Release Notes for Cisco Prime Collaboration Deployment, Release 11.5(3)

First Published: August 24, 2016

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Introduction** 1

About Cisco Prime Collaboration Deployment 1

Related Documentation 2

Obtaining Documentation and Submitting a Service Request 2

CHAPTER 2 **New and Changed Information** 3

FIPS 140-2 Compliance 3

EnhancedSecurityMode Support 3

Credential Policy for EnhancedSecurityMode 4

Re-encryption through AES 4

CLI Commands for FIPS Mode 4

Enable FIPS Mode 5

Disable FIPS Mode 5

EnhancedSecurityMode Requirements for Audit Cisco Prime Collaboration Deployment 6

Audit Framework and Audit Activities 6

User Interface Updates for Audit Framework 7

Audit Log Configuration 7

Configure Audit Logs 7

Audit Log Configuration Fields 8

Email Notification 10

Customized Logon Message 11

Configure Customized Logon Message 11

Customized Logon Message Configuration Fields 11

Limited Number of Sign-in Sessions 12

EnhancedSecurityMode Requirements for Platform Cisco Prime Collaboration Deployment 12

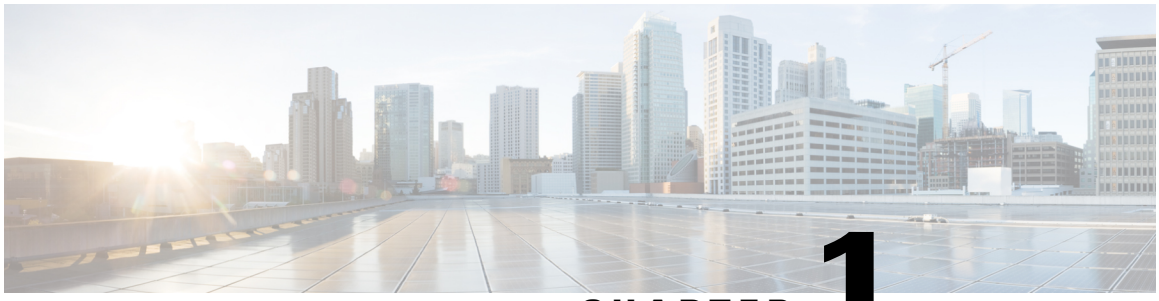
CLI Commands for EnhancedSecurityMode 13

Configure EnhancedSecurityMode 13

User Account and Sign-in Attempts on CLI and Interface 14

Configure Remote Audit Logging for Platform Logs 15
Configure Logstash Server Information 15
Configure the FileBeat Client 15
Platform CLI Commands for Security in EnhancedSecurityMode 16

CHAPTER 3 Caveats 19
Bug Search Tool 19
Resolved Caveats 20



CHAPTER 1

Introduction

- About Cisco Prime Collaboration Deployment, page 1
- Related Documentation, page 2
- Obtaining Documentation and Submitting a Service Request, page 2

About Cisco Prime Collaboration Deployment

These release notes describe new features, requirements, restrictions, and caveats for Cisco Prime Collaboration Deployment. These release notes are updated for every maintenance release.

Cisco Prime Collaboration Deployment is an application designed to assist in the management of Unified Communications applications. It allows the user to perform tasks such as migration of older software versions of clusters to new virtual machines, fresh installs, and upgrades on existing clusters.

Cisco Prime Collaboration Deployment has four primary, high-level functions:

- Migrate an existing cluster of Unified Communications servers to a new version of software (this may be MCS 7800 to virtual or virtual to virtual)
- Perform operations on existing clusters (8.6.1 or higher). Examples of these operations include:
  - Upgrade the cluster to a new version of software
  - Switch version
  - Restart the cluster
- Changing IP addresses or hostnames in the cluster on existing Release 10.x or higher clusters
- Fresh install a new Release 10.x or 11.x Unified Communications cluster

Note Cisco Prime Collaboration Deployment does not support internationalization or languages other than English.

Related Documentation

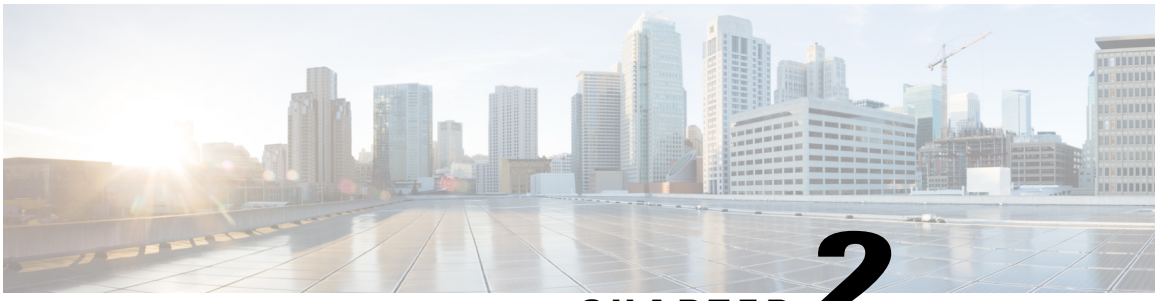
You can view documentation that is associated with supported applications.

Application	Documentation Link
Cisco Unified Communications Manager	http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html
Cisco Unified Contact Center Express	http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/tsd-products-support-series-home.html
Cisco Unity Connection	http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/tsd-products-support-series-home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.



CHAPTER 2

New and Changed Information

- FIPS 140-2 Compliance, page 3
- EnhancedSecurityMode Requirements for Audit Cisco Prime Collaboration Deployment, page 6
- EnhancedSecurityMode Requirements for Platform Cisco Prime Collaboration Deployment, page 12

FIPS 140-2 Compliance

FIPS, or Federal Information Processing Standard, is a U.S. and Canadian government certification standard that defines requirements that cryptographic modules must follow. A cryptographic module is a set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

Certain versions of Unified Communications Manager are FIPS 140-2 compliant, in accordance with the U.S. National Institute of Standards (NIST), and can operate in FIPS mode, level 1 compliance. Cisco Prime Collaboration Deployment meets FIPS 140-2 requirements by using Cisco-verified libraries.

For information about which releases are FIPS-compliant and to view their certifications, see http://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html.

For details on EnhancedSecurityMode, see EnhancedSecurityMode Support, on page 3.

Note Elliptic Curve Digital Signature Algorithm (ECDSA) ciphers are not supported in Cisco Prime Collaboration Deployment. Hence, during TLS connection, the server does not negotiate the ECDSA certificates even though the **show cert list own** CLI command may show the ECDSA self-signed certificate.

EnhancedSecurityMode Support

Once you enable the EnhancedSecurityMode, the following system enhancements are enabled by default:

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

Enabling the EnhancedSecurityMode does not enable these features by default and you have to configure them separately.

- Remote audit logging—All audit logs and event syslogs should be saved both locally and to a remote syslog server.
- System logging—All system events such as CLI logins and incorrect password attempts must be logged and saved.

Credential Policy for EnhancedSecurityMode

Once the EnhancedSecurityMode is enabled, a stricter credential policy for password changes is implemented automatically for Cisco Prime Collaboration Deployment. This mode uses the following default requirements for password changes:

- Password length should be between 14 to 127 characters.
- Password should have at least 1 lowercase, 1 uppercase, 1 digit and 1 special character.
- Any of the previous 24 passwords cannot be reused.
- Minimum age of the password is 1 day and Maximum age of the password is 60 days.
- Any newly generated password's character sequence should differ by at least 4 characters from the old password's character sequence.

Once this mode is enabled, the system enforces a stricter credential policy for all password changes automatically.

Re-encryption through AES

The encryption and decryption of application passwords is done in the `platformConfig.xml` file. During installation, the application password is re-encrypted through the Advanced Encryption Standard (AES) algorithm and is saved in the `platformConfig.xml` file.

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 5 procedure.
- **utils fips disable—**Disable FIPS mode. For details, see the Disable FIPS Mode, on page 5 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.

EnhancedSecurityMode Requirements for Audit Cisco Prime Collaboration Deployment

As part of EnhancedSecurityMode requirement, audit framework is introduced in Cisco Prime Collaboration Deployment. The audit framework includes audit activities, which are both in local server and remote server. The login sessions are limited for each user based on the CLI command configuration in the EnhancedSecurityMode.

Note By default, auditing is not enabled in Cisco Prime Collaboration Deployment. If you wish to have audit logs, you can enable auditing with or without being in FIPS mode or EnhancedSecurityMode.

For details on audit framework and audit activities, see Audit Framework and Audit Activities, on page 6.

Audit Framework and Audit Activities

As part of audit framework, you can configure logging audit details from the Cisco Prime Collaboration Deployment application.

You can configure these details from the following options:

- **Logout** button
- **Email Notification** window
- **NAT Settings** window
- **Disk Space Configuration** window
- **Audit Log Configuration** window
- **Customized Logon Message** window

If you configure audit logs for any of the above options, the updates made in the field values trigger an audit log into the local server or remote syslog server. Examples of audit log activities include enabling log rotation, configuring maximum number of files and file size, and configuring addition and modification of log files.

User Interface Updates for Audit Framework

Following new menu options have been added in the **Administration** menu of Cisco Prime Collaboration Deployment:

- Audit Log Configuration, on page 7
- Customized Logon Message, on page 11

Audit Log Configuration

Use this feature to configure audit logs through Cisco Prime Collaboration Deployment interface for local and remote syslog servers. The audit logs are sent to the syslog server in the TCP mode. You can configure audit logs through the **Audit Log Configuration** window and perform the following tasks:

- Configure application audit event levels
- Configure remote Syslog server name or IP address
- Enable or disable audit logs
- Enable or disable log rotation
- Configure maximum number of files
- Configure file size
- Configure warning threshold level for log rotation

For details on how to configure audit logs, see the Configure Audit Logs, on page 7 procedure.

Configure Audit Logs

Use this procedure to configure audit logs for local and remote syslog server through the Cisco Prime Collaboration Deployment application.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Administration** > **Audit Log Configuration**.

Step 2 Choose one of the options from the **Application Audit Event Level** drop down list to configure an audit level.

Step 3 Enter the name of remote syslog server or the IP address for the **Remote Syslog Server Name / IP** field so that the audit logs are logged into this remote server.

Step 4 (Optional) Check or uncheck the **Enable Local Audit Log** check box to enable or disable the local audit log.

- When you check this field, the audit events are logged in the local server. When you uncheck this field, audit events are not logged in the local server.
- When you check this field, the **Enable Log Rotation** field becomes active.

Step 5 (Optional) Check or uncheck the **Enable Log Rotation** check box to enable or disable the log rotation.
Note You can configure this field if **Enable Local Audit Log** is enabled.

When you check this field, you can configure the **Maximum No of Files**, **Maximum File Size(MB)**, and **Warning Threshold for Approaching Log Rotation Overwrite(%)** fields. When you uncheck the **Enable Local Audit Log** field, the default values of these fields are not applicable as they are inactive.

Step 6 Enter an integer value for the **Maximum No of Files** field to configure the maximum number of files that can be created on the server.

Step 7 Enter a value for the **Maximum File Size (MB)** field to configure the maximum file size of each log that is created on the server.

Step 8 Enter the warning threshold value for the **Warning Threshold for Approaching Log Rotation Overwrite(%)** field.

Step 9 Click **Save**.

Step 10 (Optional) Click **Reset**.
The page is reset with the default values.

Related Topics

Audit Log Configuration Fields, on page 8

Audit Log Configuration Fields

Setting	Description
Audit Level Settings section	

Setting	Description
Application Audit Event Level	From the drop-down list, choose one of the following options: • **Info—**To view the audit event level as an information message. • **Warning—**To view the audit event level as a warning message. • **Debug—**To view the audit event level as a debug message. • **Error—**To view the audit event level as an error message.
Remote SysLog Settings section	
Remote Syslog Server Name / IP	Enter the name of remote syslog server or the IP address for the audit logs to be logged in to this remote server.
Local Audit Log Settings	
Enable Local Audit Log	Check or uncheck this check box to enable or disable the local audit log. **Note** • When you check this field, the audit events are logged in the local server. When you uncheck this field, audit events are not logged in the local server. • When you check this field, the **Enable Log Rotation** field becomes active.
Enable Log Rotation	Check or uncheck this check box to enable or disable the log rotation. **Note** • You can configure this field if the **Enable Local Audit Log** field is enabled. • After you enable this field, you can configure the **Maximum No of Files**, **Maximum File Size(MB)**, and **Warning Threshold for Approaching Log Rotation Overwrite(%)** fields. When you uncheck the **Enable Local Audit Log** field, the default values of these fields are not applicable as they are not active.

Setting	Description
Maximum No of Files	Enter an integer value for the **Maximum No of Files** field to configure the maximum number of files that can be created on the server. After you check the **Enable Log Rotation** field, you can configure the value for **Maximum No of Files** field. Once the number of files reaches the configured value, the log rotation process starts. In the log rotation process, all the log files are deleted and rewritten from the log file number 1. **Note** The value for this field must be in the range of 1 to 5000.
Maximum File Size(MB)	Enter a value for the **Maximum File Size (MB)** field to configure the maximum file size of each log that is created on the server. **Note** The value for this field must be in the range of 1 to 10.
Warning Threshold for Approaching Log Rotation Overwrite(%)	Enter the warning threshold value for the **Warning Threshold for Approaching Log Rotation Overwrite(%)** field. After the configured warning threshold value is reached, an email notification is sent to users to take back up of the audit log files. These files are deleted or overwritten during log rotation. **Note** The value for this field must be in the range of 1 to 100. For details, see the Email notification topic in the *Cisco Prime Collaboration Deployment Administration Guide*.
Save	Click this button to save the changes you have made on this page.
Reset	Click this button to set the default values on this page.

Email Notification

This topic from the *Cisco Prime Collaboration Deployment Administration Guide* is updated with the following information:

You can choose to send an email notification to a user after the value that is configured in the **Warning Threshold for Approaching Log Rotation Overwrite(%)** field from the **Audit Log Configuration** window is reached. The email notification informs the user to take back up of the audit log files because they will be deleted or overwritten.

Customized Logon Message

Use this feature to display the alerts or warning messages while signing in to the Cisco Prime Collaboration Deployment application. You can configure the alerts or warning messages through the **Customized Logon Message** window and perform the following tasks:

- Upload a file with customized login message
- Enable user acknowledgment

For details on how to configure audit logs, see the Configure Customized Logon Message, on page 11 procedure.

Configure Customized Logon Message

Use this procedure to configure customized logon messages when a user signs into the Cisco Prime Collaboration Deployment application.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Administration** > **Customized Logon Message**.

Step 2 For the **Upload File** field, browse to the location of file that includes the customized logon message.

Step 3 (Optional) Check or uncheck the **Require User Acknowledgement** check box to enable or disable user acknowledgment for the file that the user receives.
If this field is enabled, users get an acknowledgment as an alert message on the Cisco Prime Collaboration Deployment sign-in page after they sign out for the first time from the same web browser instance.

Step 4 Click **Upload File**.
The file with the customized logon message is uploaded and a pop-up appears showing the file upload status.

Step 5 (Optional) Click **Delete**.
The file with the customized logon message is deleted and a pop-up appears showing the file deletion status.

Related Topics

Customized Logon Message Configuration Fields, on page 11

Customized Logon Message Configuration Fields

Setting	Description
Upload Customized Logon File	
Upload File	Click the **Browse** button to browse to the location of file that includes the customized sign-on message.

Setting	Description
Require User Acknowledgment	Check or uncheck this check box to enable or disable user acknowledgment for the file that the user receives. If this field is enabled, users get an acknowledgment as an alert message on the Cisco Prime Collaboration Deployment sign-in page. This message appears after they sign out for the first time from the same web browser instance.
Upload File	Click this button to upload the file with the customized sign-on message to the server. After you upload the file, a popup appears showing the file upload status.
Delete	Click this button to delete the file with the customized sign-on message. After you delete the file, popup appears showing the file deletion status.

Limited Number of Sign-in Sessions

An administrator can configure the sign-in session limit for each user. A user can sign in to the Cisco Prime Collaboration Deployment application through multiple windows and web browsers up to the configured number of sign-in sessions. If a user exceeds the limit of configured the number of sign-in sessions, an error message appears on the sign-in page and the user is not allowed to sign in.

An administrator can configure the limit of sign-in sessions through the following CLI command:

set session maxlimit <value>

Where the default value is 10 and maximum value is 100.

Note When users exceed the limit of configured number of sign-in sessions, they must sign out from the application in that session and sign in to another session. In case the session closes due to abrupt exit from web browser, users need to restart the Tomcat server on Cisco Prime Collaboration Deployment to allow sign-in to the new session.

EnhancedSecurityMode Requirements for Platform Cisco Prime Collaboration Deployment

You can use the command line interface (CLI) to enable the EnhancedSecurityMode in Cisco Prime Collaboration Deployment. To enable this mode, create a status file and run the scripts for applications. The applications read the status file and respond accordingly when the system is restarted.

For Cisco Prime Collaboration Deployment to work in EnhancedSecurityMode, following requirements are met:

- Sign in banner appears prior to interface sign-in prompt
- The Department of Defense (DoD) sign-in banner appears prior to console sign-in prompts
- File Transfer Protocol Secure (FTPS) or File Transfer Protocol (FTP) service and SSH are configured with the DoD sign-in banner
- The banner appears on the screen until a user signs on for further access
- Audit tools are secured from unauthorized modification
- Audit records are used through reports
- New password is verified, as per EnhancedSecurityMode credential policy, when a user changes password

Note For credential policy for EnhancedSecurityMode, see Credential Policy for EnhancedSecurityMode, on page 4.

CLI Commands for EnhancedSecurityMode

Use the following CLI commands for EnhancedSecurityMode:

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

For details, see the Configure EnhancedSecurityMode, on page 13 procedure.

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 EnhancedSecurityMode is enabled.

Step 3 To configure EnhancedSecurityMode, 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.

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 15.

Step 2 Enable the FileBeat client for remote audit logging. For procedure, see Configure the FileBeat Client, on page 15.

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 the 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:

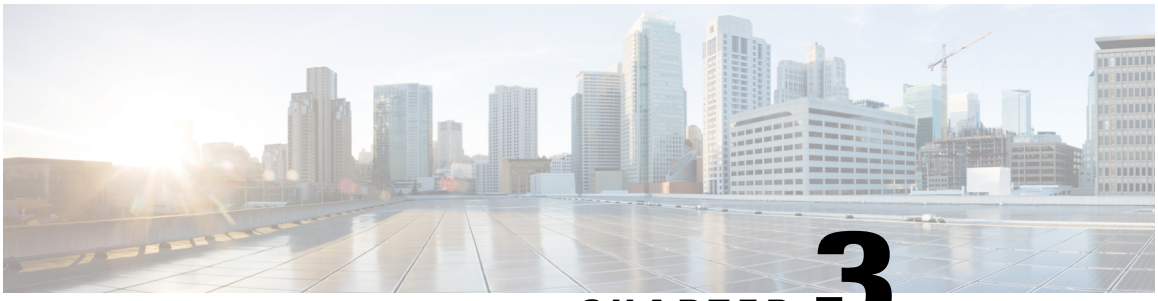
- **file view activelog**<audit log file name>
- **file get activelog** <audit log file name>
- **file delete activelog**<audit log file name>
- **file dump activelog**<audit log file name>
- **file tail activelog** <audit log file name>
- **file search activelog**<audit log file name><search string>
- **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.



CHAPTER 3

Caveats

- Bug Search Tool, page 19
- Resolved Caveats, page 20

Bug Search Tool

The system grades known problems (bugs) according to severity level. These release notes contain descriptions of the following bug levels:

- All severity level 1 or 2 bugs
- Significant severity level 3 bugs
- All customer-found bugs

You can search for open and resolved caveats of any severity for any release using the Cisco Bug Search tool, an online tool available for customers to query defects according to their own needs.

To access the Cisco Bug Search tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Follow these steps to use Cisco Bug Search tool:

1. Access the Cisco Bug Search tool: https://tools.cisco.com/bugsearch/.
2. Log in with your Cisco.com user ID and password.
3. If you are looking for information about a specific problem, enter the bug ID number in the **Search for:** field, and click **Go**.

Tip Click **Help** on the Bug Search page for information about how to search for bugs, create saved searches, and create bug groups.

Resolved Caveats

You can find the latest resolved caveat information for Cisco Prime Collaboration Deployment by using the Bug Search tool, an online tool available for customers to query defects according to their own needs.

Tip You need an account with Cisco.com to use the Bug Search tool to find open and resolved caveats of any severity for any release.

See https://tools.cisco.com/bugsearch/.