WiNG Controller and Access Point v7.9.6.0 CLI Reference Guide Delta

9039474-00 Rev AA
October 2025

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

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

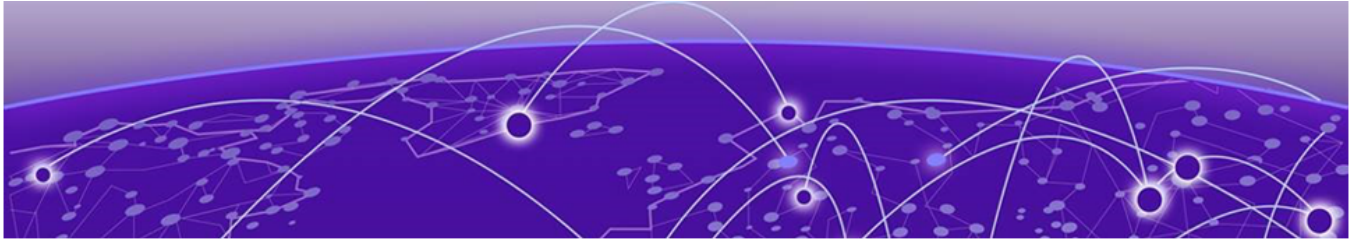
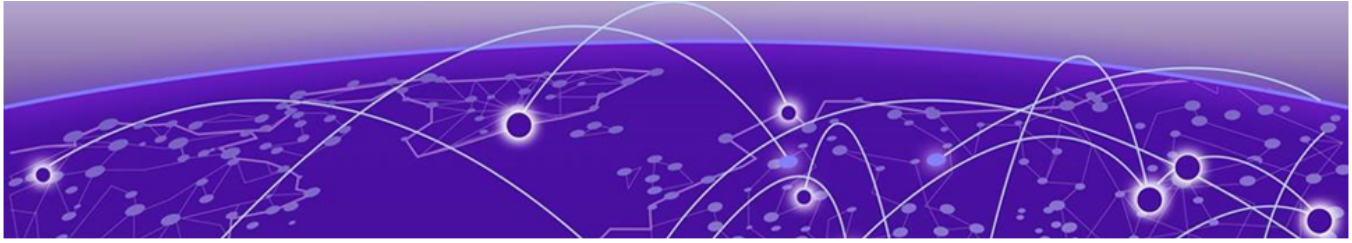


Table of Contents



About this Document

The WiNG Controller and Access Point v7.9.6.0 CLI Reference Guide Delta describes updates to CLI commands in release 7.9.6.0. Use this information in conjunction with the WiNG Controller and Access Point v7.9.5.1 CLI Reference Guide for complete instructions.

WiNG Controller 7.9.6.0 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 of 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 17). 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 17). 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 17). **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 17). **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 17). 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 17). 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 17. 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 17).
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#
```

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)