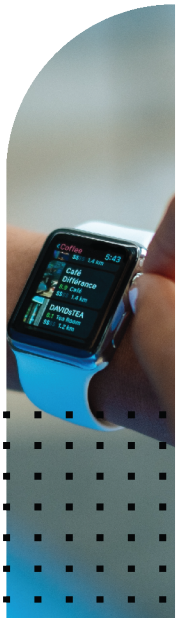
# Release Notes

## FortiAuthenticator 6.4.5



**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

**FORTINET TRAINING 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

June 29, 2023
FortiAuthenticator 6.4.5 Release Notes
23-645-834316-20230629

# TABLE OF CONTENTS

# Change log

| Date | Change Description |
|---|---|
| 2022-08-23 | Initial release. |
| 2022-08-25 | Added Accessing the Captive portals page to Special notices on page 6. |
| 2022-08-30 | Added bug 838043 to Known issues on page 19. |
| 2022-09-01 | Updated Maximum values for VM on page 25 and Maximum values for hardware appliances on page 21. |
| 2022-09-02 | Updated Upgrade instructions on page 8. |
| 2022-09-12 | Added bug 837679 to Known issues on page 19 and updated Upgrade instructions on page 8. |
| 2022-09-13 | Updated Upgrade instructions on page 8. |
| 2022-09-16 | Added bug 829271 to Resolved issues on page 16. |
| 2023-05-12 | Updated Upgrade instructions on page 8. |
| 2023-06-29 | Updated Known issues on page 19. |

# FortiAuthenticator 6.4.5 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.4.5, build 1040.

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.

## Accessing the Captive portals page

Due to an issue, the *Captive portals* page is only accessible if you go to `https://[FAC-IP]/admin/guest/captiveportalpolicy/` in the browser.

# What's new

FortiAuthenticator version 6.4.5 includes the following enhancement:

## FSSO: Zero trust tunnel related improvements

When a remote LDAP server is configured with zero trust tunnel enabled, FSSO communications to the AD servers go through a zero trust tunnel, including:

- LDAP binds/queries for domain servers auto-discovery
- LDAP binds/queries for group lookups

FortiAuthenticator now accepts DC agent connections over TLS. In **Fortinet SSO Methods > SSO > General**, **Require authentication for TS agents (disables DC agent support)** in **Enable DC/TS Agent Clients** has been renamed to **Require encryption for DC/TS agents**.

FortiAuthenticator now offers a server-side TLS support option so that FortiGate as an FSSO client can be configured to connect to FortiAuthenticator over a TLS connection.

A new **Enable encryption** toggle in the FortiGate pane in **Fortinet SSO Methods > SSO > General**.

## SAML SP/IdP Proxy: Enforce MFA

FortiAuthenticator can now enforce MFA on remote SAML IdP servers.

FortiAuthenticator now offers a new **MFA (https://refeds.org/profile/mfa)** authentication context value when creating or editing a remote SAML authentication server in **Authentication > Remote Auth. Servers > SAML**.

## Remote authentication: Restrict authentication to only imported user accounts

When configuring a realm in **Authentication > User Management > Realms**, FortiAuthenticator now offers a new **Restrict authentication to imported user account only** option to enable/disable authentication of remote users without an imported account on FortiAuthenticator.

# 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 6.4.5 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**


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 6.4.5 build 1040 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 6.4.5, 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 6.4.5 directly.
- If currently running FortiAuthenticator between 6.1.0 and 6.2.0, first upgrade to 6.3.3, then upgrade to 6.4.5.
- If currently running FortiAuthenticator 6.2.1 or later, then upgrade to 6.4.5 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.4.5 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 11.

Upgrade to and from FortiAuthenticator 6.0.6 is not recommended.

- After an upgrade to FortiAuthenticator 6.4.5, *Encryption enabled* option in *Fortinet SSO Methods* > *SSO* > *General* is enabled by default. If you have an existing setup with FSSO enabled, this encrypts all the SSO requests from FortiAuthenticator, leading to FSSO setup failure.

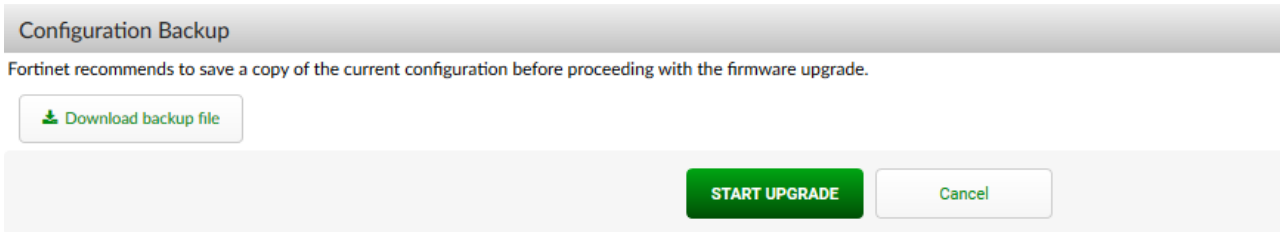
  **Workaround**: After upgrading to FortiAuthenticator 6.4.5, disable the *Encryption enabled* option in *Fortinet SSO Methods* > *SSO* > *General*.
- After an upgrade to FortiAuthenticator 6.4.5, FortiAuthenticator enforces stricter validation on the SSOMA connections. However, not all currently deployed SSOMAs support this stricter enforcement. If your deployment includes SSOMAs, it is therefore not recommended to upgrade to FortiAuthenticator 6.4.5. As of now, FortiClient 5.4.4 (Single Sign-On Mobility Agent) and above do not present client certificates to FortiAuthenticator.

## 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 6.4.5, 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 6.4.5

## 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 6.4.5:

- Microsoft Edge version 105
- Mozilla Firefox version 103
- Google Chrome version 104

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

## FortiOS support

FortiAuthenticator 6.4.5 supports the following FortiOS versions:

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

## Fortinet agent support

FortiAuthenticator 6.4.5 supports the following Fortinet Agents:

- FortiClient v.6.x , v.7.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 6.4.5 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 15 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 |
|---|---|
| **824479** | Usage profile schedule radio button selection is not applied properly. |
| **827234** | SMTP account username and password accepts more than 64 characters but does not save. |
| **823476** | User certificate binding status is blank if there are two certificate with same CN. |
| **828722** | `/api/v1/oauth/token/` gives 500 error. |
| **815465** | `Download failed` message in Automatic CRL download. |
| **827874** | LDAP User Sync Rule *Test Filter* mapping preview does not use its own Base distinguished name for user lookup. |
| **812240** | Only the first 5 admin trusted subnets are effective. |
| **819307** | Cluster Primary IP changes in the LB node after HA primary reboot. |
| **816686** | After upgrading FortiAuthenticator to 6.4.4, authentication via FortiAuthenticator Agents fails. |
| **820256** | Admin profile resets to 'Full permission ' when the remote user sync rule has user role set as 'Administrator'. |
| **827716** | Changes on syslog server configuration on FortiAuthenticator fails with an internal server error 500. |
| **811368** | Remote user sync rule not binding all the certificates to users. |
| **815459** | `/oauth/verify_token/` endpoint returns 500 server error for remote users. |
| **822273** | *User Inventory* widget is not loading. |
| **824664** | Exporting 100K+ LDAP users in FortiAuthenticator fails and shows an empty file. |
| **786610** | FortiClient session SSL connection fails. |
| **819028** | FortiAuthenticator IdP login returns a JS error. |
| **818109** | LDAPS connections using 'All Trusted CAs' fail for FSSO/Domain Manager. |
| **814826** | 500 Internal Server Error in SAML authentication after multiple wrong password entries with Fido tokens enabled. |
| **685172** | FortiAuthenticator A-P running in v6.2.1 do not sync with the secondary unit Pre-authentication warning message, CLI, and GUI Timeout. |
| **758516** | FortiAuthenticator HA: cluster out of sync if custom radius dictionary is uploaded; authentication breaks. |
| **831595** | CLI - Setting timezone and DNS does not clear GUI settings cache. |
| **826685** | Optimize middleware used in FortiAuthenticator. |

| Bug ID | Description |
|---|---|
| **817100** | LB optimizations for bulk Change log updates. |
| **769183** | FortiAuthenticator VMs need greater resiliency / improved recovery when connectivity lost to remote data drives. |
| **818813** | Memory leak in `fac_comm ssl` with client cert. |
| **810069** | IdP initiated SAML response replay attack. |
| **818129** | 'Deny' from Push response should count towards invalid attempt for lockout. |
| **820671** | FortiAuthenticator Cloud should allow admin to enter Client Application Name for including in the Push payload. |
| **820659** | Default Client Application Name is the IdP name instead of the SP name. |
| **820579** | Remove step in configuring OTP. |
| **818581** | Hide the captive portal options requiring RADIUS support. |
| **830002** | XSS observed in the password reset done page. |
| **800714** | [3rd party component upgrade required for security reasons] FortiAuthenticator - openLDAP to 2.6.2. |
| **814167** | [3rd party component upgrade required for security reasons] FortiAuthenticator - libxml2 to 2.9.14. |
| **824885** | [3rd party component upgrade required for security reasons] FortiAuthenticator - curl to 7.84. |
| **831387** | Admin user `OK` button is disabled after editing security question. |
| **833199** | JavaScript error when accessing Fine-grained Controls local groups. |
| **833195** | JavaScript error when trying to import a Trusted CA. |
| **806472** | [FortiAuthenticator Cloud] Creating a `webservice` key for an admin account on the FortiAuthenticator Cloud is failing; receive '`wrong peer certificate error`'. |
| **832127** | SAML IdP enable portal button is not working properly. |
| **832110** | FortiAuthenticator FQDN/public IP is not working when setting up via GUI until restarted. |
| **824140** | Learn Trusted CA feature not working. |
| **824930** | Read-only admin profiles giving 403 error when accessing a few pages. |
| **813844** | SYN packet sent outside the zero trust tunnel when creating a remote LDAP server with zero trust tunnel. |
| **808982** | [FortiAuthenticator Cloud] *Allow LDAP browsing* should be hidden when editing a user. |
| **808979** | [FortiAuthenticator Cloud] *Allow Radius authentication* should be hidden when editing a user. |
| **804843** | [FortiAuthenticator Cloud] 'TACACS+' role option should be hidden when editing a local user. |
| **802750** | [FortiAuthenticator Cloud] second in the back schedule is not taking effect. |
| **813148** | [FortiAuthenticator Cloud] Role selection options should be removed from admin user page. |
| **816176** | Renaming a Portal back to its original name fails, then triggers 500 error on self-service portal user login. |

| Bug ID | Description |
|---|---|
| **818620** | SAML IdP login with IAM user causes radiusd crash. |
| **818081** | [FortiAuthenticator Cloud] Full-Permission option for Admin account reverts to No-Access after logging out and back in. |
| **818176** | [FortiAuthenticator Cloud] Unable to assign any admin profile or full admin permission to a sub account. |
| **818179** | [FortiAuthenticator Cloud] 400 error for any admin account login (primary and sub account) after deleting No-Access Administrator admin profile. |
| **828130** | Attribute `msDS-SupportedEncryptionTypes` is set to `0x1F` which includes DES. |
| **810530** | FortiAuthenticator FSSO user capacity in GUI on FortiAuthenticator 3000D is incorrect. |
| **817715** | [FortiAuthenticator Cloud] Admins included in the user quota calculation. |
| **806544** | FortiAuthenticator - HA halts at 'Forming Cluster'. |
| **827303** | ZTT: Eliminate WAD inconsistency between first & subsequent connections. |
| **829271** | Remote syslog fails when using Secure connection on remote Syslog servers. |

# 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 |
|---|---|
| **566145** | Usage Profile `'TIME USAGE=Time used'` is not triggering COA or disconnect request to FortiGate. |
| **638374** | SCEP - Encryption/hash compatibility with clients. |
| **655350** | The lockout policy does not appear to apply to username/token submissions to the /auth API endpoint. |
| **676532** | When FortiAuthenticator has a RADIUS client set as subnet, RADIUS Accounting Disconnect messages are not sent. |
| **676985** | Unable to import all FTK hardware tokens from the same purchase order; need to add them all manually. |
| **680776** | AP HA secondary cannot change `mgmt` interface access configuration, and the option does not sync from the primary either. |
| **743775** | SCEP Get CA requests intermittently fails under High Scep Load. |
| **750134** | FortiAuthenticator as an LDAP server cannot export admin users from the local user base. |
| **751108** | FortiAuthenticator does not support admin OIDs from FORTINET-CORE-MIB properly. |
| **757460** | Enable Django auto-translation for any end-user page. |
| **767745** | SNMP `facSysCpuUsage` returns wrong type. |
| **767935** | A-P cluster, it forms when configured from the GUI, it does not when configured from the CLI without a restart. |
| **773020** | Revoking of certificate is not being seen with OCSP until FortiAuthenticator reboots. |
| **787013** | Changing the username attribute will cause the remote sync rule to remove existing remote users and eventually reimport them. |
| **787156** | FortiAuthenticator 6.4.1 GA OIDC HTTP Error 500. |
| **791127** | Sometimes(randomly) FortiAuthenticator fails to send email notification. |
| **791347** | Internal server error 500 happens when viewing RADIUS account sessions, probably caused by the `Called-Station-Id` attribute. |
| **795271** | E-mail address does not appear in the logs after social login authentication. |
| **796493** | LDAPS connectivity issue between FortiGate/FortiManager and FortiAuthenticator. |
| **796834** | Captive portal loops between `/portal/server?`, `200 OK` to `/portal/login/server? 302 OK back to /portal/server?` on Chrome browsers. |
| **799768** | Automatic CRL download error with 2 Identical DN. |
| **800674** | Remote sync rule does not automatically apply FortiToken logo to remote SAML users. |

| Bug ID | Description |
|---|---|
| **801009** | Remote SAML user sync rule creates one log entry for every SAML user assgined FortiToken Mobile every time the SAML sync occurs. |
| **801933** | FortiAuthenticator as an LDAP server, logs shows LDAP_FAC in the 'Source IP' field. |
| **804238** | FortiAuthenticator 6.4.1 GA SAML Logout fails. |
| **805969** | FortiAuthenticator supports Zero Trust tunnels to multiple remote LDAP servers through one FortiGate only. |
| **808748** | Self-service portal password change fails for remote LDAP users if the UPN format is used. |
| **809353** | Country code selection for guest portal user registration on iOS selects incorrect country prefix. |
| **815000** | TACACS consuming CPU resources 100% with zero connections. |
| **815280** | TACACS debug logs stop to works. |
| **815896** | FortiAuthenticator does not log an error when it cannot communicate to an external SMS provider due to invalid or expired certificate. |
| **815897** | Unable to import LDAP user from GUI by using IBM Lotus Domino LDAP. |
| **816070** | DB issue if power down during a short window when booting from factory reset. |
| **820035** | After changing the FortiAuthenticator IP address, unplugging the monitor interface did not trigger the HA failover. |
| **825665** | Wrong client IPv4 attribute for *Fortinet SSO Methods* > *SSO* > *RADIUS Accounting Sources*. |
| **826424** | Registering an already existing username on Legacy Self-serve Portal triggers 500 error. |
| **828570** | FSSO session for TS agent not logged when user and machine are in different domains. |
| **829318** | 'Users and Devices' permission set does not allow to import remote LDAP users. |
| **830386** | 'Users Audit Report' does not update timestamps in the *Last Used* column for EAP-TLS authentication used for Wireless. |
| **830884** | Username is not populated in Logs, when changes are done via API in FortiAuthenticator. |
| **837679** | Upgrade to FortiAuthenticator 6.4.5 causes SSOMA connection failure. |
| **838043** | After an upgrade to FortiAuthenticator 6.4.5, *Encryption enabled* option in *Fortinet SSO Methods* > *SSO* > *General* is enabled by default. If you have an existing setup with FSSO enabled, this encrypts all the SSO requests from FortiAuthenticator, leading to FSSO setup failure.<br>**Workaround:** After upgrading to FortiAuthenticator 6.4.5, disable the *Encryption enabled* option in *Fortinet SSO Methods* > *SSO* > *General*. |

# 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.

Similar to the FortiAuthenticator-VM, the FortiAuthenticator hardware appliances permit stacking licenses.

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

| Feature | Model | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 200E | 300F | 400E | 800F | 1000D | 2000E | 3000E | 3000F |
| **Users** (Local + Remote)[1] | 500 | 1500/3500* | 2000 | 8000/18000* | 10000 | 20000 | 40000 | 40000/240000* |
| User RADIUS Attributes | 1500 | 4500 | 6000 | 24000 | 30000 | 60000 | 120000 | 120000 |
| User Groups | 50 | 150 | 200 | 800 | 1000 | 2000 | 4000 | 4000 |
| Group RADIUS Attributes | 150 | 450 | 150 | 2400 | 600 | 6000 | 12000 | 12000 |
| FortiTokens | 1000 | 3000 | 4000 | 16000 | 20000 | 40000 | 80000 | 80000 |
| FortiToken Mobile Licenses[2] | 200 | 200 | 200 | 200 | 200 | 200 | 200 | 200 |
| LDAP Entries | 1000 | 3000 | 4000 | 16000 | 20000 | 40000 | 80000 | 80000 |
| Device (MAC-based Auth.) | 2500 | 7500 | 10000 | 40000 | 50000 | 100000 | 200000 | 200000 |
| RADIUS Client Profiles | 500 | 1500 | 2000 | 8000 | 10000 | 20000 | 40000 | 40000 |
| Remote LDAP Users Sync Rule | 50 | 150 | 200 | 800 | 1000 | 2000 | 4000 | 4000 |
| Remote LDAP User Radius Attributes | 1500 | 4500 | 6000 | 24000 | 30000 | 60000 | 120000 | 120000 |

| Feature | | Model | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 200E | 300F | 400E | 800F | 1000D | 2000E | 3000E | 3000F |
| Remote authentication servers | Remote LDAP Servers | 20 | 60 | 80 | 320 | 400 | 800 | 1600 | 1600 |
| | Remote RADIUS Servers | 20 | 60 | 80 | 320 | 400 | 800 | 1600 | 1600 |
| | Remote SAML Servers | 20 | 60 | 80 | 320 | 400 | 800 | 1600 | 1600 |
| | Remote OAuth Servers | 20 | 60 | 80 | 320 | 400 | 800 | 1600 | 1600 |
| **FSSO & Dynamic Policies** | | | | | | | | | |
| FSSO | FSSO Users | 500 | 1500 | 2000 | 8000 | 10000 | 20000 | 200000[3] | 200000 |
| | FSSO Groups | 250 | 750 | 1000 | 4000 | 5000 | 10000 | 20000 | 20000 |
| | Domain Controllers | 10 | 15 | 20 | 80 | 100 | 200 | 400 | 400 |
| | RADIUS Accounting SSO Clients | 166 | 500 | 666 | 2666 | 3333 | 6666 | 13333 | 13333 |
| | FortiGate Services | 50 | 150 | 200 | 800 | 1000 | 2000 | 4000 | 4000 |
| | FortiGate Group Filtering | 250 | 750 | 1000 | 4000 | 5000 | 10000 | 20000 | 20000 |
| | FSSO Tier Nodes | 5 | 15 | 20 | 80 | 100 | 200 | 400 | 400 |
| | IP Filtering Rules | 250 | 750 | 1000 | 4000 | 5000 | 10000 | 20000 | 20000 |

| Feature | | Model | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 200E | 300F | 400E | 800F | 1000D | 2000E | 3000E | 3000F |
| Accounting Proxy | Sources | 500 | 1500 | 2000 | 8000 | 10000 | 20000 | 40000 | 40000 |
| | Destinations | 25 | 75 | 100 | 400 | 500 | 1000 | 2000 | 2000 |
| | Rulesets | 25 | 75 | 100 | 400 | 500 | 1000 | 2000 | 2000 |
| **Certificates** | | | | | | | | | |
| User Certificates | User Certificates | 2500 | 7500 | 10000 | 40000 | 50000 | 100000 | 200000 | 200000 |
| | Server Certificates | 50 | 150 | 200 | 800 | 1000 | 2000 | 4000 | 40000 |
| Certificate Authorities | CA Certificates | 10 | 10 | 10 | 50 | 50 | 50 | 50 | 50 |
| | Trusted CA Certificates | 200 | 200 | 200 | 200 | 200 | 200 | 200 | 200 |
| | Certificate Revocation Lists | 200 | 200 | 200 | 200 | 200 | 200 | 200 | 200 |
| SCEP | Enrollment Requests | 2500 | 7500 | 10000 | 40000 | 50000 | 100000 | 200000 | 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.

* Upper limit

# 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 |
| Remote authentication servers | Authentication Policy (RADIUS and TACACS+) | 6 | Users | 100 | 5000 |
| | Remote LDAP Servers | 4 | Users / 25 | 4 | 200 |
| | Remote RADIUS Servers | 1 | Users / 25 | 4 | 200 |
| | Remote SAML Servers | 1 | Users / 25 | 4 | 200 |
| | Remote OAuth Servers | 1 | Users / 25 | 4 | 200 |
| User Management | **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 Users Sync Rule | 1 | Users / 10 | 10 | 500 |
| | Remote LDAP User Radius Attributes | 15 | Users x 3 | 300 | 15000 |
| | Realms | 2 | Users / 25 | 4 | 200 |
| **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