



Advanced Configuration

Last Updated: October 28, 2009

This chapter describes advanced configuration procedures for modifying application parameters after the initial installation and configuration process described in the section “[Configuring System Components](#)” on page 49. That earlier chapter includes commands not described in this chapter.

The advanced configuration procedures include:

- [Configuring the Hostname, page 357](#)
- [Configuring the DNS Server, page 359](#)
- [Configuring NTP Servers, page 360](#)
- [Configuring a Syslog Server, page 364](#)
- [Configuring the Clock Time Zone, page 365](#)
- [Configuring Password and PIN Parameters, page 368](#)
- [Cisco Unified CME Password Synchronization in “Configuring Password and PIN Parameters” on page 368](#)
- [PINless Voicemail in “Configuring Password and PIN Parameters” on page 368 and in “Displaying Password and PIN System Settings” on page 378.](#)

Configuring the Hostname

During the software postinstallation process, the hostname was configured. Use this procedure to change the hostname.

SUMMARY STEPS

1. **config t**
2. **hostname** *hostname*
3. **exit**
4. **show hosts**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>config t</code> Example: se-10-0-0-0# <code>config t</code>	Enters configuration mode.
Step 2	<code>hostname hostname</code> Example: se-10-0-0-0(config)# <code>hostname mainhost</code> mainhost(config)#	Specifies the hostname that identifies the local Cisco Unity Express system. Do not include the domain name as part of the hostname. The Cisco Unity Express prompt changes to reflect the hostname. If you do not enter a hostname, the prompt is formed using “se” and the IP address of the Cisco Unity Express network module.
Step 3	<code>exit</code> Example: mainhost(config)# <code>exit</code>	Exits configuration mode.
Step 4	<code>show hosts</code> Example: mainhost# <code>show hosts</code>	Displays the local hostname and DNS servers configured on the system.
Step 5	<code>copy running-config startup-config</code> Example: mainhost# <code>copy running-config startup-config</code>	Copies the configuration changes to the startup configuration.

Examples

The following commands configure the hostname:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# hostname mainhost
ca-west(config)# exit
ca-west#
```

The output from the **show hosts** command might look similar to the following:

```
ca-west# show hosts

Hostname:      mainhost
Domain:        myoffice
DNS Server1:   10.100.10.130
DNS Server2:   10.5.0.0
ca-west#
```

Configuring the DNS Server

During the software postinstallation process, the DNS server and IP addresses may have been configured. Use this procedure to change the server name and IP addresses.

SUMMARY STEPS

1. **config t**
2. **ip domain-name** *dns-server-name*
3. **ip name-server** *ip-address* [*ip-address*] [*ip-address*] [*ip-address*]
4. **exit**
5. **show hosts**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: se-10-0-0-0# config t	Enters configuration mode.
Step 2	ip domain-name <i>dns-server-name</i> Example: se-10-0-0-0(config)# ip domain-name mycompany.com	Specifies the domain name of the DNS server.
Step 3	ip name-server <i>ip-address</i> [<i>ip-address</i>] [<i>ip-address</i>] [<i>ip-address</i>] Example: se-10-0-0-0(config)# ip name-server 192.168.0.5 se-10-0-0-0(config)# ip name-server 192.168.0.5 192.168.0.10 192.168.0.12 192.168.0.20	Specifies up to four IP addresses for the DNS server.
Step 4	exit Example: se-10-0-0-0(config)# exit	Exits configuration mode.
Step 5	show hosts Example: se-10-0-0-0# show hosts	Displays the IP route destinations, gates, and masks.
Step 6	copy running-config startup-config Example: se-10-0-0-0# copy running-config startup-config	Copies the configuration changes to the startup configuration.

Examples

The following commands configure the DNS server:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# ip domain-name mycompany
se-10-0-0-0(config)# ip name-server 10.100.10.130 10.5.0.0
se-10-0-0-0(config)# exit
se-10-0-0-0#
```

The output from the **show hosts** command might look similar to the following:

```
se-10-0-0-0# show hosts

Hostname:      se-10-100-6-10
Domain:       mycompany
DNS Server1:  10.100.10.130
se-10-0-0-0#
```

Configuring NTP Servers

During the software postinstallation process, the Network Time Protocol (NTP) server may have been configured. Cisco Unity Express accepts a maximum of three NTP servers. Use this procedure to add or delete NTP servers.

Adding NTP Servers

You can designate an NTP server using its IP address or its hostname.

Cisco Unity Express uses the DNS server to resolve the hostname to an IP address and stores the IP address as an NTP server. If DNS resolves the hostname to more than one IP address, Cisco Unity Express randomly chooses one of the IP addresses that is not already designated as an NTP server.

To configure an NTP server with multiple IP addresses for a hostname, repeat the configuration steps using the same hostname. Each iteration assigns the NTP server to its remaining IP addresses.

SUMMARY STEPS

1. **config t**
2. **ntp server {hostname | ip-address} [prefer]**
3. **exit**
4. **show ntp status**
5. **show ntp configuration**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>config t</code> Example: se-10-0-0-0# <code>config t</code>	Enters configuration mode.
Step 2	<code>ntp server {hostname ip-address} [prefer]</code> Example: se-10-0-0-0(config)# <code>ntp server 10.0.3.4</code> se-10-0-0-0(config)# <code>ntp server 10.0.10.20 prefer</code>	Specifies the name or IP address of the NTP server. If more than one server is configured, the server with the prefer attribute is used first.
Step 3	<code>exit</code> Example: se-10-0-0-0(config)# <code>exit</code>	Exits configuration mode.
Step 4	<code>show ntp status</code> Example: se-10-0-0-0# <code>show ntp status</code>	Displays the NTP subsystem status.
Step 5	<code>show ntp configuration</code> Example: se-10-0-0-0# <code>show ntp configuration</code>	Displays the configured NTP servers.
Step 6	<code>copy running-config startup-config</code> Example: se-10-0-0-0# <code>copy running-config startup-config</code>	Copies the configuration changes to the startup configuration.

Examples

The following commands configure the NTP server:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# ntp server 10.100.6.9
se-10-0-0-0(config)# exit
se-10-0-0-0#
```

The output from the `show ntp status` command might look similar to the following:

```
se-10-0-0-0# show ntp status

NTP reference server 1:      10.100.6.9
Status:                     sys.peer
Time difference (secs):     3.268110099434328E8
Time jitter (secs):         0.1719226837158203
se-10-0-0-0#
```

The following example configures an NTP server with a hostname that points to two IP addresses 172.16.10.1 and 172.16.10.2:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# ntp server NTP.mine.com
se-10-0-0-0(config)# exit
se-10-0-0-0#
```

```
se-10-0-0-0# config t
se-10-0-0-0(config)# ntp server NTP.mine.com
se-10-0-0-0(config)# exit
se-10-0-0-0#
```

The output from the **show ntp status** command might look similar to the following:

```
se-10-0-0-0# show ntp status

NTP reference server 1:      172.16.10.1
Status:                      sys.peer
Time difference (secs):     3.268110099434328E8
Time jitter (secs):         0.1719226837158203

NTP reference server 1:      172.16.10.2
Status:                      sys.peer
Time difference (secs):     3.268110099434328E8
Time jitter (secs):         0.1719226837158203
se-10-0-0-0#
```

Removing an NTP Server

Remove an NTP server using its IP address or hostname.

SUMMARY STEPS

1. **config t**
2. **no ntp server** {hostname | ip-address}
3. **exit**
4. **show ntp status**
5. **show ntp configuration**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: se-10-0-0-0# config t	Enters configuration mode.
Step 2	no ntp server {hostname ip-address} Example: se-10-0-0-0(config)# no ntp server 10.0.3.4 se-10-0-0-0(config)# no ntp server myhost	Specifies the hostname or IP address of the NTP server to remove.

	Command or Action	Purpose
Step 3	exit Example: se-10-0-0-0(config)# exit	Exits configuration mode.
Step 4	show ntp status Example: se-10-0-0-0# show ntp status	Displays the NTP subsystem status.
Step 5	show ntp configuration Example: se-10-0-0-0# show ntp configuration	Displays the configured NTP servers.
Step 6	copy running-config startup-config Example: se-10-0-0-0# copy running-config startup-config	Copies the configuration changes to the startup configuration.

Displaying NTP Server Information

The following commands are available to display NTP server configuration information and status:

- **show ntp associations**
- **show ntp servers**
- **show ntp source**
- **show ntp status**

The following is sample output for the **show ntp associations** command:

```
se-10-0-0-0# show ntp associations

ind assID status  conf reach auth condition  last_event cnt
=====
  1 61253 8000   yes  yes  none    reject
```

The following is sample output for the **show ntp servers** command:

```
se-10-0-0-0# show ntp servers

      remote          refid      st t when poll reach  delay  offset jitter
=====
 10.100.6.9          0.0.0.0    16 u   - 1024   0    0.000   0.000 4000.00
space reject,      x falsetick,      . excess,          - outlyer
+ candidate,      # selected,      * sys.peer,        o pps.peer
```

The following is sample output for the **show ntp source** command:

```
se-10-0-0-0# show ntp source

192.168.0.1: stratum 16, offset 0.000013, synch distance 8.67201
0.0.0.0:      *Not Synchronized*
```

The following is sample output for the **show ntp status** command:

```
se-10-0-0-0# show ntp status

NTP reference server :      10.100.6.9
Status:                   reject
Time difference (secs):    0.0
Time jitter (secs):       4.0
```

Configuring a Syslog Server

Cisco Unity Express captures messages that describe activities in the system. These messages are collected and directed to a messages.log file on the Cisco Unity Express module hard disk, the console, or an external system log (syslog) server. The messages.log file is the default destination.

This section describes the procedure for configuring an external server to collect the messages. To view the messages, see [“Viewing System Activity Messages” on page 392](#).

Required Data for This Procedure

You need the hostname or IP address of the designated log server.

SUMMARY STEPS

1. **config t**
2. **log server address** {hostname | ip-address}
3. **exit**
4. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: se-10-0-0-0# config t	Enters configuration mode.
Step 2	log server address {hostname ip-address} Example: se-10-0-0-0(config)# log server address 10.187.240.31 se-10-0-0-0(config)# log server address logpc	Specifies the hostname or IP address of the NTP server designated as the log server.

	Command or Action	Purpose
Step 3	exit Example: se-10-0-0-0(config)# exit	Exits configuration mode.
Step 4	show running-config Example: se-10-0-0-0# show running-config	Displays the system configuration, which includes the configured log server.

Examples

The output from the **show running-config** command might look similar to the following:

```
se-10-0-0-0# show running-config

clock timezone America/Los_Angeles

hostname se-10-0-0-0

ip domain-name localdomain

ntp server 10.100.60.1
.
.
log server address 10.100.10.210

voicemail default mailboxsize 3000
voicemail capacity time 6000

end
```

Configuring the Clock Time Zone

During the software postinstallation process, the time zone of the local Cisco Unity Express module was configured. Use this procedure to change the module's time zone.

Cisco Unity Express automatically updates the clock for daylight savings time on the basis of the selected time zone.

SUMMARY STEPS

1. **config t**
2. **clock timezone** *timezone*
3. **exit**
4. **show clock detail**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>config t</code> Example: <code>se-10-0-0-0# config t</code>	Enters configuration mode.
Step 2	<code>clock timezone <i>timezone</i></code> Example: <code>se-10-0-0-0(config)# clock timezone America/Los_Angeles</code>	Specifies the local time zone. To enter a value for the <i>timezone</i> argument, you must know the phrase that represents your time zone. If you do not know the phrase, press <Enter>. A series of menus will appear to help you choose the time zone.
Step 3	<code>exit</code> Example: <code>se-10-0-0-0(config)# exit</code>	Exits configuration mode.
Step 4	<code>show clock detail</code> Example: <code>se-10-0-0-0# show clock detail</code>	Displays the time zone, clocking resolution, and current clock time.
Step 5	<code>copy running-config startup-config</code> Example: <code>se-10-0-0-0# copy running-config startup-config</code>	Copies the configuration changes to the startup configuration.

Examples

The following commands configure the clock time zone:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# clock timezone
```

```
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
```

```
1) Africa           4) Arctic Ocean    7) Australia       10) Pacific Ocean
2) Americas        5) Asia            8) Europe
3) Antarctica      6) Atlantic Ocean  9) Indian Ocean
```

```
#? 2
```

```
Please select a country.
```

```
1) Anguilla          18) Ecuador        35) Paraguay
2) Antigua & Barbuda 19) El Salvador    36) Peru
3) Argentina        20) French Guiana 37) Puerto Rico
4) Aruba             21) Greenland      38) St Kitts & Nevis
5) Bahamas          22) Grenada        39) St Lucia
6) Barbados         23) Guadeloupe     40) St Pierre & Miquelon
7) Belize           24) Guatemala      41) St Vincent
8) Bolivia          25) Guyana          42) Suriname
9) Brazil           26) Haiti           43) Trinidad & Tobago
10) Canada           27) Honduras       44) Turks & Caicos Is
11) Cayman Islands  28) Jamaica         45) United States
12) Chile            29) Martinique     46) Uruguay
```

```

13) Colombia                30) Mexico                47) Venezuela
14) Costa Rica              31) Montserrat           48) Virgin Islands (UK)
15) Cuba                    32) Netherlands Antilles 49) Virgin Islands (US)
16) Dominica                33) Nicaragua
17) Dominican Republic     34) Panama

```

#? **45**

Please select one of the following time zone regions.

```

1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Standard Time - Indiana - most locations
5) Central Time
6) Central Time - Michigan - Wisconsin border
7) Mountain Time
8) Mountain Time - south Idaho & east Oregon
9) Mountain Time - Navajo
10) Mountain Standard Time - Arizona
11) Pacific Time
12) Alaska Time
13) Alaska Time - Alaska panhandle
14) Alaska Time - Alaska panhandle neck
15) Alaska Time - west Alaska
16) Aleutian Islands
17) Hawaii

```

#? **11**

The following information has been given:

```

United States
Pacific Time

```

Therefore TZ='America/Los_Angeles' will be used.

Local time is now: Tue Jul 18 02:02:19 PDT 2006.

Universal Time is now: Tue Jul 18 09:02:19 UTC 2006.

Is the above information OK?

```

1) Yes
2) No

```

#? **1**

Save the change to startup configuration and reload the module for the new timezone to take effect.

```
se-10-0-0-0(config)# end
```

```
se-10-0-0-0#
```

The output from the **show clock detail** command might look similar to the following:

```
se-10-0-0-0# show clock detail
```

```

19:20:33.724 PST Wed Feb 4 2004
time zone:                America/Pacific
clock state:              unsync
delta from reference (microsec): 0
estimated error (microsec): 175431
time resolution (microsec): 1
clock interrupt period (microsec): 10000
time of day (sec):        732424833
time of day (microsec):   760817

```

Configuring Password and PIN Parameters

Cisco Unity Express supports the configuration of the password and personal identification number (PIN) parameters described in the following sections:

- [Configuring Password and PIN Length and Expiry Time](#), page 368
- [Configuring Password and PIN Protection Lockout Modes](#), page 370
- [Using HTTPS to Protect Passwords and PINs](#), page 376
- [Configuring PIN and Password History](#), page 376
- [Encrypting PINs in Backup Files](#), page 379
- [Displaying Password and PIN System Settings](#), page 378



Note

If you change a Cisco Unified CME user's password on Cisco Unity Express with `Configure --> Users`, the password for that user *is* updated on Cisco Unified CME. However, the reverse is not true: a user password changed on Cisco Unified CME will not be updated to Cisco Unity Express.



Note

For instructions on configuring PINless voicemail, see [“Configuring PINless Mailbox Access” on page 154](#).

Configuring Password and PIN Length and Expiry Time

Cisco Unity Express supports configuring the following two attributes of password and PIN:

- Minimum password and PIN length

To support enhanced security procedures, Cisco Unity Express has made the password and PIN length configurable. The administrator can configure the length to a value greater than or equal to 3 alphanumeric characters. This is a system-wide value, so that all subscribers must have passwords and PINs of at least that many characters. Use the GUI **Defaults > User** option or the procedure described below to configure this length.

The password length does not have to equal the PIN length.

The default length is 3 alphanumeric characters. The maximum password length is 32 alphanumeric characters. The maximum PIN length is 16 alphanumeric characters.

To set the password or PIN length to the system default values, use the **no** or **default** form of the commands.



Note

If the minimum password or PIN length is increased, existing passwords and PINs that do not conform to the new limit will automatically expire. The subscriber must reset the password at the next log in to the GUI and must reset the PIN at the next log in to the TUI.

- Password and PIN expiry time

Cisco Unity Express permits the administrator to configure the password and PIN expiry time on a system-wide basis. The expiry time is the time, in days, for which the password and PIN are valid. When this time is reached, the subscriber must enter a new password or PIN.

If this option is not configured, passwords and PINs do not expire.

Use the GUI **Defaults > User** option or the procedure described below to configure this time.

The password expiry time does not have to equal the PIN expiry time.

The valid range is 3 to 365 days.

To set the password or PIN expiry time to the system default values, use the **no** or **default** form of the commands.

SUMMARY STEPS

- **config t**
- **security password length min** *password-length*
- **security pin length min** *pin-length*
- **security password expiry days** *password-days*
- **security pin expiry days** *pin-days*
- **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: se-10-0-0-0# config t se-10-0-0-0(config)#	Enters configuration mode.
Step 2	security password length min <i>password-length</i> Example: se-10-0-0-0(config)# security password length min 5	Specifies the length of all subscribers' passwords. The default minimum value is 3; the maximum value is 32. To set the minimum password length to the system default, use the no or default form of this command.
Step 3	security pin length min <i>pin-length</i> Example: se-10-0-0-0(config)# security pin length min 4	Specifies the minimum length of all subscribers' PINs. The default value is 3; the maximum value is 16. To set the minimum PIN length to the system default, use the no or default form of this command.
Step 4	security password expiry days <i>password-days</i> Example: se-10-0-0-0(config)# security password expiry days 60	Specifies the maximum number of days for which subscribers' passwords are valid. Valid values range from 3 to 365. If this value is not configured, the passwords will not expire. To set the password expiry time to the system default, use the no or default form of this command.

	Command or Action	Purpose
Step 5	<p><code>security pin expiry days pin-days</code></p> <p>Example: <pre>se-10-0-0-0(config)# security pin expiry days 45</pre></p>	<p>Specifies the maximum number of days for which subscriber's PINs are valid. Valid values range from 3 to 365.</p> <p>If this value is not configured, the PINs will not expire.</p> <p>To set the PIN expiry time to the system default, use the no or default form of this command.</p>
Step 6	<p><code>exit</code></p> <p>Example: <pre>se-10-0-0-0(config)# exit se-10-0-0-0#</pre></p>	<p>Exits configuration mode.</p>

Examples

The following example sets the password length to 6 characters, the PIN length to 5 characters, the password expiry time to 60 days, and the PIN expiry time to 45 days.

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security password length min 6
se-10-0-0-0(config)# security pin length min 5
se-10-0-0-0(config)# security password expiry days 60
se-10-0-0-0(config)# security pin expiry days 45
se-10-0-0-0(config)# exit
```

Configuring Password and PIN Protection Lockout Modes

Starting in release 3.0, you can use both temporary and permanent lockout for passwords and PINs to help prevent security breaches.

For permanent lockout mode, the user's account is permanently locked after a specified number of incorrect passwords or PINs are entered. After the account is locked, only the administrator can unlock it and reset the password.

For temporary lockout mode, the user's account is temporarily locked after a specified number of initial incorrect passwords or PINs are entered. This lockout lasts for a specified amount of time. If the maximum number of incorrect passwords or PINs is exceeded for a second time, the account is locked for twice the specified amount of time. The lockout time continues to increase for each set of incorrect passwords or PINs until the total number of failed login attempts equals the number specified to lock the account permanently. To prevent denial-of-service attacks, the retry count is not incremented if a user tries to log in during the lockout period. If the user enters the correct password or PIN and logs in successfully, the lockout time is reset to zero. After the account is permanently locked, only the administrator can unlock it and reset the password. When the administrator unlocks the account, the retry count and disable time are also reset to zero.

To configure the behavior for permanent lockouts, specify:

- Lockout mode (set to permanent)
- Maximum number of failed login attempts allowed before the account is locked

To configure the behavior for temporary lockouts, specify:

- Lockout mode (set to temporary)
- Number of failed attempts that trigger the initial temporary lockout
- Duration of initial temporary lockout
- Number of failed attempts that will lock the account permanently

You have the following four options when using password and PIN protect:

- Password Protection with:
 - Permanent Lockout
 - Temporary Lockout
- PIN Protection with:
 - Permanent Lockout
 - Temporary Lockout

The corresponding procedures are documented in the following sections:

- [Configuring Password Protection with Permanent Lockout, page 371](#)
- [Configuring PIN Protection with Permanent Lockout, page 372](#)
- [Configuring Password Protection with Temporary Lockout, page 373](#)
- [Configuring PIN Protection with Temporary Lockout, page 375](#)

Configuring Password Protection with Permanent Lockout

Prerequisites

Cisco Unity Express 3.0 or a later version

Required Data for This Procedure

None.

SUMMARY STEPS

1. `config t`
2. `security password lockout enable`
3. `security password lockout policy perm-lock`
4. `security password perm-lock max-attempts no_of_max_attempts`
5. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: se-10-0-0-0# config t	Enters configuration mode.
Step 2	security password lockout enable Example: se-10-0-0-0(config)# security password lockout enable	Enables the password lockout feature.
Step 3	security password lockout policy perm-lock Example: se-10-0-0-0(config)# security password lockout policy perm-lock	Sets the security mode to lock out subscribers permanently when the maximum number of failed login attempts is reached.
Step 4	security password perm-lock max-attempts no_of_max_attempts Example: se-10-0-0-0(config)# security password perm-lock max-attempts 2	Specifies the maximum number of failed attempts that trigger a permanent lockout. Range is 1 to 200.
Step 5	end Example: se-10-0-0-0(config)# end	Returns to privileged EXEC mode.

Configuring PIN Protection with Permanent Lockout**Prerequisites**

Cisco Unity Express 3.0 or a later version

Required Data for This Procedure

None.

SUMMARY STEPS

1. **config t**
2. **security pin lockout enable**
3. **security pin lockout policy perm-lock**
4. **security pin perm-lock max-attempts no_of_max_attempts**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>config t</code> Example: <code>se-10-0-0-0# config t</code>	Enters configuration mode.
Step 2	<code>security pin lockout enable</code> Example: <code>se-10-0-0-0(config)# security pin lockout enable</code>	Enables the PIN lockout feature.
Step 3	<code>security pin lockout policy perm-lock</code> Example: <code>se-10-0-0-0(config)# security pin lockout policy perm-lock</code>	Sets the security mode to lock out subscribers permanently when the maximum number of failed login attempts is reached.
Step 4	<code>security pin perm-lock max-attempts no_of_max_attempts</code> Example: <code>se-10-0-0-0(config)# security pin perm-lock max-attempts 2</code>	Specifies the maximum number of failed attempts that trigger a permanent lockout.
Step 5	<code>end</code> Example: <code>se-10-0-0-0(config)# end</code>	Returns to privileged EXEC mode.

Configuring Password Protection with Temporary Lockout

Prerequisites

Cisco Unity Express 3.0 or a later version

Required Data for This Procedure

None.

SUMMARY STEPS

1. `config t`
2. `security password lockout enable`
3. `security password lockout policy temp-lock`
4. `security password temp-lock max-attempts no_of_max_attempts`
5. `security password temp-lock init-attempts no_of_init_attempts`
6. `security password temp-lock duration duration`
7. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>config t</code> Example: <code>se-10-0-0-0# config t</code>	Enters configuration mode.
Step 2	<code>security password lockout enable</code> Example: <code>se-10-0-0-0(config)# security password lockout enable</code>	Enables the PIN lockout feature.
Step 3	<code>security password lockout policy temp-lock</code> Example: <code>se-10-0-0-0(config)# security password lockout policy temp-lock</code>	Set the security mode to lock out subscribers permanently when the maximum number of failed login attempts is reached.
Step 4	<code>security password temp-lock max-attempts no_of_max_attempts</code> Example: <code>se-10-0-0-0(config)# security password temp-lock init-attempts 8</code>	Specifies the initial number of failed attempts that trigger a temporary lockout. Range is from the value of <i>init-attempts</i> to 200.
Step 5	<code>security password temp-lock init-attempts no_of_init_attempts</code> Example: <code>se-10-0-0-0(config)# security password temp-lock init-attempts 4</code>	Specifies the initial number of failed attempts that trigger a temporary lockout. Range is between 1 and the value of <i>max_attempts</i> .
Step 6	<code>security password temp-lock duration duration</code> Example: <code>se-10-0-0-0(config)# security password temp-lock duration 10</code>	Specifies the initial lockout duration (in minutes) for a temporary lockout mode. The valid range is TBD.
Step 7	<code>end</code> Example: <code>se-10-0-0-0(config)# end</code>	Returns to privileged EXEC mode.

Configuring PIN Protection with Temporary Lockout

Prerequisites

Cisco Unity Express 3.0 or a later version

Required Data for This Procedure

None.

SUMMARY STEPS

1. `config t`
2. `security pin lockout enable`
3. `security pin lockout policy temp-lock`
4. `security pin temp-lock max-attempts no_of_max_attempts`
5. `security pin temp-lock init-attempts no_of_init_attempts`
6. `security pin temp-lock duration duration`
7. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>config t</code> Example: <code>se-10-0-0-0# config t</code>	Enters configuration mode.
Step 2	<code>security pin lockout enable</code> Example: <code>se-10-0-0-0(config)# security pin lockout enable</code>	Enables the PIN lockout feature.
Step 3	<code>security pin lockout policy temp-lock</code> Example: <code>se-10-0-0-0(config)# security pin lockout policy temp-lock</code>	Set the security mode to lock out subscribers permanently when the maximum number of failed login attempts is reached.
Step 4	<code>security pin temp-lock max-attempts <i>no_of_max_attempts</i></code> Example: <code>se-10-0-0-0(config)# security pin temp-lock init-attempts 8</code>	Specifies the initial number of failed attempts that trigger a temporary lockout. Range is from the value of <i>init-attempts</i> to 200.

	Command or Action	Purpose
Step 5	<pre>security pin temp-lock init-attempts no_of_init_attempts</pre> <p>Example: <pre>se-10-0-0-0(config)# security pin temp-lock init-attempts 4</pre></p>	Specifies the initial number of failed attempts that trigger a temporary lockout. Range is between 1 and the value of <i>max_attempts</i> .
Step 6	<pre>security pin temp-lock duration duration</pre> <p>Example: <pre>se-10-0-0-0(config)# security pin temp-lock duration 10</pre></p>	Specifies the initial lockout duration (in minutes) for a temporary lockout mode. The valid range is TBD
Step 7	<pre>end</pre> <p>Example: <pre>se-10-0-0-0(config)# end</pre></p>	Returns to privileged EXEC mode.

Using HTTPS to Protect Passwords and PINs

Starting in release 3.0, you can use HTTPS to secure the transmission of user passwords and PINs between the client and server. However, by default, Tomcat web servers does not have HTTPS enabled. HTTPS communicates over TLS protocol. The default port for HTTPS is 8443. However, Cisco Unity Express uses port 443 for the HTTPS port to avoid having to include the port number in the URL. Port forwarding from 80 (HTTP) to 443 is not enabled.

The web server will automatically use HTTPS to render any parts of the GUI or web pages that are not application-specific. You can configure applications to use HTTPS using their web.xml file.

HTTPS uses public key cryptography. Therefore, the HTTPS client must download the certificate from the server. You can either generate your own certificate or import one from a certificate authority. If you want to generate your own certificate, use the **crypto** command in configuration mode, as shown below:

```
crypto key generate rsa label tomcat modulus 1024
```



Note

To use this feature, no configuration using the GUI or CLI is required.

Configuring PIN and Password History

Starting in release 3.0, this feature enables the system to track previous PINs and passwords for all users and prevent users from reusing old PINs or passwords. You can configure the depth of the PIN or the password history using either the GUI or CLI.

This section contains these procedures:

- [Configuring the Password History Depth, page 377](#)
- [Configuring the PIN History Depth, page 377](#)

Configuring the Password History Depth

Prerequisites

Cisco Unity Express 3.0 or a later version

Required Data for This Procedure

None.

SUMMARY STEPS

1. `config t`
2. `security password history depth depth`
3. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>config t</code> Example: se-10-0-0-0# <code>config t</code>	Enters configuration mode.
Step 2	<code>security password history depth depth</code> Example: se-10-0-0-0(config)# <code>security password history depth 6</code>	Forces all users to choose a password that is not in their password history list.
Step 3	<code>end</code> Example: se-10-0-0-0(config)# <code>end</code>	Returns to privileged EXEC mode.

Configuring the PIN History Depth

Prerequisites

Cisco Unity Express 3.0 or a later version

Required Data for This Procedure

None.

SUMMARY STEPS

1. `config t`
2. `security pin history depth depth`
3. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>config t</code> Example: <code>se-10-0-0-0# config t</code>	Enters configuration mode.
Step 2	<code>security pin history depth depth</code> Example: <code>se-10-0-0-0(config)# security pin history depth 6</code>	Forces all users to choose a PIN that is not in their password history list.
Step 3	<code>end</code> Example: <code>se-10-0-0-0(config)# end</code>	Returns to privileged EXEC mode.

Displaying Password and PIN System Settings

Use the following Cisco Unity Express EXEC mode command to display the password and PIN settings:

```
show security detail
```

The command output can look similar to the following:

```
se-10-0-0-0# show security detail

Password Expires:      true
Password Age:         60 days
Password Length (min): 5
Password Length (max): 32
PIN Expires:          true
PIN Age:              45 days
PIN Length (min):     4
PIN Length (max):     16
```

The following example shows the values when password expiration and the PIN length are reset to the system default values:

```
se-10-0-0-0# show security detail

Password Expires:      false
Password Length (min): 3
Password Length (max): 32
PIN Expires:          false
PIN Length (min):     3
PIN Length (max):     16
```

To display PINless voicemail settings, use the following Cisco Unity Express EXEC mode command:

```
show voicemail detail mailbox [owner]
```

This command will produce output similar to the following, showing one of the three options displayed below:

```
se-10-0-0-0# show voicemail detail mailbox cjwhite
```

```
Owner: /sw/local/users/cjwhite
Type: Personal
Description:
Busy state: idle
Enabled: true
Allow login without pin: [no |
yes - from subscriber's phone numbers |
yes - from any phone number]
Mailbox Size (seconds): 3000
Message Size (seconds): 60
Play Tutorial: false
Fax Enabled: true
Space Used (seconds): 12
Total Message Count: 1
New Message Count: 1
Saved Message Count: 0
Future Message Count: 0
Deleted Message Count: 0
Fax Message Count: 0
Expiration (days): 30
Greeting: standard
Zero Out Number:
Created/Last Accessed: Jun 05 2007 17:06:07 PDTumber: 1
```

Encrypting PINs in Backup Files

Before release 3.0, PINs were stored as clear text in LDAP and were therefore visible in the backup file. This is because user PINs are stored in LDAP, which is backed up in LDIF format. This feature applies SHA-1 hash encryption to PINs before storing them in the LDAP database. As a result, when a user logs in to voice mail, the PIN they submit is hashed and compared to the PIN attribute retrieved from the LDAP directory.

To migrate from earlier version, you must convert from a clear PIN to a hashed PIN in the LDAP directory. Typically, you do this immediately after a system upgrade from an earlier version or after a restore operation from an old backup. At this point, the clear PIN is removed from the database and replaced with the encrypted PIN.

Because encryption using SHA-1 is not reversible, after the conversion is complete, you cannot disable or turn off this feature to restore the encrypted PIN to its clear form.



Note

This feature, does not require any configuration using the GUI or CLI.
