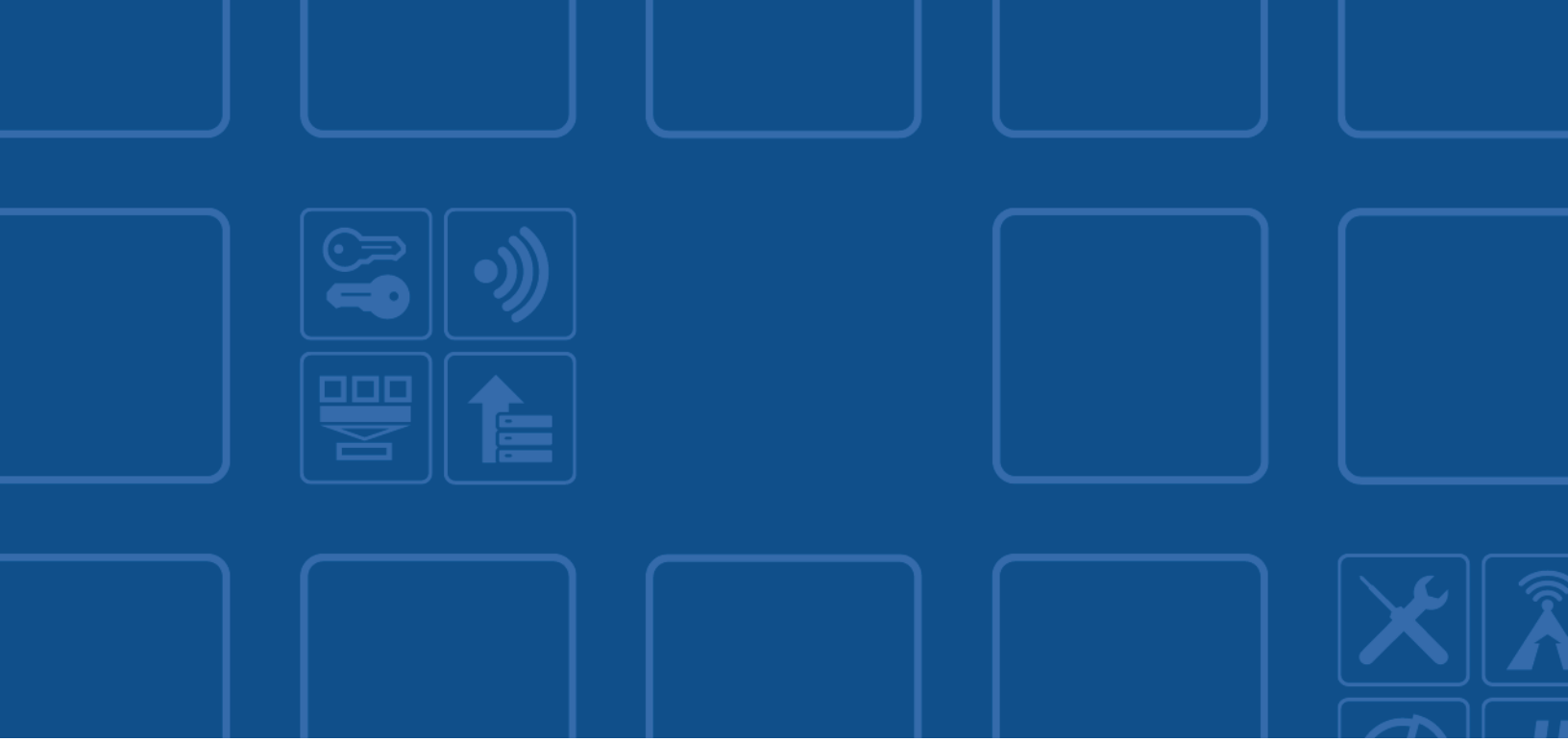
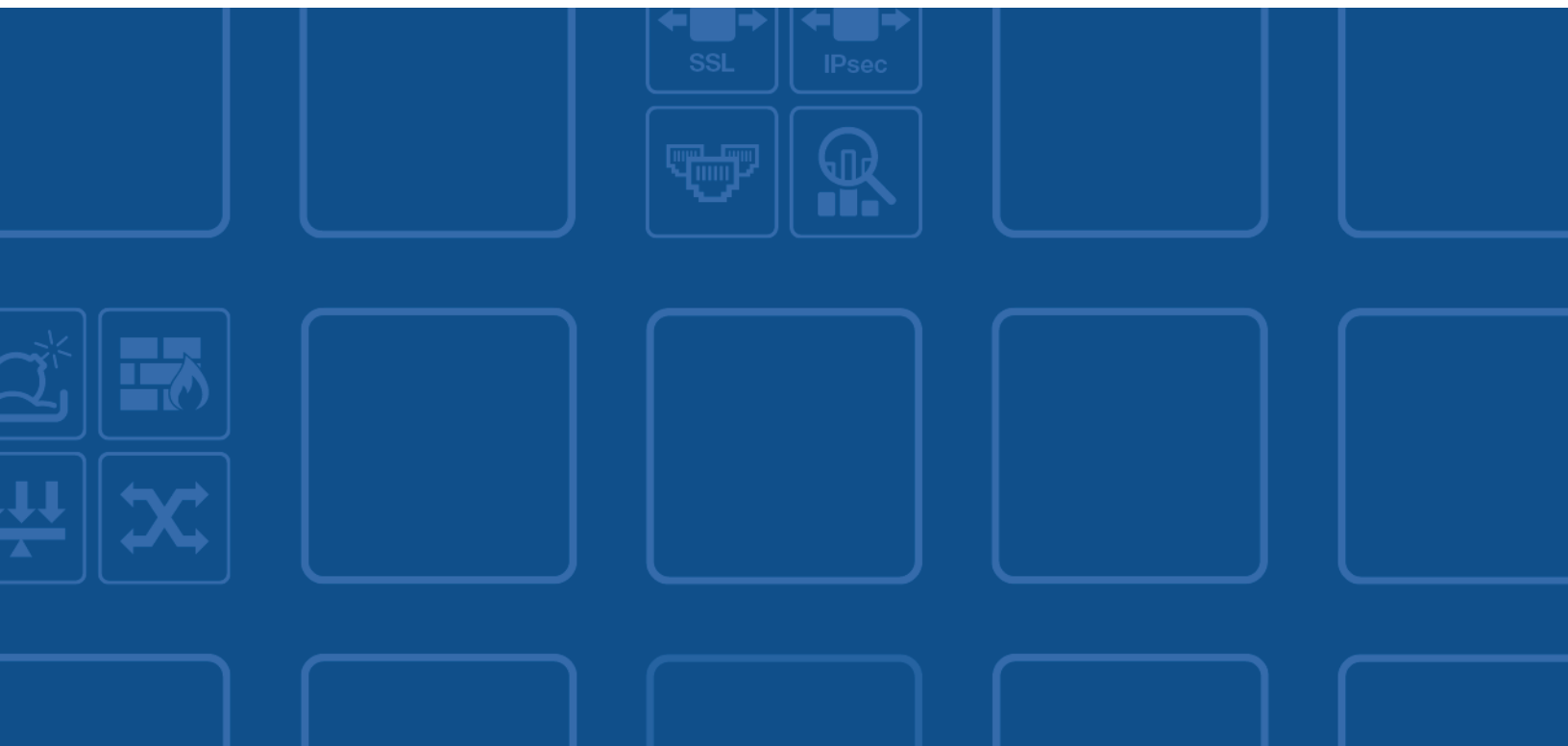


FortiWLM Wireless Manager 8.5

FIPS 140-2 and Common Criteria Technote



FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://www.fortinet.com/support/contact.html

FORTINET NSE INSTITUTE (TRAINING)

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT AND PRIVACY POLICY

https://www.fortinet.com/doc/legal/EULA.pdf

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdoc@fortinet.com

Friday, November 19, 2021

FortiWLM Wireless Manager 8.5 FIPS 140-2 and Common Criteria Technote

47-851-566289-20190620

TABLE OF CONTENTS

Introduction

Fortinet performs FIPS 140-2 and Common Criteria certifications on specific FortiWLM OS versions in combination with specific FortiWLM hardware models. At the publication date of this document, the latest CC certified version of FortiWLM is 8.5-2fips-7.

The documentation set for FortiWLM units operated in FIPS-CC mode consists of this document and the standard FortiWLM documentation set. This document covers Common Criteria specific installation instructions and explains the FortiWLMFIPS-CC mode of operation. The standard documentation is available from the Fortinet Technical Documentation web site (http://docs.fortinet.com).

For detailed information on the FortiWLM 8.5 Common Criteria certification, including the certified hardware models, refer to the FortiWLM 8.5-2fips-7 Security Target. The Security Target can be found on the Fortinet Support web site in the FortiWLM 8.5-2fips-7 firmware download directory (http://support.fortinet.com).

It is strongly suggested that all documents listed in the References section below be reviewed fully before starting configuration of FortiWLM hardware.

References

Security Target: Fortinet FortiWLM Wireless Manager 8.5 Security Target
FIPS 140-2 Security Policy: FortiWLM-100D/1000D, Version 2.2
Fortinet FortiWLM Wireless Manager 8.5 Release Notes
Fortinet FortiWLM Wireless Manager 8.5 User Guide

Certified Models

FortiWLM-100D	FortiWLM-1000D

The following items are excluded from the scope of the Common Criteria evaluation:
- The Virtual Edition of the application suite
- SNMP
- Remote Authentication
- IPv6
- Service Assurance Manager (SAM), Spectrum Manager, Wireless Intrusion Prevention System (WIPS)
- Logging to a syslog server
- Logging to FortiCloud

Installing the CC Certified Firmware

This section describes how to install the CC certified firmware on your FortiWLM unit.

Operating Environment

The following table list the Common Criteria Operating Environment assumptions and the specific product details. Note that TOE refers to the Common Criteria Target of Evaluation - i.e. the FortiWLM appliance.

Identifier	Description	Detail
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	The administrator is responsible for ensuring the physical security of the TOE. The TOE should be deployed in a secure location where access is restricted to trusted administrators.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	The TOE does not provide operating system level access. All access is through the Web-Manager GUI or CLI. Third party applications cannot be loaded onto the TOE.
OE.NO.THRU.PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.	The administrator is responsible for ensuring the through traffic is protected by other devices in the operational environment.
OE.TRUSTED.ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.	The administrator is responsible for reading the relevant product documentation and deploying the TOE in compliance with the documentation and best practices.

OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	The adminstrator is responsible for using the trusted update capability of TOE's FIPS-CC mode of operation to update the firmware as necessary.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	The administrator is responsible for ensuring the protection of their credentials (private key) on any system used to access the TOE remotely or used to host/back up the credentials.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.	The TOE provides tools for zeroizing keys and overwriting the TOE's persistent storage device(s). The administator is responsible for using the tools to destroy any residual information prior to removing the TOE from the secure operating environment.

Verifying secure delivery

Before installing the FortiWLM unit, you should take steps to ensure the unit has not been tampered with during transit. Perform the following checks to verify the integrity of the unit prior to installation.

- Courier - Fortinet only uses bonded couriers such as UPS, FedEx or DHL. Verify the shipment was received using a bonded courier.
- Shipping information - Verify the shipment information against the original purchase order or evaluation request. Verify the shipment has been received directly from Fortinet.
- External packaging - Verify the Fortinet branded packing tape sealing the packaging is intact and the packaging has not been cut or damaged to allow access to the unit.
- Internal packaging - Verify the unit is sealed in an undamaged, clear plastic bag for non-blade units. For blade units, verify the internal box packaging is intact.
- Warranty seal - Verify the unit's warranty seal is intact. The warranty seal is a small, grey sticker with the Fortinet logo and is normally placed over a chassis access screw. The chassis cannot be opened without destroying the warranty seal.

If you identify any concerns while verifying the integrity of the unit, contact your supplier immediately.

Registering the unit

Register your product in order to access firmware builds, customer support, etc. You can register your FortiWLM unit through the Fortinet Support Website. Refer to the Fortinet Support Website User Guide for details on registering your product.

Installation Requirements

Common Criteria compliant operation requires that you use the FortiWLM unit in its FIPS-CC mode of operation and that you follow secure procedures for installation and operation of the unit. You must ensure that:

- The FortiWLM unit is installed in a secure physical location.
- Physical access to the FortiWLM unit is restricted to authorized operators.

Installing the unit

The documentation shipped with your unit includes a FortiWLM QuickStart Guide and a model specific Hardware Supplement. The FortiWLM User Guide includes a Getting Started chapter that provides additional installation and configuration details. These documents provide instructions on the physical installation and initial configuration of your unit. When you have completed these procedures you will be able to access both the web-based manager and Command Line Interface (CLI).

Downloading the FIPS-CC certified firmware and MD5 check sums

To download the firmware and MD5 check sums

1. With your web browser, go to https://support.fortinet.com/ and log in using the name and password you received when you registered your unit with Fortinet Support.
2. Navigate to the FortiWLM 8.5 download page. Download the firmware build for your specific hardware model. Save the file on the management computer or on your network where it is accessible from the FortiWLM unit.
3. Download the md5sum.txt file from the same directory as the firmware. This file contains MD5 check sums for the firmware builds.

Verifying the integrity of the firmware build

Use a hashing utility to create an MD5 hash of the firmware build you downloaded. Compare the resulting hash to the corresponding hash from the `md5sum.txt` file. If the hashes match, the downloaded build is uncorrupted and unmodified.

Installing the FIPS-CC firmware build

Install the FIPS-CC firmware build on your FortiWLM unit. There are several methods to do this. Refer to the FortiWLM User Guide for more information.

Verifying the firmware version of the unit

Execute the following command from the command line:

```
show nms
```

The version line of the status display shows the FortiWLM model number, firmware version and build number. For example:

```
Software Version : 8.5, 2fips-7
```

```
Server Model : FortiWLM-1000D
```

Verify in the relevant security target or security policy document that your firmware version, build number and date are correct.

Potential Firmware issues

If the unit is not booting correctly and power cycling the unit does not clear the problem, then it may be necessary to reinstall the firmware. The firmware can be reinstalled using the FortiWLM BIOS boot menu and a remote tftp server. The BIOS can also be used to format the boot device prior to reinstalling the firmware to ensure a clean installation.

Refer to the following Technical Note for more details: Navigating the FortiGate BIOS. Although the document is titled "Navigating the FortiGate BIOS", the content is equally applicable to FortiWLM.

You may want to contact Fortinet's technical support group before attempting to use the FortiWLM BIOS tools. You can open a support ticket on the support website.

Potential Hardware issues

If the unit fails any of the startup hardware checks or displays a hardware fault during operation, contact Fortinet technical support.

Entropy

Generation of strong encryption keys requires a strong source of random data, also referred to as entropy. FortiWLM units uses an entropy token (Araneus Alea II) as a strong entropy source.

Installing the entropy token

Plug the entropy token into an available USB port on the FortiWLM unit. Note that the entropy token requires a USB-A port.

The FIPS-CC Mode of Operation

If you have verified the firmware version, you are ready to enable FIPS-CC mode.

When you enable FIPS-CC mode, the existing configuration is cleared and restrictive default settings are implemented.

You must use a console connection to enable FIPS-CC mode. Enabling FIP-CC mode is not supported via the GUI or SSH in FortiWLM.

The new password must be at least 8 characters long and must contain at least one each of:

- upper-case-letter
- lower-case-letter
- numeral
- non-alphanumeric character

Connecting via CLI and GUI Interfaces

FortiWLM supports configuration via the Command Line Interface (CLI) and the Graphical User Interface (GUI). Detailed instructions on connecting to the FortiWLM via the CLI and GUI interfaces are located in the FortiWLM User Guide.

Enabling FIPS-CC mode

Use the following steps to enable FIPS-CC mode:

1. Log in to the CLI through the console port. Use the default admin account and password. The module requires that the default password immediately be changed and verified (re-entered).

2. Enter the following commands:

```
configure terminal
   fips-cc entropy-token enable
   fips-cc status enable
```

   Note: After entering the "fips-cc status enable" command the module will prompt for the admin password to be entered.

3. Enter admin password. If authentication is successful the CLI displays the following message:

```
   Authentication Success
This operation will do factory reset with FIPS default configurations and go for reboot. Do
you want to continue?[y/N]:
```

4. Enter `y`. The FortiWLM unit restarts and is now running in FIPS-CC mode.Note: Step 1 needs to be repeated after the unit restarts.
5. Verify FIPS mode is enabled. The `show fips` CLI command output should include “fips-status : enable”.

```
Fips Configuration:

fips-status:                enable
```

Disabling FIPS-CC mode

To disable the FIPS-CC mode of operation, reset the unit to the factory default configuration using the following CLI command:

```
configure terminal
fips-cc status disable
```

Disabling FIPS-CC mode erases the current configuration and zeroizes most keys and critical security parameters. To completely zeroize the unit, refer to the instructions in the next section.

Common Criteria Compliant Operation

Use of non-CC evaluated features

FIPS-CC mode does not prevent you from using features that were not part of the evaluated configuration. However, if you use these features, you may not be operating the FortiWLM unit in strict compliance with the Security Target. Refer to the Security Target for more information.

Install Updated Certificates

By default, FortiWLM units use a certificate signed by a Fortinet Certificate Authority (CA). Administrators should install a new, signed certificates from a trusted CA. Consult the FortiWLM User Guide for additional information on replacing the default certificate.

Regarding certificate validity checking, a certificate revocation check is performed using the OCSP protocol, therefore, it is mandatory for all externally generated and uploaded certificates to have an OCSP URI. The TOE contacts the OCSP URI in the certificate to verify the revocation status of the certificate. The connection proceeds further only if the certificate is determined to remain active and not revoked.

The administrator cannot specify a default action.

Only the SAN is required and the allowed value is the DNS name. An OCSP URI is mandatory to perform OCSP revocation checks. No other fields are mandatory for certificate generation.

Key Zeroization

All keys and CSPs are zeroized by erasing the unit's boot device and then power cycling the unit. To erase the boot device, execute the following command from the CLI:

```
fips-cc status disable
```

Erasing the unit's boot device will leave the unit unbootable. The firmware can be reinstalled used the FortiWLM BIOS boot menu tools and a TFTP server.

Common Criteria Compliant Operation

Use of non-CC evaluated features

FIPS-CC mode does not prevent you from using features that are not part of the evaluated configuration. However, if you use these features, you may not be operating the FortiWLM unit in strict compliance with the Security Target. Refer to the Security Target for more information.

Installing updated certificates

By default, FortiWLM units use a certificate signed by a Fortinet Certificate Authority (CA). Administrators should install a new, externally generated and signed certificate from a trusted CA. Refer to the Certificate Management section of the he FortiWLM User Guide for guidance on replacing the default certificate. Note that certificates must include the SAN extension.

Certificate Management

The FortiWLM user interface provides the infrastructure to manage the SSL certificates for various server applications requiring SSL certificate based authorization. Navigate to the Certificate Management section in the FortiWLM GUI to create, import, and manage certificates. Refer to the Certificate Management section of the FortiWLM User Guide for further guidance.

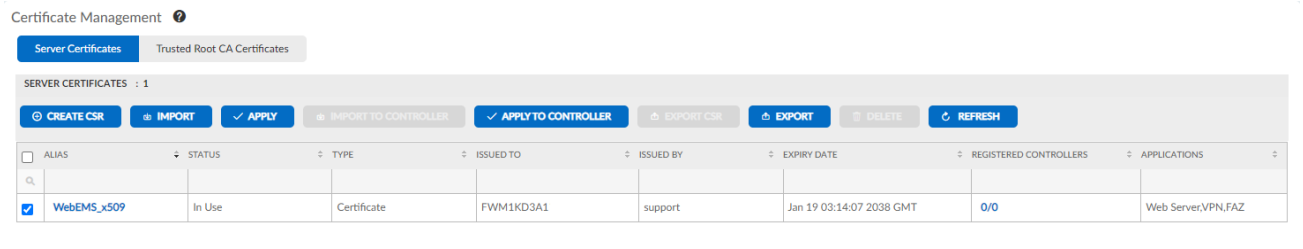


Figure 1 - Server certificate management

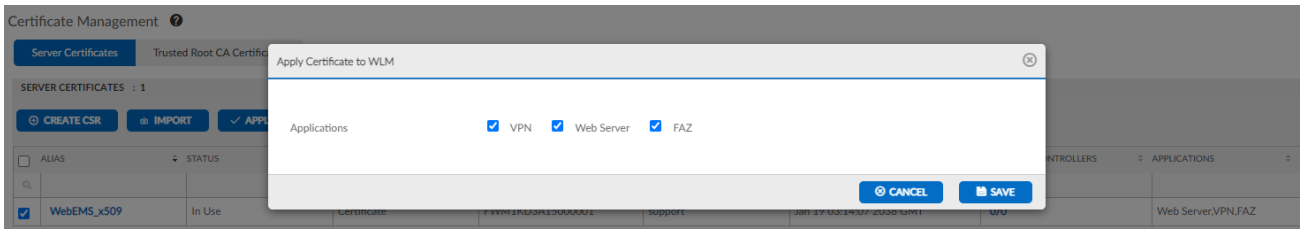
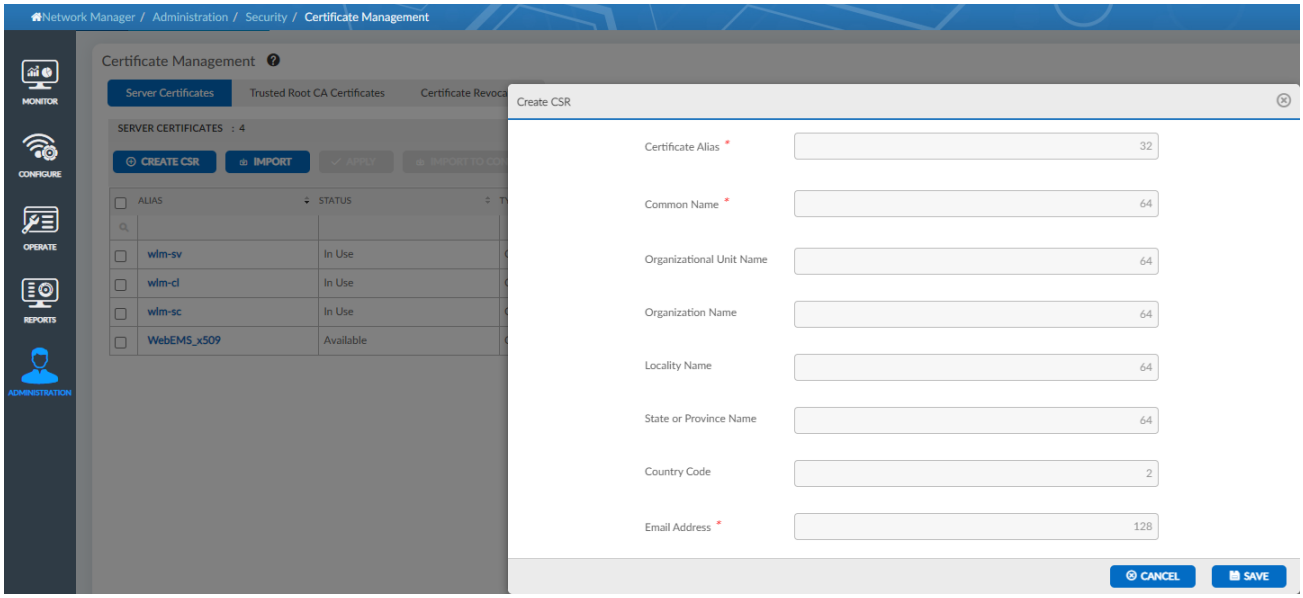


Figure 2 - Applying the server certificate to applications

Generating a Certificate Signing Request (CSR)

For detailed configuration steps on generating a CSR please refer to the section Certificate Management of the FortWLM User Guide.



FortiWLC VPN client configuration (server side)

For guidance on configuring the FortiWLC client connection on the FortiWLM (server) side, refer to the VPN Administration section of the FortiWLM User Guide. Note that the SAN/CN client attribute resource identifier must be set.

The server only allows TLS protocol version 1.2 (rejecting any other protocol version) and is restricted to the following ciphersuites by default:

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Diffie-Hellman Group 14 is used with the DHE (2048 bits) cipher suite.

Session tickets are supported and follow the structure defined by RFC 5077. Tickets are protected using AES128 CBC and HMAC SHA256. Keys are randomly generated for both algorithms.

FortiWLM does not support any fallback authentication functions.

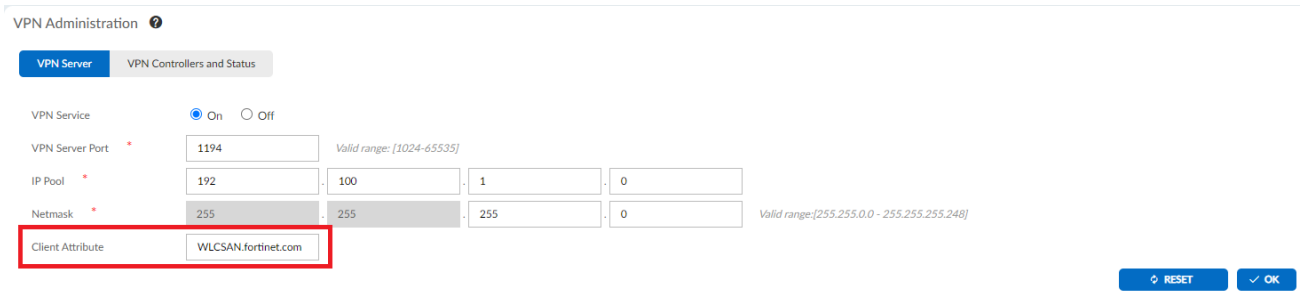


Figure 3 - VPN client configuration (server side)

FortiWLC VPN client configuration (client side)

For guidance on configuring the FortiWLC client connection on the FortiWLC (client) side, refer to the Security Certificates and the Configuring OpenVPN Client Connections sections of the FortiWLC Configuration Guide. Note that the SAN/CN server attribute resource identifier must be set.

The TLS server is capable of negotiating ciphersuites that include DHE, and ECDHE key agreement schemes. The DHE key agreement parameters are restricted to 2048 bits and are hardcoded into the server.

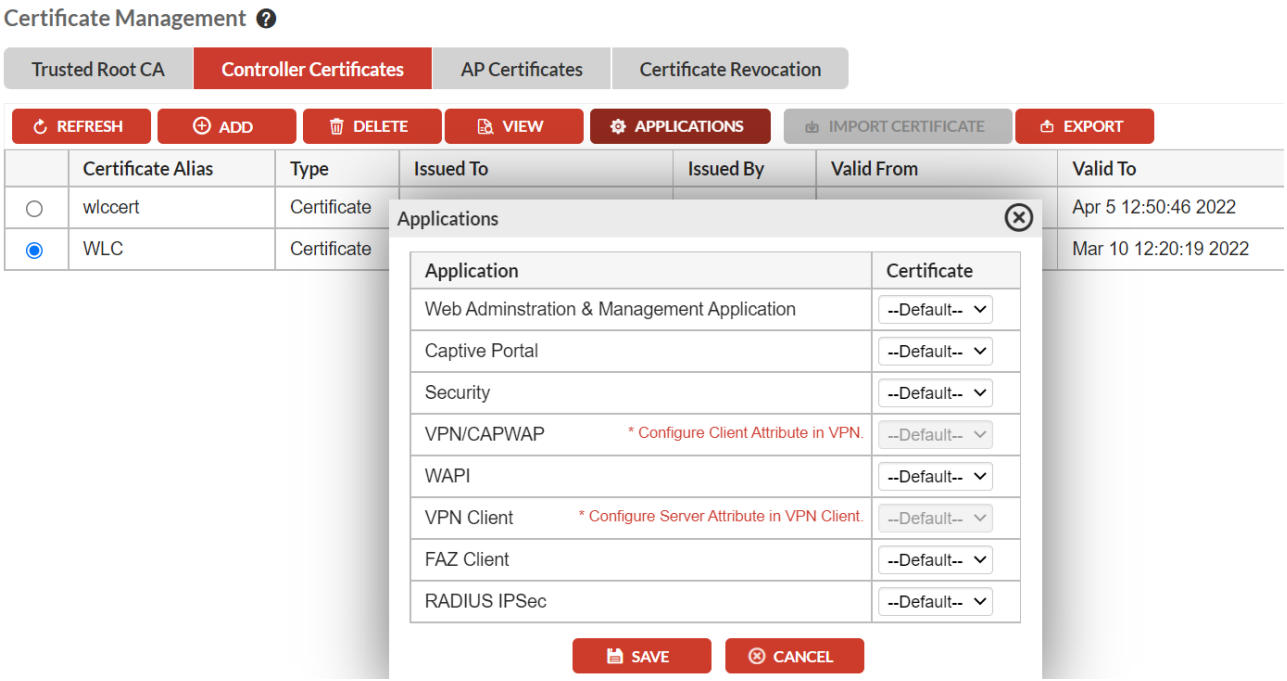


Figure 4 - Setting the VPN client certificate

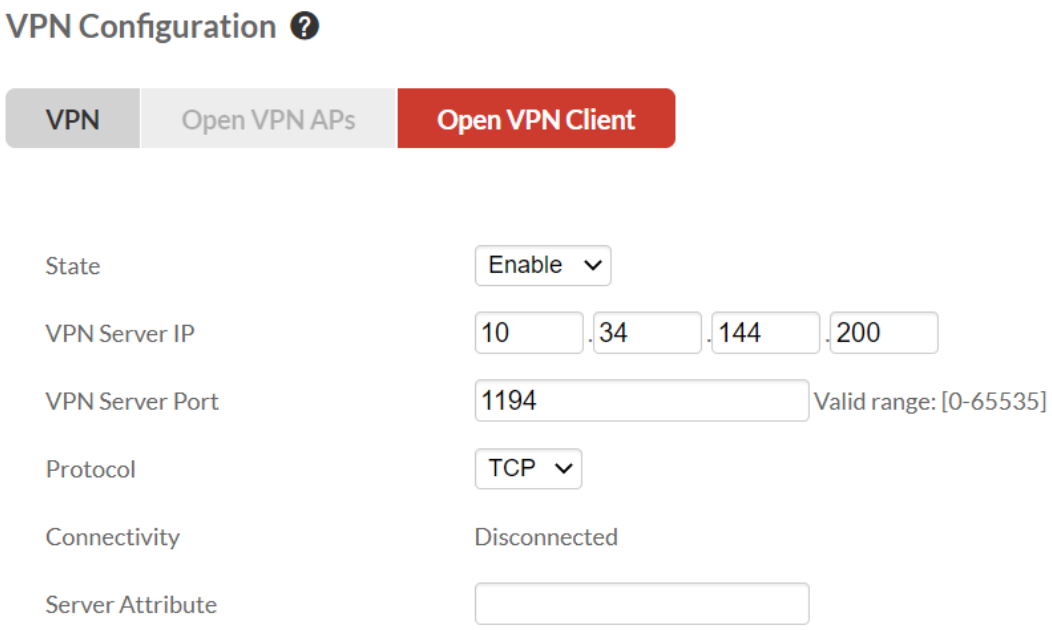


Figure 5 - VPN server configuration (client side)

Certificate revocation checks

The certificate revocation check is performed using the OCSP protocol, therefore, it is mandatory for all externally generated and uploaded certificates to have an OCSP URI. The TOE contacts the OCSP URI in the certificate to verify the revocation status of the certificate. The connection proceeds further only if the certificate is determined to remain active and not revoked. The TOE accepts the certificate, if OCSP responder is not reachable.

Administration

This section describes administration specific issues and changes to the way FortiWLM functions in the FIPS-CC mode of operation.

Remote access requirements

In FIPS-CC mode, remote administration via HTTP or Telnet is disabled by default. HTTPS, SSH or the console should be used. The FIPS-CC mode of operation restricts the cipher suites used by HTTPS and SSH to a subset of the NDcPP compliant suites. Refer to the next section for additional information. The administrator does not need to take any specific actions to ensure compliance when using HTTPS or SSH as long as the FIPS-CC mode of operation has been enabled. Session tickets are supported and follow the structure defined by RFC 5077. Tickets are protected using AES128 CBC and HMAC SHA256. Keys are randomly generated for both algorithms.

Supported TLS cipher suites

The TOE supports the following list of TLS cipher suites. The supported cipher suites are hard coded and cannot be configured by the admin.

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

TLS 1.1 supports a subset of the above suites (it does not support SHA256 or SHA384).

To use the web-based manager in FIPS-CC mode, your web browser application must use TLS 1.2 or TLS 1.1 and support one of the listed cipher suites. The ECC P-256 curve is used in ECC cipher suites and RSA 2048 bit certificates are used in RSA cipher suites. Diffie-Hellman Group 14 is used with the DHE (2048 bits) cipher suite and ECDHE (secp256r1).

SSH parameters

FortiWLM implements the following SSH parameters:

- RFCs 4251 through 4254, 5647, 5656, 6187 and 6668.
- Password-based or public key authentication using ssh-rsa, rsa-sha2-256 or rsa-sha2-512 and RSA 2048 bit certificates.
- Encryption using AES-CBC-128 and AES-CBC-256.

- Data integrity using HMAC-SHA1, HMAC-SHA2-256 and HMAC-SHA2-512.
- Key exchange using Diffie-Hellman Group 14 SHA-1 (diffie-hellman-group14-sha1).

Also, note that:

- FortiWLM examines the size of each received SSH packet. If the packet is greater than 256KB, it is automatically dropped.
- FortiWLM will re-key SSH connections after 1 hour or after an aggregate of 1 GB of data has been exchanged (whichever occurs first).

SSH rekey values are configurable for time based and traffic based thresholds, the commands for time based threshold is : ssh rekey time <time in seconds> and traffic based threshold is : ssh-server rekey data <data in MB>

SSH Authentication using RSA Keys

FortilWLM supports SSH authentication using RSA Keys. The administrator must first import the RSA public keyfor the admin account using the CLI. The configuration steps are as follows:

```
configure terminal
password-config set-pubkey-admin <setpubkey> Configures RSA Public Key for Admin User
end
```

Afterwards the admininistrator may use RSA Keys for SSH Authentication:

```
ssh admin@<WLM IP Addr>-i id_rsa -o PreferredAuthentications=publickey -c aes128-cbc
```

Configuration backup

Configuration backup files created in FIPS-CC mode are not compatible with backup files created in non-FIPS-CC mode. A FIPS-CC mode configuration backup cannot be restored in non-FIPS-CC mode and vice-versa.

You can create FIPS-CC configuration backup files to use for disaster recovery. They are valid on a replacement FortiWLM unit or to restore configuration after you exit and then re-enter FIPS-CC mode.

Refer to the FortiWLM User Guide for detailed information about creating configuration backup files.

Admin user administration

In FIPS-CC mode of operation the FortiWLM only supports the default admin user. To change the admin user password navigate to the User Administration section in the FortiWLM GUI and edit the displayed admin user account.

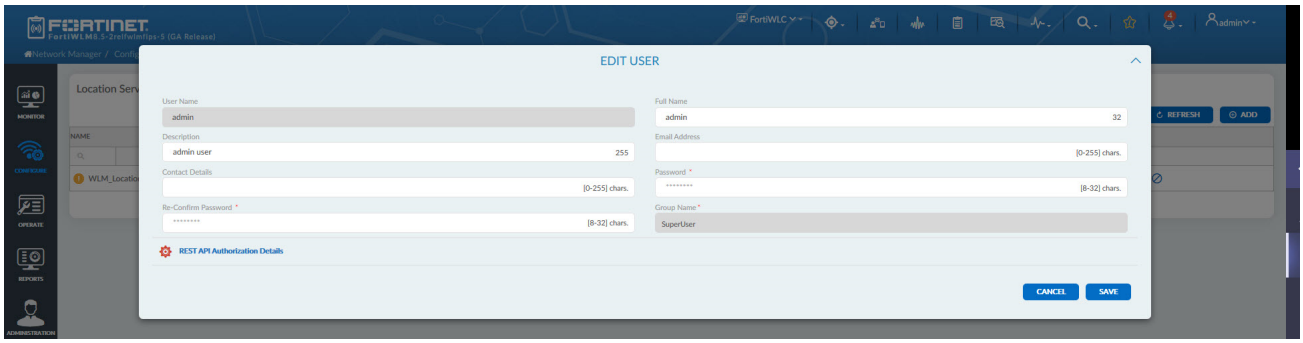


Figure 6 - User administration GUI

Password policy and authentication failure configuration

The password policy for FortiWLM is configured via the CLI using the following commands:

```
configure terminal
password-config set-pass-minlen <value> Password minimum length should be number in the
    range of 8 to 15
```

The authentication failure settings are configured using the following CLI commands:

```
configure terminal
auth-config
    reset-user admin Reset lock for admin user
    set-deny-count <value> Configures Maximum Retry Count for Locking between 1-5
    set-lock-time <value> Enter locking period as integer value in seconds
```

Configuring session timeout

To configure the session timeout in minutes for SSH and GUI sessions, navigate to Administration > System Settings > Maintenance. The default timeout is five minutes.

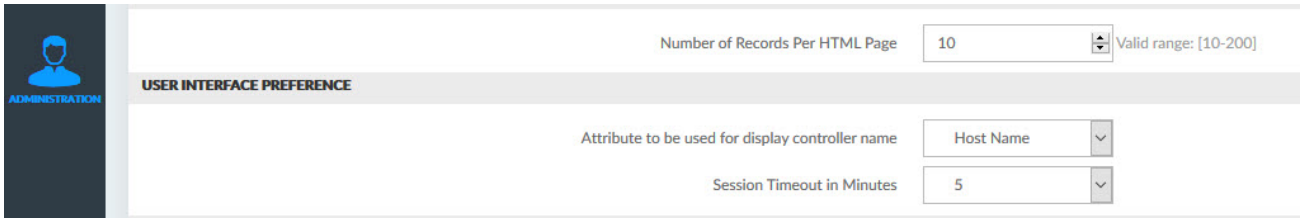


Figure 7 - User interface preferences

Configuring date and time

The FortiWLM hardware clock and Network Manager Server date and time can be set via the CLI using the following commands:

```
calendar set <MM/DD/YYYY> Enter the date in MM/DD/YYYY to set the date.
```

To verify the configured date and time run the following CLI command:

```
date
```

Configuring X.509 Certificates for FortiWLM to FortiWLC Authentication

The FortiWLM provides infrastructure to manage SSL certificates for various server applications that require SSL certificate based authorization.

Navigate to *Administration* > *Security Administration* > *Certificate Management* in the FortiWLM GUI to create, import, and manage certificates.

Figure 8 - Certificate Management

For more information see section **Certificate Management** in the *FortiWLM User Guide*.

You can apply certificates to VPN and other applications, to configure the client attribute for VPN connection, that is, the Reference Identifier of client certificate (SAN /CN of FortiWLC certificate), see section **VPN Administration** in the *FortiWLM User Guide*.

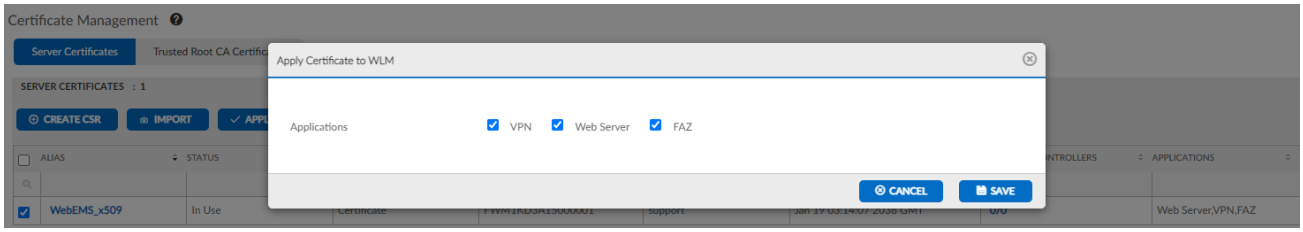


Figure 9 - Apply Certificate to WLM

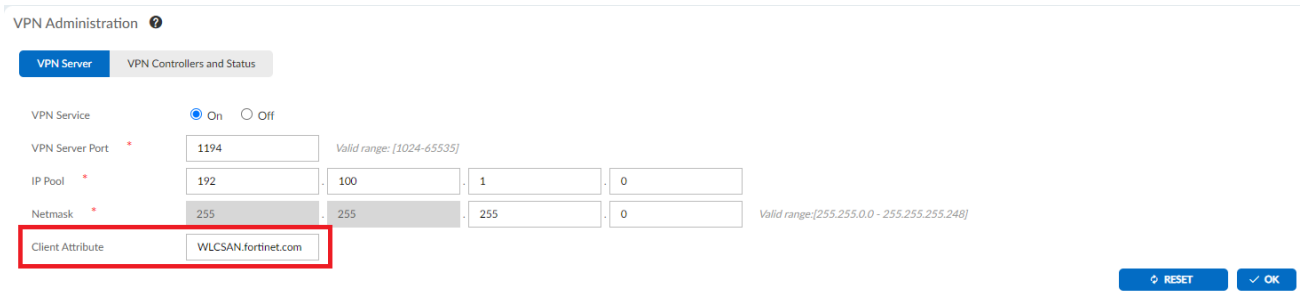


Figure 10 - VPN Administration GUI

To configure and manage certificates in FortiWLC, see section **Security Certificates** in the *FortiWLC Configuration Guide*.

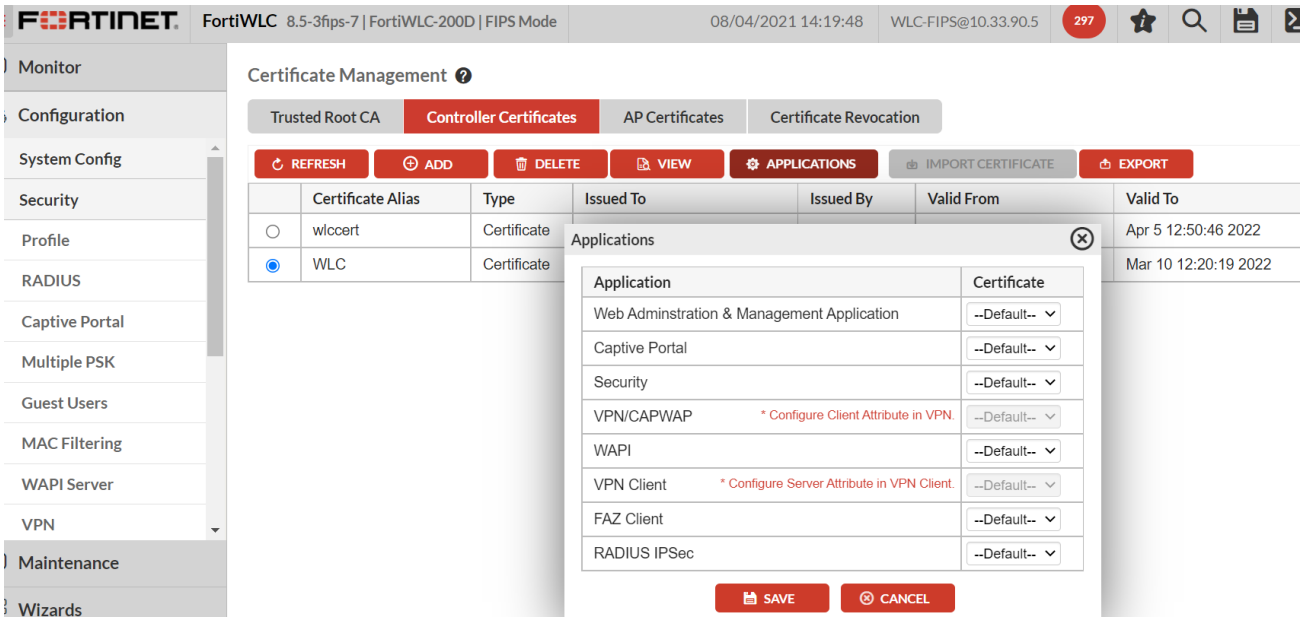


Figure 11 - FortiWLC Certificate Management

To configure the server attribute for VPN clients, that is, the Reference Identifier of Server certificate (SAN /CN of the FortiWLM certificate). See section **Configuring OpenVPN Client Connections** in the *FortiWLC User Guide*.

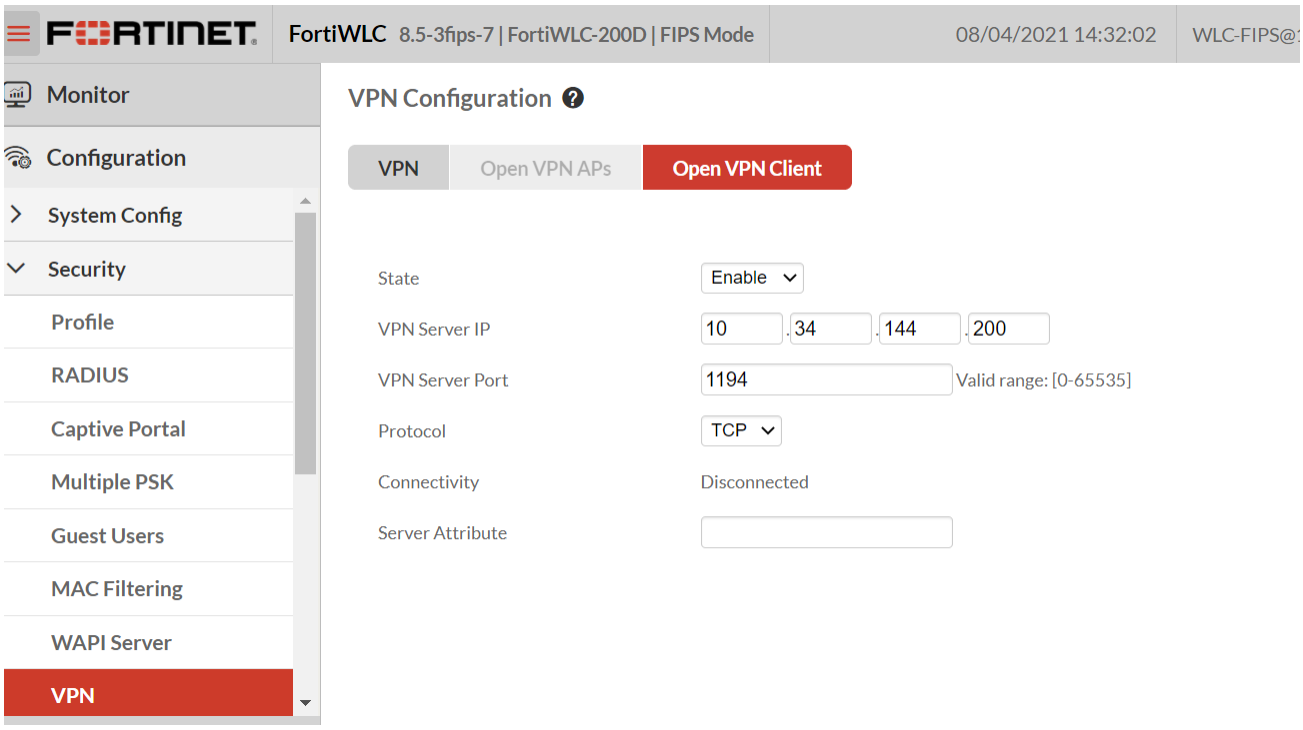


Figure 12 - FortiWLC VPN Configuration

Admin access disclaimer

In order to meet NDcPP (Network Device Protection Profile) compliance, a pre-login disclaimer banner must be enabled.

To enable the disclaimer, log in to the FortiWLM GUI using the default admin account or another account with a super_ admin access profile. Navigate to the Login Banners section of the FortiWLM GUI.

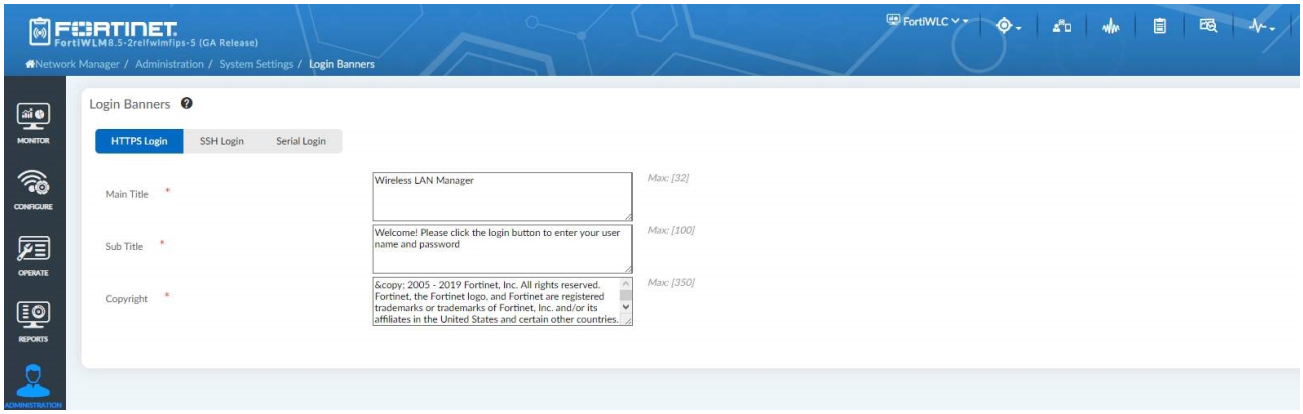


Figure 13 - Admin access disclaimers

Self-tests

The FIPS-CC mode of operation includes a set of startup and conditional self-tests. The tests include algorithm known answer tests (KATs), a firmware integrity test and a configuration bypass test. Refer to the FortiWLM 8.5 Security Policy for a complete list of the self-tests.

The administrator can run self-tests manually at any time. To run all of the tests, enter the following CLI command:

```
configure terminal
fips-cc kat all
```

To run an individual test, enter:

```
configure terminal
fips-cc kat <test_name>
```

To see the list of valid test names, enter: `fips-cc kat ?`

Trusted updates

The FIPS-CC mode of operation uses 2048 bit RSA signatures to verify the integrity of firmware update files. The firmware images are signed with a Fortinet private key and the appliance will verify the integrity of the firmware image before starting the update procedure.

If the signature is verfied, the following message is displayed on the console and the update proceeds normally:

```
Firmware image verified.
```

If the signature fails verification, the following message is displayed and the update procedure will terminate:

```
Image upgrade failed.
```

FIPS Error Mode

If one or more of the FIPS self-tests fail, the FortiWLM unit switches to FIPS Error mode. The unit shuts down all interfaces including the console and blocks traffic. To resume normal FIPS-CC mode operation, power cycle the unit. If the self-tests pass after the reboot, the unit will resume normal FIPS-CC operation. If a self-test continues to fail after rebooting, there is likely a serious firmware or hardware problem and the unit should be removed from the network until the problem is solved.

Terminating local and remote administration sessions

Local console and remote CLI administration sessions are terminated (i.e. the administrator can log out) by entering "exit" at the top level of the CLI.

Remote Web-Manager administration sessions are terminated by clicking on your user name in the top right-hand corner of the Web-Manager and then selecting "Logout".

Miscellaneous administration related changes

- By default, after three failed attempts to log on to an administrator account, the account is locked out for 5 minutes. You can change the number of attempts permitted and the length of the lockout.
- On a CLI session, when an administrator logs out or the session times out, the FortiWLM unit sends 300 carriage return characters to clear the screen. Note: if your terminal buffer is large, not all information from the session may be cleared.
- When configuring passwords or keys, the FortiWLM unit requires you to enter the password or key a second time as confirmation.
- The `maintainer` account, which allows you to reset the admin password, is disabled.
- USB auto-install options are disabled.
- The fnsysctl command, which provides some access to the underlying operating system in the default mode of operation, is not available.
- Virus attack reporting to FortiGuard Distribution Service (FDS) is disabled.

Logging

This section describes logging specific issues and changes to the way FortiWLM functions in the FIPS-CC mode of operation.

Logging to external devices

Offloading logs to a remote server over a secure connection is required to maintain CC compliance. When operating in FIPS-CC mode, FortiWLM supports log offloading over SSL to a FortiAnalyzer device only.

Log messages are cached on the local FortiWLM unit before being offloaded to the remote FortiAnalyzer device. The log messages are cached on the local disk or in system memory if the unit does not have disk storage. The log message cache is separate and distinct from local log storage.

Only TLS 1.2 protocol version is allowed and ciphersuites are restricted to the following:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

The TLS client will transmit the Supported Elliptic Curves extension in the Client Hello message by default with support for the following NIST curves: P256. Diffie-Hellman Group 14 is used with the DHE (2048 bits) cipher suite and ECDHE (secp256r1).

The reference identifier type expected and accepted for *x509_validate_string < FAZ server x509 validation string>* is the DNS name.

FortiAnalyzer configuration

Connections to a FortiAnalyzer device in the FIPS-CC mode of operation require the FortiAnalyzer's X.509 certificate be loaded onto the FortiWLM device. To configure the FortiAnalyzer device connection, use the following CLI commands.

```
configure terminal
logserver ?
   name <IPv4 address of FortiAnalyzer>
   port <Configure port number of external audit server>
   x509_validate_string < FAZ server x509 validation string>
```

A client certificate must be configured on the FortiWLM for use with the FortiWLM to FortiAnalyzer connection. Navigate to the Certificate Management section in the FortiWLM GUI to configure the client certificate.

For DNS Name matching, the hostname must be an exact match or wildcard match. In the case of a wildcard match; the wildcard must be the left-most component, wildcard matches a single component, and there are at least two non-wildcard components.

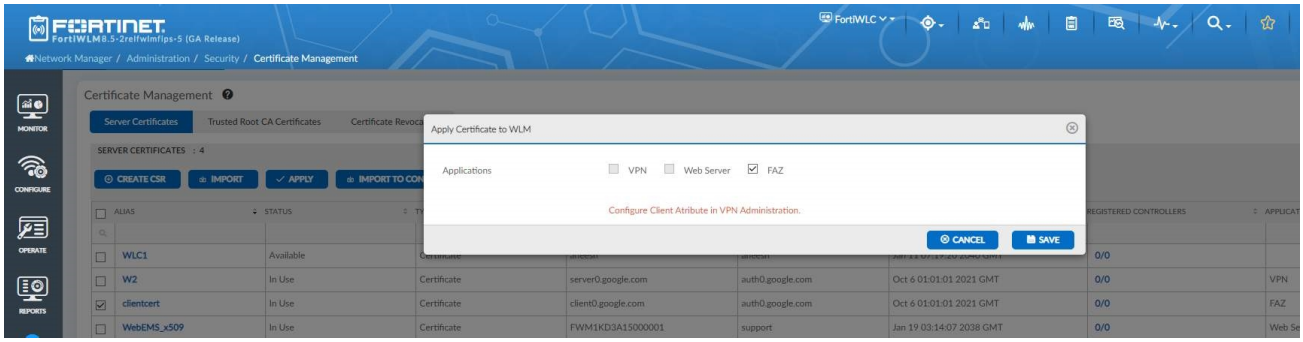


Figure 14 - Configuring a client certificate for FortiAnalyzer

Local logging

Logs are written to the FortiWLM unit's hard disk. The default log setting is to overwrite the oldest log entries once the local log capacity is reached.

The System Event Log contains log entries for when:

- Local log files are rolled (new log file created)
- Local log files are deleted (old log files are overwritten)

Clearing local logs

The local logs can be cleared from the GUI or the CLI. Clearing the local logs does not affect cached logs - i.e. logs cached for offloading to a remote FortiAnalyzer unit.

Miscellaneous Logging

- The Common Criteria protection profile requires logging of all traffic and logging of system events, including startup and shutdown of functional components. Logging is enabled by default for:
  - new security policies
  - interfaces where administrative access is enabled
  - attempts to gain administration access on network interfaces where administrative access is not enabled
  - failed connection attempts to the FortiWLM unit using TCP/IP ports other than 22 (ssh), 23 (telnet), 80 (HTTP), and 443 (HTTPS).
  - all configuration changes
  - configuration failures
  - remote IP lockout due to reaching maximum number of failed login attempts
  - log viewing
  - interface going up or down

  - other traffic: dropped ICMP packets, dropped invalid IP packets, session start and session deletion
- Logging is enabled for all event types at the information severity level.
- Memory logging is enabled on units that do not contain a hard disk. Logging includes traffic logging and all event types. Note that traffic logging to memory is available only in FIPS-CC mode and the log capacity is restricted by the available memory in the unit.
- The diskfull action is set to overwrite.

For a complete list of applicable FortiWLM audit logs, please refer to the document "Fortinet Audit Event Logging FortiWLM", pages 12-17, located at https://docs.fortinet.com/document/fortiwlm/8.5.0/fortiwlm-audit-event-logging.

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.