Extreme networks

WiNG Controller and Access Point v7.9.X.X CLI Reference Guide Delta

9039474-00 Rev AB
February 2026

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Open Source Declarations

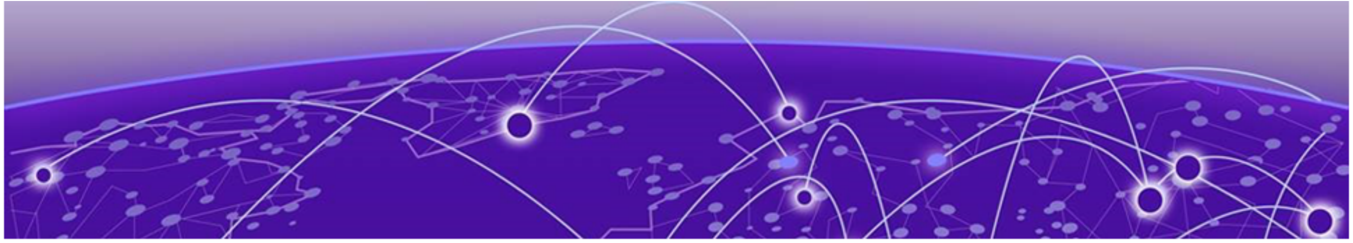
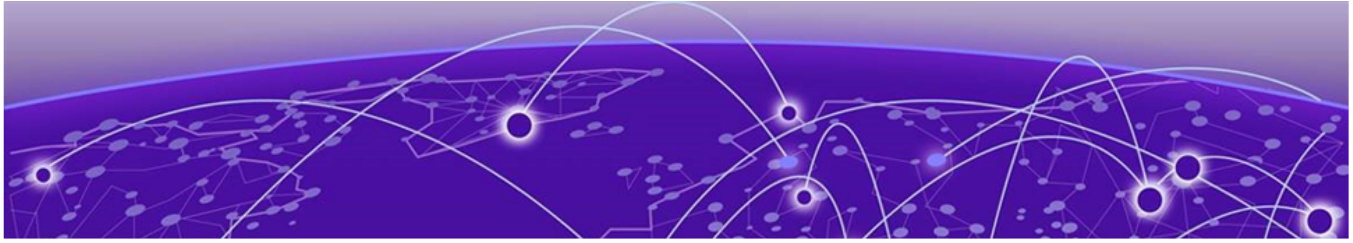


Table of Contents



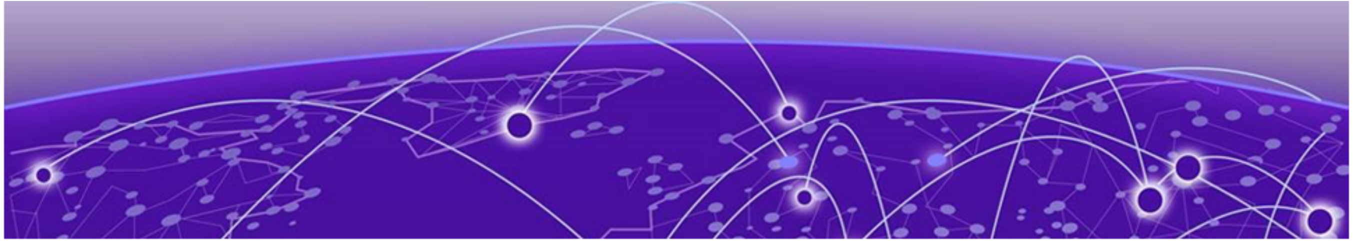
About this Document

The WiNG Controller and Access Point v7.9.X.X CLI Reference Guide Delta describes updates to CLI commands in release 7.9.6.0 and 7.9.7.0. Use this information in conjunction with the WiNG Controller and Access Point v7.9.5.1 CLI Reference Guide for complete instructions.

WiNG Controller 7.9.7.0 CLI Command Changes

The following table summarizes changes that have been made to WiNG Controller CLI commands in release 7.9.7.0.

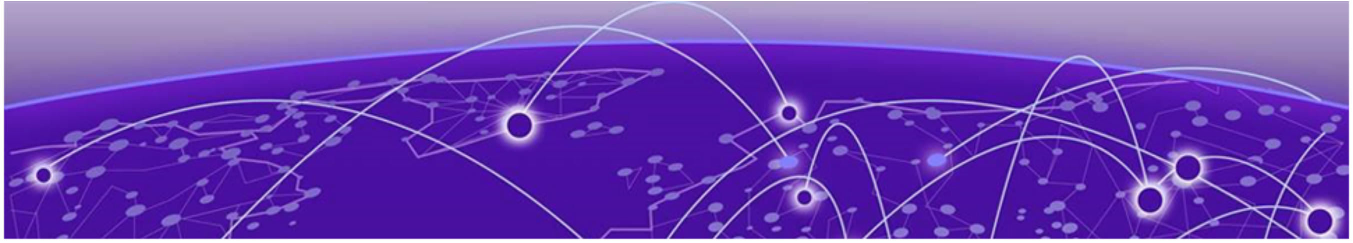
Command	Change Description
device-upgrade operational-mode	Users can now choose to migrate eligible Universal Access Points that are managed locally by WiNG to either centrally managed by ExtremeCloud IQ Controller or cloud managed by ExtremeCloud IQ.
encryption-type on page 33	GCMP encryption is supported only on AP3000, AP3000X, and AP5010. A note has been added to advise users.
bridge on page 37	Assigning Client Bridge to 6 GHz radios is not recommended, since throughput is sub-optimal.



WiNG Controller 7.9.6.0 CLI Command Changes

The following table summarizes changes that have been made to WiNG Controller CLI commands in release 7.9.6.0.

Command	Change Description
crypto pki export trustpoint	Users are now prompted to enter a password if no password is included in the command syntax.
process-monitor	This command has been added to profile and device commands to allow for configuration a watchdog process to monitor the Radio Interface Module (RIM), and re-initialize it if necessary.



User Exec Mode Commands

crypto

Enables digital certificate configuration and RSA Keypair management. Digital certificates are issued by CAs and contain user or device specific information, such as name, public key, IP address, serial number, and company name. Use this command to generate, delete, export, or import encrypted RSA Keypairs and generate Certificate Signing Request (CSR).

> **Note**
> This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported on the following devices:

- Access Points: AP3000, AP3000X, AP5010, AP310i/e, AP410i/e, AP505i, AP510i/e, AP560i, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8533.
- Service Platforms: NX5500, NX7500, NX9500, NX9600
- Virtual Platforms: CX9000, VX9000

Syntax

```
crypto [key|pki]
crypto key [export|generate|import|zeroize]
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL {background|on|passphrase}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
crypto key generate rsa <RSA-KEYPAIR-NAME> [2048|4096] {on <DEVICE-NAME>}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {background|on|passphrase}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
crypto key zeroize rsa <RSA-KEYPAIR-NAME> {force} {(on <DEVICE-NAME>)}
crypto pki [authenticate|export|generate|import|zeroise]
crypto pki authenticate <TRUSTPOINT-NAME> <LOCATION-URL> {background} {(on <DEVICE-NAME>)}
crypto pki export [request|trustpoint]
crypto pki export request [generate-rsa-key|short|use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> autogen-subject-name [<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> autogen-subject-name (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)
crypto pki export request [generate-rsa-key|short [generate-rsa-key|use-rsa-key]|use-rsa-key] <RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION> <ORGANIZATION-UNIT> (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)
crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME)}
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name]
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> autogen-subject-name {(email <SEND-TO-EMAIL>, fqdn <FQDN>,ip-address <IP>,on <DEVICE-NAME>)}
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION> <ORGANIZATION-UNIT> {(email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>,on <DEVICE-NAME>)}
crypto pki import [certificate|crl|trustpoint]
crypto pki import [certificate|crl] <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background} {(on <DEVICE-NAME>})
crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
crypto pki zeroize trustpoint <TRUSTPOINT-NAME> {del-key} {(on <DEVICE-NAME>)}
```

Parameters

```
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
```

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
export rsa <RSA-KEYPAIR-NAME>	Exports an existing RSA Keypair to a specified destination • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.
<EXPORT-TO-URL>	Specify the RSA Keypair destination address. Both IPv4 and IPv6 address formats are supported (see Usage Guidelines on page 18). After specifying the destination address (where the RSA Keypair is exported), configure one of the following parameters: background or passphrase.
background	Optional. Performs export operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on.
passphrase <KEY-PASSPHRASE> background	Optional. Encrypts RSA Keypair before exporting • <KEY-PASSPHRASE> – Specify a passphrase to encrypt the RSA Keypair. ◦ background – Optional. Performs export operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the export on.
on <DEVICE-NAME>	The following parameter is recursive and common to all of the above parameters: • on <DEVICE-NAME> – Optional. Performs export operation on a specified device ◦ <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto key generate rsa <RSA-KEYPAIR-NAME> [2048|4096] {on <DEVICE-NAME>}
```

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
generate rsa <RSA-KEYPAIR-NAME> [2048|4096]	Generates a new RSA Keypair • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. ◦ [2048|4096] – Sets the size of the RSA key in bits. The options are 2048 bits and 4096 bits. The default size is 2048 bits.

	After specifying the key size, optionally specify the device (access point or controller) to generate the key on.
on <DEVICE-NAME>	Optional. Generates the new RSA Keypair on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {background|passphrase <KEY-
PASSPHRASE> background} {(on <DEVICE-NAME>)}
```

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
import rsa <RSA-KEYPAIR-NAME>	Imports a RSA Keypair from a specified source • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.
<IMPORT-FROM-URL>	Specify the RSA Keypair source address. Both IPv4 and IPv6 address formats are supported (see Usage Guidelines on page 18). After specifying the source address (where the RSA Keypair is imported from), configure one of the following parameters: background or passphrase.
background	Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on.
passphrase <KEY-PASSPHRASE> background	Optional. Decrypts the RSA Keypair after importing • <KEY-PASSPHRASE> – Specify the passphrase to decrypt the RSA Keypair. ◦ background – Optional. Performs import operation in the background. After specifying the passphrase, optionally specify the device (access point, controller, or service platform) to perform the import on.
on <DEVICE-NAME>	The following parameter is recursive and common to the ‘background’ and ‘passphrase’ keywords: • on <DEVICE-NAME> – Optional. Performs import operation on a specific device ◦ <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto key zeroize rsa <RSA-KEYPAIR-NAME> {force} {(on <DEVICE-NAME>)}
```

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
zeroize rsa <RSA-KEYPAIR-NAME>	Deletes a specified RSA Keypair • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.

	Note: All device certificates associated with this key will also be deleted.
force	Optional. Forces deletion of all certificates associated with the specified RSA Keypair. Optionally specify a device on which to force certificate deletion.
on <DEVICE-NAME>	The following parameter is recursive and optional: • on <DEVICE-NAME> – Optional. Deletes all certificates associated with the RSA Keypair on a specified device ◦ <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki authenticate <TRUSTPOINT-NAME> <URL> {background} {(on <DEVICE-NAME>)}
```

pki	Enables Private Key Infrastructure (PKI) management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated Certificate Authority (CA) certificates.
authenticate <TRUSTPOINT-NAME>	Authenticates a trustpoint and imports the corresponding CA certificate • <TRUSTPOINT-NAME> – Specify the trustpoint name.
url	Specify CA's location. Both IPv4 and IPv6 address formats are supported (see Usage Guidelines on page 18). **Note:** The CA certificate is imported from the specified location.
background	Optional. Performs authentication in the background. If selecting this option, you can optionally specify the device (access point, controller, or service platform) to perform the export on.
on <DEVICE-NAME>	The following parameter is recursive and optional: • on <DEVICE-NAME> – Optional. Performs authentication on a specified device ◦ <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> autogen-
subject-name (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
export request	Exports CSR to the CA for digital identity certificate. The CSR contains applicant's details and RSA Keypair's public key.

[generate-rsa-key| use-rsa-key] <RSA-KEYPAIR-NAME>	Generates a new RSA Keypair or uses an existing RSA Keypair • generate-rsa-key – Generates a new RSA Keypair for digital authentication • use-rsa-key – Uses an existing RSA Keypair for digital authentication ◦ <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
autogen-subject-name	Auto generates subject name from configuration parameters. The subject name identifies the certificate.
<EXPORT-TO-URL>	Specify the CA's location. Both IPv4 and IPv6 address formats are supported (see Usage Guidelines on page 18). **Note:** The CSR is exported to the specified location.
email <SEND-TO-EMAIL>	Exports CSR to a specified e-mail address • <SEND-TO-EMAIL> – Specify the CA's e-mail address.
fqdn <FQDN>	Exports CSR to a specified Fully Qualified Domain Name (FQDN) • <FQDN> – Specify the CA's FQDN.
ip-address <IP>	Exports CSR to a specified device or system • <IP> – Specify the CA's IP address.

```
crypto pki export request [generate-rsa-key|short [generate-rsa-key|use-rsa-key]|use-
rsa-key] <RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY>
<ORGANIZATION> <ORGANIZATION-UNIT> (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-
address <IP>)
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
export request	Exports CSR to the CA for a digital identity certificate. The CSR contains applicant's details and RSA Keypair's public key.

[generate-rsa-key| short [generate-rsa-key| use-rsa-key]| use-rsa-key] <RSA-KEYPAIR-NAME>	Generates a new RSA Keypair or uses an existing RSA Keypair • generate-rsa-key – Generates a new RSA Keypair for digital authentication • short [generate-rsa-key|use-rsa-key] – Generates and exports a shorter version of the CSR ◦ generate-rsa-key – Generates a new RSA Keypair for digital authentication. If generating a new RSA Keypair, specify a name for it. ◦ use-rsa-key – Uses an existing RSA Keypair for digital authentication. If using an existing RSA Keypair, specify its name. • use-rsa-key – Uses an existing RSA Keypair for digital authentication ◦ <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
subject-name <COMMON-NAME>	Configures a subject name, defined by the <COMMON-NAME> keyword, to identify the certificate • <COMMON-NAME> – Specify the common name used with the CA certificate. The name should enable you to identify the certificate easily (2 to 64 characters in length).
<COUNTRY>	Sets the deployment country code (2 character ISO code)
<STATE>	Sets the state name (2 to 64 characters in length)
<CITY>	Sets the city name (2 to 64 characters in length)
<ORGANIZATION>	Sets the organization name (2 to 64 characters in length)
<ORGANIZATION-UNIT>	Sets the organization unit (2 to 64 characters in length)
<EXPORT-TO-URL>	Specify the CA's location. Both IPv4 and IPv6 address formats are supported (see Usage Guidelines on page 18). The CSR is exported to the specified location.
email <SEND-TO-EMAIL>	Exports CSR to a specified e-mail address • <SEND-TO-EMAIL> – Specify the CA's e-mail address.

fqdn <FQDN>	Exports CSR to a specified FQDN • <FQDN> – Specify the CA's FQDN.
ip-address <IP>	Exports CSR to a specified device or system • <IP> – Specify the CA's IP address.

```
crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {background|passphrase
<KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
export trustpoint <TRUSTPOINT-NAME>	Exports a trustpoint along with CA certificate, Certificate Revocation List (CRL), server certificate, and private key • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).
<EXPORT-TO-URL>	Specify the destination address. Both IPv4 and IPv6 address formats are supported (see Usage Guidelines on page 18). The trustpoint is exported to the address specified here.
background	Optional. Performs export operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on
passphrase <KEY-PASSPHRASE> background	Optional. Encrypts the key with a passphrase before exporting • <KEY-PASSPHRASE> – Specify the passphrase to encrypt the trustpoint. ◦ background – Optional. Performs export operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the export on.
on <DEVICE-NAME>	The following parameter is recursive and common to the 'background' and 'passphrase' keywords: • on <DEVICE-NAME> – Optional. Performs export operation on a specified device ◦ <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] <RSA-
KEYPAIR-NAME> autogen-subject-name {(email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>,on
<DEVICE-NAME>)}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated certificates.
generate	Generates a certificate and a trustpoint

self-signed <TRUSTPOINT-NAME>	Generates a self-signed certificate and a trustpoint • <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint.
[generate-rsa-key| use-rsa-key] <RSA-KEYPAIR-NAME>	Generates a new RSA Keypair, or uses an existing RSA Keypair • generate-rsa-key – Generates a new RSA Keypair for digital authentication • use-rsa-key – Uses an existing RSA Keypair for digital authentication ◦ <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
autogen-subject-name	Auto generates the subject name from the configuration parameters. The subject name helps to identify the certificate.
email <SEND-TO-EMAIL>	Optional. Exports the self-signed certificate to a specified e-mail address • <SEND-TO-EMAIL> – Specify the e-mail address.
fqdn <FQDN>	Optional. Exports the self-signed certificate to a specified FQDN • <FQDN> – Specify the FQDN.
ip-address <IP>	Optional. Exports the self-signed certificate to a specified device or system • <IP> – Specify the device's IP address.
on <DEVICE-NAME>	Optional. Exports the self-signed certificate on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] <RSA-
KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION>
<ORGANIZATION-UNIT> {(email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>,on <DEVICE-NAME>)}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated certificates.
generate self-signed <TRUSTPOINT-NAME>	Generates a self-signed certificate and a trustpoint • <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint.
[generate-rsa-key| use-rsa-key] <RSA-KEYPAIR-NAME>	Generates a new RSA Keypair, or uses an existing RSA Keypair • generate-rsa-key – Generates a new RSA Keypair for digital authentication • use-rsa-key – Uses an existing RSA Keypair for digital authentication ◦ <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.

subject-name <COMMON-NAME>	Configures a subject name, defined by the <COMMON-NAME> keyword, to identify the certificate • <COMMON-NAME> – Specify the common name used with this certificate. The name should enable you to identify the certificate easily and should not exceed 2 to 64 characters in length.
<COUNTRY>	Sets the deployment country code (2 character ISO code)
<STATE>	Sets the state name (2 to 64 characters in length)
<CITY>	Sets the city name (2 to 64 characters in length)
<ORGANIZATION>	Sets the organization name (2 to 64 characters in length)
<ORGANIZATION-UNIT>	Sets the organization unit (2 to 64 characters in length)
email <SEND-TO-EMAIL>	Optional. Exports the self-signed certificate to a specified e-mail address • <SEND-TO-EMAIL> – Specify the e-mail address.
fqdn <FQDN>	Optional. Exports the self-signed certificate to a specified FQDN • <FQDN> – Specify the FQDN.
ip-address <IP>	Optional. Exports the self-signed certificate to a specified device or system • <IP> – Specify the device's IP address.

```
crypto pki import [certificate|crl] <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background} {(on
<DEVICE-NAME>)}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
import	Imports certificates, CRL, or a trustpoint to the selected device
[certificate|crl] <TRUSTPOINT-NAME>	Imports a signed server certificate or CRL • certificate – Imports signed server certificate • crl – Imports CRL ◦ <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).
<IMPORT-FROM-URL>	Specify the signed server certificate or CRL source address. Both IPv4 and IPv6 address formats are supported (see Usage Guidelines on page 18. The server certificate or the CRL (based on the parameter passed in the preceding step) is imported from the location specified here.

background	Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on.
on <DEVICE-NAME>	The following parameter is recursive and optional: • on <DEVICE-NAME> – Optional. Performs import operation on a specified device ◦ <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background|passphrase
<KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
import	Imports certificates, CRL, or a trustpoint to the selected device
trustpoint <TRUSTPOINT-NAME>	Imports a trustpoint and its associated CA certificate, server certificate, and private key • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).
<IMPORT-FROM-URL>	Specify the trustpoint source address. Both IPv4 and IPv6 address formats are supported (see Usage Guidelines on page 18).
background	Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on.

passphrase <KEY-PASSPHRASE> background	Optional. Decrypts trustpoint with a passphrase after importing • <KEY-PASSPHRASE> – Specify the passphrase. After specifying the passphrase, optionally specify the device to perform import on. ◦ background – Optional. Performs import operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the import on.
on <DEVICE-NAME>	The following parameter is recursive and optional: • on <DEVICE-NAME> – Optional. Performs import operation on a specified device ◦ <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki zeroize trustpoint <TRUSTPOINT-NAME> {del-key} {(on <DEVICE-NAME>)}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
zeroize trustpoint <TRUSTPOINT-NAME>	Imports certificates, CRL, or a trustpoint to the selected device
[certificate|crl] <TRUSTPOINT-NAME>	Deletes a trustpoint and its associated CA certificate, server certificate, and private key • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).
del-key	Optional. Deletes the private key associated with the server certificate. Optionally specify the device to perform deletion on.
on <DEVICE-NAME>	The following parameter is recursive and optional: • on <DEVICE-NAME> – Optional. Deletes the trustpoint on a specified device ◦ <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Usage Guidelines

The system supports both IPv4 and IPv6 address formats. Provide source and destination locations using any one of the following options:

- IPv4 URLs:

  tftp://<hostname|IPv4>[:port]/path/file

  ftp://<user>:<passwd>@<hostname|IPv4>[:port]/path/file

  sftp://<user>:<passwd>@<hostname|IPv4>[:port]>/path/file

  http://<hostname|IPv4>[:port]/path/file

cf:/path/file

usb<n>:/path/file

- IPv6 URLs:

  tftp://<hostname|IPv6>[:port]/path/file

  ftp://<user>:<passwd>@<hostname|IPv6>[:port]/path/file

  sftp://<user>:<passwd>@<hostname|IPv6>[:port]>/path/file

  http://<hostname|IPv6>[:port]/path/file

When using FTP or SFTP, if a password is not specified in the URL, users are prompted to enter a password, as shown in the following examples.

Examples

```
vx9000-AA3AED#crypto pki export trustpoint default-trustpoint ftp://ftpvvdn@192.168.2.1/
certfile
Enter password:
Trustpoint exported successfully

vx9000-AA3AED#crypto pki export trustpoint default-trustpoint sftp://sftpvvdn@192.168.2.1/
certfile
Enter password:
Trustpoint exported successfully

ap510-133B3B#crypto key generate rsa local 2048 on ap510-133B3B
RSA Keypair successfully generated
ap510-133B3B#
```

device-upgrade

Note
This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported on the following devices:

- Access Points: AP3000, AP3000X, AP5010, AP310i/e, AP410i/e, AP505i, AP510i/e, AP560i, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8533.
- Service Platforms: NX5500, NX7500, NX9500, NX9600
- Virtual Platforms: CX9000, VX9000

Syntax

```
device-upgrade [<MAC/HOSTNAME>|all|ap3000|ap3000x|ap310|ap360|ap410|ap460|ap505|ap510|
ap560|ap7522|ap7532|ap7562|ap7612|ap7632|ap7662|ap8432|ap8533|cx9000|nx5500|nx7500|nx9500|
nx9600|vx9000|cancel-upgrade|load-image|rf-domain]

device-upgrade <MAC/HOSTNAME> {no-reboot|reboot-time <TIME>|upgrade-time <TIME>

device-upgrade all {force|no-reboot|reboot-time <TIME>|staggered-reboot|upgrade-time
<TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}

device-upgrade [ap3000|ap3000x|ap310|ap360|ap410|ap460|ap505|ap510|ap560|ap7522|ap7532|
ap7562|ap7612|ap7632|ap7662|ap8432|ap8533|nx5500|nx7500|nx9500|nx9600|vx9000] [all|
containing <SUB-STRING>] {force|no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-
reboot|reboot-time <TIME>}}

device-upgrade cancel-
upgrade [<MAC/HOSTNAME>|all|ap3000|ap3000x|ap310|ap360|ap410|ap460|ap505|ap510|ap560|
ap7532|ap7562|ap7612|ap7632|ap7662|ap8432|ap8533|nx5500|nx7500|nx9500|nx9600|vx9000|on rf-
domain [<RF-DOMAIN-NAME>|all]]

device-upgrade load-
image [ap3000|ap3000x|ap310|ap360|ap410|ap460|ap505|ap510|ap560|ap7522|ap7532|ap7562|
ap7612|ap7632|ap7662|ap8432|ap8533|nx5500|nx7500|nx9500|nx9600|vx9000] {<IMAGE-URL>|on
<DEVICE-OR-DOMAIN-NAME>}

device-upgrade operational-
mode [all|ap3000|ap3000-1|ap302w|ap305c|ap305c-1|ap305cx|ap310|ap310-1|ap360|ap4000|
ap4000u|ap410|ap410-1|ap410c|ap410c-1|ap460|ap460c|ap460s12c|ap460s6c|ap5010|ap505|ap5050|
ap510|ap510-1|ap560|containing|rf-domain] [centralized|xiq-cloud]

device-upgrade rf-domain [<RF-DOMAIN-NAME>|all|containing <WORD>|filter
location <WORD>] [all|ap310|ap360|ap410|ap460|ap505|ap510|ap560|ap7522|ap7532|ap7562|
ap7612|ap7632|ap7662|ap8432|ap8533|nx5500|nx7500|nx9500|nx9600|vx9000] {(<MAC/HOSTNAME>|
force|from-controller|no-reboot|reboot-time <TIME>|staggered-reboot|upgrade-time <TIME>)}
```

Parameters

```
device-upgrade <MAC/HOSTNAME> {no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-
reboot|reboot-time <TIME>}}
```

<MAC/HOSTNAME>	Upgrades firmware on the device identified by the <MAC/HOSTNAME> keyword • <MAC/HOSTNAME> – Specify the device MAC address or hostname.
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)

reboot-time <TIME>	Optional. Schedules an automatic reboot after a successful upgrade • <TIME> – Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
upgrade-time <TIME> {no-reboot| reboot-time <TIME>}	Optional. Schedules an automatic device firmware upgrade and specifies the time at which the device is to be upgraded • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: ◦ no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) ◦ reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

```
device-upgrade all {force|no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-reboot|
reboot-time <TIME>}} {(staggered-reboot)}
```

all	Upgrades firmware on all devices
force	Optional. Select this option to force upgrade on the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or staggered-reboot.
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME>	Optional. Schedules an automatic reboot after a successful upgrade • <TIME> – Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

upgrade-time <TIME> {no-reboot| reboot-time <TIME>}	Optional. Schedules an automatic firmware upgrade on all devices, of the specified type, on a specified day and time • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: ◦ no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) ◦ reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is recursive and common to all of the above. • Optional. Enables staggered reboot (one at a time), without network impact.

```
device-upgrade [ap505|ap510|ap560|ap410|ap460|ap3000|ap3000x|ap310|ap360|ap7522|ap7532|
ap7562|ap7612|ap7632|ap7662|ap8432|ap8533|nx5500|nx7500|nx9500|nx9600|vx9000] [all|
containing <SUB-STRING] {force|no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-
reboot|reboot-time <TIME>}} {(staggered-reboot)}
```

device-upgrade <DEVICE-TYPE> all	Upgrades firmware on all devices of a specific type. Select the device type. The options are: AP510, AP505, AP560, AP5010, AP410, AP460, AP3000/X, AP310, AP360, AP7612, AP7632, AP7662, AP8533, NX5500, NX7500, NX9500, NX9600, CX9000, VX9000. Checked out the GUI for VX9000 and options may include some of these, but not all. This list doesn't cover all the "supported devices" listed at the beginning of this section. Can we use something generic here? After selecting the device type, schedule an automatic upgrade and/or an automatic reboot.
force	Optional. Select this option to force upgrade on the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or staggered-reboot.
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted).
reboot-time <TIME>	Optional. Schedules an automatic reboot after a successful upgrade • <TIME> – Optional. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

upgrade-time <TIME> {no-reboot| reboot-time <TIME>}	Optional. Schedules an automatic firmware upgrade on all devices, of the specified type, on a specified day and time • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: ◦ no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) ◦ reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is recursive and common to all of the above. • Optional. Enables staggered reboot (one at a time), without network impact

```
device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|ap505|ap510|ap560|ap410|ap460|ap3000|
ap3000x|ap310|ap360|ap7522|ap7532|ap7562|ap7612|ap7632|ap7662|ap8432|ap8533|nx5500|nx7500|
nx9500|nx9600|vx9000|on rf-domain [<RF-DOMAIN-NAME>|all]]
```

cancel-upgrade	Cancels a scheduled firmware upgrade based on the parameters passed. This command provides the following options to cancel scheduled firmware upgrades: • Cancels upgrade on specific device(s). The devices are identified by their MAC addresses or hostnames. • Cancels upgrade on all devices within the network • Cancels upgrade on all devices of a specific type. Specify the device type. • Cancels upgrade on specific device(s) or all device(s) within a specific RF Domain or all RF Domains. Specify the RF Domain name.
cancel-upgrade [<MAC/HOSTNAME>| all]	Cancels a scheduled firmware upgrade on a specified device or on all devices • <MAC/HOSTNAME> – Cancels a scheduled upgrade on the device identified by the <MAC/HOSTNAME> keyword. Specify the device MAC address or hostname. • all – Cancels scheduled upgrade on all devices

cancel-upgrade <DEVICE-TYPE> all	Cancels scheduled firmware upgrade on all devices of a specific type. Select the device type. The options are: AP510, AP505, AP560, AP5010, AP410, AP460, AP3000/X, AP310, AP360, AP7612, AP7632, AP7662, AP8533, NX5500, NX7500, NX9500, NX9600, CX9000, VX9000.
cancel-upgrade on rf-domain [<RF-DOMAIN-NAME>|all]	Cancels scheduled firmware upgrade on all devices in a specified RF Domain or all RF Domains • <RF-DOMAIN-NAME> – Cancels scheduled device upgrade on all devices in a specified RF Domain. Specify the RF Domain name. • all – Cancels scheduled device upgrade on all devices across all RF Domains

```
device-upgrade load-
image [ap3000|ap3000x|ap310|ap360|ap410|ap460|ap505|ap510|ap560|ap7522|ap7532|ap7562|
ap7612|ap7632|ap7662|ap8432|ap8533|nx5500|nx7500|nx9500|nx9600|vx9000] {<IMAGE-URL>|on
<DEVICE-OR-DOMAIN-NAME>}
```

load-image <DEVICE-TYPE>	Loads device firmware image from a specified location. Use this command to specify the device type and the location of the corresponding image file. • <DEVICE-TYPE> - Specify the device type. The options are: AP3000/X, AP310, AP360, AP410, AP460, AP510, AP505, AP560, AP5010, AP7612, AP7632, AP7662, AP8533, NX5500, NX7500, NX9500, NX9600, CX9000, VX9000. After specifying the device type, provide the location of the required device firmware image.
<IMAGE-URL>	Specify the device firmware image location in one of the following formats: IPv4 URLs: • tftp://<hostname|IP>[:port]/path/file • ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file • sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file • http://<hostname|IP>[:port]/path/file • cf:/path/file • usb<n>:/path/file IPv6 URLs: • tftp://<hostname|IPv6>[:port]/path/file • ftp://<user>:<passwd>@<hostname|IPv6>[:port]/path/file • sftp://<user>:<passwd>@<hostname|IPv6>[:port]>/path/file • http://<hostname|IPv6>[:port]/path/file
on <DEVICE-OR-DOMAIN-NAME>	Specify the name of the device or RF Domain. The image, of the specified device type is loaded from the device specified here. In case of an RF Domain, the image available on the RF Domain manager is loaded. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, virtual platform, or RF Domain.

```
device-upgrade operational-
mode [all|ap3000|ap3000-1|ap302w|ap305c|ap305c-1|ap305cx|ap310|ap310-1|ap360|ap4000|
ap4000u|ap410|ap410-1|ap410c|ap410c-1|ap460|ap460c|ap460s12c|ap460s6c|ap5010|ap505|ap5050|
ap510|ap510-1|ap560|containing|rf-domain] [centralized|xiq-cloud]|containing|rf-domain]
[centralized|xiq-cloud]

device-upgrade operational-mode all [centralized|xiq-cloud]

device-upgrade operational-mode <DEVICE-TYPE> [all|containing <HOSTNAME-SUBSTRING>]
[centralized|xiq-cloud]

device-upgrade operational-mode containing <HOSTNAME-SUBSTRING> [centralized|xiq-cloud]

device-upgrade operational-mode rf-domain [<RF-DOMAIN-NAME>|
all|containing <RF-DOMAIN-NAME-SUBSTRING>|filter location
<LOCATION> [all|ap3000|ap3000-1|ap302w|ap305c|ap305c-1|ap305cx|ap310|ap310-1|ap360|ap4000|
ap4000u|ap410|ap410-1|ap410c|ap410c-1|ap460|ap460c|ap460s12c|ap460s6c|ap5010|ap505|ap5050|
ap510|ap510-1|ap560|containing|rf-domain] [centralized|xiq-cloud] [centralized|xiq-cloud]
```

operational-mode [centralized|xiq-cloud]	Resets the operational mode of eligible APs that are locally managed by ExtremeWireless WiNG to either centrally managed by ExtremeCloud IQ Controller (**centralized**) or cloud managed by ExtremeCloud IQ (**xiq-cloud**). Use this command to facilitate migration of eligible APs from on-premise, local management by ExtremeWireless WiNG to NOC management or cloud management. This command provides the following options: • Reset all eligible APs currently adopted by the controller to the defined operational mode. • Reset specified family of eligible APs to the defined operational mode. • Reset eligible APs with a specified sub-string in the hostname to the defined operational mode. • Reset eligible APs in a specified RF Domain (site) to the defined operational mode. Eligible APs—designated as <DEVICE-TYPE> in syntax below—include the following models: • **Universal APs** — AP3000, AP3000-1, AP302W, AP305C, AP305C-1, AP305CX, AP4000, AP4000U, AP410C, AP410C-1, AP460C, AP460S12C, AP460S6C, AP5010, AP5050, • **Non-Universal APs** — AP310, AP310-1, AP360, AP410, AP410-1, AP460, AP505, AP510, AP510-1, AP560 **Note:** Migration from WiNG management to ExtremeCloud IQ is supported with Universal APs only. Migration to ExremeCloud IQ Controller is supported with both Universal and Non-Universal APs.
operational-mode all [centralized|xiq-cloud]	Optional. Resets the operational mode of all eligible controller-adopted APs to **centralized** or **xiq-cloud**.
operational-mode <DEVICE-TYPE> [all|containing <HOSTNAME-SUBSTRING>] [centralized|xiq-cloud]	Optional. Resets (to **centralized** or **xiq-cloud**) the operational mode of all eligible controller-adopted APs matching the specified device type or device type containing the specified host name and sub-string. • <DEVICE-TYPE> — specifies an eligible AP • all — resets the operational mode of all APs of the specified <DEVICE-TYPE> • containing — resets the operational mode of the specified <DEVICE-TYPE> containing the specified <HOSTNAME-SUBSTRING> • [centralized|xiq-cloud] — the operational-mode

operational-mode containing <HOSTNAME-SUBSTRING> [centralized|xiq-cloud]	Optional. Resets (to **centralized** or **xiq-cloud**) the operational mode of all eligible controller-adopted APs with the specified host name and sub-string.
operational-mode rf-domain [<RF-DOMAIN-NAME>|all|containing <RF-DOMAIN-NAME-SUBSTRING>|filter location <LOCATION> [all|<DEVICE-TYPE>] [centralized|xiq-cloud]	Optional. Resets (to **centralized** or **xiq-cloud**) the operational mode of all eligible controller-adopted APs that are in all controller-managed RF Domains, or in the specified RF Domain, or in all RF Domains at a specified location. • <RF-DOMAIN-NAME> — resets the operational mode of all eligible APs in the specified RF Domain • all — resets the operational mode of all eligible APs in all controller-managed RF Domains • containing — resets the operational mode of all eligible APs within RF Domains whose name contains the sub-string identified by the <RF-DOMAIN-NAME-SUBSTRING> • filter location — resets the operational mode of all eligible APs or the specified <DEVICE-TYPE> within all RF Domains or the specified RF Domain at the specified <LOCATION> • [centralized|xiq-cloud] — the operational-mode

```
device-upgrade rf-domain [<RF-DOMAIN-NAME>|all|containing <WORD>|filter
location <WORD>] [all|ap310|ap360|ap410|ap460|ap505|ap510|ap560|ap7522|ap7532|ap7562|
ap7612|ap7632|ap7662|ap8432|ap8533|nx5500|nx7500|nx9500|nx9600|vx9000] {(<MAC/HOSTNAME>|
force|from-controller|no-reboot|reboot-time <TIME>|staggered-reboot|upgrade-time <TIME>)}
```

rf-domain [<RF-DOMAIN-NAME>|all| containing <WORD>| filter location <WORD>]	Upgrades firmware on devices in a specified RF Domain or all RF Domains. Devices within a RF Domain are upgraded through the RF Domain manager. • <RF-DOMAIN-NAME> – Upgrades devices in the RF Domain identified by the <RF-DOMAIN-NAME> keyword. ◦ <RF-DOMAIN-NAME> – Specify the RF Domain name. • all – Upgrades devices across all RF Domains • containing <WORD> – Filters RF Domains by their names. RF Domains with names containing the sub-string identified by the <WORD> keyword are filtered. Devices on the filtered RF Domains are upgraded. • filter location <WORD> – Filters devices by their location. All devices with location matching the <WORD> keyword are upgraded.
<DEVICE-TYPE>	After specifying the RF Domain, select the device type. The options are: AP410, AP460, AP510, AP505, AP560, AP3000/X, AP5010, AP7612, AP7632, AP7662, AP8533, NX5500, NX7500, NX9500, NX9600, CX9000, VX9000. After specifying the RF Domain and the device type, configure any one of the following actions: force devices to upgrade, or initiate an upgrade through the adopting controller.

<MAC/HOSTNAME>	Optional. Use this option to identify specific devices (by their MAC address/Hostnames) that are to be upgraded. Specify the device MAC address or hostname. The device should be within the specified RF Domain and of the specified device type. After identifying the devices to upgrade, configure any one of the following actions: force devices to upgrade, or initiate an upgrade through the adopting controller. **Note:** If no MAC address or hostname is specified, all devices of the type selected are upgrade
force	Optional. Select this option to force upgrade for the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or reboot-time.
from-controller	Optional. Upgrades a device through the adopted device. If initiating an upgrade through the adopting controller, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or reboot-time.
no-reboot {staggered-reboot}	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME> {staggered-reboot}	Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is common to all of the above. Optional. Enables staggered reboot (one at a time) without network impact
upgrade-time <TIME> {no-reboot| reboot-time <TIME>}	Optional. Schedules an automatic firmware upgrade • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. After a scheduled upgrade, the following actions can be performed. ◦ no-reboot – Optional. Disables automatic reboot after a successful upgrade the device must be manually restarted) ◦ reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

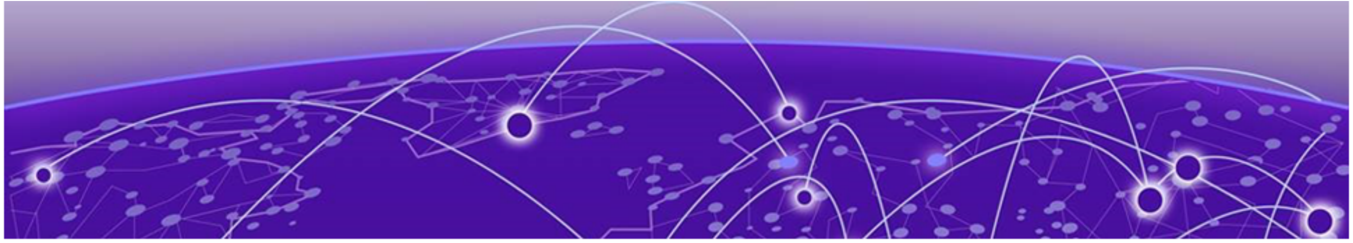
Examples

```
nx9500-6C8809#show adoption status
------------------------------------------------------------------------------------------
--------------------
DEVICE-NAME    VERSION     CFG-STAT    MSGS   ADOPTED-BY      LAST-ADOPTION
UPTIME      IPv4-ADDRESS
------------------------------------------------------------------------------------------
--------------------
ap8432-070235 7.3.0.0-001D  configured   No  nx9500-6C8809  0 days 00:16:53  0 days
00:18:11   0.0.0.0
```

```
ap7562-84A224 7.3.0.0-001D  configured   No  nx9500-6C8809  0 days 00:16:54  0 days
00:18:08   10.234.160.6
ap7532-DF9A4C 7.3.0.0-001D  configured   No  nx9500-6C8809  0 days 00:17:00  0 days
00:18:13   10.234.160.12
ap505-134038  7.3.0.0-001D  configured   No  nx9500-6C8809  0 days 00:27:25  0 days
00:28:50   10.234.160.36
------------------------------------------------------------------------------------------
--------------------
nx9500-6C8809#
```

```
nx9500-6C8809#device-upgrade all
In progress ....
--------------------------------------------------------------------------------
       CONTROLLER         STATUS                     MESSAGE
--------------------------------------------------------------------------------
  B4-C7-99-6C-88-09     Success     Number of devices added for upgrade: 4
--------------------------------------------------------------------------------
nx9500-6C8809#
```

```
nx9500-6C8809#show adoption status
------------------------------------------------------------------------------------------
------------------
DEVICE-NAME    VERSION       CFG-STAT   MSGS   ADOPTED-BY    LAST-ADOPTION
UPTIME       IPv4-ADDRESS
------------------------------------------------------------------------------------------
------------------
ap8432-070235 7.3.0.0-002D  configured   No  nx9500-6C8809  0 days 04:04:21  0 days
04:05:36  0.0.0.0
ap7562-84A224 7.3.0.0-002D  configured   No  nx9500-6C8809  0 days 04:04:19  0 days
04:05:36  10.234.160.6
ap7532-DF9A4C 7.3.0.0-002D  configured   No  nx9500-6C8809  0 days 04:04:24  0 days
04:05:37  10.234.160.12
ap505-134038  7.3.0.0-002D  configured   No  nx9500-6C8809  0 days 04:04:58  0 days
04:05:32  10.234.160.36
------------------------------------------------------------------------------------------
------------------
Total number of devices displayed: 4
nx9500-6C8809#
```



Global Configuration Commands

wlan

Configures a WLAN and enters its configuration mode. Use this command to modify an existing WLAN's settings.

A WLAN is a data-communications system that flexibly extends the functionality of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or OFDM *(Orthogonal Frequency Division Multiplexing)* modulation based technology. WLANs do not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one access point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

WLANs can provide an abundance of services, including data communications (allowing mobile devices to access applications), e-mail, file, and print services or even specialty applications (such as guest access control and asset tracking).

Each WLAN configuration contains encryption, authentication and QoS policies and conditions for user connections. Connected access point radios transmit periodic beacons for each BSS. A beacon advertises the SSID, security requirements, supported data rates of the wireless network to enable clients to locate and connect to the WLAN.

WLANs are mapped to radios on each access point. A WLAN can be advertised from a single access point radio or can span multiple access points and radios. WLAN configurations can be defined to provide service to specific areas of a site. For example, a guest access WLAN may only be mapped to a 2.4 GHz radio in a lobby or conference room providing limited coverage, while a data WLAN is mapped to all 2.4 GHz and 5.0 GHz radios at the branch site to provide complete coverage.

Supported on the following devices:

- Access Points: AP3000, AP3000X, AP5010, AP310i/e, AP410i/e, AP505i, AP510i/e, AP560i, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8533.
- Service Platforms: NX5500, NX7500, NX9500, NX9600
- Virtual Platforms: CX9000, VX9000

Syntax

```
wlan {<WLAN-NAME>|containing <WLAN-NAME>}
```

Parameters

```
wlan {<WLAN-NAME>|containing <WLAN-NAME>}
```

wlan <WLAN-NAME>	Configures a new WLAN • <WLAN-NAME> – Optional. Specify the WLAN name. **Note:** The WLAN name could be a logical representation of its coverage area (for example, engineering, marketing etc.). The name cannot exceed 32 characters.
containing <WLAN-NAME>	Optional. Configures an existing WLAN's settings • <WLAN-NAME> – Specify a sub-string in the WLAN name. Use this parameter to filter a WLAN. This option allows you to select and enter the configuration mode of one or more WLANs.

Examples

```
nx9500-6C8809(config)#wlan wlan1
nx9500-6C8809(config-wlan-wlan1)#?
Wireless LAN Mode commands:
  802.11v Configure 802.11v parameters
  accounting                             Configure how accounting records are
                                         created for this wlan
  acl                                    Actions taken based on ACL
                                         configuration [ packet drop being one
                                         of them]
  answer-broadcast-probes                Include this wlan when responding to
                                         probe requests that do not specify an
                                         SSID
  assoc-response                         Association response threshold
  association-list                       Configure the association list for
                                         the wlan
  authentication-type                    The authentication type of this WLAN
  bridging-mode                          Configure how packets to/from this
                                         wlan are bridged
  broadcast-dhcp                         Configure broadcast DHCP packet
                                         handling
  broadcast-ssid                         Advertise the SSID of the WLAN in
                                         beacons
  captive-portal-enforcement             Enable captive-portal enforcement on
                                         the wlan
  client-access                          Enable client-access (normal data
                                         operations) on this wlan
  client-client-communication            Allow switching of frames from one
                                         wireless client to another on this
                                         wlan
  client-load-balancing                  Configure load balancing of clients
                                         on this wlan
  controller-assisted-mobility           Enable controller assisted mobility
                                         to determine wireless clients' VLAN
                                         assignment
  data-rates                             Specify the 802.11 rates to be
```

```
                                         supported on this wlan
  description                            Configure a description of the usage
                                         of this wlan
  downstream-group-addressed-forwarding  Enable downstream group addressed
                                         forwarding of packets
  dpi                                    Deep-Packet-Inspection (Application
                                         Assurance)
  dynamic-vlan-assignment                Dynamic VLAN assignment configuration
  eap-types                              Configure client access based on
                                         eap-type used for authentication
  encryption-type                        Configure the encryption to use on
                                         this wlan
  enforce-dhcp                           Drop packets from Wireless Clients
                                         with static IP address
  fast-bss-transition                    Configure support for 802.11r Fast
                                         BSS Transition
  http-analyze                           Enable HTTP URL analysis on the wlan
  ip                                     Internet Protocol (IP)
  ipv6                                   Internet Protocol version 6 (IPv6)
  kerberos                               Configure kerberos authentication
                                         parameters
  mac-authentication                     Configure mac-authentication related
                                         parameters
  no                                     Negate a command or set its defaults
  nsight                                 Nsight Server
  opendns                                OpenDNS related config for this wlan
  protected-mgmt-frames                  Protected Management Frames (IEEE
                                         802.11w) related configuration
  proxy-arp-mode                         Configure handling of ARP requests
                                         with proxy-arp is enabled
  proxy-nd-mode                          Configure handling of IPv6 ND
                                         requests with proxy-nd is enabled
  qos-map                                Support the 802.11u QoS map element
                                         and frame
  radio-resource-measurement             Configure support for 802.11k Radio
                                         Resource Measurement
  radius                                 Configure RADIUS related parameters
  registration                           Enable dynamic registration of device
                                         (or) user
  relay-agent                            Configure dhcp relay agent info
  shutdown                               Shutdown this wlan
  ssid                                   Configure the Service Set Identifier
                                         for this WLAN
  t5-client-isolation                    Isolate traffic among clients
  t5-security                            Configure encryption and
                                         authentication
  time-based-access                      Configure client access based on time
  use                                    Set setting to use
  vlan                                   Configure the vlan where traffic from
                                         this wlan is mapped
  vlan-pool-member                       Add a member vlan to the pool of
                                         vlans for the wlan (Note:
                                         configuration of a vlan-pool
                                         overrides the 'vlan' configuration)
  wep128                                 Configure WEP128 parameters
  wep64                                  Configure WEP64 parameters
  wing-extensions                        Enable support for WiNG-Specific
                                         extensions to 802.11
  wireless-client                        Configure wireless-client specific
                                         parameters
  wpa-wpa2                               Modify tkip-ccmp (wpa/wpa2) related
                                         parameters

  clrscr                                 Clears the display screen
  commit                                 Commit all changes made in this
                                         session
  do                                     Run commands from Exec mode
  end                                    End current mode and change to EXEC
                                         mode
  exit                                   End current mode and down to previous
                                         mode
  help                                   Description of the interactive help
                                         system
  revert                                 Revert changes
  service                                Service Commands
  show                                   Show running system information
  write                                  Write running configuration to memory
                                         or terminal

nx9500-6C8809(config-wlan-wlan1)#
```

The following example shows how to use the ‘containing’ keyword to enter the configuration mode of an existing WLAN:

```
nx9500-6C8809(config)#wlan containing wlan1
nx9500-6C8809(config-wlan-{'containing': 'wlan1'})#
```

Related Commands

no	Removes an existing WLAN from the system

encryption-type

Sets the WLAN's encryption type

Supported on the following devices:

- Access Points: AP3000, AP3000X, AP5010, AP310i/e, AP410i/e, AP505i, AP510i/e, AP560i, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8533.
- Service Platforms: NX5500, NX7500, NX9500, NX9600
- Virtual Platforms: CX9000, VX9000

Syntax

```
encryption-type [ccmp|gcmp256|keyguard|none|tkip-ccmp|wep128|web128-keyguard|wep64]
```

Parameters

```
encryption-type [ccmp|gcmp256|keyguard|none|tkip-ccmp|wep128|web128-keyguard|wep64]
```

encryption-type	Configures the WLAN's data encryption parameters
ccmp	Configures *Advanced Encryption Standard Counter Mode CBC-MAC Protocol* (AES-128CCM/CCMP)

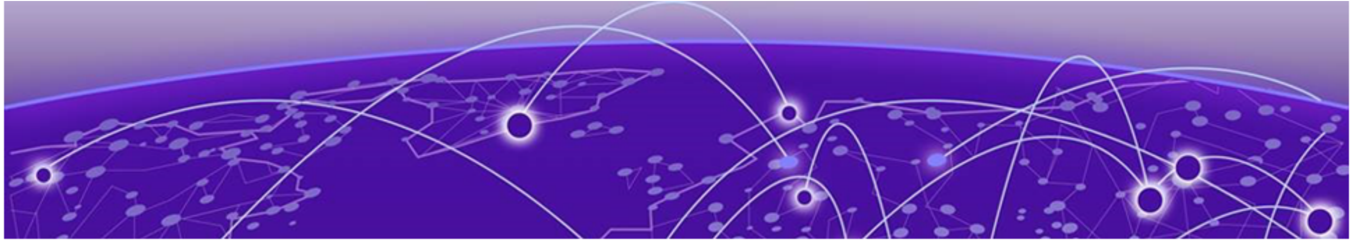
gcmp256	Configures AES-GCM *(Advanced Encryption Standard-Galois Counter Mode)* protocol (WPA3-Enterprise 192-bit) encryption mode. GCMP-256 is a block cipher which works on 256-bit blocks. **Note:** GCMP encryption is supported on AP3000, AP3000X, and AP5010 only, and must have the following parameters configured: • EAP authentication-type. For more information, see "authentication-type" command description. • Mandatory protected management frames. For more information, see "protected-mgmt-frames" command description.
keyguard	Configures Keyguard *Mobile Computing Mode* (MCM)
tkip-ccmp	Configures the TKIP and AES-CCM/CCMP encryption modes
wep128	Configures WEP with 128 bit keys
wep128-keyguard	Configures WEP128 as well as Keyguard-MCM encryption modes
wep64	Configures WEP with 64 bit keys. A WEP64 configuration is insecure when two WLANs are mapped to the same VLAN, and one uses no encryption while the other uses WEP.

Examples

```
nx9500-6C8809(config-wlan-test)#encryption-type tkip-ccmp

nx9500-6C8809(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
encryption-type tkip-ccmp
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
nx9500-6C8809(config-wlan-test)#

ap5010-12856B(config-wlan-test)#encryption-type gcmp256

ap5010-12856B(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode local
 encryption-type gcmp256
 authentication-type eap
 dynamic-vlan-assignment allowed-vlans 2-4
 protected-mgmt-frames mandatory
 protected-mgmt-frames sa-query attempts 1
 use aaa-policy test
 controller-assisted-mobility
 dpi metadata http
ap5010-12856B(config-wlan-test)#
```

Related Commands

no (wlan-config-mode)	Resets the WLAN’s encryption type to default (none)



Profile and Device Commands

process-monitor

Configures a watchdog process to monitor the Radio Interface Module (RIM). If the RIM process is not running or is killed, the watchdog re-initializes the RIM.

> **Note**
> This command and its syntax is common to both Profile and Device commands. You can apply overrides to RIM monitoring at the device level. Overrides applied at the device level take precedence.

Supported on the following devices:

- Access Points: AP3000, AP3000X, AP5010, AP310i/e, AP410i/e, AP505i, AP510i/e, AP560i, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8533.
- Service Platforms: NX5500, NX7500, NX9500, NX9600
- Virtual Platforms: CX9000, VX9000

Syntax

```
process-monitor
```

Parameters

```
process-monitor
```

process-monitor	Enables monitoring of the RIM processes and, if necessary, re-initializes the RIM

Example

```
vx9000-1A1809 (config-profile-anyap-test)# process-monitor
```

Related Commands

no	Disables monitoring of the RIM processes (applies to both profile and device configurations)
remove-override	Completely removes the override configuration from the individual device (does not apply to profile configuration)

bridge

interface-config-radio-instance

Configures the *client-bridge* (CB) parameters for radios with rf-mode set to bridge. When configured as a client bridge, the radio can authenticate and associate to the WLAN hosted on the infrastructure access point. After successfully associating with the infrastructure WLAN, the CB access point switches frames between its bridge radio and wired/wireless client(s) connected either to its GE port(s) or to the other radio, thereby providing the clients access to the infrastructure WLAN resources.

This command configures settings that define the authentication-type and encryption-type used by the CB AP to associate and communicate with the infrastructure AP. It also configures other parameters, such as channel-dwell time, wlan ssid, and so forth.

Note

- Radios configured to form the client-bridge will not service wireless clients as their RF mode is set to bridge.
- It is recommended that 6 GHz radios NOT be configured as a client bridge, since throughput is sub-optimal.

Supported in the following platforms:

- Access Points — AP302W, AP305C, AP305C-1, AP310IE, AP310i/e-1, AP360IE, AP410C, AP410C-1, AP410i/e, AP410i-1, AP460i/e, AP460C, AP505i, AP510i/e, AP510i-1, AP560i/h, AP5010, AP7622, AP7632, AP7662

Syntax

```
bridge [authentication-type|channel-dwell-time|channel-list|connect-through-bridges|eap|
    encryption-type|inactivity-timeout|keepalive|max-clients|on-link-loss|on-link-up|ssid|
    roam-criteria|wpa-wpa2]
```

```
bridge authentication-type [eap|none]
```

```
bridge eap [password|trustpoint|type|username]
```

```
bridge eap type [peap-mschapv2|tls]
```

```
bridge eap password <PASSWORD>
```

```
bridge eap username <USERNAME>
bridge eap trustpoint [ca|client] <TRUSTPOINT-NAME>
```

```
bridge eap trustpoint on-cert-expiry [continue|discontinue]
```

```
bridge channel-dwell-time <50-2000>
```

```
bridge channel-list [2.4GHz|5GHz|6GHz] <LIST>
```

```
bridge connect-through-bridges
```

```
bridge encryption-type [ccmp|none|tkip]
```

```
bridge inactivity-timeout <0-864000>
```

```
bridge keepalive [frame-type [null-data|wnmp]|interval <0-36000>]
```

```
bridge max-clients <1-64>
```

```
bridge on-link-loss shutdown-other-radio <1-1800>
```

```
bridge on-link-up refresh-vlan-interface
```

```
bridge roam-criteria [missed-beacon <1-60>|rssi-threshold <-128--40>]
```

```
bridge ssid <SSID>
```

```
bridge wpa-wpa2 psk <LINE>
```