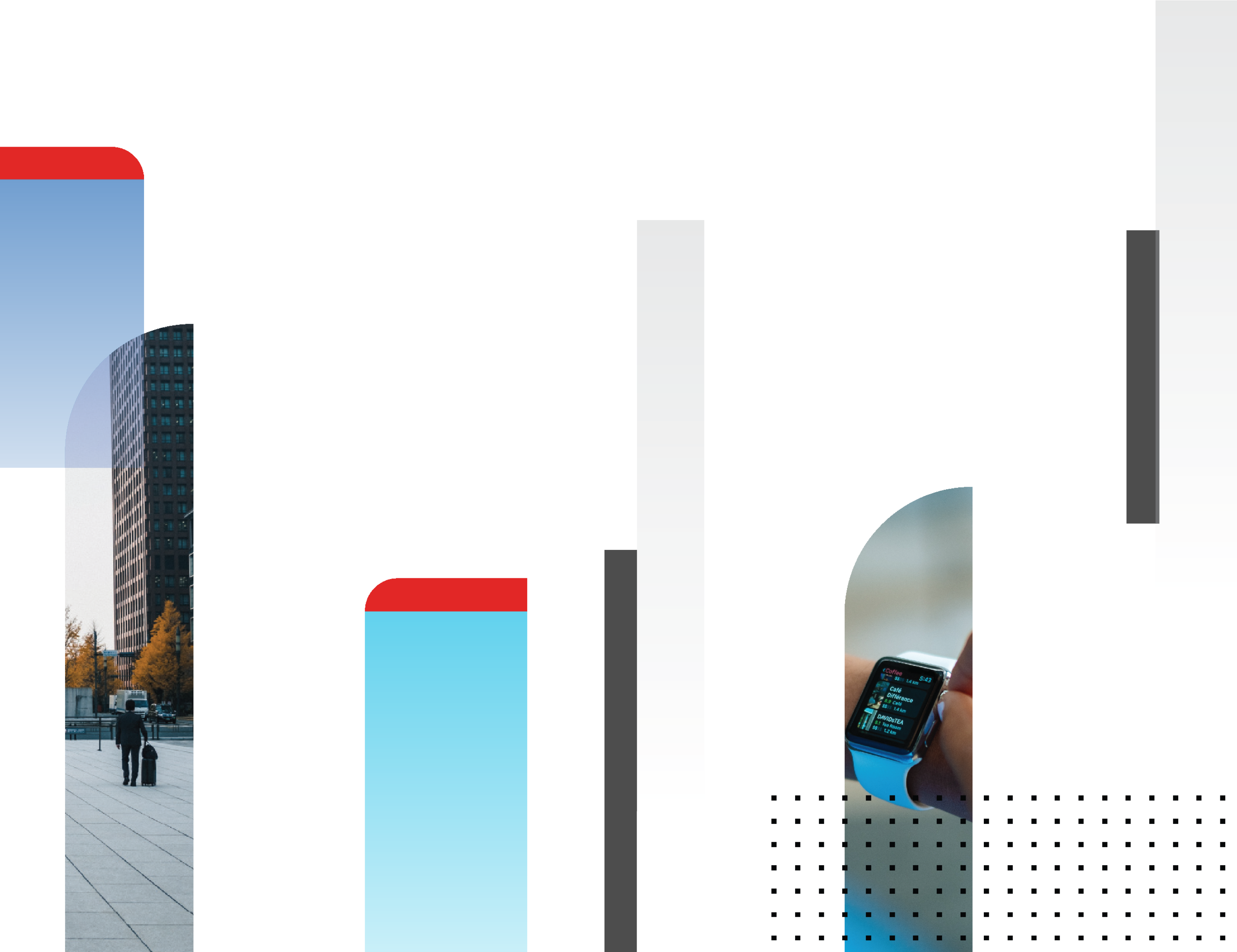
Release Notes

FortiAuthenticator 6.3.1



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

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 6.3.1 Release Notes
23-631-723299-20220302

TABLE OF CONTENTS

Change log

Date	Change Description
2021-06-08	Initial release.
2021-06-29	Added FortiAuthenticator 300F to Upgrade instructions on page 8.
2021-07-05	Added FortiAuthenticator 300F to Maximum values for hardware appliances on page 19.
2021-07-09	Updated Product integration and support on page 12.
2021-07-12	Added FortiAuthenticator Agent for Microsoft Windows 3.8 to Product integration and support on page 12.
2021-12-31	Updated Upgrade instructions on page 8.
2022-03-02	Added FortiAuthenticator Agent for Microsoft Windows 4.0 and 4.1 to Product integration and support on page 12.

FortiAuthenticator 6.3.1 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.3.1, build 0682.

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.

What's new

FortiAuthenticator version 6.3.1 includes the following new features and enhancements:

Self-Service Portal: FSSO support

FortiAuthenticator now allows you to set up an FSSO portal login page independent of the admin GUI login page using the self-service portal.

Go to the **Portal Services** tab in **Fortinet SSO Methods > SSO** to specify self-service portals used to create an FSSO session on successful end-user login. The FSSO session is removed when this end-user logs out.

Once the end-user is successfully authenticated, and given that the original request to the self-service portal contains the `user_continue_url` HTTP parameter with a valid URL, then the self-service portal redirects the end-user's browser to the URL specified in `user_continue_url` instead of the self-service portal's post-login menu page.

Customizable login and logout replacement messages are already available in **Authentication > Portals > Replacement Messages**.

TACACS+: PAP support

TACACS+ on FortiAuthenticator now supports the PAP authentication type.

Remote LDAP user synchronization rules support multiple certificate bindings

FortiAuthenticator now supports remote LDAP user synchronization rules where you can create or update user accounts with multiple certificate bindings. All certificate bindings use the same Common Name but different CAs.

Certificate binding CA dropdown available when creating or editing a remote LDAP user synchronization rule in **Authentication > User Management > Remote User Sync Rules** now allows selecting multiple CA certificates.

Inbound proxy settings for source address detection

FortiAuthenticator now allows the administrator to specify which HTTP header(s) may or may not be used to retrieve the source IP address of an HTTP request.

The **Edit System Access Settings** page in **System > Administration > System Access** has a new **Inbound Proxy** pane with related settings.

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 6.3.1 supports:

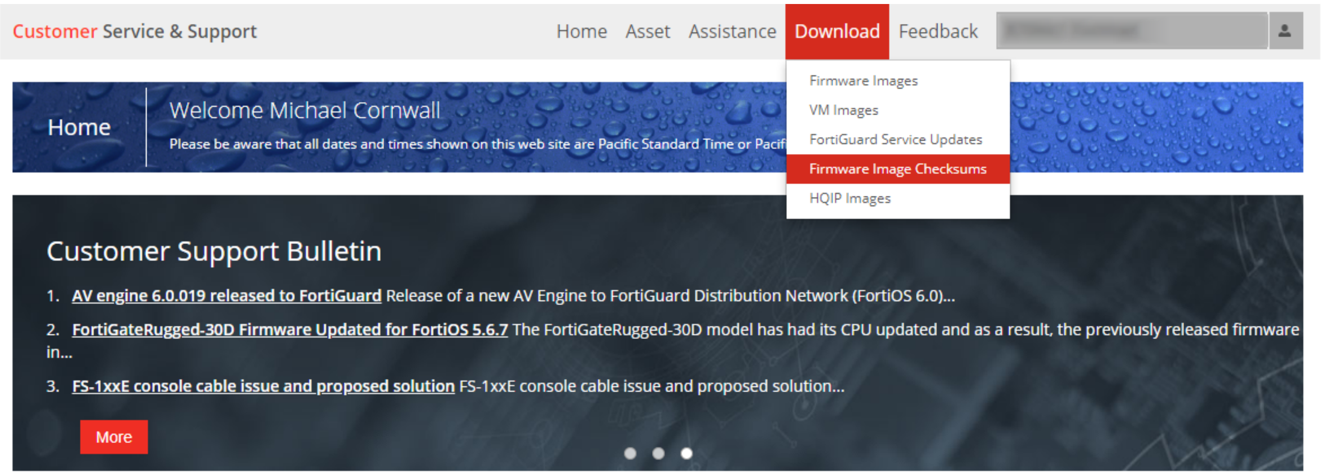
- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 300F
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator 800F
- FortiAuthenticator VM (VMWare, Hyper-V,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



Welcome Michael Cornwall

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

Customer Support Bulletin

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

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

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

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

FortiAuthenticator 6.3.1 build 0682 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 6.3.1, 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 6.3.1 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.3.1 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 10.

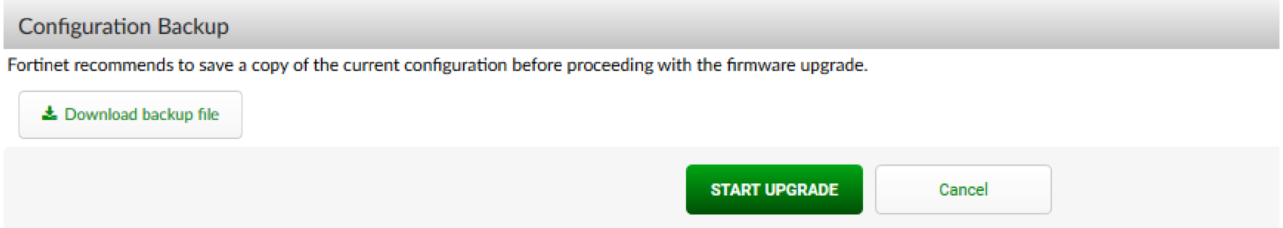
Firmware upgrade process

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 6.3.1, 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 6.3.1

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

Web browser support

The following web browsers are supported by FortiAuthenticator 6.3.1:

- Microsoft Edge version 91
- Mozilla Firefox version 89
- Google Chrome version 91

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

FortiOS support

FortiAuthenticator 6.3.1 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 6.3.1 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 6.3.1 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 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
715246	FortiAuthenticator IdP + O365 SP scenario issue after upgrade to 6.3 from 6.2.1.
717191	SNMP traps generation issues.
721431	Customized portals that refer to the now deleted uploaded images return error instead of the portal following 6.3.0 upgrade.
695110	Corporate FortiAuthenticator SAML login failure to mantis after the VPN is disconnected.
579697	GUI glitch in the admin trusted subnet.
716017	FortiAuthenticator must remain backward compatible with legacy SCEP/CRL URL paths.
526202	FortiAuthenticator does not check if the signature of CSR is valid.
631600	SCEP request by the certmonger cannot be recognized by an automatic enrollment request.
708044	Handling of HTTP "Forwarded" header is broken.
720866	FortiAuthenticator should not approve subsequent SCEP requests if the certificate has not expired.
705066	CPU climbs to 100% - Many POSTGRES SELECT processes seen.
632239	Smart Connect should not require user to select OS.
719226	SAML with token authentication does not work.
717137	FortiToken Cloud stops working after HA cluster is formed.
720286	Social login with Facebook credentials does not work.
719959	[CVE-2021-31542] Django security fixes.
719574	Running a remote sync rule with FortiToken Cloud token produces error in the logs.
712263	HTTP services - CRL Downloads (/cert/crl) enabled, HTTP access needs to be enabled warning persists.
716450	A successful SSH login or a wrong password is not logged.
715985	Hyper-V VM 6.1.2 and 6.2.0 upgrade to 6.3.0 crashes to a blinking cursor.
709744	Script errors on logging in to Microsoft Teams using SAML (FortiAuthenticator as IdP).
717230	Command injection in FortiAuthenticator CLI.
707813	"Test Token" button for an imported SAML user does not work.
713129	Add triggers to monitor changes in the passive node's TACACS+ configuration.
710914	FortiAuthenticator limits various user fields to 30 characters, causing remote LDAP sync failures unexpectedly.

Bug ID	Description
704094	LDAP sync rule fails with error "value too long for type character varying(30)" when manually syncing for the second time.
708097	Backup temporary token" does not revert back to "None" after using a FortiToken in remote SAML users authentication.
711676	Monitors interface stability period feature is not visible on FortiAuthenticator HA cluster GUI.
710959	When TACACS client subnet is already used, RADIUS client with the same subnet cannot be used.
711920	Changes to the REST API rate limit feature do not take hold until the web server is restarted.
712187	FortiAuthenticator crashes if a custom RADIUS dictionary is deleted.
713786	Remote RADIUS user authentication with any token gives 403 error in the captive self-service portal.
713816	Duplicate REST API log file is created on log rollover.
711155	Deleting remote user from the remote LDAP page is not working.
711156	No limit for remote SAML servers.
710931	Unable to import users by group membership from OpenLDAP when a group is added in an OU.
711537	Captive self-service portal "Sign in as a different user" button gives 403 error.
685172	FortiAuthenticator A-P running in v6.2.1 does not sync with the secondary unit pre-authentication warning message, CLI and GUI timeout.
710497	GUI pre-authentication warning replacement message can lock out GUI access.
712744	Wrong hint when creating a local user using FortiToken Cloud token-based authentication.
622352	Device self-enrollment fails if SCEP enrollment request has only the country specified in the Subject DN.
628516	Intermediate CAs cannot be used to sign certificates after exporting its key.
713896	Grammatical error in the token activation default message.
715544	Enable 2FA and provision FortiToken cloud does not work.
672539	Admin Profile "Certificate Management" permission unable to add nethsm.
584264	Two buttons for Add SMS license information.
715674	Portal error while trying to report a lost token.
670941	Creating a RADIUS client with the same name or IP results in error.
661251	Admin password can be changed without entering the current password by opening the "Change Password" link in a new tab.
665223	Create new RADIUS server option from the realm page is not working.
632411	Crash when setting a non-blank password that does not comply with the password policy rule.
681731	Email field should not be required for SCEP Challenge Password.
616167	SCEP stops working if we change the FQDN; need to restart FortiAuthenticator to get it to start again.

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
711940	Raid widget is showing wrong status.
709395	High CPU utilization by wmid process.
719652	DNS lookup is resolved from the cache instead directly from the DNS server.
677433	API output "HTTP 200 OK" when the SMS gateway is down.
680776	AP HA secondary cannot change mgmt interface access configuration, and the option does not sync from the primary either.
719695	EAP-TLS authentication fails on Windows 10 20H2 with TLS 1.2.
718710	FortiAuthenticator 800F RADIUS authentication services failure, and unable to login to GUI.
717175	Local users export/import feature does not work if bcrypt hash is used.
716466	Cannot import SAML user from the GSuite directory.
593089	Log filter limitation.
712899	SMTP error messages does not provide accurate information.
716014	PUSH communication does not use proxy.
718070	Need FA on the FAC2000E that cannot be accessed via GUI.
694303	Connection between FortiAuthenticator and Active directory crashes, customer cannot access the device.
673570	RADIUS accounting FSSO is not working.
665384	HA failover does not work reliably.
711721	Groups sorting differences when importing LDAP groups in SSO groups and FortiGate filtering.
632629	Smart Connect WPA2-Personal profile fails when WPA2-Enterprise settings are left in place.
704565	FortiAuthenticator only applies one captive portal policy, ignores RADIUS client IP/AP IP in portal policy selection
701758	Problem setting static IP address on a FortiAuthenticator-VM installed on a XenServer.
691009	A FortiAuthenticator-VM 6.0.4 stops authenticating and GUI freezes until reboot is applied.
577877	Allow bulk unlock for FortiToken mobile tokens.
622426	MAC address parameter in portal policy should only allow MAC addresses.
637028	SSL connection fails in case when the certificate expired issue is not explicit enough.

Bug ID	Description
717926	FSSOMA - FortiClient: reached maximum client number, cannot accept new connection.
692839	Local cert for GUI rejected despite SAN field.
697447	Octet/ASCII conversion for all RADIUS attribute-value pair inputs.
637290	No FortiToken mobile push notification with Windows agent 3.0.
691825	SMS gateway HTTP/HTTPS - Inconsistent JSON object type used for the phone number attribute.
697969	SCEP errors displayed when there is no enrollment request from client (FortiGate).
676985	Unable to import all FTK hardware tokens from the same purchase order; need to add them all manually.
669054	Unable to install FortiAuthenticator-VM-HV 6.2.0 on server 2012 R2.
704653	Users are intermittently forced to reauthenticate.
706701	FortiAuthenticator cluster is inconsistently accessible via HA interfaces from outside the HA subnet.
709007	Error when importing a remote LDAP user.
646299	Nutanix AHV KVM based Hypervisor FortiAuthenticator upgrade from 6.0.4 to 6.1.x hangs on "Waiting for Database".
693151	Allow deletion of the expired user and the local service certificates.
638374	SCEP - Encryption/hash compatibility with clients.
714927	Unable to expand FortiAuthenticator "data drive" beyond 2 TB.
676532	When FortiAuthenticator has a RADIUS client set as subnet, RADIUS accounting disconnect messages are not sent.
592837	Sponsor accounts can add guest user accounts to non guest groups.
680423	FortiAuthenticator Syslog FSSO injects speech mark (") around external user and group fields where none exist in the raw log.

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	250
	Language Files	5	50	50	50
Authentication					
General	Auth Clients (NAS)	3	Users / 3	33	1666
User Management	**Users** (Local + Remote)[1]	5	***********	100	5000

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
	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
	RADIUS Client Profiles	3	Users	100	5000
	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
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	2500	10000

[1] Users includes both local and remote users.

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

FORTINET®

www.fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.