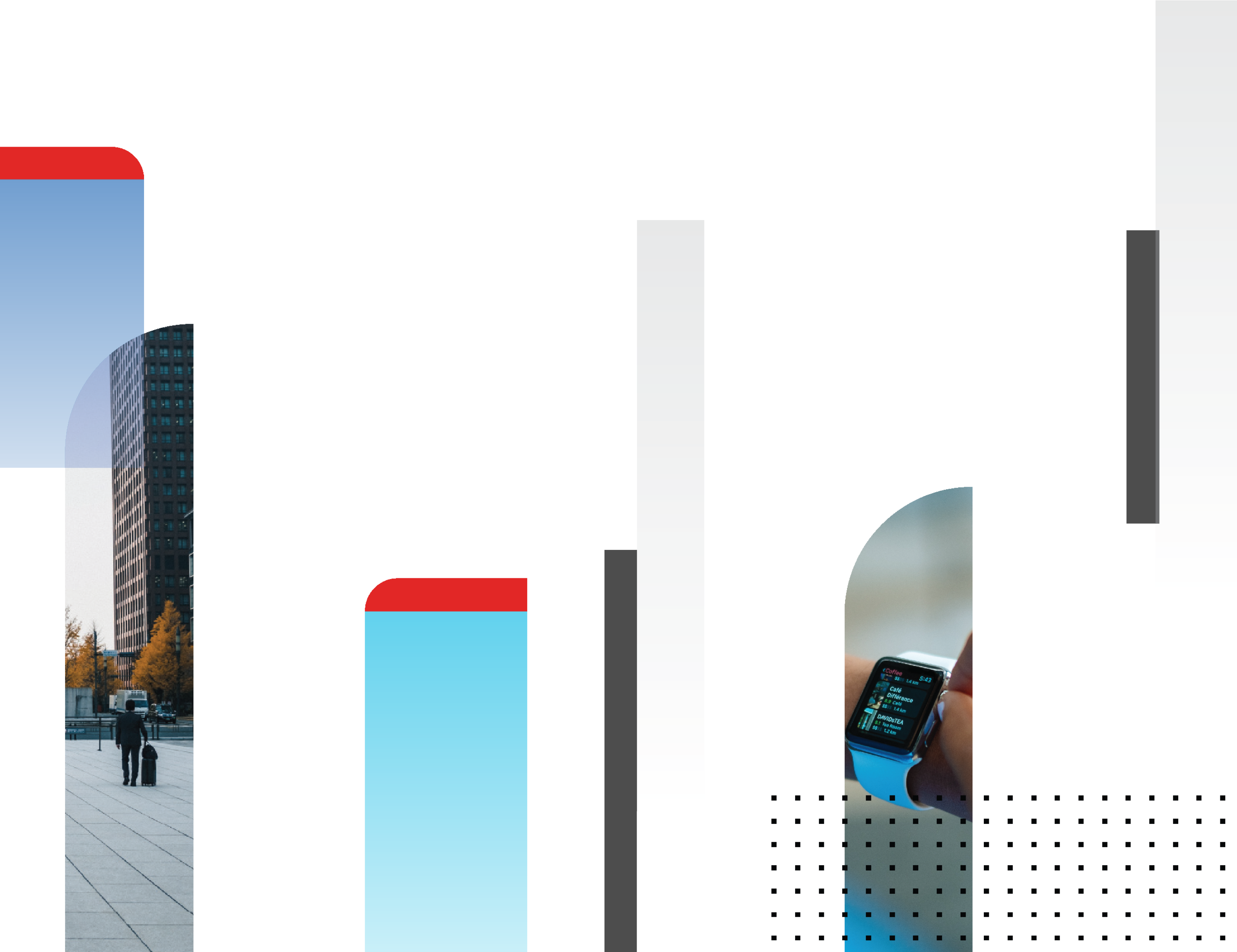
FORTINET

Release Notes

FortiAuthenticator 6.4.2



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

FORTINET VIDEO GUIDE
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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

FORTINET®

May 12, 2023
FortiAuthenticator 6.4.2 Release Notes
23-642-789555-20230512

TABLE OF CONTENTS

Change log

Date	Change Description
2022-03-17	Initial release.
2022-03-21	Updated Upgrade instructions on page 11.
2022-03-23	Updated Product integration and support on page 15.
2022-03-24	Added bug 792555 to Known issues on page 23.
2022-04-21	Removed bug 744940 from Known issues on page 23.
2022-06-15	Updated Product integration and support on page 15.
2023-05-12	Updated Upgrade instructions on page 11.

FortiAuthenticator 6.4.2 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.4.2, build 0991.

FortiAuthenticator is a user and identity management solution that provides strong authentication, wireless 802.1X authentication, certificate management, RADIUS AAA (authentication, authorization, and accounting), and Fortinet Single Sign-On (FSSO).

For additional documentation, please visit: https://docs.fortinet.com/product/fortiauthenticator/

Special notices

TFTP boot firmware upgrade process

Upgrading FortiAuthenticator firmware by interrupting the FortiAuthenticator boot process and installing a firmware image from a TFTP server erases the current FortiAuthenticator configuration and replaces it with factory default settings.

Monitor settings for GUI access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the GUI to be viewed properly without the need for scrolling.

Before any firmware upgrade

Save a copy of your FortiAuthenticator configuration before upgrading the firmware. From the administrator dropdown menu in the toolbar, go to **Restore/Backup**, and click **Download Backup File** to backup the configuration.

After any firmware upgrade

Clear your browser cache before logging in to the FortiAuthenticator GUI to ensure the pages display properly.

FortiAuthenticator does not support PEAP-MAB

FortiAuthenticator only supports MAB in clear-text and not the encapsulated MAB.

What's new

FortiAuthenticator version 6.4.2 includes the following enhancement:

Password compliance: Password cannot be the username

FortiAuthenticator now forbids using the username as password when creating or changing passwords for local user accounts. The restriction is case-insensitive.

Mixed FIDO and OTP based authentication

FortiAuthenticator now offers new options that allow a user to log in using password and OTP when FIDO is enabled, but the FIDO keys have been revoked.

Self-service portal, captive portal, and OAuth policies now include a new **Allow two-factor authentication (password and OTP) if all FIDO keys have been revoked for the user account** option in the **Authentication factors** tab when **FIDO authentication** is enabled.

The **Authentication** pane in **Authentication > SAML IdP > Service Providers** now includes:

- New **FIDO-only** and **Password and FIDO** options when **Authentication method** is set to **FIDO-only**.
- A new **Allow two-factor authentication (password and OTP) if all FIDO keys have been revoked for the user account** toggle when the **Authentication method** is **FIDO-only**.

FIDO: Admin registers the token for a user

FortiAuthenticator now allows the admin to register a FIDO key for local and remote user accounts.

New **Register FIDO key** and **Delete all FIDO keys** buttons in the **FIDO authentication** toggle when creating or editing local and remote users.

LDAP users: Send SMS/Email message to users after import

FortiAuthenticator now includes options to send a message to the end user when a user account is created with a valid mobile number and/or email address.

The message option includes Email, SMS, or both. The messages are customizable through replacement messages and can be sent to one or more end user accounts.

General tab in **Authentication > User Account Policies** is updated to include the following changes:

- **Request password reset after token verification** renamed to **Request password reset after OTP verification**.
- **Enhanced cryptography for storage of local user passwords** renamed to **Enhanced cryptography**.
- **Expire device login after** renamed to **Windows machine authentication**.
- New **Send message on remote LDAP account import** toggle with **SMS** and **Email** options.
- **Expire inactive RADIUS accounting session after** renamed to **Inactive RADIUS accounting**.
- **Session duration of authenticated TACACS+ user** renamed to **TACACS+ authentication**.
- **Look up geo-location of user IP for Web Service** renamed to **Use geolocation in FortiToken Mobile push notifications** and available in **System > Administration > System Access**.

New replacement messages in **System > Administration > Replacement Messages** to customize account import email subject, message, and the SMS.

For the remote LDAP user, the admin can manually (re)send the Email and/or SMS remote LDAP account import message to any user account using the new **Notify** button next to **Email** and **Mobile number** in **User Information** when creating or editing a remote LDAP user.

FTM activation window increased to a maximum of 30 days

The activation timeout window in **System > Administration > FortiGuard** has been increased to a maximum of 30 days.

Updated log view

The **Logs** tab in **Logging > Log Access** is updated to include the following:

- A new **Downloads** dropdown that combines all the previously available header buttons.
- A new help icon before the search bar that tells what can be looked up using the search bar.
- **Search for log records** renamed to **Search by substring (e.g. username)**.
- A new period dropdown (clock icon) to filter logs based on time period.
- A new **Reset table column widths** icon to reset the table column widths to default.

FortiAuthenticator 3000E: Additional user license

You can now add up to an additional 100,000 users license for FortiAuthenticator-3000E.

Sponsor portal: Segregation, auditing, and security related enhancements

FortiAuthenticator now includes a new **Each sponsor only has access to guest users they created** toggle in **Authentication > User Account Policies > General** to allow sponsors to view only those guest users created by the sponsor.

For enhanced security, guest user passwords are no more visible to the sponsor when the sponsor views the guest users list. When the sponsor edits or exports guest users, user password is obfuscated by default and only visible when clicked. Upon reclicking, the password is obfuscated.

When editing a guest user, clicking the **Reset Password** button assigns a new password to the guest user and displays the password.

When a sponsor creates a guest user account, the guest user is automatically assigned to the sponsor creating it.

When an admin creates a guest user account, the admin can select the sponsor using the new **Sponsor** option.

Also, the following sponsor actions now generate log events in FortiAuthenticator:

- Creating a guest user
- Deleting a guest user
- Viewing a guest user
- Modifying a guest user
- Resetting a guest user password
- Viewing a guest user password
- Printing guest user credentials
- Email guest user credentials
- Sending guest user credentials as SMS
- Exporting guest user credentials as a CSV file

Firmware upgrade via REST API

New `upgrade` endpoint to upgrade FortiAuthenticator firmware. See REST API Solutions Guide.

Self-service portal: Display FortiToken Mobile activation QR code

The self-service portal offers new options to provision the FortiToken Mobile using the QR or activation code displayed in the portal itself.

A new **Scan QR code** option while registering a token in a self-service portal to activate the token by scanning a QR code. When the **Scan QR code** option is selected, a page with the QR code appears, which can then be scanned using the FortiToken Mobile app. Alternatively, the activation code can be entered manually in the FortiToken Mobile app.

The information on the page with the QR code can be customized using the new **FortiToken Mobile Activation Scan QR Message** replacement message in **Authentication > Portals > Replacement Messages**.

Additional system information via REST API

The following new fields are available in the `systeminfo` endpoint:

- `users_usage_detail`
- `groups_usage_detail`
- `ftk_usage_detail`
- `ftm_usage_detail`
- `fsso_usage_detail`
- `ssoma_usage_detail`

For information about the new fields, see REST API Solutions Guide.

Upgrade instructions

Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator configuration, see the FortiAuthenticator Administration Guide.

To avoid any login issues for administrators, ensure the local and remote realms with administrators are in the *Legacy Self-Service Portal And OAuth Access Control Settings* pane in *System* > *Administration* > *System Access* before upgrading the FortiAuthenticator firmware from 6.4.1 and earlier.

Hardware and VM support

FortiAuthenticator 6.4.2 supports:

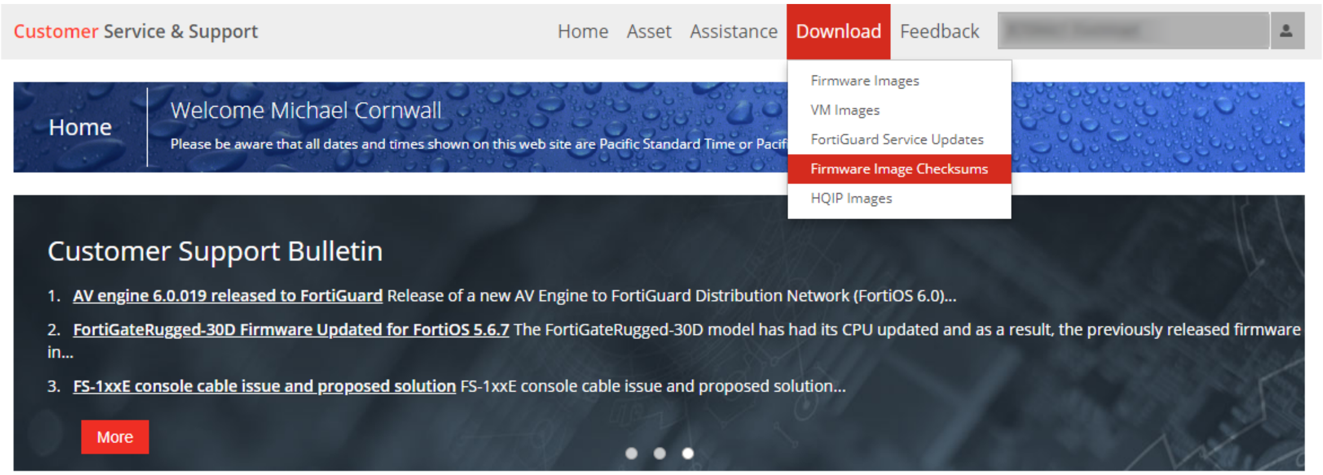
- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 300F
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 800F
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator 3000F
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, Azure, AWS, Oracle OCI, and Alibaba Cloud)

Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from the Fortinet Support website.

Customer service and support image checksum tool



Welcome Michael Cornwall

Please be aware that all dates and times shown on this web site are Pacific Standard Time or Pacif

Customer Support Bulletin

1. AV engine 6.0.019 released to FortiGuard Release of a new AV Engine to FortiGuard Distribution Network (FortiOS 6.0)...
2. FortiGateRugged-30D Firmware Updated for FortiOS 5.6.7 The FortiGateRugged-30D model has had its CPU updated and as a result, the previously released firmware in...
3. FS-1xxE console cable issue and proposed solution FS-1xxE console cable issue and proposed solution...

After logging in to the web site, in the menus at the top of the page, click **Download**, then click **Firmware Image Checksums**.

In the **Image File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

Upgrading from FortiAuthenticator 4.x/5.x/6.x

FortiAuthenticator 6.4.2 build 0991 officially supports upgrades from previous versions by following these supported FortiAuthenticator upgrade paths:

- If currently running FortiAuthenticator 6.0.5 or older, first upgrade to 6.0.7, then upgrade to 6.4.2, else the following message will be displayed: `Image validation failed: The firmware image model number is different from the appliance's.`
- If currently running FortiAuthenticator 6.0.7, then upgrade to 6.4.2 directly.
- If currently running FortiAuthenticator between 6.1.0 and 6.2.0, first upgrade to 6.3.3, then upgrade to 6.4.2.
- If currently running FortiAuthenticator between 6.2.1 and 6.3.x, then upgrade to 6.4.2 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.4.2 from FortiAuthenticator 6.0.7, you must first increase the size of the virtual hard disk drive containing the operating system image (not applicable for AWS & OCI Cloud Marketplace upgrades). See Upgrading KVM / Xen virtual machines on page 13.

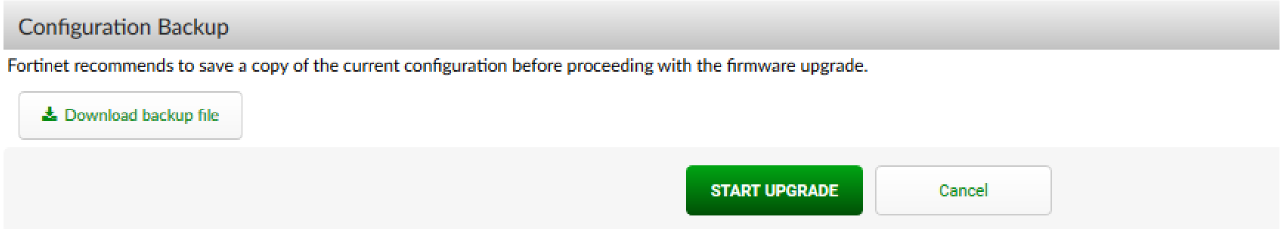
Upgrade to and from FortiAuthenticator 6.0.6 is not recommended.

Firmware upgrade process

First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator firmware, you must download the firmware image from the Fortinet Support website, then upload it from your computer to the FortiAuthenticator unit.

1. Log in to the Fortinet Support website. In the **Download** section of the page, select the **Firmware Images** link to download the firmware.
2. To verify the integrity of the download, go back to the **Download** section of the login page and click the **Firmware Image Checksums** link.
3. Log in to the FortiAuthenticator unit's web-based manager using the **admin** administrator account.
4. Upload the firmware and begin the upgrade.
   When upgrading from FortiAuthenticator 6.0.4 and earlier:
   a. Go to **System > Dashboard > Status**.
   b. In the **System Information** widget, in the **Firmware Version** row, select **Upgrade**. The **Firmware Upgrade or Downgrade** dialog box opens.
   c. In the **Firmware** section, select **Choose File**, and locate the upgrade package that you downloaded.
   When upgrading from FortiAuthenticator 6.1.0 or later.
   a. Click on the administrator name in the upper-right corner of the GUI to display the dropdown menu, and click **Upgrade**.
   b. In the **Firmware Upgrade or Downgrade** section, select **Upload a file**, and locate the upgrade package that you downloaded.
5. Select **OK** to upload the file to the FortiAuthenticator.
   Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:



Configuration Backup

Fortinet recommends to save a copy of the current configuration before proceeding with the firmware upgrade.

   It is recommended that a system backup is taken at this point. Once complete, click **Start Upgrade**.

   Wait until the unpacking, upgrade, and reboot process completes (usually 3-5 minutes), then refresh the page.

Due to a known issue in 6.0.x and earlier releases, the port5 and port6 fiber ports are inverted in the GUI for FAC-3000E models (i.e. port5 in the GUI corresponds to the physical port6 and vice-versa).

This is resolved in 6.1.0 and later, however, the upgrade process does not swap these configurations automatically. If these ports are used in your configuration during the upgrade from 6.0.x to 6.1.0 and later, you will need to physically swap the port5 and port6 fibers to avoid inverting your connections following the upgrade.

Upgrading KVM / Xen virtual machines

When upgrading existing KVM and Xen virtual machines from FortiAuthenticator 6.0.7 to 6.4.2, it is necessary to manually increase the size of the virtual hard disk drive which contains the operating system image before starting the upgrade. This requires file system write-access to the virtual machine disk drives, and must be performed while the virtual machines are in an offline state, fully powered down.

If your virtual machine has snapshots, the resize commands detailed below will exit with an error. You must delete the snapshots in order to perform this resize operation. Please make a separate copy of the virtual disk drives before deleting snapshots to ensure you have the ability to rollback.

Use the following command to run the resize on KVM:

```
qemu-img resize /path/to/fackvm.qcow2 1G
```

Use the following command to run the resize on Xen:

```
qemu-img resize /path/to/facxen.qcow2 1G
```

After this command has been completed, you may proceed with the upgrade from 6.0.7 to 6.4.2

Recovering improperly upgraded KVM / Xen virtual machines

If the upgrade was performed without completing the resize operation above, the virtual machine will fail to properly boot, instead displaying many **initd** error messages. If no snapshots are available, manual recovery is necessary.

To recover your virtual machine, you will need to replace the operating system disk with a good copy, which also requires write-access to the virtual hard disks in the file system while the virtual machines are in an offline state, fully powered down.

To recover an improperly upgraded KVM virtual machine:

1. Download the 6.0.7 GA ZIP archive for KVM, **FAC_VM_KVM-v6-build0059-FORTINET.out.kvm.zip**.
2. Extract the archive, then replace your virtual machine's **fackvm.qcow2** with the one from the archive.
3. Execute the following command:
   ```
   qemu-img resize /path/to/fackvm.qcow2 1G
   ```

To recover an improperly upgraded Xen virtual machine:

1. Download the 6.0.7 GA ZIP archive for Xen, **FAC_VM_XEN-v6-build0059-FORTINET.out.xen.zip**.
2. Extract the archive, then replace your virtual machine's **facxen.qcow2** with the one from the archive.
3. Execute the following command:
   ```
   qemu-img resize /path/to/facxen.qcow2 1G
   ```

Product integration and support

Web browser support

The following web browsers are supported by FortiAuthenticator 6.4.2:

- Microsoft Edge version 99
- Mozilla Firefox version 98
- Google Chrome version 99

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiAuthenticator 6.4.2 supports the following FortiOS versions:

- FortiOS v7.0.x
- FortiOS v6.4.x
- FortiOS v6.2.x
- FortiOS v6.0.x

Fortinet agent support

FortiAuthenticator 6.4.2 supports the following Fortinet Agents:

- FortiClient v.5.x, v.6.x for Microsoft Windows and macOS (Single Sign-On Mobility Agent)
- For FortiAuthenticator Agents for Microsoft Windows and Outlook Web Access compatibility with FortiAuthenticator, see the *Agents Compatibility Matrix* on the Fortinet Docs Library.
- FSSO DC Agent v.5.x
- FSSO TS Agent v.5.x

Other Agent versions may function correctly, but are not supported by Fortinet.

For details of which operating systems are supported by each agent, please see the install guides provided with the software.

Note: FortiAuthenticator Agent for Microsoft Windows 4.0 and above required to support emergency offline access. Also, FortiAuthenticator Agent for Microsoft Windows below 4.0 compatible for all other features.

Virtualization software support

FortiAuthenticator 6.4.2 supports:

- VMware ESXi / ESX 6/7
- Microsoft Hyper-V 2010, Hyper-V 2016, and Hyper-V 2019
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Xen Virtual Machine (for Xen HVM)
- Nutanix
- Amazon AWS
- Microsoft Azure
- Oracle OCI
- Alibaba Cloud

⚠ Support for HA in Active-Passive and Active-Active modes has not been confirmed on the FortiAuthenticator for Xen VM at the time of the release.

See FortiAuthenticator-VM on page 17 for more information.

Third-party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

- RADIUS Challenge Response - Requires support by third party vendor.
- Token Passcode Appended - Supports any RADIUS compatible system.

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client / network access server (NAS).

FortiAuthenticator-VM

For information about FortiAuthenticator-VM deployments and system requirements, see the VM installation guide on the Fortinet Docs Library.

Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please visit the Fortinet Support website.

Bug ID	Description
769953	Some of remote user sync rules stopped working after upgrade.
773306	Remote sync rule does not remove the user from FortiToken Cloud.
778088	pushd not processing FortiToken Mobile push for usernames of format "domain\user".
774659	RADIUS authentication via MSCHAPv2 fails using 8-digits FortiToken Cloud.
778835	FortiAuthenticator SAML IdP - HTTP error 500 if LDAP users with very long DN log in.
778114	Editing remote sync rules show base unit instead of previously saved value.
770154	FortiAuthenticator v6.4.1 does not support the old URL "/cert/scep" for SCEP anymore.
746567	Importing local users from CSV - FortiAuthenticator LB shows "In Sync with Anomalies".
776302	0.0.0.0/0 RADIUS client not accepted.
770193	Error 403 when clicking on "click to goto the login page".
769976	Unable to select 6 or more groups for the LDAP service directory tree.
748862	Read-only admin profile cannot view local/remote users, error 500.
763568	The timestamp of the account status for lockout is GMT 00:00 regardless of the system time.
779850	Restore Backup - Unable to "force restore" a backup from an unrecognized build.
764092	OAuth setting permissions are missing.
774212	Erroneous error message displayed when promoting local user to admin.
769877	User Management GUI shows "Backup" after FortiToken Mobile token code is used to log in successfully.
733323	PCI DSS 2FA shows different page for user that does not exist.
616489	Directory tree GUI bug when changing classes and creating new LDAP entry.
779956	Remove Scan QR code option for FortiToken Cloud.
776257	Email subject and body show up swapped in token email.
706997	Unable to make certain custom RADIUS attributes.
767313	SAML user import is broken.
771123	RADIUS: MAC auth bypass requests are crashing radiusd / preventing other logins.
765529	When IP range 0.0.0.0~255.255.255.255 is used as a RADIUS client, it has the highest priority.
761292	Azure remote IdP authentication fails if FortiAuthenticator FQDN contains upper case.

Bug ID	Description
756777	Incorrect order of the fields displayed on change_password_remote page for remote users.
766131	Import SSO Groups menu : "Select None" and "All" buttons seem dead when thousands of CN groups are present.
768948	FSSO portal login timeout value cannot be saved.
774076	FortiAuthenticator workstation check causes Windows System Event Log ID 10036 - CVE-2021-26414 and KB5004442.
741332	FortiToken Mobile email activation sent to user again when LDAP sync runs after the timeout of token activation (user should stay disabled).
771382	LDAP filters are showing the entire directory tree instead of applied filters for users.
779992	FortiAuthenticator Read-Only "Admin Profile" Shows error 500.
778478	FortiAuthenticator RADIUS policy - attribute filters do not escape '\t', '\n' and '\r' properly.
774759	SNMP not generating correct user counts when remote RADIUS users are administrators.
778053	Local user imported via API with no password will fail RADIUS authentication using OTP-only.
782363	Accessing the self service portal gives error 500.
757968	/api/v1/pushauth/: the processing of the response is delayed.
756782	FortiAuthenticator GUI cannot show how many users available in every group.
692726	Certificate expiry warning sends out an email everyday.
769954	Admin with OTP(SMS) cannot pass password prompt when making changes to admin accounts.
759691	FSSO self-service portal does not create FSSO session upon end user login.
777914	Login fails after we are redirected from portal.office.com to the IdP-FortiAuthenticator 6.4.1.
767750	GUI showing wrong URL for CRL distribution point.
768643	Password change of the logged in admin asking for reauth with menu still displayed.
771209	Captive portal randomly fails with "500 Internal Server Error".
771409	SAML IdP: auth gives error 403 when using custom attribute.
770258	SSO groups imported from LDAP do not get excluded using Fine-Grained controls.
770177	FortiAuthenticator SAML: error 403 for the SAML session details if SAML is disabled on the interface the admin is connected.
766837	Guest portal gives error 500 if a user is registering with the same phone number for the second time.
752627	Token transfer fails if includes deprovisioned token(registration id = null) and FortiAuthenticator throws unknown error.
764256	FSSO - LDAP user/group lookup is broken by addition of remote LDAP for computer-based authentication.

Bug ID	Description
758008	FortiAuthenticator joining domain and using the incorrect domain name (DNS) if the name is the same in several LDAP servers.
745497	Kerberos not working for AES.
763516	OAuth should have its own portals.
724834	Support ES6.
745433	`execute backup config ftp` upload issue when path provided.
765133	Cannot delete an expired user certificate in Firefox.
768540	Webserver leaks sockets while handling SAML authentications for remote LDAP users.
756678	Not all debug pages on FortiAuthenticator provide the option to set maximum size of the debug file.
764147	Cloud-init: DHCP client stays resident rather than exiting after boot as intended.
764052	Update to show "Memory Available" in addition to "Memory used".
773944	Default self-signed certificate expiry date is 1 year.
770375	SW RAID models (400E, 300F) fail to reformat themselves in 6.4.0 and 6.4.1.
746405	LB HA primary node (eventually) runs out of database connections when an LB node disk is full.
764376	Admin user gets locked out after other users log in via the self service portal.
752741	Sync admin permission profiles in LB-HA.
752408	Seek confirmation from the FortiAuthenticator admin when restoring configuration via GUI.
771671	Input is missing from the *Inbound Proxy* pane in the *System Access* tab.
719092	FortiAuthenticator VMware VM with Cloud-init does not work on the ESXi hypervisor.
788824	[3rd party component upgrade required for security reasons] FortiAuthenticator - Dirty Pipe vulnerability on Linux Kernel.
774147	[FG-IR-21-254] "Host" header injection.
761940	busybox vulnerabilities- precautionary upgrade.
768951	django- Precaution upgrade.
769295	[Third party] lxml vulnerabilities- precaution upgrade.
782448	Force password change on next logon produces 403 forbidden with SAML login.
613164	Google Workspace Open LDAP crashes when we try to change password.
778043	HA load balancing certificate binding and RADIUS attribute anomalies when syncing an unsync'd admin.
786034	RADIUS authentication against remote LDAP users fail if the user is not imported.
786540	SAML proxy Google Workspace login shows 500 error on the SP.
769712	Memory available always show 0 on the *Dashboard*.

Bug ID	Description
779045	500 internal server error when changing remote user password via self service portal.
781813	Remote user sync rule for the already imported user does not re-sync OTP.
762262	Password reset does not work for the remote LDAP user if the password contains 6 characters or less.
780556	Remote user sync rules fails to sync remote users when FortiToken Mobile tokens are assigned.
776256	Sponsor accounts cannot re-enable the guest users that they created.
733028	Error 404 Not Found when resending email or SMS.
604734	*Today* button for expiry guest users is 1 day ahead.
772153	Username field from the Portal registration page should not be there if mobile number is used as the username.
764179	Unable to change password of remote user unless imported in FortiAuthenticator.
763341	Dump when adding LDAP uid to a uid.
773020	Revoking of certificate is not being seen with OCSP until FortiAuthenticator reboots.
763973	Sponsor admin profile should be read-only.
764510	OAuth 2.0 / OIDC monitoring, troubleshooting and auditing.
765396	pushd leaks database connection and failed to send notification if postgres restarted.
786754	SP session for SAML FSSO are not SSO - 403 Forbidden with Chrome.
788638	FortiAuthenticator prompts for the admin password when changing a user sync rule when adding the assigned token.
665384	HA failover does not work reliably after maintenance mode is disabled on the high priority node.
782955	FortiAuthenticator fails to import 3rd party CA certificate but the GUI shows "Import Successful".
777665	CPU spikes for every 5 minutes on time based schedule and last for 1 minutes when there are users in FortiAuthenticator.
755916	[Third Party] Postgresql - precaution upgrade.
762203	FSSO server restart takes too long when the global pre-filter is modified.
787678	FortiAuthenticator TACACS+ behavior with ASCII and PAP.

Common Vulnerabilities and Exposures

Bug ID	CVE references
791452	FortiAuthenticator 6.4.2 is no longer vulnerable to the following CVE-Reference (s): • CVE-2022-0778

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please visit the Fortinet Support website.

Bug ID	Description
783685	"Obtained access token from Azure" takes too much time to process.
758516	FortiAuthenticator HA: cluster out of sync if the custom RADIUS dictionary is uploaded, auth breaks.
785585	HA load balancing anomaly for the registered captive portal user.
755752	Power supplies show voltage input fault on both CLI and GUI.
773009	FortiAuthenticator does not expand disk properly - system status shows old size, expand-partition shows new size.
769183	FortiAuthenticator VMs need greater resiliency / improved recovery when connectivity lost to the remote data drives.
787013	Changing the username attribute will cause the remote sync rule to remove existing remote users and eventually re-import them.
780611	Oauth Token API returns error when calling API /oauth/token/ with FortiToken Cloud user, but FortiToken Cloud had sent the push to FortiToken Mobile.
785634	Remote user without any FIDO keys for a FIDO enabled portal is unable to change password.
785164	Remote admin unable to create self-service portal security question.
777392	FortiAuthenticator displays entire LDAP tree when testing filter in remote user sync rule, can freeze GUI.
781506	High memory consumption on unused FortiAuthenticator-VM.
773131	FortiAuthenticator-3000F: HW Monitor PSU widget supports PSU placed in top/bottom orientation.
779771	500 internal error shows when editing an LDAP entry.
782799	FortiToken Cloud manual sync timeouts when user > 1000, but actually users are synced.
783765	SAML requests in form of POST with bindings will result in 403 error on FortiAuthenticator.
775006	Occasionally, multiple SMS are received after LDAP user import instead of just one.
779796	SAML IDP proxy for Azure is not working with the current Azure Portal.
566145	Usage Profile "TIME USAGE=Time used" is not triggering COA or disconnect request to FortiGate.
643810	CLI restore-admin command needs improvement.
749422	Rest API script is unable to modify the user info when yubikey is assigned.
775542	Admin logon with 2FA gets "Access denied" before typing the token, auth OK.
655350	The lockout policy does not appear to apply to username/token submissions to the /auth API endpoint.

Bug ID	Description
757460	Enable Django auto-translation for any end user pages.
750134	LDAP server cannot export admin users from local user base.
775083	FortiAuthenticator FSSO detects FortiAuthenticator domain-join as login event, resolves workstation name to 127.0.0.1 and forwards that login.
646299	Nutanix AHV KVM based Hypervisor- upgrading FortiAuthenticator from 6.0.4 to 6.1.x fails and hangs on "Waiting for Database".
637028	SSL connection failed in case of certificate expired issue is not explicit enough.
638374	SCEP - Encryption/hash compatibility with clients.
676532	When FortiAuthenticator has RADIUS client set as subnet, RADIUS accounting disconnect messages are not sent.
773083	Enable/disable FortiToken Cloud push notification button shuts down all the authentication methods.
770593	Minimize the use of CBC ciphersuites.
767745	SNMP facSysCpuUsage returns wrong type.
767935	A-P cluster forms when configured from the GUI, it does not when from CLI without a restart.
751108	FortiAuthenticator does not support admin OIDs from FORTINET-CORE-MIB properly.
792555	After upgrading to FortiAuthenticator 6.4.2, administrators cannot log into admin GUI unless realm configured for legacy self service portal. **Workaround:** To avoid any login issues for administrators, ensure the local and remote realms with administrators are in the *Legacy Self-Service Portal And OAuth Access Control Settings* pane in *System > Administration > System Access* before upgrading the FortiAuthenticator firmware from 6.4.1 and earlier.

Maximum values for hardware appliances

The following table lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware models.

⚠ The maximum values in this document are the maximum configurable values and are not a commitment of performance.

Feature		Model						
		200E	300F	400E	800F	1000D	2000E	3000E
System								
Network	Static Routes	50	50	50	50	50	50	50
Messages	SMTP Servers	20	20	20	20	20	20	20
	SMS Gateways	20	20	20	20	20	20	20
	SNMP Hosts	20	20	20	20	20	20	20
Administration	Syslog Servers	20	20	20	20	20	20	20
	User Uploaded Images	40	90	115	415	515	1015	2015
	Language Files	50	50	50	50	50	50	50
Realms		20	60	80	320	400	800	1600
Authentication								
General	Auth Clients (NAS)	166	500	666	2666	3333	6666	13333

Feature		Model						
		200E	300F	400E	800F	1000D	2000E	3000E
	Users (Local + Remote)[1]	500	1500	2000	8000	10000	20000	40000
	User RADIUS Attributes	1500	4500	6000	24000	30000	60000	120000
	User Groups	50	150	200	800	1000	2000	4000
	Group RADIUS Attributes	150	450	150	2400	600	6000	12000
	FortiTokens	1000	3000	4000	16000	20000	40000	80000
	FortiToken Mobile Licenses[2]	200	200	200	200	200	200	200
	LDAP Entries	1000	3000	4000	16000	20000	40000	80000
	Device (MAC-based Auth.)	2500	7500	10000	40000	50000	100000	200000
	RADIUS Client Profiles	500	1500	2000	8000	10000	20000	40000
	Remote LDAP Servers	20	60	80	320	400	800	1600
	Remote LDAP Users Sync Rule	50	150	200	800	1000	2000	4000
	Remote LDAP User Radius Attributes	1500	4500	6000	24000	30000	60000	120000
FSSO & Dynamic Policies								

Feature		Model						
		200E	300F	400E	800F	1000D	2000E	3000E
FSSO	FSSO Users	500	1500	2000	8000	10000	20000	200000[3]
	FSSO Groups	250	750	1000	4000	5000	10000	20000
	Domain Controllers	10	15	20	80	100	200	400
	RADIUS Accounting SSO Clients	166	500	666	2666	3333	6666	13333
	FortiGate Services	50	150	200	800	1000	2000	4000
	FortiGate Group Filtering	250	750	1000	4000	5000	10000	20000
	FSSO Tier Nodes	5	15	20	80	100	200	400
	IP Filtering Rules	250	750	1000	4000	5000	10000	20000
Accounting Proxy	Sources	500	1500	2000	8000	10000	20000	40000
	Destinations	25	75	100	400	500	1000	2000
	Rulesets	25	75	100	400	500	1000	2000
Certificates								
User Certificates	User Certificates	2500	7500	10000	40000	50000	100000	200000
	Server Certificates	50	150	200	800	1000	2000	4000
Certificate Authorities	CA Certificates	10	10	10	50	50	50	50
	Trusted CA Certificates	200	200	200	200	200	200	200
	Certificate Revocation Lists	200	200	200	200	200	200	200
SCEP	Enrollment Requests	2500	7500	10000	40000	50000	100000	200000

[1] Users includes both local and remote users.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

[3] For the 3000E model, the total number of concurrent SSO users is set to a higher level to cater for large deployments.

Maximum values for VM

The following table lists the maximum number of configuration objects that can be added to the configuration database for different FortiAuthenticator virtual machine (VM) configurations.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

The FortiAuthenticator-VM is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator-VM Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The **Calculating metric** column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator]-VM Base License, the number of auth clients (RADIUS and TACACS+) that can authenticate to the system is:

100 / 3 = 33

Where this relative system is not used e.g. for static routes, the **Calculating metric** is denoted by a "**-**". The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
System					
Network	Static Routes	2	50	50	50
Messaging	SMTP Servers	2	20	20	20
	SMS Gateways	2	20	20	20
	SNMP Hosts	2	20	20	20
Administration	Syslog Servers	2	20	20	20
	User Uploaded Images	19	Users / 20	19 (minimum)	250
	Language Files	5	50	50	50
Authentication					
General	Auth Clients (RADIUS and TACACS+)	3	Users / 3	33	1666

Feature		**Model**			
		Unlicensed VM	**Calculating metric**	**Licensed VM (100 users)**	**Example 5000 licensed user VM**
User Management	Authentication Policy (RADIUS and TACACS+)	6	Users	100	5000
	Users (Local + Remote)[1]	5	***********	100	5000
	User RADIUS Attributes	15	Users x 3	300	15000
	User Groups	3	Users / 10	10	500
	Group RADIUS Attributes	9	User groups x 3	30	1500
	FortiTokens	10	Users x 2	200	10000
	FortiToken Mobile Licenses (Stacked) [2]	3	200	200	200
	LDAP Entries	20	Users x 2	200	10000
	Device (MAC-based Auth.)	5	Users x 5	500	25000
	Remote LDAP Servers	4	Users / 25	4	200
	Remote LDAP Users Sync Rule	1	Users / 10	10	500
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
FSSO & Dynamic Policies					

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
FSSO	FSSO Users	5	Users	100	5000
	FSSO Groups	3	Users / 2	50	2500
	Domain Controllers	3	Users / 100 (min=10)	10	50
	RADIUS Accounting SSO Clients	10	Users	100	5000
	FortiGate Services	2	Users / 10	10	500
	FortiGate Group Filtering	30	Users / 2	50	2500
	FSSO Tier Nodes	3	Users /100 (min=5)	5	50
	IP Filtering Rules	30	Users / 2	50	2500
	FSSO Filtering Object	30	Users x 2	200	10000
Accounting Proxy	Sources	3	Users	100	5000
	Destinations	3	Users / 20	5	250
	Rulesets	3	Users / 20	5	250
Certificates					
User Certificates	User Certificates	5	Users x 5	500	25000
	Server Certificates	2	Users / 10	10	500
Certificate Authorities	CA Certificates	3	Users / 20	5	250
	Trusted CA Certificates	5	200	200	200
	Certificate Revocation Lists	5	200	200	200
SCEP	Enrollment Requests	5	Users x 5	500	25000

[1] Users includes both local and remote users.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

FORTINET®

www.fortinet.com