations.
Integrate Method	Select *Cisco-ISE*.
ServerURL/IP	Enter the IP address for Cisco ISE.
Username	Enter the username for Cisco ISE.
Password	Enter the password for Cisco ISE.
Expiry	Set the expiry in seconds.



3. Verify the *Status* is *Ready*.

5. Quarantine the endpoint

1. Attack a decoy deployed in FortiDeceptor from the endpoint. When FortiDeceptor detects the attack has occurred, a quarantine of REST API with the IP address of the endpoint will be sent to Cisco ISE.
2. In FortiDeceptor go to *Fabric* > *Quarantine Status*, to verify the quarantine was successful.

	Attacker IP	Start	End	Type	Integrated ...	Time Rema...	Status
	10.92.1.21	2021-11-02 18:0...	2021-11-02 18:13:17 PDT	Auto quarantine	fgtblocker2	1m 2s	Quarantined

3. On the endpoint, you should see the status of the network adapter becomes *Authentication failed* and DHCP server is no longer pingable.
4. In Cisco ISE, navigate to the *Live Logs*.
   - In the *Authorization Profiles* column, you should see *PermitAccess* is replaced by *DenyAccess*.
   - In the Authorization Policy column *Fortinet Policy >> Default* changes to *Fortinet Policy >> ftnt_EPS_quarantine*.

Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati...	IP Address
Identity	Endpoint ID	Endpoint Profi	Authentication Policy	Authorization Policy	Authorization	IP Address
ftnt_user1	00:0C:29:C7:73:D5	VMWare-De...	Fortinet Policy >> Default	Fortinet Policy >> ftnt_EPS_quarantine	DenyAccess	

6. Un-quarantine the endpoint

After 120 seconds, un-quarantine of REST API is sent to Cisco ISE from FortiDeceptor. At the same time, *Status* of *Quarantine Status* changes to *Quarantine stopped*.

Attacker IP	Start	End	Type	Integrated ...	Time Rema...	Status
10.92.1.21	2021-11-02 18:...	2021-11-02 18:13:17 PDT	Auto quarantine	fgtblocke...	0	Quarantine stopped

On the endpoint, the status of the network adapter is *Resumed* and the DHCP server becomes pingable.

In Cisco ISE go to *Live Logs*:

- In the *Authorization Profiles* column, *DenyAccess* changes to *PermitAccess*.
- In the *Authorization Policy* column *Fortinet Policy >> ftnt_EPS_quarantine* changes to *Fortinet Policy >> Default*.
-

Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
Identity	Endpoint ID	Endpoint Profi	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
ftnt_user1	00:0C:29:C7:73:D5	VMWare-De...	Fortinet Policy >> Default	Fortinet Policy >> Default	PermitAccess	10.92.1.21

Integrate Windows IR collector

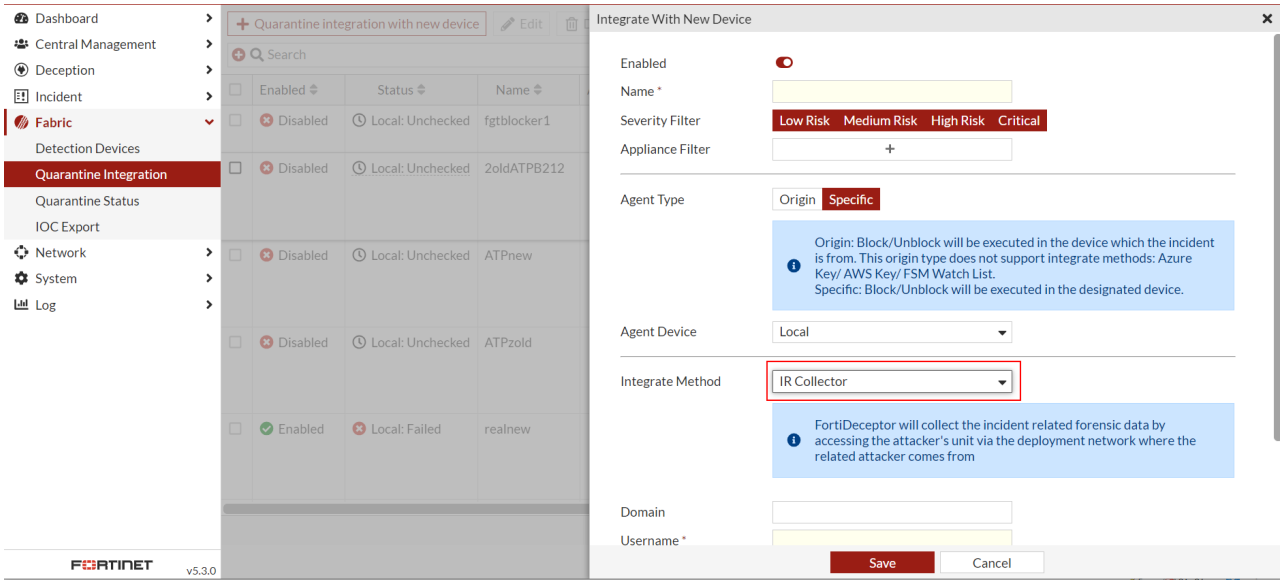
The IR Collector integration allows admins with local and domain permissions to connect to Windows endpoints remotely, copy IR tools, run commands on the endpoint and collect digital artifacts for future analysis. After the IR Collector is configured, it will collect incident related forensic data by accessing the attacker's unit via the deployment network where the attack originated from.

To configure the IR Collector:

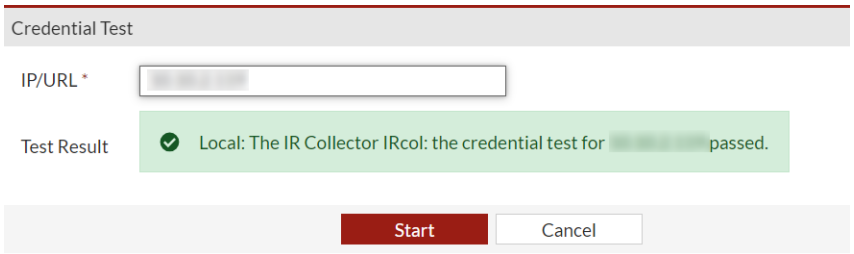
1. Go to *Fabric* > *Quarantine Integration* and click *Quarantine integration with new device*. The *Integrate With New Device* pane opens.

2. From the *Integrate method* dropdown, select *IR collector* and configure the integration settings as required.

> The *Username* should be a user who is either a local admin or a domain user with administrative privileges to access the endpoints.



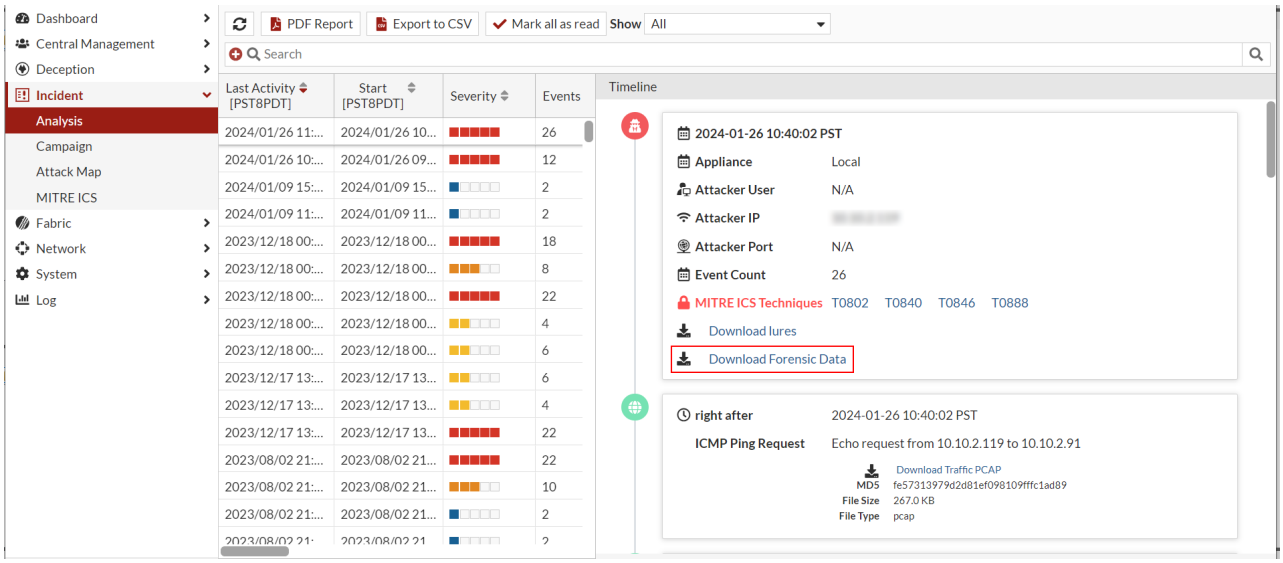
3. Click *Save*.
4. Configure the Windows endpoint. Both IR and Windows network isolation in the Fabric require the same setting for the endpoints. For information, see Mitigation using windows Remote Command on page 262.
5. After you configuring FortiDeceptor and the Windows endpoint, perform a connection check.
   a. Go to *Fabric* > *Quarantine Integration*
   b. Select the IR Collector integration and click *Credential Test*.



To download the artifacts:

1. Go to *Incident* > *Analysis*.
2. Click an incident in the table.

3. Click *Download Forensic Data*. The artifacts are saved as a Zip file.



Artifacts list

Extracted from the file system:

- IE/Firefox/Chrome History
- Named Pipes
- Prefetch Startup
- Directories
- etc.

Extracted from the registry:

- Installer Folders
- Recent Docs
- Services
- UserAssists
- Networks List

Extracted from in-memory processes:

- Opened Files

Other information:

- Drives List Network
- Drives Network Cards
- Processes
- Routing Table
- Sessions
- Sockets

Artifacts labeled *etc* are files that contain more information.

www.fortinet.com

Copyright© 2025 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 General Counsel, 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.