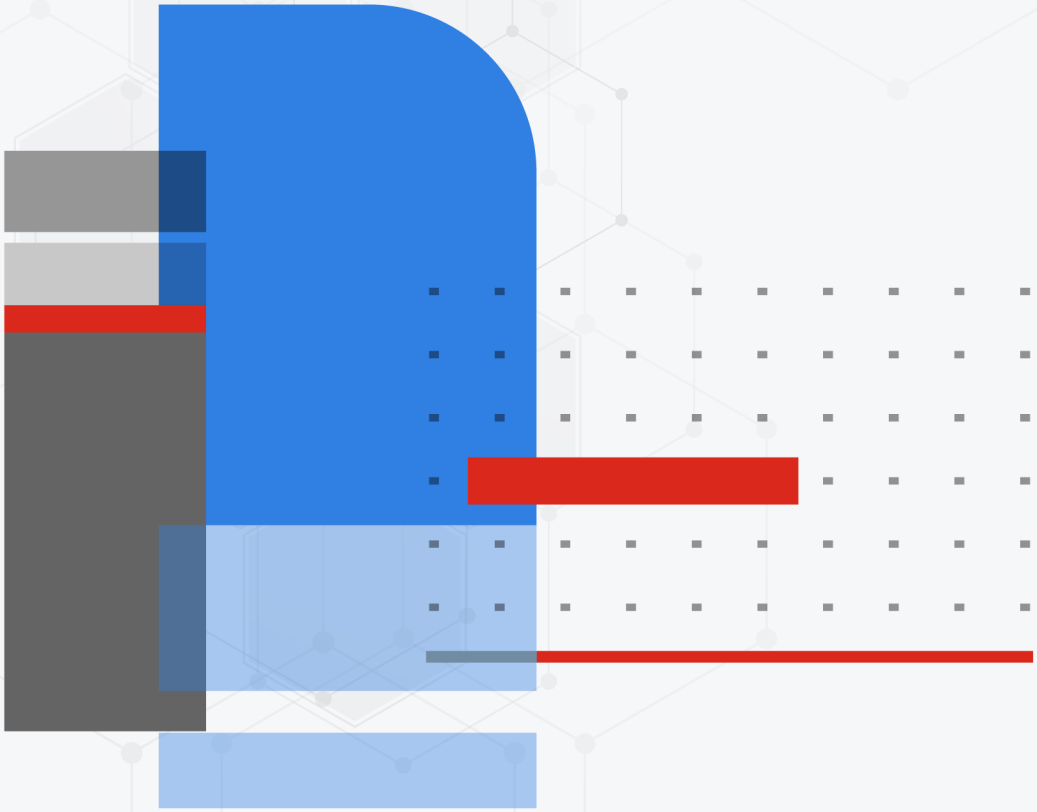
Release Notes

FortiDeceptor 6.2.1



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

January 30, 2026
FortiDeceptor 6.2.1 Release Notes
50-621-1249852-202601DD

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-01-30	Initial release.

FortiDeceptor 6.2.1 release

This document provides information about FortiDeceptor version 6.2.1 build 0280.

Supported models

FortiDeceptor version 6.2.1 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 6.2.1

FortiDeceptor version 6.2.1 contains security fixes.

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 6.2.1 officially supports the following upgrade path.

Upgrade from	Upgrade to
6.2.0	6.2.1
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 6.2.1 support

The following table lists FortiDeceptor 6.2.1 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 6.2.1. For inquires about a particular bug, please contact Customer Service & Support.

GUI

Bug ID	Description
1238553	Resolved a performance issue on the *Decoy Status* page that caused extremely long load times.

Deception

Bug ID	Description
1233505	Resolved a FortiDeceptor token compatibility issue on macOS Tahoe 26.1.
1235408	Resolved an issue where duplicate filenames in cloned directory lures caused decoy deployment to fail.
1227412	Resolved an outbreak deployment failure.

Fabric

Bug ID	Description
1234804	Resolved an issue where RADIUS authentication failed due to an excessively long shared RADIUS secret.

System

Bug ID	Description
1249246	Resolved a high memory usage issue affecting synchronization with SIEM and DaaS.
1213805	Resolved an issue where certificate files displayed incorrect issuer information after upgrading to v6.2.0.
1212663	Resolved an issue where email alerts displayed time only in GMT.

Known issues

The following issues have been identified in version 6.2.1. 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