高度な設定

この章では、「システム コンポーネントの設定」（P.57）で説明されている最初のインストールおよび設定処理の後でアプリケーション パラメータを変更するための高度な設定手順について説明します。「システム コンポーネントの設定」の章には、この章で説明されていないコマンドも含まれています。

この高度な設定手順は、次の項で構成されています。

- 「ホスト名の設定」（P.367）
- 「DNS サーバの設定」（P.369）
- 「NTP サーバの設定」（P.370）
- 「syslog サーバの設定」（P.374）
- 「クロック タイム ゾーンの設定」（P.376）
- 「パスワードおよび PIN のパラメータの設定」（P.378）
- Cisco Unified CME パスワードの同期（「パスワードおよび PIN のパラメータの設定」（P.378）を参照）
- PINless ボイスメール（「パスワードおよび PIN のパラメータの設定」（P.378）および「パスワードおよび PIN のシステム設定の表示」（P.387）を参照）
- 「CLI コマンドのスケジュール」（P.389）

ホスト名の設定

ソフトウェア インストール後のプロセスで、ホスト名は設定されています。ホスト名を変更するには、この手順を使用します。

概略手順

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

詳細手順

	コマンドまたは操作	目的
ステップ 1	**config t** **例：** `se-10-0-0-0# config t`	設定モードを開始します。

ステップ 2	**hostname** *hostname*
	
	例：
	`se-10-0-0-0(config)# hostname mainhost`
	`mainhost(config)#`
		ローカルの Cisco Unity Express システムを識別するホスト名を指定します。ホスト名の一部としてドメイン名を含めないでください。
		
		Cisco Unity Express プロンプトは、ホスト名を反映するように変更されます。ホスト名を入力しない場合、「se」と Cisco Unity Express ネットワーク モジュールの IP アドレスを使用してプロンプトが作成されます。

ステップ 3	**exit** **例：** `mainhost(config)# exit`	設定モードを終了します。
ステップ 4	**show hosts** **例：** `mainhost# show hosts`	システム上で設定されているローカル ホスト名および DNS サーバを表示します。
ステップ 5	**copy running-config startup-config** **例：** `mainhost# copy running-config startup-config`	コンフィギュレーションの変更部分をスタートアップ コンフィギュレーションにコピーします。

例

次のコマンドは、ホスト名を設定します。

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

show hosts コマンドの出力は、次の例のようになります。

```
ca-west# show hosts

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

DNS サーバの設定

DNS サーバと IP アドレスは、ソフトウェア インストール後のプロセスで設定されています。サーバ名と IP アドレスを変更するには、この手順を使用します。

概略手順

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**

詳細手順

	コマンドまたは操作	目的
ステップ 1	**config t** **例：** se-10-0-0-0# config t	設定モードを開始します。
ステップ 2	**ip domain-name** *dns-server-name* **例：** se-10-0-0-0(config)# **ip domain-name mycompany.com**	DNS サーバのドメイン名を指定します。
ステップ 3	**ip name-server** *ip-address* [*ip-address*] [*ip-address*] [*ip-address*] **例：** 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**	DNS サーバの IP アドレスを 4 つまで指定します。
ステップ 4	**exit** **例：** se-10-0-0-0(config)# exit	設定モードを終了します。
ステップ 5	**show hosts** **例：** se-10-0-0-0# show hosts	IP ルートの宛先、ゲート、およびマスクを表示します。
ステップ 6	**copy running-config startup-config** **例：** se-10-0-0-0# **copy running-config startup-config**	コンフィギュレーションの変更部分をスタートアップ コンフィギュレーションにコピーします。

例

次のコマンドは、DNS サーバを設定します。

```
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#
```

show hosts コマンドの出力は、次の例のようになります。

```
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#
```

NTP サーバの設定

Network Time Protocol（NTP; ネットワーク タイム プロトコル）は、ソフトウェア インストール後のプロセスで設定されています。Cisco Unity Express では、最大 3 つの NTP サーバを使用できます。NTP サーバを追加または削除するには、この手順を使用します。

NTP サーバの追加

NTP サーバを指定するには、その IP アドレスまたはホスト名を使用します。

Cisco Unity Express は、DNS サーバを使用して、ホスト名を IP アドレスに解決し、その IP アドレスを NTP サーバとして格納します。DNS がホスト名を複数の IP アドレスに解決した場合、Cisco Unity Express は、IP アドレスの中からまだ NTP サーバとして指定されていないものを 1 つランダムに選択します。

NTP サーバの 1 つのホスト名に複数の IP アドレスを設定する場合は、同じホスト名を使用して設定手順を繰り返します。繰り返すたびに、NTP サーバが残りの IP アドレスに割り当てられます。

概略手順

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

詳細手順

	コマンドまたは操作	目的
ステップ 1	**config t** **例：** `se-10-0-0-0# config t`	設定モードを開始します。

ステップ 2	**ntp server** {*hostname* | *ip-address*} [**prefer**]
	
	例：
	`se-10-0-0-0(config)# ntp server 10.0.3.4`
	`se-10-0-0-0(config)# ntp server 10.0.10.20 prefer`
		NTP サーバの名前または IP アドレスを指定します。
		複数のサーバを設定する場合は、**prefer** アトリビュートを含むサーバを先に使用します。

ステップ 3	**exit** **例：** `se-10-0-0-0(config)# exit`	設定モードを終了します。
ステップ 4	**show ntp status** **例：** `se-10-0-0-0# show ntp status`	NTP サブシステムの状態を表示します。
ステップ 5	**show ntp servers** **例：** `se-10-0-0-0# show ntp servers`	Network Time Protocol（NTP）サーバおよびそれらの現在のステータスのリストを表示します。
ステップ 6	**show ntp source** **例：** `se-10-0-0-0# show ntp source`	Network Time Protocol（NTP）サーバの時刻源を表示します。
ステップ 7	**show ntp association** **例：** `se-10-0-0-0# show ntp association`	すべての Network Time Protocol（NTP）サーバのアソシエーション ID およびステータスを表示します。
ステップ 8	**copy running-config startup-config** **例：** `se-10-0-0-0# copy running-config startup-config`	コンフィギュレーションの変更部分をスタートアップ コンフィギュレーションにコピーします。

例

次のコマンドは、NTP サーバを設定します。

```
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#
```

次の例は、**show ntp status** コマンドのサンプル出力を示しています。

```
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#
```

次の例は、**show ntp servers** コマンドのサンプル出力を示しています。

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

remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.100.10.65 127.127.7.1    8 u  933 1024  377    0.430   -1.139   0.158
space reject,       x falsetick,       .excess,          - outlyer
+ candidate,        # selected,        * sys.peer,        o pps.peer
```

次の例は、**show ntp source** コマンドのサンプル出力を示しています。

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

127.0.0.1: stratum 9, offset 0.000015, synch distance 0.03047
10.100.10.65: stratum 8, offset -0.001124, synch distance 0.00003
```

次の例は、**show ntp association** コマンドのサンプル出力を示しています。

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

ind assID status  conf reach auth condition  last_event cnt
===========================================================
  1 37773  9624   yes   yes  none  sys.peer   reachable  2
```

次の例では、NTP サーバのホスト名が 172.16.10.1 と 172.16.10.2 の 2 つの IP アドレスを指すように設定されます。

```
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#
```

次の例は、**show ntp status** コマンドのサンプル出力を示しています。

```
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#
```

NTP サーバの削除

NTP サーバを削除するには、その IP アドレスまたはホスト名を使用します。

概略手順

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**

詳細手順

	コマンドまたは操作	目的
ステップ 1	**config t** **例：** se-10-0-0-0# config t	設定モードを開始します。
ステップ 2	**no ntp server** {*hostname* | *ip-address*} **例：** se-10-0-0-0(config)# **no ntp server 10.0.3.4** se-10-0-0-0(config)# **no ntp server myhost**	削除する NTP サーバのホスト名または IP アドレスを指定します。
ステップ 3	**exit** **例：** se-10-0-0-0(config)# exit	設定モードを終了します。
ステップ 4	**show ntp status** **例：** se-10-0-0-0# show ntp status	NTP サブシステムの状態を表示します。
ステップ 5	**show ntp configuration** **例：** se-10-0-0-0# show ntp configuration	設定されている NTP サーバの状態を表示します。
ステップ 6	**copy running-config startup-config** **例：** se-10-0-0-0# **copy running-config startup-config**	コンフィギュレーションの変更部分をスタートアップ コンフィギュレーションにコピーします。

NTP サーバ情報の表示

次のコマンドを使用すると、NTP サーバの構成情報とステータスを表示できます。

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

次の例は、**show ntp associations** コマンドのサンプル出力を示しています。

```
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
```

次の例は、**show ntp servers** コマンドのサンプル出力を示しています。

```
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
```

次の例は、**show ntp source** コマンドのサンプル出力を示しています。

```
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*
```

次の例は、**show ntp status** コマンドのサンプル出力を示しています。

```
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
```

syslog サーバの設定

Cisco Unity Express は、システムのアクティビティを説明するメッセージを取り込みます。これらのメッセージは収集され、Cisco Unity Express モジュールのハードディスクの messages.log ファイル、コンソール、または外部システム ログ（syslog）サーバに転送されます。messages.log ファイルは、デフォルトの転送先です。

この項では、メッセージを収集するために外部サーバを設定する手順について説明します。メッセージを表示する方法については、「システム アクティビティ メッセージの表示」（P.404）を参照してください。

この手順に必要なデータ

指定されたログ サーバのホスト名または IP アドレスが必要です。

概略手順

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

詳細手順

	コマンドまたは操作	目的
ステップ 1	**config t** **例：** `se-10-0-0-0# config t`	設定モードを開始します。

ステップ 2	**log server address** {*hostname* | *ip-address*}
	
	例：
	`se-10-0-0-0(config)# log server address 10.187.240.31`
	`se-10-0-0-0(config)# log server address logpc`
		ログ サーバとして指定された NTP サーバのホスト名または IP アドレスを指定します。

ステップ 3	**exit** **例：** `se-10-0-0-0(config)# exit`	設定モードを終了します。
ステップ 4	**show running-config** **例：** `se-10-0-0-0# show running-config`	システム コンフィギュレーションを表示します。これには、設定されたログ サーバが含まれます。

例

show running-config コマンドの出力は、次の例のようになります。

```
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
```

クロック タイム ゾーンの設定

ローカル Cisco Unity Express モジュールのタイム ゾーンは、ソフトウェア インストール後のプロセスで設定されています。モジュールのタイム ゾーンを変更するには、この手順を使用します。

Cisco Unity Express は自動的に、選択されたタイム ゾーンに基づいて、クロックをサマータイムに更新します。

概略手順

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

詳細手順

	コマンドまたは操作	目的
ステップ 1	**config t** **例：** `se-10-0-0-0# config t`	設定モードを開始します。
ステップ 2	**clock timezone** *timezone* **例：** `se-10-0-0-0(config)# clock timezone America/Los_Angeles`	ローカル タイム ゾーンを指定します。*timezone* 引数の値を入力するには、タイム ゾーンを表すフレーズを知っている必要があります。 フレーズが不明の場合は、Enter キーを押します。タイム ゾーンを選択できる一連のメニューが表示されます。
ステップ 3	**exit** **例：** `se-10-0-0-0(config)# exit`	設定モードを終了します。
ステップ 4	**show clock detail** **例：** `se-10-0-0-0# show clock detail`	タイム ゾーン、時間分解能、および現在の時刻を表示します。
ステップ 5	**copy running-config startup-config** **例：** `se-10-0-0-0# copy running-config startup-config`	コンフィギュレーションの変更部分をスタートアップ コンフィギュレーションにコピーします。

例

次のコマンドは、クロック タイム ゾーンを設定します。

```
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#
```

show clock detail コマンドの出力は、次の例のようになります。

```
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
```

パスワードおよび PIN のパラメータの設定

Cisco Unity Express は、パスワードおよび個人識別番号（PIN）のパラメータの設定をサポートします。これについて次の項で説明します。

- 「パスワードおよび PIN の長さと有効期限の設定」（P.378）
- 「パスワードおよび PIN の保護およびロックアウト モードの設定」（P.380）
- 「PIN およびパスワードの履歴の設定」（P.386）
- 「バックアップ ファイルの PIN の暗号化」（P.388）
- 「パスワードおよび PIN のシステム設定の表示」（P.387）

（注） Cisco Unity Express で [Configure] -->[Users] を使用して Cisco Unified CME ユーザのパスワードを変更した場合、そのユーザのパスワードは Cisco Unified CME で更新されます。ただし、その逆は当てはまりません。つまり、Cisco Unified CME で変更したユーザ パスワードは、Cisco Unity Express で更新されません。

（注） PINless ボイスメールを設定する方法については、「PINless メールボックス アクセスの設定」（P.159）を参照してください。

パスワードおよび PIN の長さと有効期限の設定

Cisco Unity Express は、パスワードおよび PIN について、次の 2 つの属性の設定をサポートします。

- パスワードおよび PIN の最小長

  拡張セキュリティ手順をサポートするため、Cisco Unity Express では、パスワードおよび PIN の長さが設定可能になっています。管理者は、この値の長さを 3 文字以上の英数字として設定できます。すべてのユーザがそれ以上の文字数のパスワードと PIN を持つように、この値がシステム全体に適用されます。この長さを設定するには、GUI の [Defaults] > [User] オプションを使用するか、次に説明する手順を実行します。

パスワードの長さは、PIN の長さと同じにする必要はありません。

デフォルトの長さは、英数字 3 文字です。パスワードの最大長は、英数字 32 文字です。PIN の最大長は、英数字 16 文字です。

パスワードまたは PIN の長さをシステム デフォルト値に設定するには、コマンドの **no** 形式または **default** 形式を使用します。

（注） 最小のパスワードまたは PIN の長さを大きくした場合、新しい制限に適合しない既存のパスワードおよび PIN は、自動的に期限切れになります。ユーザは、GUI に次回ログインするときにパスワードをリセットし、TUI に次回ログインするときに PIN をリセットする必要があります。

- パスワードおよび PIN の有効期限

  Cisco Unity Express では、管理者はパスワードおよび PIN の有効期限をシステム全体ベースで設定できます。有効期限は、パスワードおよび PIN が有効な時間（日数）です。この時間に達したら、ユーザは新しいパスワードまたは PIN を入力する必要があります。

  このオプションが設定されていない場合、パスワードおよび PIN は無期限に有効です。

  この時間を設定するには、GUI の [Defaults] > [User] オプションを使用するか、次に説明する手順を実行します。

  パスワードの有効期限は、PIN の有効期限と同じにする必要はありません。

  有効な範囲は 3 ～ 365 日です。

  パスワードまたは PIN の有効期限をシステム デフォルト値に設定するには、コマンドの **no** 形式または **default** 形式を使用します。

概略手順

- **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**

詳細手順

	コマンドまたは操作	目的

ステップ 1	**config t**
	
	例：
	`se-10-0-0-0# config t`
	`se-10-0-0-0(config)#`
		設定モードを開始します。

ステップ 2	**security password length min** *password-length* **例：** `se-10-0-0-0(config)# security password length min 5`	すべてのユーザのパスワードの長さを指定します。デフォルトの最小値は 3、最大値は 32 です。 最小のパスワードの長さをシステム デフォルトに設定するには、コマンドの **no** 形式または **default** 形式を使用します。

	コマンドまたは操作	目的
ステップ 3	**security pin length min** *pin-length* **例：** `se-10-0-0-0(config)# security pin length min 4`	すべてのユーザの PIN の最小長を指定します。デフォルトの値は 3、最大値は 16 です。 最小の PIN の長さをシステム デフォルトに設定するには、コマンドの **no** 形式または **default** 形式を使用します。
ステップ 4	**security password expiry days** *password-days* **例：** `se-10-0-0-0(config)# security password expiry days 60`	ユーザのパスワードの最大有効日数を指定します。有効な値の範囲は 3 ～ 365 です。 この値が設定されていない場合、パスワードは無期限に有効です。 パスワードの有効期限をシステム デフォルトに設定するには、コマンドの **no** 形式または **default** 形式を使用します。
ステップ 5	**security pin expiry days** *pin-days* **例：** `se-10-0-0-0(config)# security pin expiry days 45`	ユーザの PIN の最大有効日数を指定します。有効な値の範囲は 3 ～ 365 です。 この値が設定されていない場合、PIN は無期限に有効です。 PIN の有効期限をシステム デフォルトに設定するには、コマンドの **no** 形式または **default** 形式を使用します。

ステップ 6	**exit**
	
	例：
	`se-10-0-0-0(config)# exit`
	`se-10-0-0-0#`
		設定モードを終了します。

例

次の例では、パスワードの長さが 6 文字、PIN の長さが 5 文字、パスワードの有効期限が 60 日、PIN の有効期限が 45 日に設定されています。

```
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
```

パスワードおよび PIN の保護およびロックアウト モードの設定

リリース 3.0 以降では、パスワードおよび PIN に対する一時的なロックアウトおよび無期限のロックアウトを使用し、セキュリティ侵害の防止に役立てることができます。

無期限のロックアウト モードでは、誤ったパスワードまたは PIN が指定した回数だけ入力されると、そのユーザのアカウントが無期限にロックされます。アカウントがロックされると、そのアカウントのロックを解除してパスワードをリセットできるのは管理者だけになります。

一時的ロックアウト モードでは、誤ったパスワードまたは PIN が指定した回数だけ初期入力されると、そのユーザのアカウントが一時的にロックされます。このロックアウトは、指定した時間だけ継続します。次回、誤ったパスワードまたは PIN が最大回数を超えると、そのアカウントは指定した時間の 2 倍だけロックされます。誤ったパスワードまたは PIN のセットが入力されるたびにロックアウト時間

が増加し、ログインの合計失敗回数が指定回数に達すると、アカウントが無期限にロックされます。DoS 攻撃（サービス拒絶攻撃）を防止するため、ユーザがロックアウト期間中にログインしようとした場合は、再試行カウントが増加しません。ユーザが正しいパスワードまたは PIN を入力して正常にログインすると、ロックアウト時間が 0 にリセットされます。アカウントが無期限にロックされると、そのアカウントのロックを解除してパスワードをリセットできるのは管理者だけになります。管理者がアカウントのロックを解除すると、再試行カウントと無効時間も 0 にリセットされます。

無期限のロックアウトの動作を設定するには、次のものを指定する必要があります。

- ロックアウト モード（permanent に設定）
- アカウントがロックされるまでに許可するログイン試行の最大失敗回数

一時的なロックアウトの動作を設定するには、次のものを指定する必要があります。

- ロックアウト モード（temporary に設定）
- 最初の一時的ロックアウトをトリガーする失敗試行の回数
- 最初の一時的ロックアウトの期間
- アカウントが無期限にロックされる失敗試行の回数

パスワードおよび PIN の保護を使用する場合は、次の 4 つのオプションがあります。

- パスワードの保護方法
  - 無期限のロックアウト
  - 一時的ロックアウト
- PIN の保護方法
  - 無期限のロックアウト
  - 一時的ロックアウト

次の項で、それぞれの手順について説明します。

- 「無期限のロックアウトによるパスワード保護の設定」（P.381）
- 「無期限のロックアウトによる PIN 保護の設定」（P.382）
- 「一時的ロックアウトによるパスワード保護の設定」（P.383）
- 「一時的ロックアウトによる PIN 保護の設定」（P.384）

無期限のロックアウトによるパスワード保護の設定

前提条件

Cisco Unity Express 3.0 以降のバージョン

この手順に必要なデータ

なし。

概略手順

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**

詳細手順

	コマンドまたは操作	目的
ステップ 1	**config t** **例：** `se-10-0-0-0# config t`	設定モードを開始します。
ステップ 2	**security password lockout enable** **例：** `se-10-0-0-0(config)# security password lockout enable`	パスワードのロックアウト機能を有効にします。
ステップ 3	**security password lockout policy perm-lock** **例：** `se-10-0-0-0(config)# security password lockout policy perm-lock`	ログイン試行が最大失敗回数に達したときに、ユーザを無期限にロックアウトするようにセキュリティモードを設定します。
ステップ 4	**security password perm-lock max-attempts** *no_of_max_attempts* **例：** `se-10-0-0-0(config)# security password perm-lock max-attempts 2`	無期限のロックアウトをトリガーする失敗試行の最大回数を指定します。範囲は 1 ～ 200 です。
ステップ 5	**end** **例：** `se-10-0-0-0(config)# end`	特権 EXEC モードに戻ります。

無期限のロックアウトによる PIN 保護の設定

前提条件

Cisco Unity Express 3.0 以降のバージョン

この手順に必要なデータ

なし。

概略手順

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**

詳細手順

	コマンドまたは操作	目的
ステップ 1	**config t** **例：** `se-10-0-0-0# config t`	設定モードを開始します。
ステップ 2	**security pin lockout enable** **例：** `se-10-0-0-0(config)# security pin lockout enable`	PIN のロックアウト機能を有効にします。
ステップ 3	**security pin lockout policy perm-lock** **例：** `se-10-0-0-0(config)# security pin lockout policy perm-lock`	ログイン試行が最大失敗回数に達したときに、ユーザを無期限にロックアウトするようにセキュリティモードを設定します。
ステップ 4	**security pin perm-lock max-attempts** *no_of_max_attempts* **例：** `se-10-0-0-0(config)# security pin perm-lock max-attempts 2`	無期限のロックアウトをトリガーする失敗試行の最大回数を指定します。
ステップ 5	**end** **例：** `se-10-0-0-0(config)# end`	特権 EXEC モードに戻ります。

一時的ロックアウトによるパスワード保護の設定

前提条件

Cisco Unity Express 3.0 以降のバージョン

この手順に必要なデータ

なし。

概略手順

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**

詳細手順

	コマンドまたは操作	目的
ステップ 1	**config t** **例：** `se-10-0-0-0# config t`	設定モードを開始します。
ステップ 2	**security password lockout enable** **例：** `se-10-0-0-0(config)# security password lockout enable`	PIN のロックアウト機能を有効にします。
ステップ 3	**security password lockout policy temp-lock** **例：** `se-10-0-0-0(config)# security password lockout policy temp-lock`	ログイン試行が最大失敗回数に達したときに、ユーザを無期限にロックアウトするようにセキュリティモードを設定します。
ステップ 4	**security password temp-lock max-attempts** *no_of_max_attempts* **例：** `se-10-0-0-0(config)# security password temp-lock init-attempts 8`	一時的ロックアウトをトリガーする失敗試行の初期回数を指定します。範囲は *init-attempts* の値～ 200 です。
ステップ 5	**security password temp-lock init-attempts** *no_of_init_attempts* **例：** `se-10-0-0-0(config)# security password temp-lock init-attempts 4`	一時的ロックアウトをトリガーする失敗試行の初期回数を指定します。範囲は、1 ～ *max_attempts* の値です。
ステップ 6	**security password temp-lock duration** *duration* **例：** `se-10-0-0-0(config)# security password temp-lock duration 10`	一時的ロックアウト モードの初期ロックアウト時間（分）を指定します。有効な範囲は未定です。
ステップ 7	**end** **例：** `se-10-0-0-0(config)# end`	特権 EXEC モードに戻ります。

一時的ロックアウトによる PIN 保護の設定

前提条件

Cisco Unity Express 3.0 以降のバージョン

この手順に必要なデータ

なし。

概略手順

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**

詳細手順

	コマンドまたは操作	目的
ステップ 1	**config t** **例：** `se-10-0-0-0# config t`	設定モードを開始します。
ステップ 2	**security pin lockout enable** **例：** `se-10-0-0-0(config)# security pin lockout enable`	PIN のロックアウト機能を有効にします。
ステップ 3	**security pin lockout policy temp-lock** **例：** `se-10-0-0-0(config)# security pin lockout policy temp-lock`	ログイン試行が最大失敗回数に達したときに、ユーザを無期限にロックアウトするようにセキュリティ モードを設定します。
ステップ 4	**security pin temp-lock max-attempts** *no_of_max_attempts* **例：** `se-10-0-0-0(config)# security pin temp-lock init-attempts 8`	一時的ロックアウトをトリガーする失敗試行の初期回数を指定します。範囲は *init-attempts* の値～ 200 です。
ステップ 5	**security pin temp-lock init-attempts** *no_of_init_attempts* **例：** `se-10-0-0-0(config)# security pin temp-lock init-attempts 4`	一時的ロックアウトをトリガーする失敗試行の初期回数を指定します。範囲は、1 ～ *max_attempts* の値です。
ステップ 6	**security pin temp-lock duration** *duration* **例：** `se-10-0-0-0(config)# security pin temp-lock duration 10`	一時的ロックアウト モードの初期ロックアウト時間（分）を指定します。有効な範囲は未定です。
ステップ 7	**end** **例：** `se-10-0-0-0(config)# end`	特権 EXEC モードに戻ります。

PIN およびパスワードの履歴の設定

リリース 3.0 以降では、この機能を使用すると、すべてのユーザに対して以前の PIN とパスワードが追跡され、ユーザが古い PIN またはパスワードを再使用することが防止されます。PIN またはパスワードの履歴数の設定には、GUI と CLI のどちらも使用できます。

この項では、次の手順について説明します。

パスワードの履歴数の設定

前提条件

Cisco Unity Express 3.0 以降のバージョン

この手順に必要なデータ

なし。

概略手順

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

詳細手順

	コマンドまたは操作	目的
ステップ 1	**config t** **例：** `se-10-0-0-0# config t`	設定モードを開始します。
ステップ 2	**security password history depth** *depth* **例：** `se-10-0-0-0(config)# security password history depth 6`	すべてのユーザが、強制的にパスワード履歴リストにないパスワードを選択するようにします。
ステップ 3	**end** **例：** `se-10-0-0-0(config)# end`	特権 EXEC モードに戻ります。

PIN の履歴数の設定

前提条件

Cisco Unity Express 3.0 以降のバージョン

この手順に必要なデータ

なし。

概略手順

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

詳細手順

	コマンドまたは操作	目的
ステップ 1	**config t** **例：** `se-10-0-0-0# config t`	設定モードを開始します。
ステップ 2	**security pin history depth** *depth* **例：** `se-10-0-0-0(config)# security pin history depth 6`	すべてのユーザが、強制的にパスワード履歴リストにない PIN を選択するようにします。
ステップ 3	**end** **例：** `se-10-0-0-0(config)# end`	特権 EXEC モードに戻ります。

パスワードおよび PIN のシステム設定の表示

パスワードおよび PIN の設定を表示するには、次の Cisco Unity Express EXEC モードのコマンドを使用します。

show security detail

このコマンドの出力は、次のようになります。

```
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
```

次の例は、パスワードの有効期限と PIN の長さがシステムのデフォルト値にリセットされた場合の値を示しています。

```
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
```

PINless ボイスメールの設定を表示するには、Cisco Unity Express EXEC モードで次のコマンドを使用します。

show voicemail detail mailbox *[owner]*

このコマンドでは、次のような出力が生成され、次に示す 3 つのオプションのいずれかが表示されます。

```
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
```

バックアップ ファイルの PIN の暗号化

リリース 3.0 以前は、PIN が LDAP にクリア テキストで格納されたため、バックアップ ファイル内で参照することができました。これは、ユーザ PIN が LDAP に格納され、それが LDIF 形式でバックアップされるためです。今回の機能では、PIN を LDAP データベースに格納する前に SHA-1 ハッシュ暗号化が適用されます。このため、ユーザがボイスメールにログインすると、送信された PIN はハッシュ化され、LDAP ディレクトリから取得された PIN アトリビュートと比較されます。

以前のバージョンから移行するには、LDAP ディレクトリでクリア PIN をハッシュ化 PIN に変換する必要があります。一般的に、この変換は、システムが以前のバージョンからアップグレードされた直後、または古いバックアップからの復元操作後に行います。このとき、クリア PIN がデータベースから削除され、暗号化された PIN に置き換えられます。

SHA-1 を使用した暗号化は元に戻せないため、変換の完了後にこの機能を無効またはオフにし、暗号化された PIN をクリア形式に復元することはできません。

（注） この機能は GUI または CLI を使用して設定する必要がありません。

CLI コマンドのスケジュール

Cisco Unity Express 8.0 以降では、CLI コマンド ブロックの実行をスケジュールできるようになりました。コマンド ブロックはインタラクティブに入力します。記号のデリミタ文字を使用して実行の開始と停止を行います。一連のコマンドの実行は EXEC モードで開始されますが、コマンド ブロック内でのモード変更コマンドが許可されています。

Cisco Unity Express 8.0 では次の制限があります。

- コマンド ブロックの最大サイズは、改行文字も含めて 1,024 文字です。
- ブロック内のコマンドには、カンマ「,」やデリミタ文字を使用できません。たとえば、デリミタ文字を「#」に設定している場合、この文字はコマンド ブロック内で使用できません。
- システム管理者だけが、コマンド ブロックの実行をスケジュールできます。
- CLI コマンドは、システムの superuser 特権で実行されます。
- これらのコマンド ブロックの実行に対する通知はありません。エラー メッセージおよび結果を確認できるのは、ログ ファイルだけです。

注意 CLI コマンドは注意深くスケジュールしてください。インタラクティブなコマンドを使用すると、実行が停止されます。いくつかのコマンドは、システムを不安定にすることがあります。

前提条件

Cisco Unity Express 8.0 以降のバージョン

この手順に必要なデータ

なし。

概略手順

1. **kron schedule** [*name*]
2. **description**
3. **repeat every** {*number* **days at** *time* |*number* **weeks on** *day* | *number* **months on day** *date* | *number* **years on month** *month*} **at** *time*

（注） **repeat every** コマンドの代わりに、次のいずれかのコマンドを使用することもできます。

- **repeat once at** *time*
- **repeat daily at** *time*
- **repeat monthly on day** *date* **at** *time*
- **repeat weekly on** *day* **at** *time*
- **repeat yearly on month** *month* **at** *time*

4. **start-date** *date*
5. **stop-date** *date*
6. **commands** *delimiter*

7. **exit**
8. **show kron schedules**
9. **show kron schedule detail job**

詳細手順

	コマンドまたは操作	目的
ステップ 1	**kron schedule** [*name*] **例：** `se-10-0-0-0# kron schedule kron1011`	kron スケジュール設定モードを開始します。
ステップ 2	**description** *description* **例：** `se-10-0-0-0(kron-schedule)# description backup`	（オプション）スケジュール設定した kron ジョブの説明を入力します。
ステップ 3	**repeat every** {*number* **days** | *number* **weeks on** *day* | *number* **months on day** *date* | *number* **years on month** *month*} **at time** *time* **例：** `se-10-0-0-0(kron-schedule)# repeat every 2 days at time 10:00`	スケジュール設定した定期的な kron ジョブの実行頻度を指定します。1 回限りの kron ジョブを設定するには、**repeat once** コマンドを使用します。また、前述の（注）で示した他の **repeat** コマンドのいずれかを使用することもできます。
ステップ 4	**start-date** *date* **例：** `se-10-0-0-0(kron-schedule)# start-date 05/30/2009`	スケジュール設定した定期的な kron ジョブの実行開始日を指定します。
ステップ 5	**stop-date** *date* **例：** `se-10-0-0-0(kron-schedule)# stop-date 10/20/2009`	スケジュール設定した定期的な kron ジョブの実行終了日を指定します。

ステップ 6	**commands** *delimiter*
	
	例：
	`se-10-0-0-0(kron-schedule)# commands %`
	`Enter CLI commands to be executed. End with the character '%'. Maximum size is 1024 characters, it may not contain symbol %.`
	
	`%show version`
	`show running-config`
	`config t`
	`hostname aaa`
	
	`%`
	`se-10-0-0-0(kron-schedule)#`
		インタラクティブ モードを開始します。このモードでは、スケジュール設定した kron ジョブにコマンド ブロック内のコマンドを入力できます。デリミタ文字を使用してコマンド ブロックを区切ります。
		
		（注） 任意の記号をデリミタにできます。「%」記号は、例示だけを目的として使用しています。

ステップ 7	**exit**	kron スケジュール設定モードを終了します。

	コマンドまたは操作	目的
ステップ 8	**show kron schedules** **例：** `se-10-0-0-0# show kron schedule`	スケジュール設定した kron ジョブのリストを表示します。
ステップ 9	**show kron schedule detail job** *name* **例：** `se-10-0-0-0# show kron schedule detail job kron1011`	スケジュール設定した特定の kron ジョブについての情報を表示します。

例

show kron schedules コマンドのサンプル出力を次に示します。

```
se-10-0-0-0# show kron schedules
Name          Schedule                          Commands
krj1          Every 1 days at 12:34             show ver,sh run,conf t,host...
Total: 1
```

show kron schedule detail job コマンドのサンプル出力を次に示します。

```
se-10-0-0-0# show kron schedule detail job krj1
Job Name        krj1
Description
Schedule        NOT SET
Last Run        NEVER
Last Result
Next Run        NEVER
Active          from 2010/02/15 until INDEFINITE
Disabled
CLI Commands
                show ver
                sh run
                conf t
                hostname aaa
se-10-0-0-0#
```