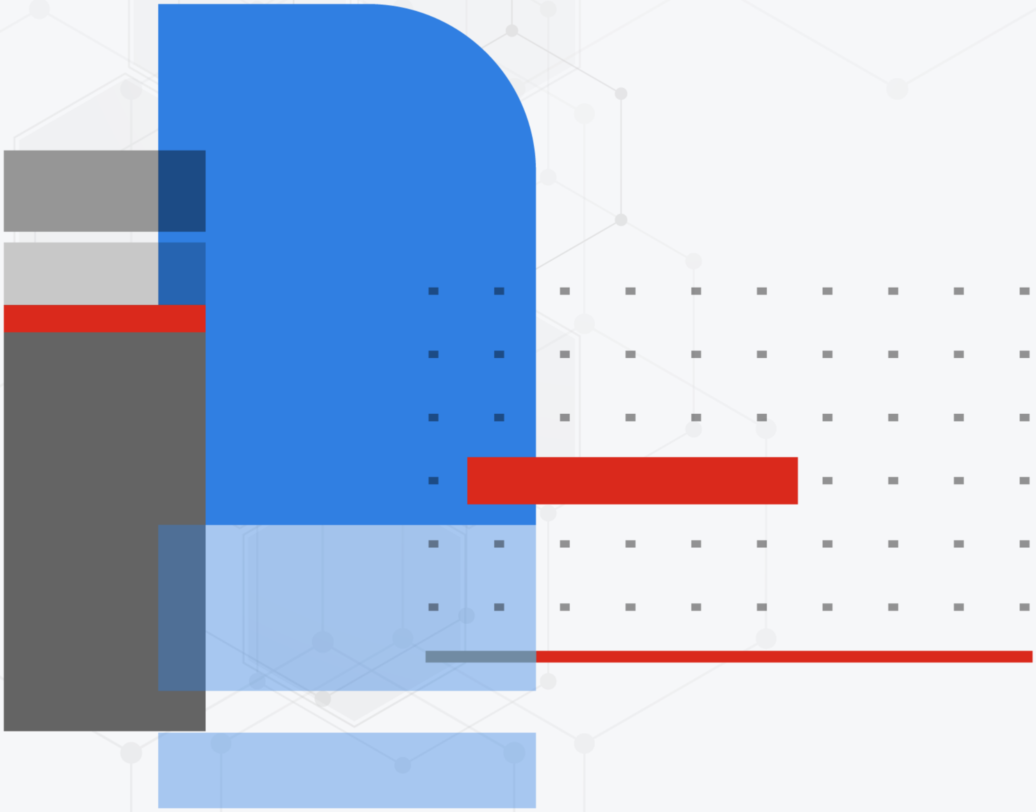
FORTINET

Release Notes

FortiDeceptor 6.2.0



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

October 07, 2025
FortiDeceptor 6.2.0 Release Notes
50-620-1207486-202510DD

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-10-03	Initial release.

FortiDeceptor 6.2.0 release

This document provides information about FortiDeceptor version 6.2.0 build 0058.

Supported models

FortiDeceptor version 6.2.0 supports the following models:

FortiDeceptor	FDC-100G, FDR-100G, FDC-1000G,
FortiDeceptor VM	FDC-VM (VMware ESXi, KVM, Hyper-V, AWS, GCP, and Azure), FDCVME (Fortideceptor Edge)
FortiDeceptor-EDGE	FDC-VM (VMware ESXi, KVM, Hyper-V, AWS, GCP, and Azure), FDCVME (Fortideceptor Edge)

What’s new in FortiDeceptor 6.2.0

The following is a list of new features and enhancements in 6.2.0. For details, see the *FortiDeceptor Administration Guide* in the Fortinet Document Library.

New Decoys & Capabilities

We have the support of the Decoy Customization feature with additional Linux operating systems, including Debian 11.7 and 11.9. The supported services include HTTP, HTTPS, GIT, SAMBA, SSH, SMTP, TCPListener, FTP, Radius, and ICMP.

Decoy customization module:

- We have improved the Custom Image feature to allow importing and exporting custom images from the FortiDeceptor. The Export & Import feature supports the transfer of custom images between different FortiDeceptor appliances.
- We have also improved the ability to re-customize a current custom decoy image by allowing for adjustment of the HDD space, based on the existing custom decoy image.

New Management Capabilities:

FortiDeceptor Edge support:

- We have expanded the FortiDeceptor Edge appliance to support a local FortiDeceptor Manager. Now a single local FortiDeceptor manager can manage hundreds of FortiDeceptor Edge appliances.

Manager of Manager:

- We have introduced a new management mode for FortiDeceptors called *Manager of Managers*. This mode allows centralized management of remote FortiDeceptor managers from a single console. The top-level manager, or TOP CM, will manage all remote FortiDeceptor managers as clients, with a focus on administration, entities, and permission control. The TOP CM will also serve as a proxy console for accessing the remote FortiDeceptor managers.

When upgrading Central Managers, you must first upgrade all CM clients to version 6.2.0 before upgrading the CM manager itself to 6.2.0.

Outbreak vulnerabilities

We have expanded *Outbreak Vulnerability* to include the following vulnerabilities:

- CrushFTP Authentication Bypass Attack: FDC
- Langflow Unauth RCE Attack: FDC
- SimpleHelp Support Software Attack: FDC
- Apache Tomcat RCE: FDC
- Microsoft .NET Framework Information Disclosure
- PTZOptics NDI and SDI Cameras Attack: FDC
- Ivanti Cloud Services Appliance Zero-Day Attack: FDC

Incident Alerts Reporting

- We have added support for the MITRE ATT&CK framework, which can be accessed both as a separate menu option and within incident alerts themselves. This provides enhanced visibility into incident alerts on the network. The MITRE ATT&CK framework is a globally recognized knowledge base that categorizes adversary tactics, techniques, and procedures (TTPs) observed in real-world cyber attacks. It serves as a useful tool for cyber security teams to detect, analyze, and defend against threats by mapping security controls to known attacker behaviors.

Integration

- We expanded the *Integration* module to include On-premise FortiAnalyzer using the OFTP protocol and added a new integration with FortiAnalyzer Cloud using the OFTP protocol.

Deception Tokens

- We have enhanced the *Token Tool* package to enable users to upgrade the package directly from the FortiDeceptor Update Server or FortiDeceptor GUI, rather than waiting for a new release.
- We have added support for filtering by IP address in the *Token Campaign* page.
- We have expanded the *Lure Resources* configuration to allow for the upload of PKCS12/PEM format keys and certificates, with or without a passphrase. These keys and certificates can be applied to any decoy service when using the Decoy Deployment Wizard.

General

- We have added support for CEF syslog messages over TLS 1.2 and above.
- We have enhanced the password complexity policy for automatically generated lures.
- We continue to improve upon the GUI migration, as well as improving the menu Dashboard and the *Custom Decoy Image* menu with a Neutrino component.
- We have improved the password complexity policy support to align with Active Directory requirements when generating lures automatically with the Decoy Deployment Wizard.
- We are continuing the GUI migration to Neutrino, including pages such as the *Deployment Wizard*, *Deception Token*, and *Deception OS*.
- We have added support for PROFINET layer 2 packets over UDP with traffic proxy enabling FortiDeceptor Edge to work with the local FortiDeceptor Manager and DAAS platform.

Installation and upgrade

Installation information

For information about initial setup of FortiDeceptor on the FortiDeceptor models , FDR-100G, FDC-1000G, see the *FortiDeceptor 1000G QuickStart Guide*.

For information about installing FortiDeceptor VM models, see the *FortiDeceptor VM Install Guide*.

All guides are available in the Fortinet Document Library.

Upgrade information

Download the latest version of FortiDeceptor from the Fortinet Customer Service & Support portal.

Before any firmware upgrade, save a copy of your FortiDeceptor configuration. See Back up or restore the system configuration.

To upgrade the FortiDeceptor firmware:

1. Go to *Dashboard > System Information > Firmware Version*.
2. Click *[Update]*.
3. Select *Choose File*, locate the firmware image on your management computer.
4. Click *Submit* to start the upgrade.

After the upgrade is complete, you will be prompted to change your password the next time you log into FortiDeceptor.

Updating the FortiDeceptor firmware will not update the existing VM Images. However, it will re-initialize the existing Deception VMs to include bug fixes and enhancements.

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.

Upgrade path

FortiDeceptor 6.2.0 officially supports the following upgrade path.

Upgrade from	Upgrade to
6.1.0	6.2.0
6.0.2	6.2.0
6.0.1	6.2.0
6.0.0	6.2.0
5.3.1	6.2.0
5.2.0	6.2.0
5.0.0	6.2.0
4.3.0	6.2.0

When upgrading Central Managers, you must first upgrade all CM clients to version 6.2.0 before upgrading the CM manager itself to 6.2.0.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Fortinet Customer Service & Support portal located at https://support.fortinet.com. After logging in select *Download > Firmware Image Checksums*, enter the image file name including the extension, and select Get Checksum Code.

Product integration and support

FortiDeceptor 6.2.0 support

The following table lists FortiDeceptor 6.2.0 product integration and support information:

Web Browsers	• Microsoft Edge version 42 and later • Mozilla Firefox version 61 and later • Google Chrome version 59 and later • Opera version 54 and later • Other web browsers may function correctly but are not supported by Fortinet.
Virtualization Environment	• AWS • Azure • GCP • Hyper-V • KVM • VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7 and 7.0. • Nutanix Acropolis Only FDCVME is supported on Nutanix.
FortiOS	• 6.4.0 and later
FortiAnalyzer	• FDC-VM, FDCVMS, FDC1KF, FDC1KG, FDR1HG, FDC1HG: v7.2.5 v7.4.3 • FDCVME: v7.4.7 v7.6.2 • FAZ 7.6.2 or later • FAZ 7.4.7 or later
FortiManager	• 7.6.0 or later
FortiSandbox	• 4.0.2 or later
FortiSOAR	• 7.0 or later
FortiSIEM	• 6.3.3 or later
FortiNAC	• 8.8.2 or later

Resolved issues

The following issues have been fixed in version 6.2.0. For inquires about a particular bug, please contact Customer Service & Support.

GUI

Bug ID	Description
967417	The GUI supports migrating the Deception Token Image menu with Neutrino component.
1132240	Upgrading the token tool package from FDC VM image server and GUI is supported.
960911	Windows Customization based on existing customized images is supported.
1146040	Quarantine Status page can now be filtered by IP/MAC/Name.
1037477	Add Fabric Connector widget in FortiGate dashboard for FortiDeceptor v5.3.
1162108	The *File Size* validation error message have been improved.
1162234	Renamed the license menu from *FDC License* to *License*.
1055530	Updated the *System Certificate* page to prevent deletion of certificates that are currently in use.
1156795	Updated timezone display logic to consistently show time based on the login user's timezone setting across all locations.
1160211	Fixed an issue where the *Token Deployment Status* did not update after uninstalling the FortiDeceptor Token via EMS.

CLI

Bug ID	Description
1162311	Users can be delete with \.
1180463	Fixed the exception in `diag test network`.

Central Management

Bug ID	Description
1152371	Implemented Top Management mode.
1132711	Time synchronization between CM client and edge with CM manager or DaaS is supported.
955665	User can synchronize firmware for multiple selected clients from the Manager.
1205636	MITRE now includes T numbers for decoys operating on 100G networks and running on clients.
1123839	Fixed the *Monitor IP* no longer shows *Deploy IP* in the *Decoy Wizard*.
1187695	Fixed an issue where no asset were discovered using the CM client.
1210072	Fixed an issue in CM mode where uploading the all_in_one service package for *Outbreak* resulted in an error message.

Deception

Bug ID	Description
950747	Added support for import and export of custom images and lure resources and configuration from/to remote file server.
1102937	Added password complexity policy for automatically generated lures.
1210558	Fixed ARP spoofing detection in CM.
1157348	File paths for SMB users have been simplified, and sharename visibility has been removed.
1184673	Fixed the Max decoy license reached message in Deployment Map.
1207339	Fixed an issue on French Windows decoys where incidents displayed the password as *N/A* for usernames with French characters.
834466	Improved handling of user-provided certificates on FGT decoys.
1205661	Fixed an issue where opening honey document files did not trigger an incident.
1156565	Set proper upload file size restriction for lure resource.
1205406	we should highlight the potential conflict for tcplistener ports to non-system ports Implemented a mechanism to highlight potential conflicts between *tcplistener* ports and non-system ports.

Incident

Bug ID	Description
1155469	Implement the traffic scanner with IPS tool to report incidents.

Fabric

Bug ID	Description
900359	FortiDeceptor supports integrating with FAZ over OFTP protocol.
1101015	FortiDeceptor logs can be integrated with FAZ Cloud.
993134	Added support to filter by IP for *Fabric Status* page and *Token Campaign* page.
1201363	Updated SentinelOne REST APIs.
1209639	Fixed the *Status* wait time.
1181169	AD connector now blocks only those usernames that are confirmed by the Active Directory services of Windows decoys.
1190601	The *Credential Test* no longer fails to test the related credential.

Network

Bug ID	Description
1060703	FortiDeceptor with v1 license cannot create a deployment network.
1162873	FortiDeceptor integration with ISE now successfully performs quarantine actions; the previous *Message not found* error has been addressed.

System

Bug ID	Description
1173059	DaaS client can supports accepting the firmware image from DaaS server and installs automatically.
1102931	FortiDeceptor supports CEF syslog messages over TLS1.2 and later.
1131699	Edge devices are able to synchronize system time with the DaaS server.
1133200	Fixed the Configuration File Restoration Error on Firmware v6.1.0: File Size Exceeds Limit.
1174878	Fixed the Incident public API to 't get the correct result when timezone is not UTC.
1207499	Fixed the file size calculation consistency in backup and restore.
1206440	Fixed an issue where the OCSP stamp in the certificate of the global FDN server could not be verified.
1138830	Fixed a certificate handling issue where a SHA384 certificate uploaded to the unit appeared as SHA256 in the browser and was not trusted.

FortiDeceptor Cloud

Other

Bug ID	Description
1176019	License counts no longer differ between the *License Detail* and *Shared License* column in the FDC module status table.
1202471	Corrected the incident report PDF cover page to display the *Report Date* in the login user's timezone instead of UTC.

FDC-VM

Bug ID	Description
1149007	Addressed a log error in VME with DaaS where the system failed to retrieve fabric blocks data.

Known issues

The following issues have been identified in version 6.2.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

CLI

Bug ID	Description
976074	Not all CLI commands support `[Tab]` auto-completion

Central Management

Bug ID	Description
1206781	The *Upgrade* button is disabled when selecting all online clients and manager.
1207666	The *Approve Hold Restart* message is truncated and unreadable in appliances with more than 100 clients.
1208348	The *System Resources* section in the *Manager Dashboard* shows more deployed decoys than the maximum allowed number of Decoy VMs.
1208350	The *System Resources* section of the *Client Dashboard* displays an incorrect count of active decoys.
1207718	The *Deployment Map* is not sorting for Deployment Networks when managing more than 100 clients.
1205640	Deployment networks may appear disorganized in the *Deployment Map*.
1208319	The appliance list in the *Upgrade* section is not sorted

Deception

Bug ID	Description
1208599	When applying Custom Decoys, the original customized images may continue to appear in a loading state while a re-customized image is being applied.
1208302	Lure Resources – Password complexity lure can overwrite fake user lure with defined services. In *Lure Resources*, the password complexity lure may overwrite afake user lure that includes defined.

Incident

Bug ID	Description
1121745	Filtering incidents by MAC address may result in an error.

Other

Bug ID	Description
1123875	Forensic Data Collection API does not support VLAN deployment network on edge appliance.

www.fortinet.com