FIPS, CC, and UCAPL Support in Cisco CMX

Cisco CMX supports the Federal Information Processing Standard 140-2 (FIPS). FIPS is a standard published by the National Institute of Standards and Technology (NIST) and is used to accredit cryptographic modules in software components. The US Federal government requires that all IT products dealing with Sensitive, but Unclassified (SBU) information meet these standards. If your system needs to be FIPS compliant, you can enable FIPS. Once you do so, the system uses the cryptographic algorithms defined by the NIST for FIPS for all encrypted communication between its internal and external components.

The Common Criteria for Information Technology Security Evaluation (referred to as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. Main focus of CC is to establish secure connection with external entities. Another main focus is providing extensive audit logging functionality to capture all the important configuration activities and system events within the product.

Cisco CMX supports FIPS and Common Criteria through a single mode called FIPS mode. Going forwards FIPS mode in Cisco CMX is referred to both FIPS and CC features and functionalities. If you need to enable FIPS and CC on Cisco CMX, you need to enable FIPS mode on Cisco CMX. Once you do so, the system uses the cryptographic algorithms defined by the NIST for FIPS for all encrypted communication between its internal and external components. Additionally all the connection in and out of CMX (e.g. Web connection, controller connection, rsyslog server connection) are encrypted using TLS, HTTPS or IPSec.

The U.S. Department of Defense Unified Capabilities Approved Products List (UCAPL) mode is a higher level of security than FIPS alone. Its purpose is to maintain a single consolidated list of products that have completed interoperability and cybersecurity certification. Less secure protocols, such as HTTP, TLS ver. 1, and RSA 1024 are no longer supported.

Once you have enabled FIPS mode, you have the option to enable UCAPL mode. UCAPL requires a 15-20 character password, and a fixed timeout period of ten minutes, among other restrictions.

Note

- FIPS and UCAPL mode commands are available only to users with CMX admin user credentials through the Cisco CMX command line. Refer to Cisco CMX Command Reference, release 10.6 for more information.
- When FIPS or UCAPL authentication mode is enabled, you cannot enable or disable IPSec service. It is enabled by default when FIPS or UCAPL mode is enabled.
- When FIPS or UCAPL authentication mode is enabled, you can use the IPSec commands to restart, stop, or start IPSec services, and change or check authentication type.
- All IPSec commands are available when FIPS mode is disabled.

  For more information about IPSec commands, see the Cisco Connected Mobile Experiences (CMX) Command Reference Guide, at:

  https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-command-reference-list.html
- (CSCvo95518) Cisco CMX Release 10.6.2 and later with FIPS mode enabled can establish a Network Mobility Services Protocol (NMSP) connection with Cisco Catalyst 9800 wireless controllers running Release 16.12, with FIPS and CC mode enabled.

  In contrast, Cisco CMX Release 10.6.2 and later with FIPS mode enabled cannot establish an NMSP connection with Cisco WLCs running Release 8.x.

Note Before enabling FIPS mode on Cisco CMX, remove all the non-FIPS complian controllers from Cisco CMX. Otherwise, establishing NMSP connectivity after restarting Cisco CMX services will require an extensive amount of time.

FIPS Mode Requirements

FIPS mode initiates a set of interoperability and cybersecurity configuration changes designed to bring your CMX systems into compliance with the the Federal Information Processing Standard 140-2 (FIPS).

Authentication Requirements

- CMX sessions time out after no more than 30 minutes.
- Imported controllers in FIPS mode must be updated to Secure Socket Shell (SSH) authentication, to enable their Network Mobility Services Protocol (NMSP) connection.

Log in Requirements

There are no additional log in requirements for FIPS.

Password Requirements

- Password length: 8-20 characters.
- Minimum: one lowercase (a-z), one uppercase (A-Z), one digit (0-9), one special character (!@&-).

Protocol Requirements

- Transport Layer Security (TLS) 1.1 or higher.
- Internet protocol security (IPsec) for User Datagram Protocol (UDP) connection.
- Advanced Encryption Standard (AES) 256.
- Secure Hash Algorithm (SHA) 1 or higher.
- One of the following:
  - Rivest, Shamir, and Adelman (RSA) 2048 or higher.
  - Elliptic Curve Digital Signature Algorithm (ECDSA) with a National Institute of Standards and Technology (NIST) curve of P-256 or higher.

UCAPL Mode Requirements

UCAPL mode initiates a set of interoperability and cybersecurity configuration changes designed to bring your CMX systems into compliance with the the U.S. Department of Defense Unified Capabilities Approved Products List (UCAPL). UCAPL mode requires encryption of the `/opt` disk partition, as well as the following authentication, login, password, and protocols.

Note FIPS mode is a required prerequisite for UCAPL mode. Once FIPS has been enabled, the UCAPL mode option becomes available through the CMX **cmxctl config fips ucaplmode** command.

Authentication Requirements

- Two-factor authentication—Every user needs a signed client certificate. If your certificate is for user Tom, you can't log in as user Harry.
- Users are limited to ten open CMX windows at a time.
- CMX sessions will time out after ten minutes of user inactivity.
- Cisco Prime authentication is required when importing controllers and maps.

Log in Requirements

- User accounts are disabled for 30 minutes after three consecutive unsuccessful logins in one hour. The user sees a message when his account has been temporarily disabled. An admin can re-enable the user.
- There is a four-second delay between login prompts following a failed login.

Password Requirements

- Password length: 15-20 characters.
- Minimum: one lowercase (a-z), one uppercase (A-Z), one digit (0-9), one special character (!@&-).
- No more than three consecutive repeating characters.
- Password cannot match any of the last five passwords.
- A password change is required every 60 days.
- Password changes are limited to one password change per user per day.
- A user must log in again after a password change.

Protocol Requirements

- Transport Layer Security (TLS) 1.1 or higher.
- Internet protocol security (IPsec) for User Datagram Protocol (UDP) connection.
- Advanced Encryption Standard (AES) 256.
- Secure Hash Algorithm (SHA) 1 or higher.
- One of the following:
    - Rivest, Shamir, and Adelman (RSA) 2048 or higher.

- Elliptic Curve Digital Signature Algorithm (ECDSA) with a National Institute of Standards and Technology (NIST) curve of P-256 or higher.

Setting up FIPS or UCAPL Mode Correctly

Cisco recommends that you follow this general command deployment order when deploying FIPS or UCAPL mode. Your requirements may vary. For a full description and usage guidelines for each of these commands, see the *Cisco Connected Mobile Experiences (CMX) Command Reference Guide*, at:

https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-command-reference-list.html

Before you begin

You must run the following commands before enabling FIPS or UCAPL mode.

- To enable remote audit logging, run the **cmxctl config audit settings** command.
- To install remote syslog server certificate, run the **cmxctl config certs importrsyslogca** command.

Procedure

Step 1 Connect to CMX via SSH.

Step 2 Enter the **cmxctl config auth settings** command to enable strong password authentication, set minimum password length, set the number of unsuccessful login attempts, and set session timeout time.

Step 3 Enter the **cmxctl config certs keytype** command to select a keytype: RSA (the default) or ECDSA.

Step 4 Enter the **cmxctl config certs clear** command to clear out old or existing certificates.

Step 5 Enter the **cmxctl config certs createcsr** command to generate a new private and public keypair for the CMX server, and create a Certificate Signing Request (CSR). See Creating a Certificate Signing Request, on page 6 for more information.

Step 6 Have your certificates signed by authenticating third parties. See Installing Certificates in Cisco CMX for more information.

Step 7 Enter the **cmxctl config certs importcacert** command to install the concatenated CA certificates.

Step 8 Enter the **cmxctl config certs importservercert** command to install the concatenated server certificates.

Note When certificates are imported, there is a validity check that verifies the start date and end date. If the dates are not within the range or if the certificates are going to expire soon (withhin 30 days), an alert is generated on **System > Alerts** tab. The alert will be generated once a day until certificate expires or new valid certificate is installed.

Step 9 Enter the **cmxctl config fips verify** command to verify that your CMX system is correctly configured to support FIPS mode. See Verifying FIPS Readiness, on page 10 for more information.

Step 10 Enter the **cmxctl config audit settings** command to enable and manage the remote logging of system events (syslogs).

Step 11 Enter the **cmxctl config certs importrsyslogca** command to create, import, or manage security key certificates.

Step 12 Enter the **cmxctl config fips enable** command to enable FIPS mode.

The command restarts the CMX services.

Note When FIPS or UCAPL authentication mode is enabled, access to the command line through PuTTY or other standard SSH clients is restricted. In these cases, we recommend that you connect directly from a console, or use the VMWare vSphere console.

Step 13 Optionally, enter the **cmxctl config fips ucaplmode enable** command to enable UCAPL mode.

The CMX `/opt` partition must be encrypted before you can enable UCAPL. We recommend that you enable encryption at installation, or as soon as possible afterward. The encryption process requires time proportional to the amount of data present on the `/opt` partition.

The command restarts the CMX services. You must enter the encryption passphrase each time the device restarts, before logging in.

Choosing an Encryption Key Type

You can select a supported encryption algorithm for FIPS and UCAPL mode using the **cmxctl config certs keytype** command. Options are Rivest–Shamir–Adleman (RSA), or Elliptic Curve Digital Signature Algorithm (ECDSA).

Procedure

Step 1 Connect to Cisco CMX via SSH or through the console.

Step 2 Enter the **cmxctl config certs keytype** command.

Step 3 Select the encryption algorithm you prefer. See the following example:

```
Please enter key type [RSA / ECDSA] [RSA]: RSA
Keytype is set to RSA.
```

Creating a Certificate Signing Request

You can create a certificate signing request (CSR) with a corresponding public and private keypair using the **cmxctl config certs createcsr** command. When generating a CSR, you can now configure the Subject Alternative Name (SAN) as an extension in the certificate. You can set SAN to Public FQDN entry of the Cisco CMX server. The same SAN value is used as the default value for the **Common Name** field. You can override this default value by entering another value for common name.

Note If FIPS mode is enabled in Cisco CMX, certification validation is performed every time when CMX services are restarted. If certificate validation fails, Cisco CMX will not restart.

Procedure

Step 1 Connect to Cisco CMX via SSH or through the console.

Step 2 Enter the **cmxctl config certs clear** command to remove certificate files in the /opt/cmx/srv/certs directory.

Step 3 Enter the **cmxctl config certs createcsr** command.

The output and certificate information will vary, depending upon whether you chose the RSA or ECDSA encryption algorithm. Follow the prompts for your system. See the following example.

```
For SAN field of CSR, enter FQDN for CMX server []: servername.domain.com
Keytype is RSA, so generating RSA key with length  4096
Generating RSA private key, 4096 bit long modulus
...........
........
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]: US
State or Province Name (full name) [Some-State]: CA
Locality Name (eg, city) []: San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Cisco Systems, Inc.
Organizational Unit Name (eg, section) []: Enterprise
Common Name (e.g. server FQDN or YOUR name) [servername.domain.com]:
wirelesstestserver.domain.com
Email Address []:email@yourco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
The CSR is in: /opt/cmx/srv/certs
The Private key is in: /opt/cmx/srv/certs

CSR created successfully.
```

The new CSR and the Private key are both stored in the `/opt/cmx/srv/certs` directory.

Viewing Stored Certificates

You can see the certificates stored in the CMX /opt/cmx/srv/certs directory using the **cmxctl config certs show** command.

Procedure

Step 1 Connect to Cisco CMX via SSH or through the console.

Step 2 Enter the **cmxctl config certs show** command.

Your certifications display, similar to this example:

```
Certificate details

************************  Certificate Listing  ********************
======================================================================
**********************  CA Certificate(s)  ************************
======================================================================
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            b6:c0:fc:05:f6:27:45:1a
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=CA, L=San Jose, O=MSE, CN=RootCA
        Validity
            Not Before: Jul 19 05:17:33 2018 GMT
            Not After : Jul 18 05:17:33 2021 GMT
        Subject: C=US, ST=CA, L=San Jose, O=MSE, CN=RootCA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:ba:f2:2b:cd:87:90:23:f0:64:f5:83:d5:f2:90:
                    43:1a:16:36:c9:67:1a:82:f1:8f:6b:eb:1c:47:f1:
                    c4:fd:bf:55:98:ab:06:c0:90:dc:d7:13:1f:d3:2f:
                    12:e8:f2:74:66:65:7c:49:12:72:0c:27:9c:2e:84:
                    7e:29:a8:b6:18:62:5f:c2:97:a4:1c:e7:45:a2:cb:
                    f3:35:f3:64:15:e5:f0:27:6f:f1:07:61:41:9b:4c:
                    96:b3:56:d4:28:a4:85:90:86:52:4c:04:bc:da:38:
                    cc:f8:05:5b:3e:5c:03:b4:59:ec:8b:c9:5d:eb:61:
                    76:ba:20:3f:64:6c:25:5d:50:1e:85:37:ad:09:b2:
                    4a:fa:58:15:89:91:d9:5f:b8:9d:dd:64:31:8b:a4:
                    df:99:ff:ae:72:19:f8:a3:93:81:b9:4e:07:74:74:
                    95:b6:42:7b:5a:7d:38:92:4a:f4:86:5a:54:66:f0:
                    c1:fe:38:31:df:24:1c:40:94:36:67:8b:b3:56:93:
                    62:26:29:c2:cd:7f:7d:66:9d:f1:78:54:88:4f:6c:
                    b3:b7:80:54:05:03:09:c9:f9:14:65:8a:21:00:b5:
```

Validating Mutual Certificate During NMSP Connection in FIPS Mode

Cisco CMX establishes TLS/HTTPS connection with external systems. Cisco CMX uses NMSP and Northbound notification receivers (HTTP type) for establishing connection with Cisco Catalyst 9800 Series Wireless Controller. Certificate exchange is initiated during the SSL/TLS handshake when connections are successfully established between Cisco CMX and controller. However, certificates were not mutually validated by both connections.

To validate certificates on both sides, you must configure the following:

- For Cisco CMX: Configure or import controller CA certificate and Northbound Receiver's certificate for validating the certificate.
- For Cisco Wireless LAN Controller: Import Cisco CMX CA certificate.

Note

- Certificate validation happens only if FIPS is enabled on both Cisco CMX and controller. For example, if Cisco CMX is in FIPS mode, you can only synchronization and validate certificates if FIPS is enabled in controller.
- Cisco CMX Release 10.6.2 and later with FIPS mode enbaled can establish a NMSP connection with Catalyst 9800 Wireless LAN Controllers running Release 16.12 with FIPS/CC mode enabled. However, Cisco CMX Release 10.6.2 and later with FIPS mode enabled cannot establish a NMSP connection with controller running Release 8.x.
- We recommend that before enabling FIPS mode in Cisco CMX, remove all non-FIPS compliant controllers from Cisco CMX. Otherwise, establishing NMSP connectivity after restarting Cisco CMX services will require an extensive anount of time.

To validate certificates, perform the following steps:

Procedure

Step 1 To export CA certificates from Cisco CMX, enter this command and copy the certificate text that needs to be added into the unified controller. **cmxctl config certs exportnmspca**

Step 2 To import Cisco CMX CA certificates into unified controller, enter this command. **crypto pki trustpool import terminal**

Information similar to the following appears:

```
CMX-eWLC-1(config)# crypto pki trustpool import terminal
% Enter PEM-formatted CA certificate.
% ENd with a blank line or "quit" on a line by itself.
<<Copy the Cisco CMX certificate text here>>
% PEM files import succeeded.
```

Step 3 To export controller CA certificate, enter the following commands:

a) To find the trustpoint label, enter the **show wireless management trustpoint** and note down the trustpoint, for example ewlc-tp1.

b) To export CA certificate, enter the **crypto pki export <trustpoint> pem terminal** command and copy and paster the CA certificate contents (BEGIN-END block) into a file.

Note In this command, replace <*trustpoint*> with the trustpoint name from Step 3a. You can ignore "General Purpose Certificate' output.

Step 4 To import controller CA certificate into Cisco CMX, enter this command: **cmxctl config certs importcontrollerca <filename>** command.

Ensure that the file is in PEM format. You can also merge multiple CA certificates into a single file.

Step 5 Restart Cisco CMX services for the changes to take effect.

Step 6 (Optional) To view the installed certificates, run the **cmxctl config certs show** command.

Verifying FIPS Readiness

The **cmxctl config fips verify** command displays a simple grid, which identifies whether or not your CMX system is correctly configured to support FIPS mode. Cisco recommends that you run this command before trying to enable FIPS.

Procedure

Step 1 Use Secure Shell (SSH) to connect to Cisco CMX.

Step 2 Enter the **cmxctl config fips verify** command.
In this example, the command output indicates that the certificate authority (CA), server, and client certificates are not ready to support FIPS.

```
[cmxadmin@cmx]# cmxctl config fips verify

Certificates Required

+--------------------------------------+
| CA Certificate                | True |
+--------------------------------------+
| Server Certificate            | True |
+--------------------------------------+
| Server Key                    | True |
+--------------------------------------+
| Rsyslog CA Certificate        | False|
+--------------------------------------+

Certificate Validation

+--------------------------------------+
| CA Cert Validation            | True |
+--------------------------------------+
| Server Cert Validation        | True |
+--------------------------------------+
| Client Cert Validation        | True |
+--------------------------------------+

Security Configuration

+--------------------------------------+
| Strong Password               | True |
+--------------------------------------+
| Security Parameters           | True |
+--------------------------------------+

Audit Logging

+--------------------------------------+
| Audit Logging Status          | False|
+--------------------------------------+
```

What to do next

If the system shows any out-of-compliance areas (False), check Setting up FIPS or UCAPL Mode Correctly, on page 5 to address the discrepancies.

Enabling and Managing FIPS Mode

Use the **cmxctl config fips** commands to verify your CMX system is ready for Federal Information Processing Standards (FIPS) mode, to enable or disable FIPS mode, and to show its running status.

You should take precautions while performing **cmxctl config fips disable**. Ensure that you do not perform any delete action by running the **cmxctl config certs clear** on certificates such as ca.crt, server.crt and so on while FIPS is enabled. The FIPS mode will then go into a deadlock situation and can never be disabled. This is because even for disabling the FIPS mode, system checks for certificates and if not found, it will fail to disable FIPS stating the error - "Problem in disbaling FIPS mode". And if you try to add self-signed certificates, they will not get added because FIPS is enabled. We recommend that you do not attempt to clear certificates while FIPS is enabled. Ensure that you adhere to the necessary precationary measures when Cisco CMX is in FIPS mode.

Procedure

Step 1 Connect to CMX via SSH.

Step 2 Enter the **cmxctl config fips verify** command, to confirm that all the necessary security and certificate requirements are in place.

```
[cmxadmin@cmx]# cmxctl config fips verify
Certificates Required

+-------------------------------------+
| CA Certificate                | True |
+-------------------------------------+
| Server Certificate            | True |
+-------------------------------------+
| Server Key                    | True |
+-------------------------------------+
| Rsyslog CA Certificate        | False|
+-------------------------------------+

Certificate Validation

+-------------------------------------+
| CA Cert Validation            | True |
+-------------------------------------+
| Server Cert Validation        | True |
+-------------------------------------+
| Client Cert Validation        | True |
+-------------------------------------+

Security Configuration

+-------------------------------------+
| Strong Password               | True |
+-------------------------------------+
| Security Parameters           | True |
+-------------------------------------+
```

```
Audit Logging

+--------------------------------------+
| Audit Logging Status          | False|
+--------------------------------------+
```

Step 3 Enter the **cmxctl config fips enable** command to start FIPS mode.
The CMX processes restart.

What to do next

Using a console, enter the **cmxctl config fips status** command, to verify that FIPS is running on your Cisco CMX device.

Configuring Notification Listener in FIPS Mode

In FIPS mode, notifications are sent to only those notification listeners with the **Receiver Type** set as "HTTPS". If Receiver type is set to HTTP, that notification listener will not receive any notification in FIPS mode.

For more information about how to create a notification, see #unique_294.

After FIPS mode is enabled (and Cisco CMX services restarted), you will need to change the **Receiver type** of every listener to **HTTPS** in order to receive notifications.

When the Receiver Type is HTTPS, you must import CA certificate corresponding to the Notification listener (CA that signed the Server Certificate of the notification listener). The certificate file needs to be in PEM format. This is mandatory field.

After all the listeners are modified to set Receiver Type as **HTTPS** and corresponding CA certificate is imported, you must restart the Cisco CMX services for the certificate changes to take effect.

When notifications are generated, Cisco CMX establishes HTTPS connection with notification listener and use the CA certificate to validate the listener's certificate before sending the notification. If the certificate validation fails, the notification is not sent to the listener.

Enabling and Managing UCAPL Mode

Use the **cmxctl config fips ucapl** commands to enable or disable the U.S. Department of Defense Unified Capabilities Approved Products List (UCAPL) mode, and to show its running status.

Before you begin

The CMX `/opt` partition must be encrypted before you can enable UCAPL.

Procedure

Step 1 Connect to CMX command line either from a console, or from a VMWare vSphere console.

Step 2 Enter the **cmxctl config fips ucaplmode enable** command to start UCAPL mode.

The CMX processes restart.

What to do next

Using a console, enter the **cmxctl config fips ucaplmode status** command, to verify that UCAPL mode is running on your Cisco CMX device.

Enabling Logging in UCAPL mode

Cisco CMX release 10.6 supports logging HTTP headers and access to important files and folders when UCAPL mode is enabled.

Logging HTTP Headers

You can log all the HTTP headers received in every incoming HTTPS request to local syslog i.e. /var/log/messages. This feature can be turned on or off using command given below.

Note This operation of logging all the headers is CPU intensive and can cause performance degradation. So use it cautiously and turn it off when not required.

Procedure

Step 1 To enable this feature, run the **cmxctl config fips ucaplmode logHTTPHeaders** command.

```
[cmxadmin@cmx]# cmxctl config fips ucaplmode logHTTPHeaders
Enable HTTP Headers Logging [yes / no] [no]: yes
Restarting haproxy service
True
Done
The nodeagent service is currently running with PID: 1470
Attempting to restart Haproxy
.....
Service Haproxy has successfully restarted
logHTTPHeaders is enabled.
```

Step 2 To view these logs, run the **cmxctl config audit view** command.

Step 3 (Optional) To disable this feature, run the **cmxctl config fips ucaplmode logHTTPHeaders** command.

```
[cmxadmin@cmx]# cmxctl config fips ucaplmode logHTTPHeaders
Enable HTTP Headers Logging [yes / no] [no]:
Restarting haproxy service
True
Done
The nodeagent service is currently running with PID: 1470
Attempting to restart Haproxy
.....
```

```
Service Haproxy has successfully restarted
logHTTPHeaders is disabled.
```

Logging File Access

You can log access to important files and folders, whenever those files/folders are added/deleted/modified, while in UCAPL mode. This feature can be turned on or off using command given below.

Procedure

Step 1 To enable this feature, run the **cmxctl config fips ucaplmode logFileAccess** command.

```
[cmxadmin@cmx]# cmxctl config fips ucaplmode logFileAccess
Enable File Access Logging [yes / no] [no]: yes
Restarting Audit Service
Stopping logging:                                          [  OK  ]
Redirecting start to /bin/systemctl start auditd.service
```

Step 2 (Optional) To disable the feature, run the **cmxctl config fips ucaplmode logFileAccess** command.

```
[cmxadmin@cmx]# cmxctl config fips ucaplmode logFileAccess
Enable File Access Logging [yes / no] [no]:
Restarting Audit Service
Stopping logging:                                          [  OK  ]
Redirecting start to /bin/systemctl start auditd.service
```

Setting Up External Server Authentication

Cisco CMX supports external AAA server authentication. Use external AAA authentication servers, such as Radius Server, and AD and allow Cisco CMX to delegate CMX's authentication functionality to the external AAA server. With this, CMX users can be directly managed, added, and deleted directly in the AAA server.

When the feature is enabled, the local user management for CMX GUI users is suspended and local GUI users are deleted. When a CMX user tries to log in to the CMX GUI, CMX authenticates the user against the credentials stored in this external AAA server. After the user is authenticated, CMX provides access to the GUI based on the user's role in CMX. From end-user perspective, this authentication by the AAA server is transparent and there is no change in the GUI behavior.

Procedure

Step 1 To configure external RADIUS authentication, run the **cmxctl config authserver** command.

Step 2 Use these subcommads as required:

a) **cmxctl config authserver delete**: Removes the external RADIUS authentication server.

b) **cmxctl config authserver settings**: Sets the external RADIUS authentication server.

c) **cmxctl config authserver show**: Shows the external server configuration.

Configuring Cisco CMX Users in the External Authentication Server

Before enabling this feature, the passwords and roles of the Cisco CMX GUI users should be configured in the external authentication server. A Cisco CMX user's ID and the role should be configured exactly as expected by Cisco CMX in this external authentication server.

Apart from this, a secret shared key should also be configured on the external authentication server. Later,the same shared key should be configured on Cisco CMX.

Configuring an External Authentication Server in Cisco CMX

You can configure an external authentication server using the **cmxctl config authserver settings** command. Provide the server IP address, shared secret key (which is already configured in the external authentication server, as described earlier), the local user name as a **Last Resort** user and the password.

If the connection to the external AAA server is lost due to some reason, a user can log in using this **Last Resort** user credentials, in which case, authentication is done by the Cisco CMX server itself. Thus, the system can function properly even if connectivity to the external AAA server is lost.

The following example shows how to configure an external RADIUS authentication server.

```
[cmxadmin@cmx]# cmxctl config authserver settings
Enter external RADIUS authentication server host : 1.2.3.4
Enter RADIUS server shared secret key : password
Configure local account. This account can be used if RADIUS server is not reachable.
Enter username : cmxadmin
Enter password :
Repeat for confirmation:
External RADIUS authentication server configured successfully
```

Configuring an External AAA Server with Cisco CMX

You can authenticate Cisco CMX users to connect with an external AAA server. For every authentication request, the server must sent Access-Accept or Access-Reject response packet depending upon the outcome of the authentication.

An external AAA server must be configured with the following details for AAA server and Cisco CMX to work together to perform external authentication. There are two types of AAA servers: Cisco ISE and freeradius.

Note In Cisco CMX Release 10.6.3, the External Authentication (AAA) feature is enabled without the Federal Information Processing Standard 140-2 (FIPS) or the U.S. Department of Defense Unified Capabilities Approved Products List (UCAPL) mode. Prior to Cisco CMX Release 10.6.3, the External Authentication (AAA) feature was only available with UCAPL mode enabled.

Procedure

Step 1 Access-Accept response must include the following Vendor Specific Attribute (VSA) information with value as appropriate role corresponding to the authenticated user.

a) Provide the **Attribute** value as **`Cisco-AVpair`**. For this VSA, provide **Type** as **`1`**.

b) Enter "shell:cmx-user-role=<ROLE>", wherein values for <ROLE> can be "Admin", "System", "Manage", "Location" and "Read Only".

Note Value string is case-sensitive.

Step 2 For **freeradius AAA server**, the sample string for role **Admin** in "users" is **`Cisco-AVPair = "shell:cmx-user-role=Admin"`**.

Step 3 For **Cisco ISE**, follow the steps:

a) In section **Policy> Policy Elements> Dictionaries > System> Radius> Radius Vendors** (if not configured already), add Vendor or Vendor specific attribute (VSA).

- **Vendor ID**: Enter the value as **`9 (Cisco Systems)`**.
- **VSA Type/ID**: Enter the value as **`1`**.

b) Add a Network Device Profile and associate correct vendor dictionary that contains VSA.

c) Add Cisco CMX as a Network Device and associate correct Network Device Profile.

d) Create authorization policies that sends Access-Accept packets in response to authentication requests.

- In the response, add Vendor Specific Attribute (Vendor ID=9 for Cisco Systems) named "cisco-avpair" (Type = 1) with a value of "shell:cmx-user-role=<ROLE>". <ROLE> can have the values "Admin", "System", "Manage", "Location" and "Read Only".

Note Value string is case-sensitive.

e) Create one authorization policy for every role that needs to be supported.

f) Create Policy Set with required authorization policies.

For more information on ISE configuration, see https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215525-use-radius-for-device-administration-wit.html.

Displaying External Authentication Server Settings

To display the settings of the currently configured external authentication server, run the **cmxctl config fips ucaplmode authserver show** command.

```
[cmxadmin@cmx]# cmxctl config fips ucaplmode authserver show
External RADIUS authentication server host : 1.2.3.4
RADIUS server shared secret key : password
Local user : cmxadmin
```

Deleting External Authentication Server Settings

To delete the currently configured external authentication server settings, run the **cmxctl config fips ucaplmode authserver delete** command.

When these settings are deleted, CMX reverts to local user management. Standard CMX UI users are re-created locally and their passwords are set to default. If new users were added to External Authentication Server, prior to disabling feature, you will need to configure those users in CMX UI as well.

Note If you have this feature enabled and later disable FIPS mode, this feature is also disabled and External Authentication Server details are deleted. Then CMX reverts to local user management as described above.

The following example shows how to delete the configured external authentication server settings.

```
[root@server]# cmxctl config fips ucaplmode authserver delete
External RADIUS authentication server is removed.
```

Validating Client Certificates

Use the **cmxctl config certs clientcertvalidation** command when CMX is in FIPS or UCAPL mode to obtain a valid, signed client certificate for every CMX user ID.

Procedure

Step 1 Connect to CMX through SSH or the console.

Step 2 (Optional) Use the **cmxctl config {FIPS | ucaplmode} status** command to verify whether FIPS or UCAPL is currently enabled.or not.

Step 3 Use the **cmxctl config certs clientcertvalidation** command to enforce CMX validation of client certificates.

Setting Up a UCAPL Automatic Backup

Cisco CMX supports automatic weekly backups in the U.S. Department of Defense Unified Capabilities Approved Products List (UCAPL) mode. You can enable the backups before or after entering UCAPL mode, but the backups will not begin until UCAPL is enabled.

Procedure

Step 1 Connect to the CMX CLI either from a console or SSH.

Step 2 Enter the **cmxctl config fips ucaplmode autobackup** command to configure the automatic backup:

```
[cmxadmin@cmx]#cmxctl config fips ucaplmode autobackup
CMX Auto Backup is currently disabled.
```

Step 3 Respond to the following prompt: **Do you want to enable it? (yes/no) [yes]:**

Click **Yes** or press **Enter** to enable auto backup if CMX is already in UCAPL mode. If CMX is not in this mode, auto backups begin, when UCAPL mode is enabled. The default option is **yes**.

```
CMX Auto Backup frequency is weekly.
Please select day and hour of the week to run the auto-backup.
```

Step 4 Respond to the following prompt: **Day of the week: [0=Sunday, 1=Monday ... 6=Saturday] [0]:**

Enter a number from **0** (Sunday) to **6** (Saturday) to specify the day of the week the backup should be performed. The default is **Sunday**.

Step 5 Respond to the following prompt: **Hour of the day: [0-23] [2]:**

Enter a number from **0** (midnight) to **23** (11 p.m.) to specify the hour of the backup. The default is **2** a.m.

If UCAPL mode is already enabled, your confirmation will resemble this:

```
CMX auto-backup is now enabled.
Redirecting to /bin/systemctl restart crond.service
auto-backup will execute every Saturday at 10:10 AM
```

If UCAPL mode is not yet enabled, your confirmation will resemble this:

```
CMX auto-backup is configured. But, it will be enabled only when UCAPL mode is enabled.
Redirecting to /bin/systemctl restart crond.service
auto-backup will execute every Monday at 9:10 AM
```

Step 6 (Optional) To disable autobackup, run the **cmxctl config fips ucaplmode autobackup** command again, and enter **yes** or press **Enter** when prompted.

```
[cmxadmin@cmx]#cmxctl config fips ucaplmode autobackup
CMX Auto Backup is currently enabled.

Do you want to disable it ? (yes/no) [yes]:yes
CMX Auto Backup is now disabled.
Redirecting to /bin/systemctl restart crond.service
```

Working with the Certificate Revocation List

Cisco CMX supports certificate validation of the Certificate Revocation List (CRL) as per FIPS/CC requirement. There are three options for supporting the CRLs in Cisco CMX. Once CRL is installed properly, then Cisco CMX server certificate is validated against CA certificate and against CRL as well. If the Cisco CMX server certificate is revoked and reflected in the CRL then the Cisco CMX server certificate validation will fail and Cisco CMX services will fail to start in FIPS mode.

The available options are:

- **Automatic download of CRL if CA certificate support CDP extension**—If the CA certificate that has signed the CMX server certificate is being imported contains a CRL Distribution Point (CDP) extension in the CA certificate, then the CDP extension contains the URL where CRL can be downloaded from. CMX attempts to download this URL from the internet (if access is available).
- **Manual import of CRL (in PEM format)**—If the internet access is not available on CMX server (directly or through HTTP proxy), then you can download the CRL from its location and import the downloaded file into CMX.

- **Configuring URL for the CRL for periodic automatic download**—In this option, the URL of the CRL file can be configured directly into CMX. CMX will then download the CRL periodically – once a day and update it. This will keep the CRL file up-to-date as the CRLs as periodically updated.

Manual Import of CRL

To import the CRL file, follow the below steps:

Before you begin

Download the CRL from its location. This CRL file will be mostly in DER format. Before you import into Cisco CMX, you will need to covert it from DER to PEM format. On a separate server, you can convert the CRL file from DER to PEM format. To convert the CRL file, run the **openssl x509 -inform der -in crlfile -out crl.pem** command.

Procedure

Step 1 SCP the CRL file in PEM format to Cisco CMX.

Step 2 Run the **cmxctl config certs importcrl** command to import the CRL file.

```
[cmxadmin@cmx]# cmxctl config certs importcrl
Enter the full path of the CRL file /home/cmxadmin/server.crl.pem
Successfully transferred the file
CRL file imported successfully
CMX Certificate validation against CRL is successful.
0
```

Step 3 To configure the the CRL URL, run the **cmxctl config certs importcrlurl** command.

```
[cmxadmin@cmx]# cmxctl config certs importcrlurl
Please enter URL to downlaod CRL: http://example.com/testca.crl
Redirecting to /bin/systemctl restart crond.service
```

Note If internet access is available directly (or via proxy), configuring URL of the CRL into Cisco CMX will be the best option for supporting CRL, as it will automatically download the CRL once a day and keep the local copy up-to-date.

Disk Wipeout

This feature allows a Cisco CMX user to wipe out the entire disk including data and executables. This feature can be used when you no longer need to use the system and want to de-commission it and/or use for some other purpose.

After performing this operation, system will not boot as usual and will not provide the normal login prompt. The system becomes unusable and all the data on the disk is deleted and not accessible anymore.

Note This disk wipeout feature is currently available only in FIPS mode. System needs to be in FIPS mode in order to use this command. Additionally, this command is available only from console window and it is not allowed from SSH session.

To wipeout the disk, run the **cmxos wipeoutdisk** command from console window.

```
[root@server]# cmxos wipeoutdisk
WARNING: This command will wipe out the entire disk.
It will remove entire CMX installation along with all the existing data.
Once completed, this box will not be useable.
Do you want to continue? [y/N]: y
lave you closed all SSH sessions to this CMX? [y/Nl: y
WARNING: This is your last chance.
If you want to take backup, please exit now.
Vou can take backup and transfer it to some other machine.
I*hen execute this command again.
Do you want to continue with disk wipeout? [y/N]: y_
Stopping the CMX services

nonit.service is not a native service, redirecting to /sbin/chkconfig.
cuting /sbin/chkconfig min it off
Stopping nodeagent Process...

cuting shutdown
```

If the disk was encrypted previously, it will prompt for the disk encryption password in order to clean the disk. This password will not be asked if the disk was not encrypted earlier. The operation will take half an hour or more based on the total disk space.

```
Welcome to emergency mode! After logging in, type "journalctl -xb" to view
system logs, "systemctl reboot"
to reboot, "systemctl default" or ÄD to
boot into default mode.
Error getting authority: Error initializing authority: Error sending credentials:
Error sending mess
age: Broken pipe (g-io-error-quark, 44)

Entered Rescue mode on Sun Jan 27 14:27:48 UTC 2019.
Proceeding with disk wipeout...
Wiping out OUA disk
Jnmounting /opt partition ...
/opt disk is encrypted. Removing encryption ...
Enter passphrase to be deleted:
WARNING!

Hiis is the last keyslot. Device will become unusable after purging this key.
Are you sure? (Type uppercase yes): YES
Logical volume vg_cmx/lv_opt is used by another device.
Wiping out the disk now. This operation will take long time.
shred: /dev/sda3: pass 1/2 (random)...
shred: /dev/sda3: pass 1/2 (random)...502MiB/121GiB 0/
shred: /dev/sda3: pass 1/2 (random)...
1.0GiB/121GiB 0/
shred: /dev/sda3: pass 1/2 (random)... 1.5GiB/121GiB lx
```

Once the operation is complete, press **Enter** to continue. After rebooting, system will not boot as usual and you cannot login to the Linux system or Cisco CMX.