Release Notes

FortiAuthenticator 6.5.1

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

August 29, 2023
FortiAuthenticator 6.5.1 Release Notes
23-651-892074-20230829

TABLE OF CONTENTS

Change log

Date	Change Description
2023-03-12	Initial release.
2023-03-13	Updated Upgrade instructions on page 8.
2023-03-16	Removed bug 871196 from Known issues on page 17.
2023-04-05	Updated Upgrading from 4.x/5.x/6.x on page 9. Added bugs 899505 and 900916 to Known issues on page 17.
2023-05-12	Updated Hardware and VM support on page 8.
2023-06-29	Updated Known issues on page 17.
2023-08-01	Added bug 900550 to Known issues on page 17.
2023-08-29	Updated Upgrading from 4.x/5.x/6.x on page 9.

FortiAuthenticator 6.5.1 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.5.1, build 1295.

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 6.5.1 is a patch release. There are no new features. See Resolved issues on page 15 and Known issues on page 17 for more information.

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.

FortiAuthenticator 6.5.1 requires at least 4GB of RAM.

- Hardware and VM support on page 8
- Image checksums on page 8
- Upgrading from 4.x/5.x/6.x on page 9

Hardware and VM support

FortiAuthenticator 6.5.1 supports:

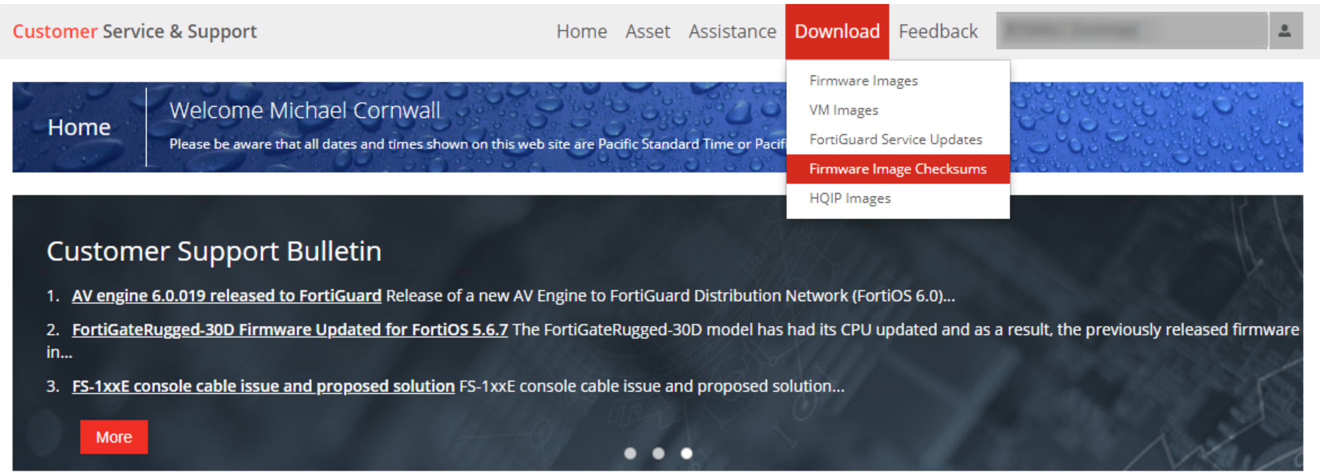
- FortiAuthenticator 200E
- FortiAuthenticator 300F
- FortiAuthenticator 400E
- FortiAuthenticator 800F
- FortiAuthenticator 2000E
- FortiAuthenticator 3000E
- FortiAuthenticator 3000F
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, Azure, AWS, Oracle OCI, and Alibaba Cloud)

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 4.x/5.x/6.x

FortiToken Mobile/Cloud provisioning is broken (bug ID 899505 in Known issues on page 17) for FortiAuthenticator 200E/400E/3000E in this firmware release. If you are using 2FA with these models, it is therefore not recommended to upgrade to FortiAuthenticator 6.5.1.

FortiAuthenticator 6.5.1 build 1295 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 6.5.1, 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 6.5.1 directly.
- If currently running FortiAuthenticator between 6.1.0 and 6.2.0, first upgrade to 6.3.3, then upgrade to 6.5.1.
- If currently running FortiAuthenticator 6.2.1 or later, then upgrade to 6.5.1 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.5.1 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.

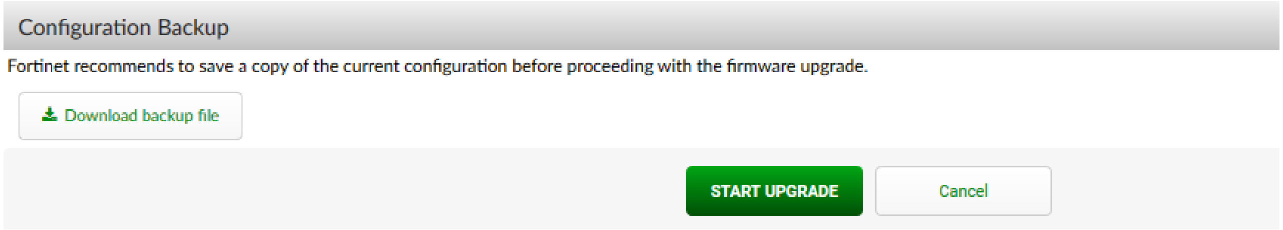
Ensure the hypervisor provides at least 4GB of memory to the FortiAuthenticator-VM.

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 6.5.1, 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 6.5.1

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

FortiAuthenticator supports the following:

- Web browser support on page 12
- FortiOS support on page 12
- Fortinet agent support on page 12
- Virtualization software support on page 13
- Third-party RADIUS authentication on page 13

Web browser support

The following web browsers are supported by FortiAuthenticator6.5.1:

- Microsoft Edge version 110
- Mozilla Firefox version 109
- Google Chrome version 110

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

FortiOS support

FortiAuthenticator6.5.1 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 6.5.1 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

FortiAuthenticator6.5.1 supports:

- VMware ESXi / ESX 6/7/8
- 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 14 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
875536	User account extension gives `CSRF token missing or incorrect`.
884050	Unable to establish ZTNA connection for LDAP.
869560	A-P, SNMP/Syslog updates do not take effect on the passive node when HA is started from the CLI. Reboot may fix it.
884397	After upgrading FortiAuthenticator to 6.5.0, the SAML POST will receive a `CSRF cookie not set` or `CSRF token missing or incorrect` (HTTP 403).
888780	FortiToken Cloud status error when returning too many users from the FortiToken Cloud server.
887546	IP lockout policy does not work on FortiAuthenticator 3000E.
886590	OAuth authentication breaks after an upgrade.
886978	`REST_API` CLI debug not enabled.
884774	`db_mond` crashes if clients come and go immediately.
890248	`db_mond` log output.
889518	FortiAuthenticator sends a FIN packet to the mail server after a successful TCP handshake.
878986	Maximum FortiGate session number reached; unable to accept a new connection.
886587	Upgrading FortiAuthenticator previously downgraded from 6.4+ to pre-6.4 back to 6.5.0 causes factory reset.
888939	Direct upgrade of HA-LB cluster from 6.0.7 to 6.5.0 fails.
885149	`pushd` randomly crashes.
882044	`JS Uncaught` type error on the *SSO > Windows Event Log Source* page.
883829	Page not found or unreachable showing when updating the ZTNA tunnel setting if the ZTNA entry is being used.
887276	SAML IdP breaks after upgrading from 6.0.2 - 6.0.7 - 6.4.6/6.5.0.
886152	LB - Sync MAC devices linked with a sync'ed user and the ones which are not linked to any user.
885476	Tabs are being replaced with `#011` in TACACS+ logs and potentially other places using syslog for centralized logging.
855618	Unable to delete local user accounts in the Safari browser.
866709	Admin password recheck issues.
883323	Removing and readding an OAuth portal with the same name will cause Error 500.

Bug ID	Description
886094	`push` REST API timeout log fix.
873972	Single group is passed by FortiAuthenticator as IdP when FIDO only authentication is used in SP setting.

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.
576931	Admin logout GUI glitch.
603105	LDAP user import uses server IP from DB despite browser using/showing unsaved one.
619259	'Export key and Certificate' option should be grayed out for an intermediate CA whose root uses HSM.
620127	Changing from `maint-mode-no-sync` to `maint-mode-sync` does not appear to restore syncing.
637028	SSL connection failed in case of an expired certificate issue is not explicit enough.
643810	`restore-admin` CLI command needs improvement.
680776	AP HA secondary cannot change the `mgmt` interface access configuration, and the option does not sync from primary either.
741765	REST API `/api/v1/tacpluspolicyclient/` endpoint does not recognize `policy_name` or `client_name` parameters.
743775	SCEP Get CA requests intermittently fail under high SCEP load.
751108	FortiAuthenticator does not support admin OIDs from `FORTINET-CORE-MIB` properly.
756414	Incorrect Italian translation of *Next* button displayed on the reset password page.
766453	Check the reason for FortiAuthenticator 400E auto reboot.
775026	Sponsor is able to edit static routing settings.
776247	Importing guest users via CSV does not add them to newly created user groups.
781832	Token bypass not working for FIDO enabled self-service portal,
787855	Single sign-on for one FortiAuthenticator as password and another as OTP not working as intended.
801933	FortiAuthenticator as LDAP server; logs shows `LDAP_FAC` in the *Source IP* field.
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 UPN format is used.
814255	Custom RADIUS attributes disappear on HA secondary after failover and we get 500 crash when clicking into RADIUS policy.
835267	Narrowing the browser window causes GUI elements to overlap.
835564	Narrow browser size to the smallest window size will cause all UI element to overlap display.

Bug ID	Description
837728	Local services cannot use cert with >97 character subject length.
837791	TACACS+ authentication fails when the authentication process takes long.
838850	Portal Policy on the Firefox web browser boxes not aligned properly.
838976	Windows log events in FSSO are dropping after some time.
841996	*Back* button in the user lookup page does not navigate back to the original user list page.
842886	Upgrading FortiAuthenticator in HA-LB removes the MAC-address records form the LB node.
843334	KVM model does not obey hypervisor soft restart/shutdown commands.
847399	Resizing the window causes GUI fields to overlap in *Logs* page.
848434	Usability of *User Group* GUI.
850023	HA Cluster not forming due to differing smartconnect primary key name (upgrade path mismatch, but should work).
850906	If the user has only an email token for it's second factor authentication, and the portal has *Allow users to temporarily use email token authentication if an email was pre-configured* enabled under *Fortitoken Revocation*, the user should not be able to use *Switch to email token authentication*.
854050	t takes a long time for FortiAuthenticator to reflect active certificates in the GUI after successful SCEP enrollment request.
857399	FortiAuthenticator fails to send out COA disconnect to FortiGate.
858383	NTLM authentication failure under load.
861027	RADIUS attribute name should be only unique within the dictionary, not across all dictionaries.
861112	NTLM authentication does not work with child domain.
861557	FortiAuthenticator remote user sync rules - Set Group Filter not working if OU has special characters in name, e.g., `( , ) , +`.
861611	Smart Connect for Android running on version 12 and 13 never installed the configuration profile.
862394	In FortiAuthenticator CLI, a user can change DNS addresses even if we assign `No-Access/Read-only` admin profile.
863635	FIDO users status bug on SAML.
864201	Updating the image variable in SAML IdP replacement HTML editor could trigger 500 error.
865372	FortiNAC can overwhelm FortiAuthenticator with many TACACS+ logins on the same service account.
866392	FortiAuthenticator GUI/captive portal access freezes/become unresponsive during peak hours.
866686	JavaScript error when using the filter button on local users page.
866700	*Sign in as a different user* does not work on a proxy setup in SAML.
867289	FortiAuthenticator drops FSSO events with `work queue full, dropping logon` error.

Bug ID	Description
868659	Change *Western Sahara* to *Morocco (Southern Provinces)* in the phone number country code.
868810	FortiAuthenticator HA device with low priority stays primary.
868829	IP lockout not being logged in on FortiAuthenticator logs.
869768	Unable to delete a user group.
870097	Machine authentication cache expiry.
872573	Enable CSP on user pages.
872920	Portal policy realms table values are in the wrong column.
873050	403 Forbidden error while doing SAML authentication after OAuth succeeds.
874256	Failed FIDO token authentication and reauthentication FIDO token using SP SAML portal causes error occurred.
874285	Unable to use FortiAuthenticator images in System replacement messages.
874293	FortiAuthenticator picks the incorrect IP from proxied requests from the header when multiple headers are used in a request.
876009	FortiAuthenticator ignores the groups filtering rules and sends all SSO groups to FortiGate if the FortiGate is configured with FQDN.
877745	Javascript errors being thrown by all(?) search filters.
877815	SAML IdP's IAM button should not be displayed if the SAML IdP portal is disabled.
877819	JavaScript error when enabling SSO on legacy self service portal.
878665	500 error when launching a Smart Connect profile that contains a CSR for Android.
878673	Certificate GUI filter by status times out when there are thousands of revoked certificates.
878828	After a reboot, FortiAuthenticator shows 500 Internal Server Error when synchronizing hardware tokens.
878854	Some users fail to authenticate through SSL VPN.
879091	Upgrade from 6.3.3 to 6.5.0 gives error in `wad-service` logs.
879570	*Select All* checkbox for Remote user sync rule does not select all the rules in Firefox without private window.
879613	HA boots into unstable state when cluster peer is not found.
881135	Javascript error when changing FortiAuthenticator GUI log history period.
881296	SNMP v3 with non-ENG letter pass gives authentication failed.
882098	FortiAuthenticator HA is out of sync and web server crashes when clicking on *Packet Capture* with 500 Internal server error.
882489	Error in logs for FTM authentication with `mschapv2`.
884299	HA Load balancer node is not synchronizing.

Bug ID	Description
884316	SAML IdP Login Success Page: last login information not shown when the previous IdP session was cleared.
884713	500 error when accessing SAML IdP with `http`.
884902	Unable to import 10k plus groups from Azure via SAML in FortiAuthenticator.
887081	SAML: Launching SP-initiated SAML session for a user with FIDO AUTH produces server errors.
887135	Admin password recheck popup should have a *Cancel* button.
887645	Content security policy errors when trying to create new FTMs.
887938	Read-only profile page does not show the correct information.
889196	SAML sync rule groups input should be disabled when no server is selected.
889706	FortiAuthenticator Remote user sync rules - Test filter not working if OU has special characters in name, e.g., `( , ) , +`.
890725	SAML token-only login displays password page instead of the token page.
890922	Login page not found after successful user registration.
899505	Unable to provision FortiToken Mobiles on FortiAuthenticator 200E/400E/3000E in 6.5.0/6.5.1.
900916	WAD-enforced administrator/service access rules are only applied to the first four interfaces. The rest is still handled in Python.
900550	2FA codes via SMS is not working.

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	2000E	3000E	3000F
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	1015	2015	2015
	Language Files	50	50	50	50	50	50	50
Realms		20	60	80	320	800	1600	1600
Authentication								
General	Auth Clients (NAS)	166	500	666	2666	6666	13333	13333

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

Feature		Model						
		200E	300F	400E	800F	2000E	3000E	3000F
Remote authentication servers	Remote LDAP Servers	20	60	80	320	800	1600	1600
	Remote RADIUS Servers	20	60	80	320	800	1600	1600
	Remote SAML Servers	20	60	80	320	800	1600	1600
	Remote OAuth Servers	20	60	80	320	800	1600	1600
FSSO & Dynamic Policies								
FSSO	FSSO Users	500	1500	2000	8000	20000	200000[3]	200000
	FSSO Groups	250	750	1000	4000	10000	20000	20000
	Domain Controllers	10	15	20	80	200	400	400
	RADIUS Accounting SSO Clients	166	500	666	2666	6666	13333	13333
	FortiGate Services	50	150	200	800	2000	4000	4000
	FortiGate Group Filtering	250	750	1000	4000	10000	20000	20000
	FSSO Tier Nodes	5	15	20	80	200	400	400
	IP Filtering Rules	250	750	1000	4000	10000	20000	20000
Accounting Proxy	Sources	500	1500	2000	8000	20000	40000	40000
	Destinations	25	75	100	400	1000	2000	2000
	Rulesets	25	75	100	400	1000	2000	2000

Feature		Model						
		200E	300F	400E	800F	2000E	3000E	3000F
Certificates								
User Certificates	User Certificates	2500	7500	10000	40000	100000	200000	200000
	Server Certificates	50	150	200	800	2000	4000	40000
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	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.

FURTINET®

www.fortinet.com