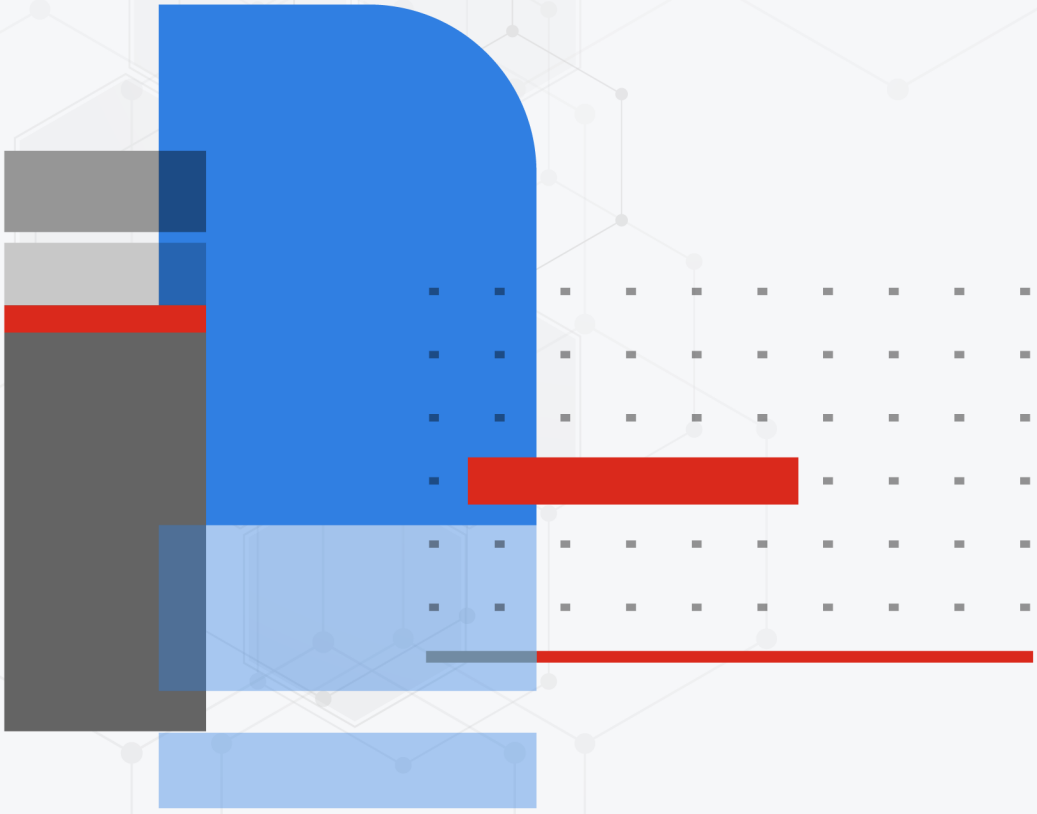
Release Notes

FortiDeceptor 6.1.0



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

September 09, 2025
FortiDeceptor 6.1.0 Release Notes
50-610-1129273-202509DD

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-02-24	Initial release.
2025-05-09	Updated Product integration and support on page 10
2025-09-09	Updated Upgrade information on page 8.

FortiDeceptor 6.1.0 release

This document provides information about FortiDeceptor version 6.1.0 build 0058.

Supported models

FortiDeceptor version 6.1.0 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)

What's new in FortiDeceptor 6.1.0

The following is a list of new features and enhancements in 6.1.0. For details, see the *FortiDeceptor Administration Guide* in the Fortinet Document Library.

New Decoys & Capabilities

- **Windows Decoy**: We have added corresponding documents and data on the Windows system and services to mimic the real system used for Windows-based Decoy, and avoid the threat actor fingerprinting the compromised asset as a decoy.
- **Linux Decoy**: We added corresponding documents and data on the Linux system, as well as services to mimic the real system used for Windows-based Decoy, and avoid the threat actor fingerprinting the compromised asset as a decoy.
- The new **Credentials Theft Protection Decoy** has been expanded by adding the CITRIX gateway decoy, allowing you to deploy the CITRIX gateway decoy in the DMZ and get alerts only against VPN login with a legitimate user credential in the network. (FortiDeceptor will leverage the A/D connector to retrieve the username list from the A/D server and validate it using a legitimate user credential.) This innovation allows you to expose the Decoy to the internet network while filtering all the scanning noise and focusing on VPN access attempts using a legitimate user credential in your network.
- We have improved the ability to add decoys to a Windows Domain network and allowed the addition of the pre-template Windows 10 decoy template.
- Deception Lure expands the attack surface and maximizes the deception coverage. We have improved the lure resource feature to allow end users to specify the services for customization of the uploaded lure resources.

- We have expanded the Outbreak vulnerability and added the following vulnerabilities:
  - Mitel MiCollab Unauthorized Access Attack
  - Palo Alto Networks PAN-OS Management Interface Vulnerabilities
  - Apache Struts 2 Remote Code Execution
  - Palo Alto Networks Expedition Missing Authentication Vulnerability
- We have added support for LDAP service events for decoys that are part of the Active Directory Domain. LDAP (Lightweight Directory Access Protocol) is a network protocol for accessing and managing directory services. For example, LDAP injection is a type of attack that targets vulnerabilities in implementations of the LDAP.
- We improved the decoy configuration and template by allowing the end-user to delete a specific decoy (IP address) from a decoy VM with multiple network interfaces (IP address) without deleting the entire decoy VM.
- FortiDeceptor expands the network Asset Discovery module with nine new OT protocols and one IT protocol. For the OT protocols, we have added **Saia-Burgess Controls/Ether-S-Bus (sbus)**, **Tridium/Niagara Fox**, **IEC 61850 MMS**, **FF-HSE, Opensafety-UDP**, **Opensafety-Powerlink**, and **Telnet**. The new asset discovery generates the asset inventory using passive network sniffing for network threat visibility and decoy deployment automation.

Deception Tokens

- FortiDeceptor integration with FortiClient (EMS) for Deception tokens deployment will allow a more flexible way to deploy the Deception tokens, including devices outside the internal network.
- In addition, the integration with FortiClient (EMS) will allow to quarantine /un-quarantine a threat actor that the FortiDeceptor detects.

FortiDeceptor Integration

- FortiDeceptor integration connector works with Splunk to update the "watch list" with deception credentials that were deployed in real-time across the real endpoints and servers. The integration also automatically identifies if a threat actor uses deception credentials across the network by checking the real-time Splunk logs.
- We improved the integration between FortiDeceptor and Cisco ISE (NAC solution) that allows the endpoint quarantine by MAC address to support ANC-POLICY instead of EPS-STATUS because of the change in the Cisco ISE technology from version 1.4.
- We improved the FortiDeceptor Quarantine integration with Checkpoint and added support for cloud management and local appliances.

General

- We added support for customized profiles for fabric and SAML SSO users to add more flexibility to the end-user access to the FortiDeceptor Web management console.
- We added support for the reserved subnet for decoy deployment customization to avoid network overlapping with customer network VLANs.

- We added a configuration backup and restore securely with encryption, based on a user-provided password and random salt. The backup will cover network definition, lure resources, decoy tokens, decoy templates, deployed decoys (without booting them up, triggering the download first upon recovery), safe list, fabric connectors configuration, network settings, and system settings.
- We expanded the FortiDeceptor API by adding the option to collect forensic data from a particular IP without a security event, allowing a more flexible mode to use the forensics tools by SOC and incident response teams.
- We added the option to export *Decoy Status* via API and XSL/CSV file via GUI.
- We continue to work on the GUI migration and improving the menu Dashboard and the custom Decoy Image menu with a neutrino component.
- We implemented a new dashboard widget to display the traffic statistics data for each physical interface.
- We improved the Decoy Deployment wizard and allowed the end user to provide different input for the domain account to allow the Decoy to join the domain

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 6.1.0 officially supports the following upgrade path.

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

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 6.1.0 support

The following table lists FortiDeceptor 6.1.0 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 6.1.0. For inquires about a particular bug, please contact Customer Service & Support.

GUI

Bug ID	Description
105662	FortiDeceptor should allow the API Key and Authorization Token to contain any characters in the *Fabric > Quarantine Integration* page.
1107945	Cloud VME client deployment wizard does not permit cloud specific MAC addresses to be entered.
1055705	There is no *Progress Update* indication in the GUI when running a firmware update.
1092930	Cannot download the PDF report after upgrading to version 6.0.1.

Central Management

Bug ID	Description
1113740	Edge client : The deployment network under the trunk port cannot be connected.
1061697	FortiDeceptor CM manager deployment network on local manager is always disabled with v1 license.

Deception

Bug ID	Description
1045747	A decoy created from a saved template throws password errors unless the lures are regenerated.
1071900	Deception Token Package fails to install.
1107842	Custom *Redhat 9 - bash decoy_strace_installation.sh* returns error message: *Kernel*

Bug ID	Description
	module build failed.
1093263	Custom Linux: The custom Redhat and Ubuntu OS, customized on 5.2 and 5.3, fail to start the HTTPS server in v6.0.2.

Fabric

Bug ID	Description
1022691	Allow each agent device set up one FortiGate fabric upstream device.

Network

Bug ID	Description
1060703	FortiDeceptor with v1 license cannot create a deployment network.

Other

Bug ID	Description
1105555	Port scan syslog shows incorrect *victim ip*.

Known issues

The following issues have been identified in version 6.1.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

GUI

Bug ID	Description
1093997	The time zones in the Dashboard are not correct.

Central Management

Bug ID	Description
944721	Edge device in DMZ mode can deploy decoys on multiple interfaces.

Deception

Bug ID	Description
1118972	Customized *Win11_24H2_English_x64* always stalls at the Windows logo page.
1097394	The deception OS *voipv1* does not detect *GTPv2-C*.
834466	Improve FortiGate decoy user-provided certificate.

Fabric

Bug ID	Description
1034295	FortiDeceptor URL should start with *http://* or *https://* in the *Fabric > Quarantine Integration*page.

Bug ID	Description
1125014	Quarantine Status: *End Time* is updated as *Start Time* plus *Expiry* after blocker fails.

System

Bug ID	Description
1055530	Users should not be allowed to delete used certificates in the *System Certificate* page
1124138	VLAN license: When shutting down a FortiDeceptor, the VLAN does not change to *Disabled* according to the VLAN license number.
1071436	Enhance rescue system with factory reset feature.

Log

Bug ID	Description
1086453	VME removes meaningless syslog.

www.fortinet.com