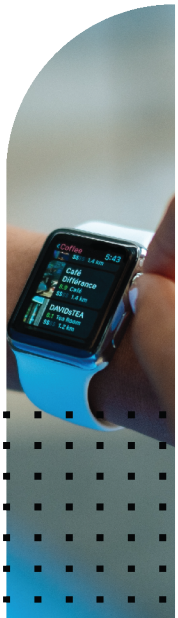
Release Notes

FortiAuthenticator 6.4.0



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

March 2, 2022
FortiAuthenticator 6.4.0 Release Notes
23-640-738205-20220302

TABLE OF CONTENTS

Change log

Date	Change Description
2021-08-05	Initial release.
2021-08-11	Updated Upgrade instructions on page 10.
2021-08-20	Updated Upgrade instructions on page 10.
2021-10-04	Updated Maximum values for VM on page 26.
2021-10-13	Updated Special notices on page 6 and Maximum values for VM on page 26.
2021-12-13	Updated Upgrade instructions on page 10.
2021-12-31	Updated Upgrade instructions on page 10.
2022-03-02	Added FortiAuthenticator Agent for Microsoft Windows 4.0 and 4.1 to Product integration and support on page 14.

FortiAuthenticator 6.4.0 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.4.0, build 0888.

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 6.4.0 includes the following enhancement:

User Portal: LDAP users can set their security questions and answers

FortiAuthenticator now allows LDAP users to set up and edit security questions and answers in the user portal similar to local users.

SAML IdP: Support for multiple domains with O365

FortiAuthenticator now allows configuring the SAML IdP service with a Service Provider (SP) containing multiple IdP prefixes.

When creating or editing a SAML SP in **Authentication > SAML IdP > Service Providers**, you can configure alternate IdP prefixes.

SAML IdP and User Portals: FIDO2 authentication

FortiAuthenticator now offers FIDO (Fast IDentity Online) service for SAML and general API based authentication.

A new `fido` field is available in `localusers`, `ldapusers`, and `radiususers` endpoints providing the ability to enable or disable FIDO authentication for local and remote user accounts. For information about the new `fido` field, see the REST API Solutions Guide.

When creating or editing a local or remote user in **Authentication > User Management > Local Users/ Remote Users**, the following options have been renamed:

- **Password-based authentication** to **Password authentication**.
- **Token-based authentication** to **One-Time Password (OTP) authentication**.

A new **FIDO authentication** toggle is available that allows using FIDO authenticators.

The **Create New/Edit Remote LDAP User Synchronization Rule** window in **Authentication > User Management > Remote User Sync Rules** now has a new **FIDO authentication** toggle to enable FIDO authentication for synced user accounts. Also, the **Token-based authentication sync priorities** option in **Synchronization Attributes** has been renamed to **OTP method assignment priority**.

A new **FIDO Revocation** toggle is available in the **Pre-Login Services** pane when creating or editing a portal in **Authentication > Portals > Portals**. **Token Revocation** toggle has been renamed to **FortiToken Revocation**. It also has new **Allow FIDO token registration/revocation** toggles for FIDO token management when **Token Registration** is enabled in the **Post-Login Services** pane.

A new **FIDO authentication (effective once a token has been registered)** toggle is available in the **Authentication factors** tab when creating or editing a captive portal policy or a self-service portal policy in **Authentication > Portals > Policies**.

The following options have been renamed in the **Authentication factors** tab:

- **Mandatory two-factor authentication** to **Mandatory password and OTP**.
- **Verify all configured authentication factors** to **Every configured password and OTP factors**.
- **Password-only authentication** to **Password-only**.
- **Token-only authentication** to **OTP-only**.

The above options were also renamed for RADIUS policies and TACACS+ policies in **Authentication > RADIUS Service > Policies** and **Authentication > TACACS+ Service > Policies** respectively.

With the inclusion of FIDO authentication, FortiTokens are no longer the only MFA method that can be self-registered. Therefore, the self-service portal main page now offers a **Multi-Factor** menu item replacing FortiTokens. The **Multi-Factor** menu item now offers FIDO token management capabilities.

The following replacement messages related to FIDO authentication have been added to **Authentication > Portals > Replacement Messages**:

- **FIDO Login Page**
- **FIDO Login Password Page**
- **User Fido Reset Email Subject**
- **User Fido Reset Receipt Email Message**

When creating or editing a SAML SP in **Authentication > SAML IdP > Service Providers**, **FIDO-only** and **Password and FIDO** authentication methods are now available.

A new **Use FIDO-only authentication if requested by the SP** toggle is also available.

The following authentication methods have been renamed:

- **Mandatory two-factor authentication** to **Mandatory password and OTP**.
- **Verify all configured authentication factors** to **Every configured password and OTP factors**.
- **Password-only authentication** to **Password-only**.
- **Token-only authentication** to **OTP-only**.

The following replacement messages related to FIDO authentication have been added to **Authentication > SAML IdP > Replacement Messages**:

- **Login Fido Page** (username only)
- **Login Fido Password Page**

Guest Portal: Restrict groups available to sponsors

When creating or editing a local user group in **Authentication > User Management > User Groups**, there is a new **Guest Group** toggle that allows including or excluding this local user group from the list of groups that sponsors can assign to new guest user accounts.

Format option for mobile number in SMS gateways

When creating or editing an SMS gateway in **System > Messaging > SMS Gateways**, you can now specify whether the mobile number is sent as a **JSON String** or **JSON Number** using the **Send Mobile Number as** option in **HTTP/HTTPS** pane.

Ability to unlock FTMs in bulk

Using the new **Unlock** option in the **FortiTokens** tab available in **Authentication > User Management > FortiTokens**, you can unlock all the selected FortiTokens at once.

Usage Profile: Reset the user's usage

A new **Clear** option to clear the cumulative RADIUS accounting sessions in the **Cumulative** tab available in **Monitor > Authentication > RADIUS Sessions**.

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.

Hardware and VM support

FortiAuthenticator 6.4.0 supports:

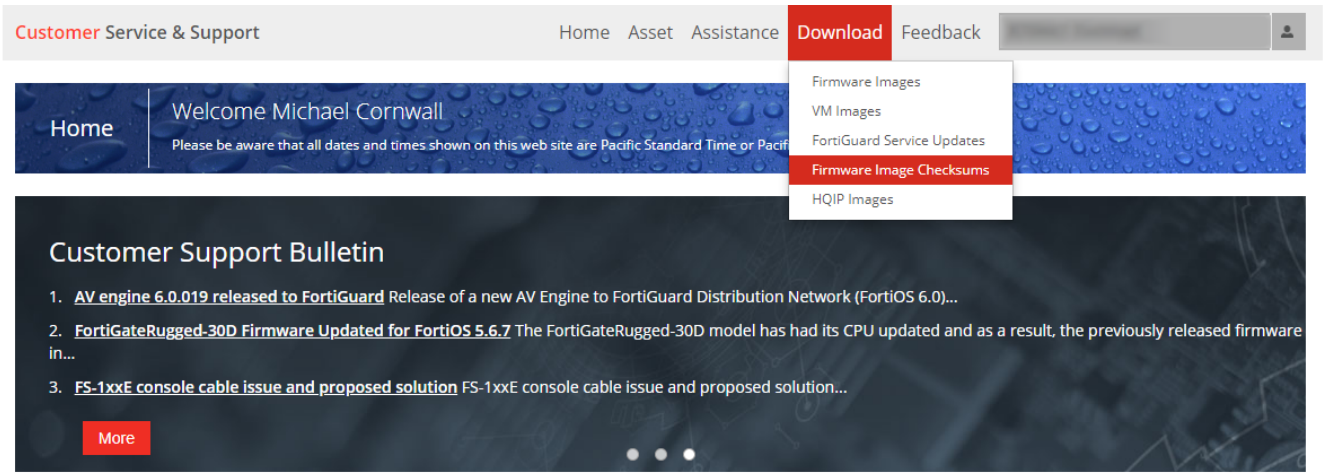
- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 300F
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator 800F
- FortiAuthenticator VM (VMWare, Hyper-V, 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



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 6.4.0 build 0888 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 6.4.0, 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 6.4.0 directly.
- If currently running FortiAuthenticator between 6.1.0 and 6.2.0, first upgrade to 6.3.3, then upgrade to 6.4.0.
- If currently running FortiAuthenticator between 6.2.1 and 6.3.x, then upgrade to 6.4.0 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.4.0 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 12.

Upgrade to and from FortiAuthenticator 6.0.6 is not recommended.

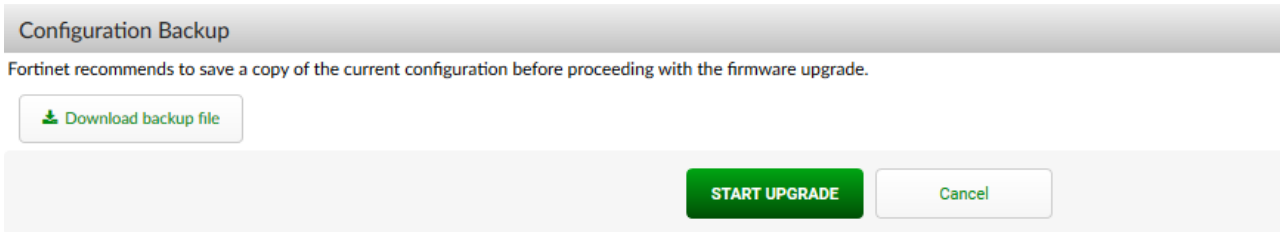
Firmware upgrade process

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:



   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 6.4.0, 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 6.4.0

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 6.4.0:

- Microsoft Edge version 92
- Mozilla Firefox version 90
- Google Chrome version 92

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

FortiOS support

FortiAuthenticator 6.4.0 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 6.4.0 supports the following Fortinet Agents:

- FortiClient v.5.x, v.6.x for Microsoft Windows and macOS (Single Sign-On Mobility Agent)
- FortiAuthenticator Agent for Microsoft Windows 2.6, 3.7, 3.8, 4.0, and 4.1.
- FortiAuthenticator Agent for Outlook Web Access 2.2
- 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.

Virtualization software support

FortiAuthenticator 6.4.0 supports:

- VMware ESXi / ESX 6/7
- Microsoft Hyper-V 2010, Hyper-V 2012 R2, and Hyper-V 2016
- 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 16 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
737532	Ship Windows Agent 3.8 with FortiAuthenticator 6.4.0.
736014	Case sensitivity is ignored by REST API rate limit feature.
726668	A-P cluster: Link down status of the monitored interface does not trigger failover.
656260	Improve FortiAuthenticator logging on failure to send push notifications.
733985	Built-in Big Switch Network RADIUS attributes fail to send ACCESS-ACCEPT.
692839	Local cert for GUI rejected despite SAN field.
709007	Error when importing a remote LDAP user.
632629	Smart Connect WPA2-Personal profile fails when WPA2-Enterprise settings are left in place.
704565	FortiAuthenticator only applies one captive portal policy and ignores RADIUS client IP/AP IP in portal policy selection.
725339	Update 6.3.1 produces 503 server error for GUI under heavy SCEP traffic.
714927	Unable to expand FortiAuthenticator "data drive" beyond 2 TB.
697447	Octet/ASCII conversion for all RADIUS attribute-value pair inputs.
729018	Concatenated style OTP is not working with Windows-AD authentication being enabled.
622426	MAC address parameter in portal policy should only allow MAC addresses.
693151	Allow deletion of the expired user and the local service certificates.
717175	Local users export/import feature does not work if `bcrypt` hash is used.
722579	Proxy allowlist input visible when "Configure valid FORWARDED by values" is not checked.
735902	Unable to get DN when creating an LDAP server.
735267	Double crash in 500 error.
697200	SAML configuration requires domain name with ".", but does not warn.
694116	Poor handling and usability in Self Service Portal > Pre-login > Register New User.
723629	SAML local override user does not work.
601883	Test SMS does not work when adding a gateway.
694112	Clickable area extends beyond the buttons in the Self-service Portal.
721954	Better error display for FortiToken mobile when FortiAuthenticator does not have a license.

Bug ID	Description
724559	Portal policy changes in the RADIUS response does not take effect.
724829	Unable to save portal policy with "NA - stay in login page" selected.
727824	Unable to delete SSO Filtering Objects.
707876	Revisit categories mentioned in the download "Debug Report" dropdown.
702758	The firmware certificate should not be allowed to be selected in the GUI.
558004	FortiAuthenticator built-in redirect page allows manual entry of page title and unformatted text content.
603112	Leaving form with unsaved data often leads to error 404.
696756	Revisit authentication labels tagged with the keyword "RADIUS".
715189	18120 should not be allowed in the Authentication port.
730038	Improve the SNMP GUI.
694409	User Registration Receipt Email Message in Authentication > Portals > Replacement Messages needs formatting.
723335	Updating the common name in a remote sync rule does not update the FortiAuthenticator user cert binding common name on subsequent synchronizations.
731869	Libxml2 2.9.11 security fixes - Precaution upgrade.
729487	Unable to edit secondary cluster member's HA settings.
691101	MAC device belonging to user setting resets to no user after updating it from API.
736016	Internal server error in the self-service portal remote RADIUS user profile.
730435	Unable to import remote users from the remote LDAP server page.
735314	Imported remote LDAP users do not appear in the remote LDAP users section until the page is refreshed.
730421	500 internal server error when using the test filter in a remote user sync rule.
606406	Switch SAML SP Azure APIs to use Microsoft Graph instead of the Azure Active Directory graph.
706122	REST API rate limit feature does not distinguish between users with the same username but different realms.
732033	Remote admin users should be able to log in to FortiAuthenticator without prefixing their realms.
732106	Unable to make any changes to user information in self-service portal 500 error.
731137	email_admin FortiAuthenticator login and CLI issues.
732101	Two cancel buttons on Force Password Change page.
733370	Revoking user certificate creates a blank dialog.
725883	Unable to edit security questions through the legacy self-service portal.
672526	Admin profile for "Maintenance" can disable admins and regular users.

Bug ID	Description
731299	New Fortinet RADIUS VSA for FortiPortal (Fortinet-Fpc-Tenant-User-Sites) 42.
581283	Crash when using too many diacritic characters in the name field.
603854	User can exceed the limited amount of MAC devices created per user.
692053	TACACS import clients from GUI need to be more robust.
640222	Remote LDAP sync rules should not be able to sync usernames with special characters as admins.
672524	Admin profile for "Portals" cannot access the help button.
690990	The cancel button on the user page for LDAP Remote Authentication should close the dialog.
704895	FortiAuthenticator allows invalid group assignment when importing users via CSV file.
718365	HA Cluster not able to access management port IP address.
700474	SAML user filter does not work.
696078	SAML "Remote user sync rule" overwrites manually entered user information even when the imported data is blank.
660939	Test token code is missing the username in the email sent out.
606911	Adding a permission set through the user page does not appear until the page is refreshed.
665571	Relabel 'Ha' to 'HA' in the HA Settings page.
719599	Restrict number of API requests should not be able to have empty value.
723938	Remote user sync rule GUI logs show failed message even though user successfully syncs.
694569	Purge disabled users feature does not work.
718647	FortiBootloader firmware upgrade to 6.1.0 and later.
735090	RADIUS proxy setup fails when the push notification is enabled on remote RADIUS.
736675	RADIUS crashes if it receives a RADIUS packet with State=1, but the user is not previously authenticated.
732203	FortiAuthenticator 400E: failed to activate the FortiToken mobile license.

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
730474	FortiAuthenticator IdP proxy fails to proxy SAML assertions received from remote IdP when user attribute with same name exists.
733788	FortiAuthenticator Agent does not support UPN username format (as imported to the FortiAuthenticator).
665384	HA failover does not work reliably.
711940	Raid widget is showing wrong status.
566145	Usage Profile "TIME USAGE=Time used" is not triggering COA or disconnect request to FortiGate.
730640	When signing a CSR via SCEP, FortiAuthenticator returns "Unable to sign request, Unable to find a unique name".
737921	6.3.2 HTTP GUI service disabled produces a 403 for IdP metadata URL.
737078	Private IPv6 address added to SSO list instead of public IPv6 when received from a RADIUS accounting source.
735782	Alcatel RADIUS VSA dictionary needs to be updated.
731626	Limit of 64 characters in SAN DNS field for CSR/Certificate creation.
737727	Change in the password complexity rule is not taking effect.
721189	SMS : No update on number of sent messages on the dashboard.
729674	FortiToken mobile license status on LB nodes shows Unknown.
676532	When FortiAuthenticator has a RADIUS client set as subnet, RADIUS accounting disconnect messages are not sent.
711721	Groups sorting differences when importing LDAP groups in SSO Groups and FortiGate filtering.
712251	Column resize or sort does not work properly in tables of FortiAuthenticator.
712899	SMTP error messages does not provide accurate information.
723825	LDAP with G Suite sometime requires trusting multiple CA certificates.
723065	HA Connection status still shows connected even when the primary FortiAuthenticator is already shutdown.
736980	FortiToken mobile activation code not sent or wrong credentials when authentication activity exceeds 14 per minute.
646764	CLI "get disk *" commands fail on KVM.
733585	No log for policy priority change.

Bug ID	Description
735652	LB HA: Unnecessary deletion on load-balancer causes really long resync delays.
620127	Changing from maint-mode-no-sync to maint-mode-sync does not appear to restore syncing.
677932	SCEP returns 200 on bad requests.
506543	[500k+ users] Secondary's SNMP SQL query to obtain user count is obnoxiously slow (postgres needs vacuum full).
706422	LB should not delete certificates if they are used by config_setting table but not synced.
731442	Remote RADIUS case sensitive does not work well.
734462	Extraneous "No search results" message appears under RADIUS Attributes section in user group page.
579174	FortiToken mobile for a remote radius user on the FortiAuthenticator server and also on the FortiAuthenticator client fails to work.
506112	This post REST API call fails to activate the FortiGuard messaging license.
733073	Forgot password token verification email has misleading title and description.
731214	500 Internal server error when end user has duplicate certificate bindings.
736017	Revoked FIDO token should display time in local time and not UTC.
734034	Unable to see MAC devices limit in Portals settings for Firefox.
736652	HOTP token out of sync is always allowed in to self-service portal.
737638	Missing username in Oauth Request causes 500 server error.
734892	FIDO pop-up message when saving user local information.
712166	SCEP gives wrong validation message if "Renewal Days" expiry is left empty.
613164	G suite open LDAP crashes when we try to change password.
736062	PCI enabled FIDO authentication portal does not work with a FIDO user.
734474	LDAP users are able to enable security question through Self-service portal without actually setting a security question.
706998	GUI crashes during password recovery using Email address method if the Email is not associated with any user account.
737640	Sync rule with multiple OTP assignment methods fails to sync users over if they are missing any one of the LDAP attributes.
732406	Editing security question results in duplicate UI in pop-up.
736670	api/v1/ssoauth/ API request returns 500 internal error occassionally.
734475	"Internal Server Error" when local user enables security question without setting the security question through captive portal.
736020	"None" option for token assignment missing in self-service portal MFA page.

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 (NAS devices) that can authenticate to the system is:

100 / 10 = 10

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.

www.fortinet.com