FORTINET

Release Notes

FortiAuthenticator 6.5.2

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

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

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 6.5.2 Release Notes
23-652-914362-20230829

TABLE OF CONTENTS

Change log

Date	Change Description
2023-05-16	Initial release.
2023-05-23	Updated What's new on page 7.
2023-05-29	Updated What's new on page 7.
2023-05-31	Moved bug 901776 from Resolved issues on page 18 to Known issues on page 22. Added bug 680776 to Resolved issues on page 18.
2023-06-20	Updated Fortinet agent support on page 15.
2023-06-29	Updated Known issues on page 22.
2023-08-01	Added bug 900550 to Known issues on page 22.
2023-08-29	Updated Upgrading from 4.x/5.x/6.x on page 12.

FortiAuthenticator 6.5.2 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.5.2, build 1329.

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 6.5.2 includes the following enhancement:

SAML IdP: Optional CAPTCHA input

FortiAuthenticator now offers optional CAPTCHA input for the SAML IdP login workflow after `n` failed login attempts from the same source IP address.

A new **Enable captcha on SAML IdP login** toggle in the **IP Lockout Policy Settings** pane when setting up user lockout policy in **Authentication > User Account Policies > Lockouts**.

Using the new **Display captcha after** field, you can set the number of failed login attempts from the same source IP address, after which the CAPTCHA challenge must be completed to log in. Set **Display captcha after** to `0` to require users to complete the CAPTCHA challenge on every login.

In **Authentication > SAML IdP > General**, a read-only **Captcha** option displays the current state of the CAPTCHA setting from Lockouts. Using the pen icon, you can edit the CAPTCHA setting in Lockouts.

The following SAML IdP login replacement messages in **Authentication > SAML IdP > Replacement Messages** have been modified to include the CAPTCHA image and field:

- **Login Username and Password Page**
- **IAM Login Page**
- **Login Fido Password Page**

New remote TACACS+ server

FortiAuthenticator now supports setting up a remote TACACS+ server.

You can now add remote TACACS+ users to FortiAuthenticator. These users are restricted to the Administrator role for administrative access to the FortiAuthenticator.

Single Sign-On for SSOMA trusted endpoints

FortiAuthenticator now allows SAML IdP login without entering the username/password even if there are no existing IdP sessions, provided the endpoint runs the ZTNA agent and SSOMA reporting to FortiAuthenticator FSSO module.

The **General** page in **Authentication > SAML IdP** includes the following new options:

- **Trusted endpoint single sign-on**: When enabled, SSOMA endpoints can log in without reentering username and password.

The username login page includes a new **Trusted Endpoint Single Sign-On** button that allows single sign-on for trusted endpoints when **Trusted endpoint single sign-on** is enabled.

Note: The legacy login page does not offer the new **Trusted Endpoint Single Sign-On** button.

- **Listening port**: Trusted endpoints TLS-connect to this TCP port to present their client certificate to the FortiAuthenticator.
- **Enforce MFA**:When enabled, FortiAuthenticator enforces token-based settings configured for the SP during trusted endpoint single sign-on. When disabled, token-based verification is bypassed for trusted endpoints.
- **Enforce IP matching**: When enabled, the source IP address of the endpoint connecting to the listening port must match one of the IP addresses reported by the SSOMA to do a successful trusted endpoint authentication. For example, if the endpoint is on a private network and its connection to the FortiAuthenticator is being NAT'ed, this option should be disabled.

Portals: Modernized look

FortiAuthenticator now offers a modern look for every web portal page. The modernized portal web pages have a more responsive design.

SmartConnect for Android 11 and above

The self-service portal now offers the following:

- Legacy SmartConnect application to end-users with Android OS 10 and earlier.
- The FortiGuest SmartConnect application to end-users with Android OS 11 if the SmartConnect profile is configured for `WPA2-Personal/PSK` or `WPA2-Enterprise/PEAP`.
- The legacy SmartConnect application to end-users with Android OS 11 if the SmartConnect profile is configured for something other than `WPA2-Personal/PSK` or `WPA2-Enterprise/PEAP`.
- CA certificate download links for Signing CA certificate(s), Local CA certificate(s), and Trusted CA certificate(s) to end-users with Android OS 11 and above, provided these are configured in the SmartConnect profile.

New profiler tool for FastAPI debugging

FortiAuthenticator now includes a profiler tool.

In the extended debug logs, a new **Enable FastAPI Debug Mode** button is available when **FastAPI** is selected in **Log Categories > Web Server**.

OAuth: Configurable expiry for refresh tokens

FortiAuthenticator now offers the ability to specify an expiry period for refresh tokens.

FortiAuthenticator keeps track of the refresh token expiry when issuing a refresh token. The refresh token never expires if the expiry period is configured as `0`. FortiAuthenticator does not issue a new OAuth token using an expired refresh token.

If the specified refresh token is expired and the `/oauth/token/` endpoint is called with `grant_type=refresh_token`, it now returns error code `400 Bad Request`.

When creating a relying party in **Authentication > OAuth Service > Relying Party**, a new **Refresh token expiry** field is available. Using the **Refresh token expiry** field, you can set the amount of time for which the issued refresh token is valid upon authorization.

EAP-TLS: Accept any client certificate signed by a trusted CA

A new **Trusted CA(s)** option in **Authentication mode** available in the **Identity sources** tab when creating or editing a RADIUS policy in **Authentication > RADIUS Service > Policies**. The RADIUS policies also include a list of trusted CA certificates. This allows FortiAuthenticator to successfully authenticate any endpoint presenting a valid client certificate signed by one of the trusted CA certificates. The new **Authentication mode** option is only available when the **Authentication type** is **Client Certificates (EAP-TLS)**.

The **Authentication mode** contains the following two options:

- **Certificate bindings:** Legacy mode that uses certificate bindings.
- **Trusted CA(s):** Accepts all the valid client certificates signed by one of the trusted CAs.

When the **Authentication mode** is set as **Trusted CA(s)**, the RADIUS daemon ignores any configured certificate bindings and only verifies that the client certificate is:

- Signed by one of the trusted CAs
- Not expired
- Not revoked (if CRL is configured)

When the **Authentication mode** is set as **Trusted CA(s)**, the **Identity sources** tab offers the following new options:

- **Local CA certificates**
- **Trusted CA certificates**

Since FortiAuthenticator does not match the authenticating endpoints with a user account, FortiAuthenticator cannot use RADIUS attributes specified in user accounts or user groups to return in the RADIUS **Accept-Accept** response. This new type of EAP-TLS RADIUS policy allows specifying a set of RADIUS attributes to be included in all **Accept-Accept** responses.

When the **Authentication mode** is set as **Trusted CA(s)**, the **RADIUS response** tab includes a new **Additional Attributes** pane. In the **Additional Attributes** pane, you can add RADIUS attributes to be included with the **Accept-Accept** response.

The **Additional Attributes** pane is similar to the **Additional Attributes For MAC Authentication Bypass** pane available in the **RADIUS response** tab when the **Authentication type** is **MAC authentication bypass (MAB)**.

FortiAuthenticator logs the result of the authentication attempts and includes the username specified in the EAP-TLS request as part of the log entry.

SAML IdP proxy: Bypass MFA if SAML assertion indicates external IdP enforced MFA

FortiAuthenticator performs MFA in case the remote SAML IdP does not indicate that it performed MFA.

A new **Attempt token-based authentication locally if external IdP does password-only authentication** toggle is available when creating or editing a remote SAML server in **Authentication > Remote Auth. Servers > SAML**.

The options is only available when the **Type** is **Proxy** and **Authentication context** is **MFA**.

LDAP attributes in BASE64 format can be added to SAML assertions

FortiAuthenticator now supports adding LDAP attributes in BASE64 format to SAML assertions.

When creating or editing an SP in **Authentication > SAML IdP > Service Providers**, a new **LDAP custom attribute (BASE64)** available in the **User attribute** dropdown in the **Assertion Attributes** pane.

Also, the **LDAP custom attribute** has been renamed to **LDAP custom attribute (ASCII/UTF8)**.

Increased Windows machine authentication maximum value

When editing general user account policy in **Authentication > User Account Policies > General**, the maximum allowed value for **Windows machine authentication** has been increased to 10080 minutes, i.e., 7 days.

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 6.5.2 requires at least 4GB of RAM.

Hardware and VM support

FortiAuthenticator 6.5.2 supports:

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

Image checksums

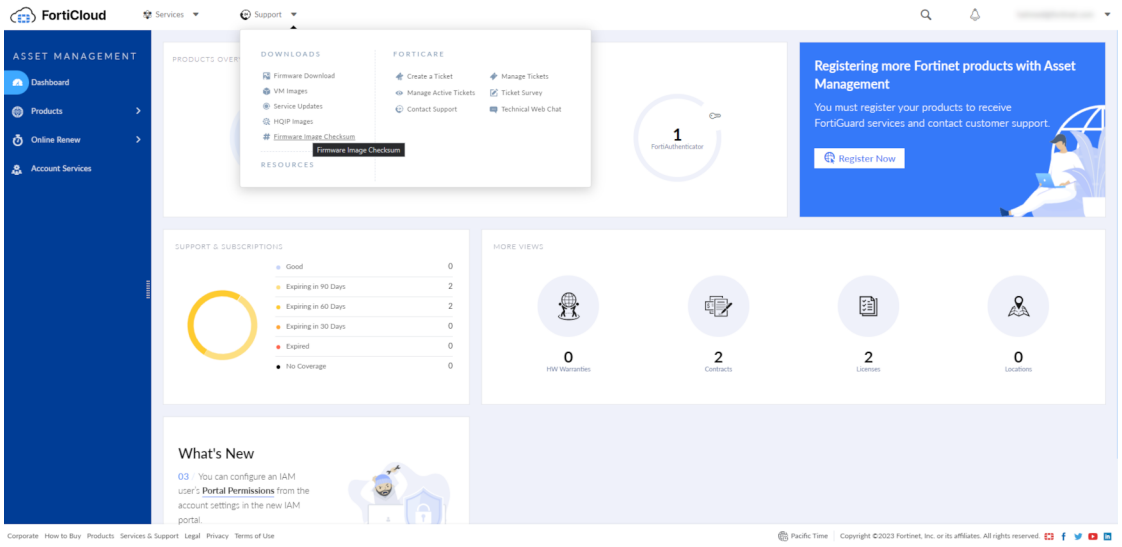
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available on FortiCloud.

FortiCloud image checksum tool

After logging in to FortiCloud, in the menus at the top of the page, click **Support**, then click **Firmware Image Checksum**.

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



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

FortiAuthenticator 6.5.2 build 1329 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 6.5.2, else the following message will be displayed: `Image validation failed: The firmware image model number is different from the appliance's.`
- If currently running FortiAuthenticator 6.0.7, then upgrade to 6.5.2 directly.
- If currently running FortiAuthenticator between 6.1.0 and 6.2.0, first upgrade to 6.3.3, then upgrade to 6.5.2.
- If currently running FortiAuthenticator 6.2.1 or later, then upgrade to 6.5.2 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.5.2 from FortiAuthenticator 6.0.7, you must first increase the size of the virtual hard disk drive containing the operating system image (not applicable for AWS & OCI Cloud Marketplace upgrades). See Upgrading KVM / Xen virtual machines on page 13.

Upgrade to and from FortiAuthenticator 6.0.6 is not recommended.

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 FortiCloud, then upload it from your computer to the FortiAuthenticator unit.

1. Log in to the FortiCloud. In the **Support > Download** section of the page, select the **Firmware Download** 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 Checksum** 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:
   ```
   Fortinet recommends to save a copy of the current configuration before proceeding with 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 6.5.2, it is necessary to manually increase the size of the virtual hard disk drive which contains the operating system image before starting the

upgrade. This requires file system write-access to the virtual machine disk drives, and must be performed while the virtual machines are in an offline state, fully powered down.

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

Use the following command to run the resize on KVM:

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

Use the following command to run the resize on Xen:

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

After this command has been completed, you may proceed with the upgrade from 6.0.7 to 6.5.2

Recovering improperly upgraded KVM / Xen virtual machines

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

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

To recover an improperly upgraded KVM virtual machine:

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

To recover an improperly upgraded Xen virtual machine:

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

Product integration and support

FortiAuthenticator supports the following:

Web browser support

The following web browsers are supported by FortiAuthenticator6.5.2:

- Microsoft Edge version 113
- Mozilla Firefox version 113
- Google Chrome version 113

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

FortiOS support

FortiAuthenticator6.5.2 supports the following FortiOS versions:

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

Fortinet agent support

FortiAuthenticator 6.5.2 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.

Note that the FortiAuthenticator Agents for Microsoft Windows and OWA download files are now available in the `FortiTrustID_Agents` folder in *Support* > *Firmware Download* on FortiCloud.

- 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

FortiAuthenticator6.5.2 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 17 for more information.

Third-party RADIUS authentication

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

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

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

FortiAuthenticator-VM

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

Resolved issues

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

Bug ID	Description
904022	Revoked certificates still count against FortiAuthenticator license counts.
910417	`secp256r1` (Elliptic Curve / EC) HTTPS certificate not allowing `TLS1_2`.
878828	After a reboot, FortiAuthenticator shows `500 Internal Server Error` when synchronizing hardware Tokens.
902466	OAuth authentication fails when user is administrator on FortiAuthenticator.
861557	FortiAuthenticator remote user sync rules - Set Group Filter not working if OU has special characters in name, e.g., (,) , +.
908291	FortiAuthenticator does not properly revoke a user certificate.
881296	SNMP v3 with non-ENG letter pass gives authentication failed.
901259	Issues accessing FortiAuthenticator via DNAT-ed IP address.
899791	*Radius Attributes* option is not visible under local users when logged in with a user having full access set in admin profile.
904790	In a captive portal, clicking *Register* then *Cancel* gives error 404.
848434	Usability of *User Group* GUI.
869768	Unable to delete a user group.
905143	SAML logout returns `Internal Server Error`.
808748	Self-service portal password change fails for remote LDAP users if UPN format is used.
892321	FortiAuthenticator does not show the list of local users correctly after upgrading to 6.5.0.
890072	Incorrect warning message when deleting a remote user sync rule.
837728	Local services cannot use a certificate with >97 character subject length.
892306	Local users view does not display the complete group name.
850023	HA Cluster not forming due to differing smartconnect primary key name (upgrade path mismatch, but should work).
884902	Unable to import 10k plus groups from Azure via SAML in FortiAuthenticator.
862394	In FortiAuthenticator CLI, a user can change DNS addresses even if we assign `No-Access/Read-only` admin profile.
901185	FortiAuthenticator radiusd crashes with complete authentication failure seen with certain high volume EAP traffic patterns.

Bug ID	Description
838976	Windows log events in FSSO are dropping after some time.
893632	FortiAuthenticator unable to decode assertion after upgrading to 6.5.0.
899505	Unable to provision FortiToken Mobiles on FortiAuthenticator 200E/400E/3000E in 6.5.0/6.5.1.
854050	It takes a long time for FortiAuthenticator to reflect active certificates in the GUI after successful SCEP enrollment request.
892944	Windows and OWA Agent stopped working after upgrade to 6.5.0.
866392	FortiAuthenticator GUI/captive portal access freezes/become unresponsive during peak hours.
873050	403 Forbidden error while doing SAML authentication after OAuth succeeds.
901109	WAD-enforced admin/service access rules: Admin access does not apply to the HA admin interface.
878673	Certificate GUI filter by status times out when there are thousands of revoked certificates.
904049	The copy button does not work on the 500 error page.
902515	Device reboots before configuration backup finishes downloading the firmware upgrade.
908157	Unable to export guest users in Firefox.
906588	GUI crashes when you click *Create New* in the *Services* tab in *Authentication* >*TACACS+ Service* > *Authorization*.
898767	Use proper and consistent casing for OAuth.
903771	LDAP user profile view in the self-service portal is broken.
899909	Exception in the *Result* window in *Self-service* > *Password Change*.
603105	LDAP user import uses server IP from DB despite browser using/showing unsaved one.
877745	Javascript errors being thrown by all(?) search filters.
874285	Unable to use FortiAuthenticator images in System replacement messages.
889196	SAML sync rule groups input should be disabled when no server is selected.
741765	REST API `/api/v1/tacpluspolicyclient/` endpoint does not recognize `policy_name` or `client_name` parameters.
901111	WAD-enforced admin/service access rules stop applying when the interface IP address is changed.
903356	Rebooting cluster passive node breaks application of new settings if the role remains unchanged.
903163	CLI pre-authentication warning is not applied when the setting is only toggled on. **Note**: Toggling off works. Changing the warning message may make the CLI pre-authentication warnings to work.
900916	WAD-enforced admin/service access rule only applies to the first four interfaces; rest still enforced in Python.
865372	FortiNAC can overwhelm FortiAuthenticator with many TACACS+ logins on the same service account.

Bug ID	Description
887938	Read-only profile page does not show the correct information.
870942	Return proper responses to HTTP OPTIONS requests.
891245	[3rd party component upgrade required for security reasons] FortiAuthenticator - `django` to 3.2.18 or 4.0.10.
872779	[3rd party component upgrade required for security reasons] FortiAuthenticator - `curl` to 8.0.1.
907192	GUI crash in OAuth authorization when no scope is provided to FortiAuthenticator.
874256	Failed FIDO token authentication and reauthentication FIDO token using SP SAML portal causes error occurred.
911436	Clicking *Enter* during verification field on *Account Registration* resends the code rather than submitting the code.
897201	The inbound proxy feature does not work when *Get proxy IP from FORWARDED HTTP header* is enabled.
907204	No error message reported when LDAP password reset via email/security question is rejected by the remote LDAP server.
911038	Remote LDAP user unable to use Smart Connect.
911381	`/api/v1/oauth/verify_token/` request fails for the remote LDAP admin user.
907788	Upgrading the HA cluster from 6.4.7 GA to latest 6.5.2 build (1315) causes FortiToken Cloud license error in the *License* widget.
910022	403 error when trying to do SAML logout with *Use ACS URL from SP authentication request* enabled.
904565	Multiple TACACS+ authentications within a few seconds result in error if the user contains a rule.
868829	IP lockout not being logged in on FortiAuthenticator logs.
905670	FortiAuthenticator should not send out authentication requests for disabled TACACS+ users.
861027	RADIUS attribute name should be only unique within the dictionary, not across all dictionaries.
868836	TACACS+ failed authentications not counting towards IP lockouts.
894106	Deleting an OAuth portal triggers 500 Error.
900570	400 error when using LDAP custom attribute in the SAML SP initiated login.
876703	Unable to view supported methods and available fields using `/schema` at the end of the endpoint.
900124	User lookup never displays the first few users.
897728	Inbound proxy settings - GUI allows submitting duplicate values in *FORWARDED by values*.
898621	Group membership text is misaligned when there are large number of groups in the SAML session.
787852	TACACS+ attribute value pair for authorization services shows undefined entries.
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*.

Bug ID	Description
877815	SAML IdP IAM button should not be displayed if the SAML IdP portal is disabled.
889706	FortiAuthenticator Remote user sync rules - Test filter not working if OU has special characters in name, e.g., (,) , +.
905076	Deprovisioning FortiToken Cloud token causes `WAD_12 (ftcd` crash.
895125	In SAML IdP and SP login portals, specifying a realm that does not exist triggers 500 error.
901732	Unable to reset password for remote user on self-service/captive portal.
905391	FortiAuthenticator as SAML IdP not returning remote LDAP groups in SAML assertions.
884316	SAML IdP Login Success Page: last login information not shown when the previous IdP session was cleared.
870678	Recovery password and recovery token fails to send alternative email address.
907162	FortiToken Cloud status should show `service unreachable` when unable to reach the ForitToken Cloud server.
680776	AP HA secondary cannot change the mgmt interface access configuration, and the option does not sync from the primary either.

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 FortiCloud.

Bug ID	Description
620127	Changing from `maint-mode-no-sync` to `maint-mode-sync` does not appear to restore syncing.
646299	Nutanix AHV KVM based Hypervisor FortiAuthenticator upgrade from 6.0.4 to 6.1.x fails and hangs on `Waiting for Database`.
751108	FortiAuthenticator does not support admin OIDs from `FORTINET-CORE-MIB` properly.
755752	Power supplies show voltage input fault on both CLI and GUI.
756414	Incorrect Italian translation of *Next* button displayed on the reset password page.
766453	Check the reason for FortiAuthenticator 400E auto reboot.
781832	Token bypass is not working for FIDO enabled self-service portal.
801933	FortiAuthenticator as an LDAP server: log shows `LDAP_FAC` in the *Source IP* field.
805969	FortiAuthenticator supports Zero Trust tunnels to multiple remote LDAP servers through one FortiGate only.
816070	DB issue if the power is down during a short window when booting from factory reset.
842886	Upgrading FortiAuthenticator in HA-LB removes the MAC-address records form the LB node.
871533	Incorrect FIDO token does not count towards user lockout.
876009	FortiAuthenticator ignores the groups filtering rules and send all the SSO groups to FortiGate if the FortiGate is configured with FQDN.
876897	FortiAuthenticator memory usage showing in the widget does not match with memory usage from SNMP (`facSysMemUsage`).
877432	Selecting Cloud option for group membership on SAML SP and displays 500 error if we do not select an OAuth server.
878854	Remote LDAP usernames over 255 characters fail to authenticate through the SSL VPN.
890725	SAML token-only login displays password page instead of the token page.
891801	FortiAuthenticator only sends accounting responses in random bursts with large delays.
894888	User Lookup does not display token information with view-only admin profiles.
897852	Logs and SNMP trap for loss of LB HA connectivity.
899836	Passwords expires one day earlier than expected.
900664	Certificate only smart connect in iOS does not work.
901379	HA cluster failover causes FortiAuthenticator to give up on logging.

Bug ID	Description
901776	SAML Logout using POST returns `CSRF token missing or incorrect` (HTTP 403).
904099	IAM login link does not work if the SP initiates `AuthnRequest` with HTTP-POST binding.
904353	Daylight saving time (DST) time zone change for Egypt starting end of April.
905091	GUI should not show success message for user change when the FortiToken Cloud provisioning has failed.
905423	CRL download URL over http is not available.
905593	Admin username is missing in log details after upgrading.
905764	Display filter is not working correctly for pending third party user certificates.
906339	RADIUS attributes cannot be added to local users via REST API (Error: local variable 'vendor' referenced before assignment).
907286	FortiAuthenticator LDAP server does not support PW+OTP concatenation for FortiToken Cloud-issued FortiToken Mobile tokens.
908054	Failing to use certificate for EAP: 'RADIUS EAP certificate has multiple subject alternative name 'DNS' which is not allowed.'
908091	When timezone = GMT, London, user audit report download fails with internal server error 500.
908142	Using Yubikey as OTP second factor increases drift/counter unexpectedly.
908753	Number of Users for MAC device group is always zero.
908759	HA LB anomaly for MAC device group membership upon connection.
909099	Refresh button for widgets gets grayed out for a while after clicking on it and becomes clickable again after a couple of minutes.
909342	The status of the hardware tokens is "Missing seed" if imported through the serial number file.
910398	SAML debugging option *Do not return to Service Provider...wait for user input* is not working.
913354	Self-device enrollment is broken for FortiToken 300.
913854	Switching between dynamic and static RADIUS attributes for LDAP user groups causes GUI to display an invalid dropdown.
913981	Non-admininstrator SAML FIDO authentication ends with error 500.
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	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