FortiADC - Release Notes

Version 6.0.0

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

July 24, 2020
FortiADC 6.0.0 Release Notes
01-600-650988-20200724

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-07-24	FortiADC 6.0.0 Release Notes initial release.
2020-07-30	Added bug 653209 to Known Issues

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 6.0.0, Build 0038.

To upgrade to FortiADC 6.0.0, see FortiADC Upgrade Instructions.

FortiADC provides load balancing, both locally and globally, and application delivery control. For more information, visit: https://docs.fortinet.com/product/fortiadc.

What's new

FortiADC 6.0.0 offers the following new features:

Server Load Balance

- **Kubernetes Connector (Ingress controller)**
  The FortiADC Kubernetes connector is a FortiADC built-in connector, which is used to sync Kubernetes objects (service, nod, pod) and update it to VS automatically.

  Note: The K8s connector currently works with K8s Service API version 1 only. Support is not guaranteed for later versions.
- **MSSQL load balance**
  Support load balancing for MSSQL servers in the scenario where one primary replica and multiple secondary replicas are used. It allows FortiADC to forward the read SQL requests (e.g. “select”) to multiple secondary servers and other write requests to the primary server.
- **NTLM authentication**
  NTLM is a suite of Microsoft security protocols intended to provide authentication, integrity, and confidentiality to users. This authentication mechanism allows clients to access resources using their Windows credentials, and is typically used within corporate environments to provide single sign-on functionality to intranet sites.
- **HTTP Form based authentication with FortiToken cloud**
  FortiToken Cloud offers two-factor authentication as a service to Fortinet customers. This feature support the authentication with FortiToken Cloud for the HTTP virtual server access.
- **Error page enhancement**
  Supports more code statuses for error page (in addition to 502), so now the error page can be used for any error..
- **TLS1.3 enhancement**
  Update TLS1.3 cipher list, and have more configuration checks for TLS1.3 settings
- **Keep client address for L7 DNS virtual server**
  In some deployments for security/audit reasons, backend real server requires the original client address. In this feature we can keep client address unchanged when forwarding the DNS request to real server.

Security

- **CAPTCHA action support for WAF and DDoS**
  CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart) is a type of challenge–response test used to distinguish human from machine input, typically as a way of thwarting spam and automated extraction of data from websites. It can be used in WAF and DDoS module as a new action.
- **API security gateway**
  The feature provides an API gateway for backend API services. It processes essential checks to API requests, such as user authentication, rate limiting, source IP limiting, request method/header limiting, and header attaching, to mitigate the attacks to backend API services.

- **HTTP headers security**
  Some HTTP headers are designed to provide another layer of security to mitigate web attacks and security vulnerabilities. This feature allows FortiADC to attach these HTTP security headers while forwarding HTTP traffic. These HTTP security headers include content-security-policy, x-xss-protection header, HTTP strict-transport-security(HSTS), x-frame-options, x-content-type-options.
- **Support X-HTTP-Method-Override in Request Method Rule**
  There exists attacks that use a trusted HTTP methods such as GET or POST, but adding HTTP headers such as X-HTTP-Method, X-HTTP-Method-Override, or X-Method-Override to bypass the HTTP method restriction rules are applied by FortiADC. This feature allows FortiADC to check these HTTP headers while checking HTTP method rules to avoid such security bypassing.

System

- **Fabric Connector**
  New Security Fabric provides a visionary approach to integrate internal and external security connectors, including Central Manager, FortiSandbox, and FortiGSLB.
- **External Connector**
  FortiADC offers external connectors for 3rd party applications.

  The following external connector categories are available in the Security Fabric: Private SDN and Authentication.
- **Splunk App**
  Splunk App is an application runs on Splunk platform to analyze and display the information from the collected log data.

  For FortiADC, customer configure the Splunk Connector to the Splunk Server, and then get all the customized graphs from the Splunk App
- **FortiToken Cloud support for administrator**
  FortiADC provide administrator login management with FortiToken Cloud as a two-factor authentication.
- **Add secure flag when use HTTPs to access ADC to avoid cookie leaking**
  Secure enhancement to enable secure flag in HTTPS response prevents authentication cookie from leaking to HTTP connections. Added https-redirect option to redirect all HTTP connection to HTTPS, enabled by default.
- **HA MAC address changes to management interface MAC**
  We allow customers to configure different virtual MAC for HA interface, which previously may have caused MAC issues on the peer switch. To avoid these issues, we reuse the same MAC of the physical interface.
- **Upgrade FortiGuard authentication method to be more secure**

GUI

- **New FortiGate-like theme**
- **More cohesive information in FortiView**
  Show all statistics of Real Servers of Virtual Server in one form.

  Show all the values of each real server of each virtual server, not using the graph
- **WAF pages enhancement**
  WAF profile and signature pages redesign

Hardware and VM support

FortiADC 6.0.0 supports the following hardware models:

- FortiADC 200D
- FortiADC 300D
- FortiADC 400D
- FortiADC 700D
- FortiADC 1500D
- FortiADC 2000D
- FortiADC 4000D
- FortiADC 100F
- FortiADC 200F
- FortiADC 300F
- FortiADC 400F
- FortiADC 1000F
- FortiADC 2000F
- FortiADC 4000F
- FortiADC 5000F

FortiADC Release 6.0.0 supports deployment of FortiADC-VM in the following virtual machine environments:

VM environment	Tested Versions
VMware	ESXi 3.5, 4.x, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7
Microsoft Hyper-V	Windows Server 2012 R2
KVM	Linux version 3.19.0 qemu-img v2.0.0, qemu-img v2.2
Citrix Xen	XenServer 6.5.0
Xen Project Hypervisor	4.4.2, 4.5

Known issues

This section highlights the major known issues discovered in FortiADC 6.0.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Known issues

Bug ID	Description
652955	missing partial up counter in FortiView GLB Host
625103	If customized ciphers are enabled, FortiADC will not check the conflict between cipher suite and certificate type
653209	If your password includes any of the following special characters: backslash (\), single quote ('), or double quote ("), you may get an incorrect password error when entering in your password. **Workaround:** When entering in your password, add a backslash (\) before each of the special characters and enclose the entire password in double quotes. For example, if your password is 1\2"3'4, you should type "1\\2\"3\'4" during authentication. This issue is scheduled to be fixed in the next release.

Resolved issues

The following issues have been resolved in FortiADC 6.0.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Resolved issues

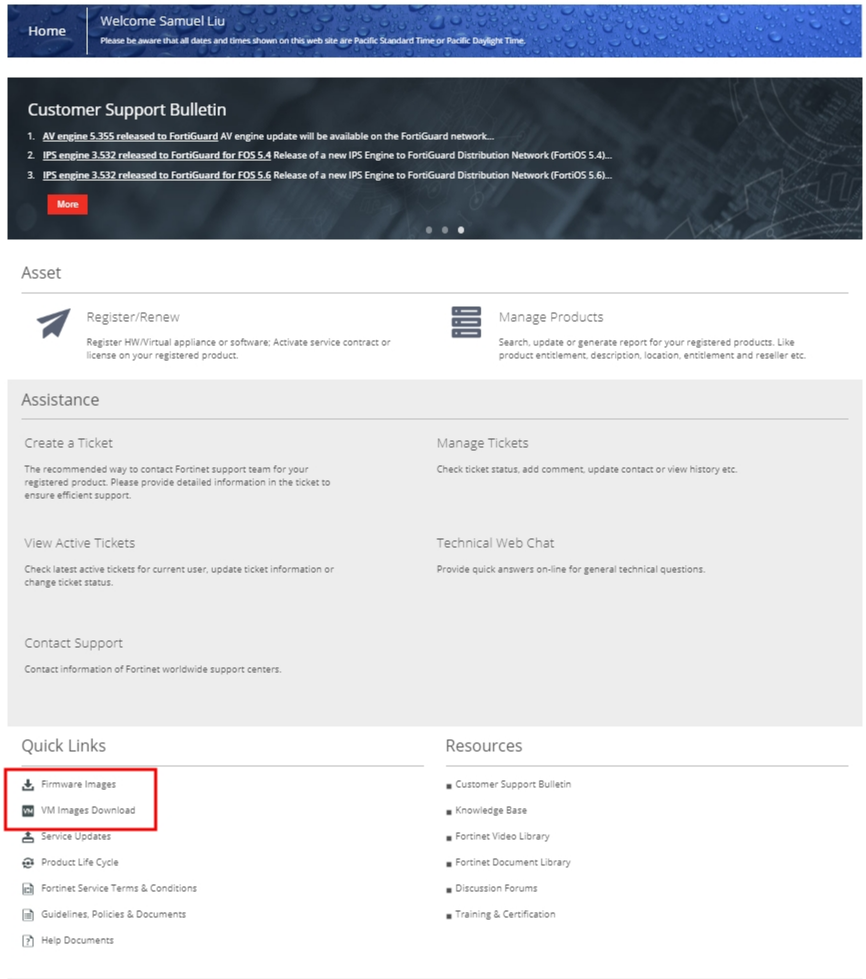
Bug ID	Description
643217	RCA of System Debug File - GUI Not Accessible
633350	i40e driver issue causes 2000F port 17,18 to go down intermittently.
628261	L2 Load Balancing configured along with Content Routing rules cause break to Content Routing
627651	Connection reset by L7 SMTP VS
626517	Generic error message with admin user configuration
631910	The virtual tunnel/LLB hit count overflows
622287	All-in-one debug enhancement
633570	SNAT doesn't work for the existing session after reboot
628586	Httproxy crash on the slb with LEAST CONNECTION, and script persistence cal_server_from_hash
0631258	SCEP - not able to generate local certificate from EJBCA CA server
644221	Shutdown of Hyper-V instance fails
638415	HA AP slave node with dedicated management should use master node as FDS proxy
641421	httproxy-ssl crashed 4 times
640543	SNAT wrongly NATed after LLB failover
625266	FortiADCManager - [NFR] Request old password before allowing a user to change their password
625035	40G interface not processing broadcast traffic, save promiscuous mode workaround after reload
626517	Generic error message with admin user configuration

Image checksums

To verify the integrity of the firmware file, use a checksum tool and 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 Fortinet software and firmware releases are available from Fortinet Customer Service & Support. After logging in to the web site, near the bottom of the page, click the Firmware Image Checksums button. (The button appears only if one or more of your devices has a current support contract.) In the File Name field, enter the firmware image file name including its extension, then click Get Checksum Code.

Customer Service & Support image checksum tool



Welcome Samuel Liu

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

Customer Support Bulletin

1. AV engine 5.355 released to FortiGuard AV engine update will be available on the FortiGuard network...
2. IPS engine 3.532 released to FortiGuard for FOS 5.4 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.4)...
3. IPS engine 3.532 released to FortiGuard for FOS 5.6 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.6)...

Asset

Register/Renew

Register HW/Virtual appliance or software; Activate service contract or license on your registered product.

Manage Products

Search, update or generate report for your registered products. Like product entitlement, description, location, entitlement and reseller etc.

Assistance

Create a Ticket

The recommended way to contact Fortinet support team for your registered product. Please provide detailed information in the ticket to ensure efficient support.

Manage Tickets

Check ticket status, add comment, update contact or view history etc.

View Active Tickets

Check latest active tickets for current user, update ticket information or change ticket status.

Technical Web Chat

Provide quick answers on-line for general technical questions.

Contact Support

Contact information of Fortinet worldwide support centers.

Quick Links

- Firmware Images
- VM Images Download
- Service Updates
- Product Life Cycle
- Fortinet Service Terms & Conditions
- Guidelines, Policies & Documents
- Help Documents

Resources

- Customer Support Bulletin
- Knowledge Base
- Fortinet Video Library
- Fortinet Document Library
- Discussion Forums
- Training & Certification

Upgrade notes

In version 6.0.0, stricter checks have been added to manage IPs with ports used by all VS/mgmt service etc. If any conflicts are detected, an error message will be displayed: "The specified IP address and port are used by others."

When first upgrading from 5.x to 6.0, if there are any IP/port conflicts in the old configuration, you will see the following warning message in both the GUI and CLI shell: "Configure objects representing ip:port pairs are conflicted with pairs in other configure objects". The conflict ip+port service might not working.

There are two options for addressing these conflicts:

1. **Fix the conflicts.** Find the conflicts and correct them by using different ip:port pairs.
   All detected conflict objects are logged in "address_book_conflicts.log". In the GUI, go to **System > Debug**. After generating and downloading the debug file, you can find the file in the directory named "CMDB".

   After you have fixed the conflicts, you can verify by rebooting the system and checking whether the system still displays the error or warning message.
2. **Keep using the configuration with these conflicts.**
   You can remove the warning by entering the following in CLI:
   ```
   config system global
   set addrbook disable
   end
   ```
   Note: the conflicting ip:port pairs can make some service ports unavailable.