CLI Commands for EnhancedSecurityMode and FIPS Mode

CLI Commands for EnhancedSecurityMode

Use the following CLI commands for EnhancedSecurityMode:

- **admin:utils EnhancedSecurityMode**
- **utils EnhancedSecurityMode disable**
- **utils EnhancedSecurityMode enable**
- **utils EnhancedSecurityMode status**

Configure EnhancedSecurityMode

An administrator can use this procedure on Cisco Prime Collaboration Deployment to configure EnhancedSecurityMode. When this mode is enabled, the following system enhancements are updated automatically:

- Stricter credential policy for password changes is implemented
- TCP becomes the default protocol for remote audit logging
- FIPS mode is enabled

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils EnhancedSecurityMode status** command to confirm whether Enhanced Security Mode is enabled.

Step 3 To configure Enhanced Security Mode, run one of the following commands on a node:

- To enable this mode, run the **utils EnhancedSecurityMode enable** command.
- To disable this mode, run the **utils EnhancedSecurityMode disable** command.

CLI Commands for FIPS Mode

Use the following CLI commands for FIPS mode on Cisco Prime Collaboration Deployment:

- **utils fips enable**—Enable FIPS mode. For details, see the Enable FIPS Mode, on page 2 procedure.
- **utils fips disable**—Disable FIPS mode. For details, see the Disable FIPS Mode, on page 3 procedure.
- **utils fips status**—Provide the details whether FIPS mode is enabled or disabled on a server.

Note The disaster recovery system CLI commands are supported in FIPS mode. For details on these commands, see the CLI Commands and Disaster Recovery System chapter of the *Cisco Prime Collaboration Deployment Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Enable FIPS Mode

You can enable the FIPS mode through CLI.

Caution Before you enable FIPS mode, we strongly recommend that you perform a system backup. If FIPS checks fail at start-up, the system halts and requires a recovery CD to be restored.

Procedure

Step 1 Start a CLI session.

Step 2 In the CLI, enter **utils fips enable**

The following prompts appear:

```
admin:utils fips enable

Security Warning : The operation will regenerate certificates for

1)Tomcat
2)IPsec
```

```
Any third party CA signed certificates that have been uploaded for the above
components will need to be re-uploaded.
********************************************************************************
This will change the system to FIPS mode and will reboot.
********************************************************************************

Do you want to continue (yes/no) ?
```

Step 3 Enter **yes**.

The following message appears:

```
Generating certificates...Setting FIPS mode in operating system.
FIPS mode enabled successfully.
******************************************************
It is highly recommended that after your system restarts
that a system backup is performed.
******************************************************
The system will reboot in a few minutes.
```

Cisco Prime Collaboration Deployment reboots automatically.

Disable FIPS Mode

You can disable FIPS mode through the CLI using the following procedure:

Procedure

Step 1 Start a CLI Session.

Step 2 In the CLI, enter **utils fips disable**

The following prompts appear:

```
admin:utils fips disable

Security Warning : The operation will regenerate certificates for

1)Tomcat
2)IPsec

Any third party CA signed certificates that have been uploaded for the above
components will need to be re-uploaded.
********************************************************************************
This will change the system to NON-FIPS mode and will reboot.
********************************************************************************

Do you want to continue (yes/no) ?
```

Step 3 Enter **yes**.

Cisco Prime Collaboration Deployment reboots and is restored to non-FIPS mode.

Note Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.

User Account and Sign-in Attempts on CLI and Interface

Following table lists the scenarios when a user signs in to the Cisco Prime Collaboration Deployment application or CLI and the result of sign in attempts:

User Sign-in Scenario	Result of Sign-in Attempt
Sign-in with the valid credentials	Sign-in is successful and the application home page is accessible
Sign-in with invalid credentials	Sign-in fails
Sign-in after exceeded number of attempts on the application	Account is locked after three consecutive unsuccessful attempts
Sign-in after exceeded number of attempts on the CLI	CLI sign-in fails due to locked account even though the user types in the correct password
Sign-in to the application after the lockout period expires	After 5 minutes of lockout period, the application is available for you to sign-in
Sign-in to CLI after the lockout period expires	After 5 minutes of lockout period expiry, the account gets unlocked and you can sign-in to the CLI
Sign-in to the application when the account is locked due to inactivity	Account gets locked due to inactivity of the session
Sign-in to the application after account lockout, which is caused due to inactivity, is resolved	Sign-in is successful

Configure Remote Audit Logging for Platform Logs

Complete the following tasks to add remote audit logging support for platform audit logs, remote support logs, and csv files. For these types of logs, the FileBeat client and logstash server are used.

Before you begin

Ensure that you have set up an external logstash server.

Procedure

Step 1 Configure the FileBeat client with the external logstash server details, such as IP addresses, ports, and file types. For procedure, see Configure Logstash Server Information, on page 5.

Step 2 Enable the FileBeat client for remote audit logging. For procedure, see Configure the FileBeat Client, on page 5.

Configure Logstash Server Information

Use this procedure to configure the FileBeat client with the external logstash server information, such as IP address, port number, and downloadable file types.

Before you begin

Make sure that you have set up your external logstash server.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils FileBeat configure** command.

Step 3 Follow the prompts to configure the logstash server details.

Configure the FileBeat Client

Use this procedure to enable or disable the FileBeat client for uploads of platform audit logs, remote support logs, and csv files.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils FileBeat status** command to confirm whether the FileBeat client is enabled.

Step 3 Run one of the following commands:

- To enable the client, run the **utils FileBeat enable** command.
- To disable the client, run the **utils FileBeat disable** command.

Step 4 Repeat this procedure on each node.

Note Do not run any of these commands on all nodes simultaneously.

Platform CLI Commands for Security in EnhancedSecurityMode

When EnhancedSecurityMode is enabled, an administrator can restrict the following options to prevent unauthorized access:

- View audit log
- Download audit log
- Delete audit log
- Enable or disable audit demon

The administrator can restrict the above options by running the following platform CLI commands:

- **file view activelog<audit log file name>**
- **file get activelog <audit log file name>**
- **file delete activelog<audit log file name>**
- **file dump activelog<audit log file name>**
- **file tail activelog <audit log file name>**
- **file search activelog<audit log file name><search string>**
- **file view inactivelog <audit log file name>**
- **file get inactivelog <audit log file name>**
- **file delete inactivelog <audit log file name>**
- **file dump inactivelog <audit log file name>**
- **file tail inactivelog <audit log file name>**
- **file search inactivelog <audit log file name><search string>**
- **utils auditd enable**
- **utils auditd disable**
- **utils auditd status**

Where, **<audit log file name>** can be one of the following audit log files:

- `/var/log/active/audit/AuditApp`
- `/var/log/active/audit/vos`
- `/var/log/inactive/audit/AuditApp`
- `/var/log/inactive/audit/vos`

Note In a non-EnhancedSecurityMode, the group ownership is ccmsyslog when the permission is 640. However, as part of EnhancedSecurityMode requirement, the file permission is modified to 600 with file group ownership by root. Hence, by default, the files saved at the `/var/log/active/syslog` location are changed to the permission of 600 with the ownership to root.