Enhanced Security Mode in Cisco Unity Connection

Enhanced Security Mode in Cisco Unity Connection

Overview

When Unity Connection is enabled to operate in EnhancedSecurityMode, the system implements a set of strict security and risk management controls that secure the system deployment.

The EnhancedSecurityMode includes the following features:

- **Stringent Password Requirements:** A strict credential policy is implemented for new user passwords and for existing passwords when they are modified. See the Credential Policy, on page 2section.
- **Remote Audit Logging:** All audit logs and event syslogs are saved locally as well as to a remote syslog server.

  See the Remote Audit Logging, on page 2section.
- **System logging:** All system events, such as CLI logins and incorrect password attempts are logged and saved.
- **Limit log-on:** The maximum number of concurrent sessions for an interface can be configured. Any new session beyond the configured maximum limit gets disconnected. In EnhancedSecurityMode, the default value of Maximum Concurrent Sessions for **Telephony Interface (Per User)** is 2 and of **Maximum Concurrent Sessions for IMAP Interface (Per User)** is 5. For more information, see Passwords, PINs, and Authentication Rule Management chapter.
- **Disable Inactive Users:** The number of days for user inactivity timeout can be configured. If a user does not login to the voicemail account for the configured numbers of days, the account is disabled and further access is denied.

  In EnhancedSecurityMode , the default value of **User Inactivity Timeout (in Days)** is 90. For more information, see Passwords, PINs, and Authentication Rule Management

Role Based Access

In EnhancedSecurityMode , a new privilege "Super Custom Administrator" is added to the privilege list on the Custom Roles page. With the help of the "Super Custom Administrator" privilege, a system administrator can create two levels of administrator hierarchies in the system.

Credential Policy

Once the EnhancedSecurityMode is enabled, a stringent credential policy for new passwords and password changes can be implemented for platform administrator. This policy enforces the following default requirements for passwords:

- Credential Length should be between 14 to 127 characters.
- Password should contain at least 1 lowercase, 1 uppercase, 1 digit and 1 special character.
- Stored Number of Previous Credentials are 24, any of the previous 24 passwords cannot be reused.
- Credential Expires After minimum limit of 1 day and maximum limit is 60 days.
- Minimum Number of Character Changes between Successive Credentials must be at least 4.

After enabling the EnhancedSecurityMode , the administrator can use the Authentication Rules to modify any of the password requirements to enforce stringent password policy for all password changes. For information on credential policies, see the "Passwords, PINs, and Authentication Rule Management " chapter.

Remote Audit Logging

To comply with the security requirements, you must configure remote audit logging in Unity Connection.

In EnhancedSecurityMode , the system uses TCP as the default protocol to send audit events and alarms to the remote syslog server. Unlike UDP, which is used while the system is in normal operating mode, TCP contains mechanisms to guarantee delivery of all packets. However, if you prefer, you can reconfigure the system to use UDP while in this mode.

If a transfer failure occurs, the TCPRemoteSyslogDeliveryFailed alarm and alert are triggered to notify administrator about the TCP transfer failure. A throttling mechanism ensures that not more than one alarm and one alert are sent per hour. This ensures that administrator is not flooded with identical alarms and alerts. Administrator can use the local audit logs as a backup while communications are reestablished.

Prerequisites for Enhanced Security Mode

- FIPS 140-2 Mode Setup: FIPS mode must be enabled before you enable the Enhanced Security Mode . If FIPS mode is not already enabled, you will be prompted to enable FIPS mode when you attempt to enable EnhancedSecurityMode .
- Set up a remote syslog server and configure IPSec between Unity Connection and the remote server, including the gateways in between.
- Set up smart host and configure IPSec between Unity Connection and exchange where exchange acts as a smart host, including the gateways in between. For information on setting up IPsec configuration, see the "IPSEC Management" section in the "Security" chapter of the *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 15*at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/os_administration/guide/b_15cucosagx.html.

- Before enabling the Enhanced Security Mode on the Unity Connection server, ensure that the security password length is minimum of 14 characters. In case of upgrading Unity Connection, password needs to be updated if the prior version was EnhancedSecurityMode enabled.

Configuration Task Flow in EnhancedSecurityMode

Step 1 Enable the EnhancedSecurityMode in Unity Connection. See the Configuring the EnhancedSecurityMode, on page 3 section.

Step 2 Confirm that the system credential policy meets the security guidelines. See the Configuring Credential Policy, on page 3section.

Step 3 Configure Audit Framework for the mode.

Set up the audit logging framework for Unity Connection, which includes setting up remote syslog servers for all audit logs and alarms. See the Configuring Audit Framework, on page 4section.

Configuring the EnhancedSecurityMode

Use the following procedure to enable or disable the **EnhancedSecurityMode**. However, FIPS mode must be enabled before enabling the **EnhancedSecurityMode**.

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils EnhancedSecurityModestatus** command to confirm whether the status of the mode status is set to enabled or disabled.

Step 3 Run the following command to enable the **EnhancedSecurityMode** if the mode is disabled:

```
utils EnhancedSecurityMode enable
```

Similarly, you can run the **utils EnhancedSecurityMode disable** command to disable the mode.

Step 4 Repeat this procedure for all nodes of Cisco Unity Connection.

Configuring Credential Policy

Use the following procedure to update the system credential policies.

Step 1 Log in to Cisco Unity Connection Administration.

Step 2 Select **Authentication Rules** > **Edit Authentication Rule**.

Step 3 Update the authentication rules as per your requirement.

Step 4 Click **Save**.

For information on credential policies, see the "Passwords, PINs, and Authentication Rule Management" chapter.

Configuring Audit Framework

Complete the following tasks to set up audit requirements for the **EnhancedSecurityMode** in Unity Connection.

Step 1 Configure Remote Audit Log.

Set up your audit log configuration for remote audit logging.

Step 2 Configure Remote Audit Log Transfer Protocol.

(Optional) When the **EnhancedSecurityMode** is enabled, by default, the system uses TCP as the transfer protocol for remote audit logs. You can use this procedure to reconfigure the system to use UDP.

Step 3 In RTMT, set up the email server for email alerts.

Step 4 Set up the email notification for the TCPRemoteSyslogDeliveryFailed alert.

Configuring Remote Audit Logs

Before configuring remote audit logs for a Unity Connection system running in EnhancedSecurityMode, make sure that:

- You must have already set up your remote syslog server.
- You must also have configured IPSec between each cluster node and the remote syslog server, including the gateways in between.

  For information on setting up IPsec configuration, see the "IPSEC Management" section in the "Security" chapter of the *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 15*at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/os_administration/guide/b_15cucosagx.html .

Step 1 In Cisco Unified Serviceability, select**Tools** > **Audit Log Configuration**.

Step 2 From the Server drop-down menu select any server in the cluster except the publisher node and click **Go**.

Step 3 Check the **Apply to All Nodes** check box.

Step 4 In the **Server Name** field, enter the IP Address or fully qualified domain name of the remote syslog server.

Step 5 Complete the remaining fields in the Audit Log Configuration window. For help with the fields and their descriptions, see the online help.

Step 6 Click **Save**.

Configuring Remote Audit Log Transfer Protocol

Use the following procedure to configure the transfer protocol for remote audit logs. In the **EnhancedSecurityMode**, the default setting is TCP.

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils remotesyslog show protocol** command to confirm the protocol that is configured.

Step 3 If you need to change the protocol, do the following:

To configure TCP, run the **utils remotesyslog set protocol tcp** command.

To configure UDP, run the **utils remotesyslog set protocol udp** command.

Step 4 Restart the node.

Step 5 Repeat this procedure for all Unity Connection cluster nodes.

Configuring Email Server for Alert Notifications

Use the following procedure to set up your email server for alert notifications.

Step 1 In the Real-Time Monitoring Tool's System window, click **Alert Central**.

Step 2 Choose **System** > **Tools** > **Alert** > **Config Email Server**.

Step 3 In the **Mail Server Configuration** popup, enter the details for the mail server.

Step 4 Click **OK**.

Enabling Email Alerts

Use the following procedure to set up an email alert for the TCPRemoteSyslogDeliveryFailed alarm.

Step 1 In the Real-Time Monitoring Tool System area, click **Alert Central**.

Step 2 In the Alert Central window, select **TCPRemoteSyslogDeliveryFailed**.

Step 3 Select **System** > **Tools** > **Alert** > **Config Alert Action**.

Step 4 In the Alert Action popup, select **Default** and click **Edit**.

Step 5 In the Alert Action popup, **Add a recipient**.

Step 6 In the popup window, enter the address where you want to send email alerts and click **OK**.

Step 7 In the Alert Action popup, make sure that the address appears under **Recipients** and that the **Enable** check box is checked.

Step 8 Click **OK**.