Configuring Root Access Control

This chapter contains the following sections:

Prerequisites

Before enabling FIPS mode (also knows as Root Access Control, or RAC), ensure that you have access to console of MSE server/VM. By enabling FIPS mode/RAC , SSH access is disabled, so console is the only access available later on.

Overview

In MSE 8.0 Release, Root Access Feature (RAC) is introduced in Connected Mobile Experience (CMX) as part of FIPS/CC/UCAPL compliance. Users who seek for FIPS compliance can use this feature.

- Before the Root Access Control is Enabled
  When the MSE establishes SSL connection with the Cisco Wireless LAN Controller (WLC), it sends a list of supported cryptographic ciphers (including both FIPS and non-FIPS compliant ciphers) to the WLC as part of SSL handshake. The WLC selects a cipher from the list and responds to the MSE with the chosen cipher. The subsequent NMSP message exchanged between the MSE and the WLC will be encrypted using the chosen cipher. In this case, MSE can interoperate with the following:
  - Cisco WLC 8.0 and earlier releases.
  - Cisco IOS XE Release 3E and earlier releases.
- After the Root Access Control is Enabled
  - SSH will be disabled
  - Root password gets changed and hidden from the user
  - Weak ciphers will be disabled in SSL and SSH connections

When the MSE establishes SSL connection with the WLC, it sends a list of FIPS complaint cryptographic ciphers to the WLC as part of the SSL handshake. In this case, the MSE can only interoperate with the WLC release that are FIPS compliant (that include Cisco WLC Release 8.0 and Cisco IOS XE Release 3E Release). The MSE cannot establish SSL connection to WLC releases that are non-FIPS compliance.

Note RAC configuration is not synchronized on both the primary and secondary MSE. In HA mode, if RAC needs to be enabled, it needs to be enabled on both Primary and Secondary MSE. In case of failover or failback, the RAC configurations work on the active server properly.

Using Remote Support

You will have the limited privileges and cannot perform operations such as upgrade or troubleshoot, if the RAC is enabled. Remote support feature provides you privileged access.

To make use of the remote support feature, follow these steps:

SUMMARY STEPS

1. Enable Remote Support through setup.sh command.
2. Create a remote account and get a passphrase.
3. Provide the passphrase to TAC and get it decoded to actual password.
4. Using this password, you can now login as remote account which grants the root privileges to the user.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Enable Remote Support through setup.sh command.	**Note** Only Admin user can enable this.
Step 2	Create a remote account and get a passphrase.	
Step 3	Provide the passphrase to TAC and get it decoded to actual password.	
Step 4	Using this password, you can now login as remote account which grants the root privileges to the user.	You can now perform privileged operations. **Important** While Remote Support is enabled and Remote Account is active, the CMX is not FIPS compliant. Hence it is advised to delete Remote Account and Disable Remote Support when privileged access is no longer needed. Once the Remote account is deleted and Remote Support is disabled, the CMX become FIPS compliant. **Note** Remote account has a validity period of 30 days. If the account is not deleted before that, the account expires at the end of the validity period.

Enabling Root Access Control

To enable the RAC, follow these steps:

Step 1 Install MSE using root user.

Step 2 Enter the following command:
```
/opt/mse/setup/setup.sh
```

Step 3 Select option "Remote Access Control" by entering the number corresponding to this option.

Step 4 Configure Root Access Control
```
Configure Root Access Control? (Y)es/(S)kip/(U)se default [Skip]:y
```

Step 5 Enable Root Access Control.
```
Enable Root Access Control? (Y)es/(S)kip/(U)se default [Skip]:y
```

Step 6 Enter new user id for admin user.
```
Enter admin username:
```
Note mseadmin is a group id and cannot be entered as user id.

Step 7 Enter new password.
```
Enter new password:
```

Step 8 Re-type new password to confirm the password.
```
Re-type new password:
```

Step 9 Select option "Verify and apply changes" by entering the number corresponding to this option.

Step 10 Verify the setup information.
```
Is the above information correct (yes or no):yes
```

Step 11 Ignore the warning message which states Cisco Prime Infrastructure communication password is mandatory.
```
Ignore and proceed (yes/no):yes
```

Step 12 Press enter to continue.
All the SSH sessions will be terminated within a minute.

Working in RAC Mode

To work in RAC mode, follow these steps:

Step 1 Log into the console of the MSE server.

Step 2 Use admin user credentials while enabling RAC.

Step 3 Use the following commands that are aliased for special purpose to provide pseudo permissions to admin user.

Note Do not enter the full path or relative path of the command to run it. Just enter the command name as is. For example, you need to run "setup.sh" command instead of "/opt/mse/setup/setup.sh" or "./setup.sh" command.

- setup.sh
- msed

- getserverinfo
- gethainfo
- apacheserverd

Some commands are restricted and admin user cannot execute them (example reboot). To execute restricted command, admin user should make use of Remote Support feature.

Enabling Remote Support and Creating Remote Account

To enable remote support and create remote account, follow these steps:

Step 1 Log into console using admin user credentials.

Step 2 Execute the command `setup.sh`.

Step 3 Select option "Remote Support" by entering the number corresponding to this option.

Step 4 Configure remote support.

```
Configure remote support? (Y)es/(S)kip/(U)se default [Skip]:y
```

Step 5 Enable remote support.

```
Enable remote support? (Y)es/(S)kip/(U)se default [Skip]:y
```

Step 6 Select option "Create Remote Account" by entering the number corresponding to this option.

Step 7 Configure remote account.

```
Configure remote account? (Y)es/(S)kip/(U)se default [Skip]:y
```

Step 8 Create remote account and generate passphrase.

```
Create remote account and generate passphrase? (Y)es/(S)kip/(U)se default
[Skip]:y
```

Step 9 Enter new user id for remote account.

Step 10 The setup script displays the following message to confirm the account creation: "Remote account created successfully". It displays the remote account passphrase, which is required later on to generate the remote account password.

Step 11 Enter the validity of the account in days. The default value is 14 and maximum value is 30 days.

Step 12 Select option "Verify and apply changes" by entering the number corresponding to this option.

Step 13 Verify the setup information.

```
Is the above information correct (yes or no):yes
```

Step 14 Ignore the warning message which states Cisco Prime Infrastructure communication password is mandatory.

```
Ignore and proceed (yes/no):yes
```

MSE restarts.

Note Remote user is disabled by one of the following ways:

1. After the validity period, the remote user is automatically expired by the system.
2. Login as admin user and delete the remote user. For more information, see the Disabling Remote Support and Deleting Remote Account, on page 5.
3. Login as a remote user and disable the RCA, which in turn disables the remote support and deletes the remote account. For more information, see the Disabling Root Access Control, on page 6.

Generate Remote User Password and Logging in as Remote User

To generate remote user password and logging in as remote user, follow these steps:

Step 1 Open a case with Cisco TAC to generate the remote user password by providing the remote user name and passphrase.

Step 2 Log into the console window of MSE with remote user id and new password.

Step 3 Enter the command `id` to verify that the user has root privileges.
You can now operate the MSE with full root privileges.

Disabling Remote Support and Deleting Remote Account

To disable remote support and deleting remote account, follow these steps:

Step 1 Log into console using admin user credentials.

Step 2 Execute the command `setup.sh`.

Step 3 Select option "Delete Remote Account" by entering the number corresponding to this option.

Step 4 Disable remote support.

```
Disable remote support? (Y)es/(S)kip/(U)se default [Skip]:y
```

Step 5 Select option "Verify and apply changes" by entering the number corresponding to this option.

Step 6 Verify the setup information.

```
Is the above information correct (yes or no):yes
```

Step 7 Ignore the warning message which states Cisco Prime Infrastructure communication password is mandatory.

```
Ignore and proceed (yes/no):yes
```

MSE restarts.

Disabling Root Access Control

To disable the RAC, follow these steps:

Step 1 Log into MSE console with remote user credentials.

Step 2 Change to a directory other than $HOME or its sub-directory, as $HOME will be deleted as part of disabling RAC.

Step 3 Execute the command `/opt/mse/setup/setup.sh`.

Step 4 Select option "Remote Access Control" by entering the number corresponding to this option.

Step 5 Configure Root Access Control.

```
Configure Root Access Control? (Y)es/(S)kip/(U)se default [Skip]:y
```

Step 6 Disable the Root Access Control.

```
Disable Root Access Control? (D)isable/(S)kip/(U)se default [Skip]:d
```

The admin user gets deleted, and SSH access is re-enabled.

Step 7 Configure root password.

Step 8 Select option "Verify and apply changes" by entering the number corresponding to this option.

Step 9 Verify the setup information.

```
Is the above information correct (yes or no):yes
```

Step 10 Press enter to continue.
The session will be deleted in one minute.

Step 11 Use SSH to log into MSE using root credentials.

SHA2 Cryptographic Cipher Support

- Before the Root Access Control is Enabled
  When the MSE establishes SSL connection with the Cisco Wireless LAN Controller (WLC), it sends a list of supported cryptographic ciphers (including both FIPS and non-FIPS compliant ciphers) to the WLC as part of SSL handshake. The WLC selects a cipher from the list and responds to the MSE with the chosen cipher. The subsequent NMSP message exchanged between the MSE and the WLC will be encrypted using the chosen cipher. In this case, MSE can interoperate with the following:
  - Cisco WLC 8.0 and earlier releases.
  - Cisco IOS XE Release 3.6E and earlier releases.
- After the Root Access Control is Enabled
  When the MSE establishes SSL connection with the WLC, it sends a list of FIPS complaint cryptographic ciphers to the WLC as part of the SSL handshake. In this case, the MSE can only interoperate with the WLC release that are FIPS compliant (that include Cisco WLC Release 8.0 and Cisco IOS XE Release 3E Releases). The MSE cannot establish SSL connection to WLC releases that are non-FIPS compliance.