S: script (ccn application) to show ccn trigger sip

Last Updated: July 10, 2012

script (ccn application)

secure-messaging incoming (mailbox)

secure-messaging outgoing (mailbox)

security password

security password history depth

security password lockout enable

security password lockout policy

security password perm-lock max-attempts

security password temp-lock duration

security password temp-lock init-attempts

security password temp-lock max-attempts

security pin

security pin history depth

security pin lockout enable

security pin lockout policy

security pin perm-lock max-attempts

security pin temp-lock duration

security pin temp-lock init-attempts

security pin temp-lock max-attempts

security pin trivialcheck

security ssh

security ssh knownhost

service imap

service phone-authentication

service voiceview

service voiceview session terminate

session idletimeout (IMAP)

session idletimeout (VoiceView Express)

session security

show aaa accounting event

show aaa accounting service

show aaa policy

show backup

show backup history

show backup schedule detail job

show backup schedules

show backup server

show calendar biz-schedule

show calendar holiday

show call-agent

show ccn call application

show ccn call fax incoming

show ccn call route

show ccn document–IVR Only

show ccn engine

show ccn prompts

show ccn reporting historical

show ccn scripts

show ccn sip subscription mwi

show ccn status ccm-manager

show ccn subsystem edbs dbprofile–IVR Only

show ccn subsystem email–IVR Only

show ccn subsystem fax–IVR Only

show ccn subsystem jtapi

show ccn subsystem sip

show ccn trigger all

show ccn trigger http–IVR Only

show ccn trigger jtapi

show ccn trigger sip

script (ccn application)

To specify the script used by the application, use the **script** command in Cisco Unity Express configuration application mode. To delete the script, use the **no** form of this command.

script *script-name* [**description** "*description*"]

no script *script-name*

Syntax Description

script-name	Specifies the script used by the application.
description "description"	(Optional) Specifies an optional description of the script, which must be written in double quotes. The default value for the description is the name of the script.

Defaults

The default description is the name of the script.

Command Modes

Configuration application

Command History

Cisco Unity Express Version	Modification
1.0	This command was introduced on the Cisco Unity Express network module and in Cisco Unified Communications Manager Express 3.0.
1.1	This command was implemented on the advanced integration module (AIM) and in Cisco Unified Communications Manager 3.3(3).
1.1.2	This command was implemented on the Cisco 2800 series and Cisco 3800 series routers.

Examples

The following example assigns the aa.aef file as the script for the Auto Attendant application.

```
se-10-0-0-0# config t
se-10-0-0-0(config)# ccn application autoattendant
se-10-0-0-0(config-application)# script aa.aef description "AutoAttendant Script"
se-10-0-0-0(config-application)# end
se-10-0-0-0(config)# exit
```

Related Commands

Command	Description
ccn application	Configures the CCN applications, such as voice mail and auto attendant.
show ccn application	Displays the CCN application details.

secure-messaging incoming (mailbox)

To label all the incoming messages received by the mailbox as secure, use the **secure-messaging** command in Cisco Unity Express mailbox configuration mode. To remove the security setting from the mailbox, use the **no** form of this command.

secure-messaging incoming

no secure-messaging incoming

Syntax Description

incoming	Specifies that all incoming messages received by this mailbox are labelled secure.

Command Default

Secure messaging is not enabled.

Command Modes

Cisco Unity Express mailbox configuration

Command History

Cisco Unity Express Release	Modification
8.6	This command was introduced.

Usage Guidelines

If secure messaging is enabled, subscribers accessing Cisco Unity Express using the Telephony User Interface (TUI) or VoiceView Express interface can view, forward or send messages marked Secure. Subscribers accessing Cisco Unity Express using the web voicemail interface or through Cisco Unified Personal Communicator must use a secure HTTPS session to view, forward or send messages marked Secure.

Examples

The following example configures the mailbox to support secure messaging of incoming messages:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# voicemailbox owner johnsmith
se-10-0-0-0(config-mailbox)# secure-messaging incoming
```

Related Commands

Command	Description
secure-messaging outgoing (mailbox)	Configures secure messaging settings for all outgoing messages sent from a mailbox.
voicemail secure-messaging outgoing	Configures the global security properties for all outgoing messages.
voicemail secure-messaging (location)	Labels all the incoming messages to a network location as secure.

secure-messaging outgoing (mailbox)

To configure secure messaging settings for all outgoing messages sent from a mailbox, use the **secure-messaging outgoing** command in Cisco Unity Express mailbox configuration mode. To return the mailbox to the default value, use the **no** form of this command.

secure-message outgoing {**always** | **ask** | **never** | **private**}

no secure-message outgoing {**always** | **ask** | **never** | **private**}

Syntax Description

always	All outgoing messages are always marked secure.
ask	Messages are marked secure only when users mark them secure.
never	Messages are never marked secure.
private	Messages are marked secure only when users mark them private.

Command Default

The default is the global secure messaging setting configured using the **voicemail secure-messaging outgoing** command in configuration mode.

Command Modes

Cisco Unity Express mailbox configuration

Command History

Cisco Unity Express Release	Modification
8.6	This command was introduced.

Usage Guidelines

If secure messaging is enabled, subscribers accessing Cisco Unity Express using the Telephony User Interface (TUI) or VoiceView Express interface can view, forward or send messages marked secure. Subscribers accessing Cisco Unity Express using the web voicemail interface or through Cisco Unified Personal Communicator must use a secure HTTPS session to view, forward or send messages marked secure.

Examples

The following example configures the user mailbox so that all outgoing messages are always marked secure:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# voice mailbox owner user8
se-10-0-0-0(config-mailbox)# secure-messaging outgoing always
```

Related Commands

Command	Description
secure-messaging incoming (mailbox)	Labels all the incoming messages received by the mailbox as secure.

Command	Description
voicemail secure-messaging outgoing	Configures the global security properties for all outgoing messages.
voicemail secure-messaging (location)	Labels all the incoming messages to a network location as secure.

security password

To configure system-wide password length and expiry time, use the **security password** command in Cisco Unity Express configuration mode. To reset the password length and expiry time to system defaults, use the **no** or **default** form of this command.

security password {**length min** *password-length* | **expiry days** *password-days*}

no security password {**length min** | **expiry**}

default security password length min

Syntax Description

length min *password-length*	Minimum length of all subscribers' passwords. Valid values range from 3 to 32.
expiry days *password-days*	Maximum number of days for which subscribers' passwords are valid. Valid values range from 3 to 365. If this value is not configured, passwords will not expire.

Defaults

Password length = 3
Passwords do not expire.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
2.1	This command was introduced.

Usage Guidelines

To control security on your system, the password length and expiry times can be configured on a system-wide basis.

- The administrator can configure the length to a value greater than or equal to 3 alphanumeric characters. This is a system-wide value, so all subscribers must have passwords of at least that many characters.
- The password length does not have to equal the PIN length.
- The expiry time is the time, in days, for which the password is valid. When this time is reached, the subscriber must enter a new password.
- If the expiry time is not configured, passwords do not expire.
- The password expiry time does not have to equal the PIN expiry time.
- Additionally, the GUI **Defaults > User** menu option configures these settings.

Examples

The following example sets the password length to 6 characters and the password expiry time to 60 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 password expiry days 60
se-10-0-0-0(config)# end
```

The following example resets the password length to the system default:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# default security password length min
se-10-0-0-0(config)# end
```

The following example resets the password expiry time to the system default:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# no security password expiry
se-10-0-0-0(config)# end
```

Related Commands

Command	Description
security pin	Configures PIN length and expiry time for the local system.
show security detail	Displays the password and PIN settings.

security password history depth

To force all users to choose a password that is not in their password history list, use the **security password history depth** command in Cisco Unity Express configuration mode. Use the **no** form of this command to enable users to choose any password.

security password history depth *depth*

no security password history depth *depth*

Syntax Description

depth	Specifies how many of a user's previous passwords are compared to the new password. Range is from 1 to 10.

Command Default

The system does not track users' password history. The default value for history depth is 1.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

Use the **security password history depth** command in Cisco Unity Express configuration mode to force all users to choose a password that is not in their password history lists. You must also specify how many of the user's previous password are compared to the new password. This value is the "depth" and is an integer ranging from 1 to 10.

Examples

The following example sets the password history depth to 6:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security password history depth 6
```

Related Commands

Command	Description
show security detail	Displays the system-wide password and PIN settings.

security password lockout enable

To enable the password lockout feature, use the **security password lockout enable** command in Cisco Unity Express configuration mode. Use the **no** form of this command to disable the password lockout feature.

security password lockout enable

no security password lockout enable

Syntax Description

This command has no arguments or keywords.

Command Default

The password lockout feature is disabled.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

Use the **security password lockout enable** command in Cisco Unity Express configuration mode to enable the password lockout feature. The **no** form of this command disables the password lockout. When lockout is disabled, the **show security details** command does not display any information related to the password lockout feature.

Examples

The following example enables the password lockout feature:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security password lockout enable
```

Related Commands

Command	Description
show security detail	Displays the system-wide password and PIN settings.
show user detail username	Displays the PIN and password login status for a specific subscriber.

security password lockout policy

To specify whether subscribers are locked out permanently, or temporarily, when the maximum number of failed login attempts is reached, use the **security password lockout policy** command in Cisco Unity Express configuration mode. Use the **no** form of this command to return to the default setting and set the Lockout policy to “temporary.”

security password lockout policy {perm-lock | temp-lock}

no security password lockout policy {perm-lock | temp-lock}

Syntax Description

perm-lock	Subscribers are permanently locked out when the maximum number of failed login attempts is reached.
temp-lock	Subscribers are temporarily locked out when the maximum number of failed login attempts is reached.

Command Default

- Lockout policy is set to **temp-lock**.
- Lockout duration is set 5 minutes.
- Number of initial login attempts is set to 3.
- Number of maximum login attempts is set to 24.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

Use the **security password lockout policy** command in Cisco Unity Express configuration mode to specify whether subscribers are locked out permanently, or temporarily, when the maximum number of failed login attempts is reached. After an account is locked, only the administrator can unlock it and reset the password.

When you change the policy from temporary to permanent, all the configuration values for the temporary locks are reset. The **no** version of this command resets the maximum attempt value for a permanent lock and sets the policy to **temp-lock**.

Examples

The following example sets the lockout policy to **perm-lock**:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security password lockout policy perm-lock
```

Related Commands

Command	Description
show security detail	Displays the system-wide password and PIN settings.
show user detail username	Displays the PIN and password login status for a specific subscriber.

security password perm-lock max-attempts

To configure the maximum number of failed attempts that will trigger a permanent lockout, use the **security password perm-lock max-attempts** command in Cisco Unity Express configuration mode. Use the **no** form of this command to remove the maximum number of failed attempts.

security password perm-lock max-attempts *no_of_max_attempts*

no security password perm-lock max-attempts *no_of_max_attempts*

Syntax Description

no_of_max_attempts	Maximum number of failed attempts allowed before a permanent lockout. Range is from 1 to 200.

Command Default

The maximum number of failed attempts is set to 24.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

To use this command, the lockout policy must be set to **perm-lock**.

Use the **security password perm-lock max-attempts** command in Cisco Unity Express configuration mode to configure the maximum number of failed attempts allowed before an account is permanently locked. After an account is locked, only the administrator can unlock it and reset the password.

The valid range is from 1 to 200.

Examples

The following example sets the maximum number of failed attempts to 6:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security password perm-lock max-attempts 6
```

Related Commands

Command	Description
show security detail	Displays the system-wide password and PIN settings.
show user detail username	Displays the PIN and password login status for a specific subscriber.

security password temp-lock duration

To configure the initial lockout duration for a temporary lockout, use the **security password temp-lock duration** command in Cisco Unity Express configuration mode. Use the **no** form of this command to remove the initial lockout duration.

security password temp-lock duration *duration*

no security password temp-lock duration *duration*

Syntax Description

duration	Initial lockout duration (in minutes) for a temporary lockout. The valid range is from 1 to infinity.

Command Default

The initial lockout duration is set to 5 minutes.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

To use this command, the lockout policy must be set to **temp-lock**.

Use the **security password temp-lock duration** command in Cisco Unity Express configuration mode to configure the initial lockout duration for a temporarily lockout. After an account is locked, only the administrator can unlock it and reset the password.

The valid range is 1 to infinity.

Examples

The following example sets the initial lockout duration to 10:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security password temp-lock duration 10
```

Related Commands

Command	Description
show security detail	Displays the system-wide password and PIN settings.
show user detail username	Displays the PIN and password login status for a specific subscriber.

security password temp-lock init-attempts

To configure the initial number of failed attempts that will trigger a temporary lockout, use the **security password temp-lock init-attempts** command in Cisco Unity Express configuration mode. Use the **no** form of this command to remove the initial number of failed attempts.

security password temp-lock init-attempts *no_of_init_attempts*

no security password temp-lock init-attempts *no_of_init_attempts*

Syntax Description

no_of_init_attempts	Initial number of failed attempts allowed before a temporary lockout. Range is between 1 and the value of *max_attempt*s.

Command Default

The initial number of failed attempts is set to 3.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

To use this command, the lockout policy must be set to **temp-lock**.

Use the **security password temp-lock init-attempts** command in Cisco Unity Express configuration mode to configure the initial number of failed attempts before an account is temporarily locked. The temporary lockout lasts for the amount specified by the **security password temp-lock duration** command.

The number of initial attempts should be less than the number of maximum attempts specified by the command. The valid range is between 1 and the value of *max_attempt*s.

Examples

The following example sets the initial number of failed attempts to 6:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security password temp-lock init-attempts 6
```

Related Commands

Command	Description
security password temp-lock duration	Configures the initial lockout duration for a temporary lockout.
security password temp-lock max-attempts	Configures the maximum number of failed attempts that will trigger a temporary lockout

Command	Description
show security detail	Displays the system-wide password and PIN settings.
show user detail username	Displays the PIN and password login status for a specific subscriber.

security password temp-lock max-attempts

To configure the maximum number of failed attempts that will trigger a temporary lockout, use the **security password temp-lock max-attempts** command in Cisco Unity Express configuration mode. Use the **no** form of this command to remove the maximum number of failed attempts.

security password temp-lock max-attempts *no_of_max_attempts*

no security password temp-lock max-attempts *no_of_max_attempts*

Syntax Description

no_of_max_attempts	Maximum number of failed attempts allowed before a temporary lockout. Range is from the number set for initial attempts to 200.

Command Default

The maximum number of failed attempts is set to 24.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

To use this command, the lockout policy must be set to **temp-lock**.

Use the **security password temp-lock max-attempts** command in Cisco Unity Express configuration mode to configure the maximum number of failed attempts allowed before an account is temporarily locked. After an account is locked, only the administrator can unlock it and reset the password.

The valid range is from the number set for initial attempts to 200.

Examples

The following example sets the maximum number of failed attempts to 6:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security password temp-lock max-attempts 6
```

Related Commands

Command	Description
show security detail	Displays the system-wide password and PIN settings.
show user detail username	Displays the PIN and password login status for a specific subscriber.

security pin

To configure system-wide personal identification number (PIN) length and expiry time, use the **security pin** command in Cisco Unity Express configuration mode. To reset the PIN length and expiry time to system defaults, use the **no** or **default** form of this command.

security pin {**length min** *pin-length* | **expiry days** *pin-days*}

no security pin {**length min** | **expiry**}

default security pin length min

Syntax Description

length min *pin-length*	Minimum length of all subscribers' PINs. Valid values range from 3 to 16.
expiry days *pin-days*	Maximum number of days for which subscribers' PINs are valid. Valid values range from 3 to 365. If this value is not configured, PINs will not expire.

Defaults

PIN length = 3
PINs do not expire.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
2.1	This command was introduced.

Usage Guidelines

To control security on your system, the PIN length and expiry times can be configured on a system-wide basis.

- The administrator can configure the length to a value greater than or equal to 3 alphanumeric characters. This is a system-wide value, so all subscribers must have PINs of at least that many characters.
- The PIN length does not have to equal the password length.
- The expiry time is the time, in days, for which the PIN is valid. When this time is reached, the subscriber must enter a new PIN.
- If the expiry time is not configured, PINs do not expire.
- The PIN expiry time does not have to equal the password expiry time.
- Additionally, the GUI **Defaults > User** menu option configures these settings.

Examples

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

```
se-10-0-0-0# config t
```

```
se-10-0-0-0(config)# security pin length min 5
se-10-0-0-0(config)# security pin expiry days 45
se-10-0-0-0(config)# end
```

The following example resets the PIN length to the system default:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# default security pin length min
se-10-0-0-0(config)# end
```

The following example resets the PIN expiry time to the system default:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# no security pin expiry days
se-10-0-0-0(config)# end
```

Related Commands

Command	Description
security password	Configures password length and expiry time for the local system.
show security detail	Displays the password and PIN settings.

security pin history depth

To force all users to choose a PIN that is not in their PIN history lists, use the **security pin history depth** command in Cisco Unity Express configuration mode. Use the **no** form of this command to enable users to choose any PIN.

security pin history depth *depth*

no security pin history depth *depth*

Syntax Description

depth	Specifies how many of a user's previous PINs are compared to the new PIN. Range is from 1 to 10.

Command Default

The system does not track users' PIN history. The default value for history depth is 1.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

Use the **security pin history depth** command in Cisco Unity Express configuration mode to force all users to choose a PIN that is not in their PIN history lists. You must also specify how many of the user's previous PINs are compared to the new PIN. This value is the "depth" and is an integer ranging from 1 to 10.

Examples

The following example sets the PIN history depth to 6:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security pin history depth 6
```

Related Commands

Command	Description
show security detail	Displays the system-wide password and PIN settings.
show user detail username	Displays the PIN and password login status for a specific subscriber.

security pin lockout enable

To enable the PIN lockout feature, use the **security pin lockout enable** command in Cisco Unity Express configuration mode. Use the **no** form of this command to disable the PIN lockout feature.

security pin lockout enable

no security pin lockout enable

Syntax Description

This command has no arguments or keywords.

Command Default

The PIN lockout feature is disabled.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

Use the **security pin lockout enable** command in Cisco Unity Express configuration mode to enable the PIN lockout feature. The **no** form of this command disables the PIN lockout. When lockout is disabled, the **show security details** command does not display any information related to the PIN lockout feature.

Examples

The following example enables the PIN lockout feature:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security pin lockout enable
```

Related Commands

Command	Description
show security detail	Displays the system-wide password and PIN settings.
show user detail username	Displays the PIN and password login status for a specific subscriber.

security pin lockout policy

To specify whether subscribers are locked out permanently, or temporary, when the maximum number of failed login attempts is reached, use the **security pin lockout policy** command in Cisco Unity Express configuration mode. Use the **no** form of this command to return to the default setting and set the lockout policy to "temporary."

security pin lockout policy {perm-lock | temp-lock}

no security pin lockout policy {perm-lock | temp-lock}

Syntax Description

perm-lock	Subscribers are permanently locked out when the maximum number of failed login attempts is reached.
temp-lock	Subscribers are temporarily locked out when the maximum number of failed login attempts is reached.

Command Default

- Lockout policy is set to **temp-lock**.
- Lockout duration is set 5 minutes.
- Number of initial login attempts is set to 3.
- Number of maximum login attempts is set to 24.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

Use the **security pin lockout policy** command in Cisco Unity Express configuration mode to specify whether subscribers are locked out permanently, or temporary, when the maximum number of failed login attempts is reached. After an account is locked, only the administrator can unlock it and reset the PIN.

When you change the policy from temporary to permanent, all the configuration values for the temporary locks are reset. The **no** version of this command resets the maximum attempt value for a permanent lock and sets the policy to **temp-lock**.

Examples

The following example sets the lockout policy to **perm-lock**:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security pin lockout policy perm-lock
```

Related Commands

Command	Description
show security detail	Displays the system-wide password and PIN settings.
show user detail username	Displays the PIN and password login status for a specific subscriber.

security pin perm-lock max-attempts

To configure the maximum number of failed attempts that will trigger a permanent lockout, use the **security pin perm-lock max-attempts** command in Cisco Unity Express configuration mode. Use the **no** form of this command to remove the maximum number of failed attempts.

security pin perm-lock max-attempts *no_of_max_attempts*

no security pin perm-lock max-attempts *no_of_max_attempts*

Syntax Description

no_of_max_attempts	Maximum number of failed attempts allowed before a permanent lockout. Range is from 1 to 200.

Command Default

The maximum number of failed attempts is set to 24.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

To use this command, the lockout policy must be set to **perm-lock**.

Use the **security pin perm-lock max-attempts** command in Cisco Unity Express configuration mode to configure the maximum number of failed attempts allowed before an account is permanently locked. After an account is locked, only the administrator can unlock it and reset the PIN.

The valid range is 1 to 200.

Examples

The following example sets the maximum number of failed attempts to 6:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security pin perm-lock max-attempts 6
```

Related Commands

Command	Description
show security detail	Displays the system-wide password and PIN settings.
show user detail username	Displays the PIN and password login status for a specific subscriber.

security pin temp-lock duration

To configure the initial lockout duration for a temporary lockout, use the **security pin temp-lock duration** command in Cisco Unity Express configuration mode. Use the **no** form of this command to remove the initial lockout duration.

security pin temp-lock duration *duration*

no security pin temp-lock duration *duration*

Syntax Description

duration	Initial lockout duration (in minutes) for a temporary lockout. The valid range is from 1 to infinity.

Command Default

The initial lockout duration is set to 5.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

To use this command, the lockout policy must be set to **temp-lock**.

Use the **security pin temp-lock duration** command in Cisco Unity Express configuration mode to configure the initial lockout duration for a temporarily lockout. After an account is locked, only the administrator can unlock it and reset the PIN.

The valid range is 1 to infinity.

Examples

The following example sets the initial lockout duration to 10:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security pin temp-lock duration 10
```

Related Commands

Command	Description
show security detail	Displays the system-wide password and PIN settings.
show user detail username	Displays the PIN and password login status for a specific subscriber.

security pin temp-lock init-attempts

To configure the initial number of failed attempts that will trigger a temporary lockout, use the **security pin temp-lock init-attempts** command in Cisco Unity Express configuration mode. Use the **no** form of this command to remove the initial number of failed attempts.

security pin temp-lock init-attempts *no_of_init_attempts*

no security pin temp-lock init-attempts *no_of_init_attempts*

Syntax Description

no_of_init_attempts	Initial number of failed attempts allowed before a temporary lockout. Range is between 1 and the number set for maximum attempts.

Command Default

The initial number of failed attempts is set to 3.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

To use this command, the lockout policy must be set to **temp-lock**.

Use the **security pin temp-lock init-attempts** command in Cisco Unity Express configuration mode to configure the initial number of failed attempts before an account is temporarily locked. The temporary lockout lasts for the amount specified by the **security pin temp-lock duration** command.

The number of initial attempts should be less than the number of maximum attempts as set by the command.

The valid range is between 1 and the number set for maximum attempts.

Examples

The following example sets the initial number of failed attempts to 6:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security pin temp-lock init-attempts 6
```

Related Commands

Command	Description
security pin temp-lock duration	Configures the initial lockout duration for a temporary lockout.
security pin temp-lock max-attempts	Configures the maximum number of failed attempts that will trigger a temporary lockout

Command	Description
show security detail	Displays the system-wide password and PIN settings.
show user detail username	Displays the PIN and password login status for a specific subscriber.

security pin temp-lock max-attempts

To configure the maximum number of failed attempts that will trigger a temporary lockout, use the **security pin temp-lock max-attempts** command in Cisco Unity Express configuration mode. Use the **no** form of this command to remove the maximum number of failed attempts.

security pin temp-lock max-attempts *no_of_max_attempts*

no security pin temp-lock max-attempts *no_of_max_attempts*

Syntax Description

no_of_max_attempts	Maximum number of failed attempts allowed before a temporary lockout. Range is from the number set for initial attempts to 200.

Command Default

Maximum number of failed attempts is set to 24.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

To use this command, the lockout policy must be set to **temp-lock**.

Use the **security pin temp-lock max-attempts** command in Cisco Unity Express configuration mode to configure the maximum number of failed attempts allowed before an account is temporarily locked. After an account is locked, only the administrator can unlock it and reset the PIN.

The valid range is from the number set for initial attempts to 200.

Examples

The following example sets the maximum number of failed attempts to 6:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security pin temp-lock max-attempts 6
```

Related Commands

Command	Description
show security detail	Displays the system-wide password and PIN settings.
show user detail username	Displays the PIN and password login status for a specific subscriber.

security pin trivialcheck

To enable the PIN security validation feature, use the **security pin trivialcheck** command in Cisco Unity Express configuration mode. Use the **no** form of this command to disable the PIN security validation feature.

security pin trivialcheck

no security pin trivialcheck

Syntax Description

This command has no arguments or keywords.

Command Default

The PIN trivialcheck validation feature is disabled.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
8.6.4	This command was introduced.

Usage Guidelines

Use the **security pin trivialcheck** command in Cisco Unity Express configuration mode to enable the PIN security validation feature. The **no** form of this command disables the “PIN trivialcheck” validation.

The **show security detail** command indicates whether the PIN trivialcheck feature is enabled or disabled. The **show running-config** command output contains “security pin trivialcheck” if the PIN trivialcheck feature is enabled; if the feature is disabled, the output does not contain any indication of the feature.

This feature enforces additional validations for a new PIN requested by a user. When the feature is not enabled, a smaller set of validations is enforced.

Validation	Enforced at all times	Enforced when PIN trivialcheck enabled
PIN cannot contain any other characters other than digits from 0 to 9.	Y	Y
PIN cannot contain digits less than the minimum length of PIN configured.	Y	Y
PIN cannot contain more than maximum length for PIN: 16 digits.	Y	Y
Previous n number of PINs cannot be reused if history depth is set to n.	Y	Y
The PIN cannot match the numeric representation of the first or last name of the user.		Y

Validation	Enforced at all times	Enforced when PIN trivialcheck enabled
The PIN cannot contain the primary or alternate phone extensions of the user.		Y
The PIN cannot contain the reverse of the primary or alternate phone extensions of the user.		Y
The PIN cannot contain groups of repeated digits, such as "408408" or "123123."		Y
The PIN cannot contain only two different digits, such as "121212."		Y
A digit cannot be used more than two times consecutively, such as "28883."		Y
The PIN cannot be an ascending or descending group of digits, such as "012345" or "987654."		Y
The PIN cannot contain a group of numbers that are dialed in a straight line on the keypad when the group of digits equals the minimum credential length that is allowed. For example, if 3 digits are allowed, the user could not use "123," "456," or "789" as a PIN.		Y

Examples

The following example enables the PIN trivialcheck validation feature:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security pin trivialcheck
```

Related Commands

Command	Description
security pin	Configures system-wide PIN length and expiry time.
show security detail	Displays the system-wide password and PIN settings.
show user detail username	Displays the PIN and password login status for a specific subscriber.

security ssh

To configure system-wide SSH length and expiry time, use the **security ssh** command in Cisco Unity Express configuration mode. To reset the PIN length and expiry time to system defaults, use the **no** or **default** form of this command.

security ssh {**length min** *ssh-length* | **expiry days** *ssh-days*}

no security ssh {**length min** | **expiry**}

default security ssh length min

Syntax Description

length min *ssh-length*	Minimum length of all subscribers' SSHs. Valid values range from 3 to 16.
expiry days *ssh-days*	Maximum number of days for which subscribers' PINs are valid. Valid values range from 3 to 365. If this value is not configured, SSHs will not expire.

Defaults

SSH length = 3
SSHs do not expire.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
2.1	This command was introduced.

Usage Guidelines

To control security on your system, the SSH length and expiry times can be configured on a system-wide basis.

- The administrator can configure the length to a value greater than or equal to 3 alphanumeric characters. This is a system-wide value, so all subscribers must have SSHs of at least that many characters.
- The SSH length does not have to equal the password length.
- The expiry time is the time, in days, for which the SSH is valid. When this time is reached, the subscriber must enter a new SSH.
- If the expiry time is not configured, SSHs do not expire.
- The SSH expiry time does not have to equal the password expiry time.
- Additionally, the GUI **Defaults > User** menu option configures these settings.

Examples

The following example sets the SSH length to 5 characters and the SSH expiry time to 45 days.

```
se-10-0-0-0# config t
```

```
se-10-0-0-0(config)# security ssh length min 5
se-10-0-0-0(config)# security ssh expiry days 45
se-10-0-0-0(config)# end
```

The following example resets the SSH length to the system default:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# default security ssh length min
se-10-0-0-0(config)# end
```

The following example resets the SSH expiry time to the system default:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# no security ssh expiry days
se-10-0-0-0(config)# end
```

Related Commands

Command	Description
security password	Configures password length and expiry time for the local system.
show security detail	Displays the password and SSH settings.

security ssh knownhost

To configure the MD5 (Message-Digest algorithm 5) fingerprint and type of host key for the SSH (Secure Shell) server's host key, use the **security ssh** command in Cisco Unity Express configuration mode. Use the **no** form of this command to remove the MD5 fingerprint.

security ssh knownhost *host* **{ssh-rsa | ssh-dsa}** *fingerprint-string*

no security ssh knownhost *host* **{ssh-rsa | ssh-dsa}** *fingerprint-string*

Syntax Description

host	Hostname or IP address of the SSH server.
ssh-rsa	The RSA encryption algorithm was used to create this fingerprint for an SSH server's host key.
ssh-dsa	The DSA (Digital Signature Algorithm) was used to create this fingerprint for an SSH server's host key.
fingerprint-string	MD5 fingerprint string.

Command Default

No server authentication performed for the specified host.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

Use the **security ssh** command in Cisco Unity Express configuration mode to configure the MD5 fingerprint of the SSH server's host key. When the fingerprint is configured, the local SSH/SFTP client performs server authentication by comparing the configured fingerprint with the one returned from the SSH server.

The *host* argument can be either a hostname or a IP address.

If the fingerprint is not configured, no server authentication is performed. The fingerprint will not be saved in the startup configuration when you use the **write** command.

Examples

The following example specifies the MD5 fingerprint of a SSH-RSA server's host key:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# security ssh knownhost server.cisco.com ssh-rsa
a5:3a:12:6d:e9:48:a3:34:be:8f:ee:50:30:e5:e6:c3
```

Related Commands

Command	Description
backup server authenticate	Retrieves the fingerprint of the backup server’s host key.
show security ssh known-hosts	Displays a list of configured SSH (Secure Shell) servers and their fingerprints.

service imap

To enter the IMAP configuration mode for configuring IMAP parameters, use the **service imap** command in Cisco Unity Express configuration mode. To set all IMAP parameters to their default values and to disable the IMAP feature, use the **no** form of this command.

service imap

no service imap

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
2.3	This command was introduced.
3.0	This command was implemented on the advanced integration module (AIM).

Usage Guidelines

This command is not available on the AIM in version 2.3 and earlier.

Examples

The following example enters the IMAP configuration mode:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# service imap
se-10-0-0-0(config-imap)#
```

Related Commands

Command	Description
enable (IMAP)	Enables the IMAP feature.
groupname	Configures voice-mail group parameters.
maxsessions (IMAP)	Sets the maximum number of concurrent IMAP sessions.
session idletimeout (IMAP)	Specifies the IMAP session idletimeout value.
session security	Sets the IMAP client connection type.
show imap configuration	Displays all IMAP configuration parameters.
show imap sessions	Displays all active IMAP sessions.

service phone-authentication

To enter the VoiceView Express authentication mode, use the **service phone-authentication** command in Cisco Unity Express configuration mode. To disable service phone authentication, use the **no** form of this command.

service phone-authentication

no service phone-authentication

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default value.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
2.3	This command was introduced.
3.0	This command was implemented on the advanced integration module (AIM).

Usage Guidelines

This command is not available on the AIM in version 2.3 and earlier.

Examples

The following example enters VoiceView Express authentication mode:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# service phone-authentication
se-10-0-0-0(config-phone-authentication)#
```

Related Commands

Command	Description
enable (VoiceView Express)	Enables the VoiceView Express feature.
fallback-url (Cisco Unified Communications Manager Express Only)	Configures a fallback authentication server.
service voiceview	Enters VoiceView Express configuration mode.
service voiceview session terminate	Terminates an active VoiceView Express session.
session idletimeout (VoiceView Express)	Specifies the VoiceView Express session idletimeout value.
show phone-authentication configuration	Displays the VoiceView Express phone authentication parameters.

Command	Description
show voiceview configuration	Displays all VoiceView Express configuration parameters.
show voiceview sessions	Displays all active VoiceView Express sessions.

service voiceview

To enter VoiceView Express configuration mode for configuring VoiceView Express parameters, use the **service voiceview** command in Cisco Unity Express configuration mode. To set all VoiceView Express parameters to their default values, use the **no** form of this command.

service voiceview

no service voiceview

Syntax Description

This command has no arguments or keywords.

Defaults

VoiceView Express parameters are set to their default values.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
2.3	This command was introduced.
3.0	This command was implemented on the advanced integration module (AIM).

Usage Guidelines

This command is not available on the AIM in version 2.3 and earlier.

Examples

The following example enters VoiceView Express configuration mode:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# service voiceview
se-10-0-0-0(config-voiceview)#
```

Related Commands

Command	Description
enable (VoiceView Express)	Enables the VoiceView Express feature.
fallback-url (Cisco Unified Communications Manager Express Only)	Configures a fallback authentication server.
service phone-authentication	Enters VoiceView Express phone authentication mode.
service voiceview session terminate	Terminates an active VoiceView Express session.
session idletimeout (VoiceView Express)	Specifies the VoiceView Express session idletimeout value.
show phone-authentication configuration	Displays the VoiceView Express phone authentication parameters.

Command	Description
show voiceview configuration	Displays all VoiceView Express configuration parameters.
show voiceview sessions	Displays all active VoiceView Express sessions.

service voiceview session terminate

To terminate an active VoiceView Express session, use the **service voiceview session terminate** command in Cisco Unity Express EXEC mode.

service voiceview session terminate mailbox *mailbox-id*

Syntax Description

mailbox *mailbox-id*	ID of the mailbox that has the active VoiceView Express session.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
2.3	This command was introduced.
3.0	This command was implemented on the advanced integration module (AIM).

Usage Guidelines

This command is not available on the AIM in version 2.3 and earlier.

The system displays an error message if no VoiceView Express session is active for the mailbox or if the mailbox ID is invalid.

.The command does not display any message indicating the session was terminated.

Examples

The following illustrates the **service voiceview session terminate** command:

```
se-10-0-0-0# service voiceview session terminate mailbox user1
se-10-0-0-0#
```

Related Commands

Command	Description
enable (VoiceView Express)	Enables the VoiceView Express feature.
fallback-url (Cisco Unified Communications Manager Express Only)	Configures a fallback authentication server.
service phone-authentication	Enters VoiceView Express phone authentication mode.
service voiceview	Enters VoiceView Express configuration mode.
session idletimeout (VoiceView Express)	Specifies the VoiceView Express session idletimeout value.
show phone-authentication configuration	Displays the VoiceView Express phone authentication parameters.
show voiceview configuration	Displays all VoiceView Express configuration parameters.
show voiceview sessions	Displays all active VoiceView Express sessions.

session idletimeout (IMAP)

To set the inactivity timeout interval for IMAP sessions, use the **session idletimeout** command in IMAP configuration mode. To set the idletimeout to the default value, use the **no** or **default** form of this command.

session idletimeout *minutes*

no session idletimeout

default session idletimeout

Syntax Description

minutes	Number of minutes of inactivity for each IMAP session. Valid values are 30 to 120 minutes. The default value is 30 minutes.

Defaults

Idletimeout is 30 minutes.

Command Modes

IMAP configuration

Command History

Cisco Unity Express Version	Modification
2.3	This command was introduced.
3.0	This command was implemented on the advanced integration module (AIM).

Usage Guidelines

This command is not available on the AIM in version 2.3 and earlier.

Restart the IMAP server after changing any IMAP configuration parameters so that the new parameter values become active.

Examples

The following example sets the IMAP session idletimeout value to 45 minutes:

```
se-10-0-0-0#config t
se-10-0-0-0(config)# service imap
se-10-0-0-0(config-imap)# session idletimeout 45
```

Related Commands

Command	Description
enable (IMAP)	Enables the IMAP feature.
groupname	Configures voice-mail group parameters.
maxsessions (IMAP)	Sets the maximum number of concurrent IMAP sessions.
service imap	Enters IMAP configuration mode.
session security	Sets the IMAP client connection type.

Command	Description
show imap configuration	Displays all IMAP configuration parameters.
show imap sessions	Displays all active IMAP sessions.

session idletimeout (VoiceView Express)

To set the inactivity timeout interval for VoiceView Express sessions, use the **session idletimeout** command in VoiceView Express configuration mode. To set the idletimeout to the default, use the **no** or **default** form of this command.

session idletimeout *minutes*

no session idletimeout

default session idletimeout

Syntax Description

minutes	Number of minutes of inactivity for each VoiceView Express session. Valid values are 5 to 30 minutes. The default value is 5 minutes.

Defaults

Idletimeout is 5 minutes.

Command Modes

VoiceView Express configuration

Command History

Cisco Unity Express Version	Modification
2.3	This command was introduced.
3.0	This command was implemented on the advanced integration module (AIM).

Usage Guidelines

This command is not available on the AIM in version 2.3 and earlier.

After a VoiceView Express session is idle for the configured number of minutes, the system disconnects the session.

The timeout is a system-wide parameter and cannot be configured for individual subscribers or groups.

Examples

The following example sets the VoiceView Express session idletimeout value to 15 minutes:

```
se-10-0-0-0#config t
se-10-0-0-0(config)# service voiceview
se-10-0-0-0(config-voiceview)# session idletimeout 15
```

Related Commands

Command	Description
enable (VoiceView Express)	Enables the VoiceView Express feature.
fallback-url (Cisco Unified Communications Manager Express Only)	Configures a fallback authentication server.

Command	Description
service phone-authentication	Enters VoiceView Express phone authentication mode.
service voiceview	Enters VoiceView Express configuration mode.
service voiceview session terminate	Terminates an active VoiceView Express session.
show phone-authentication configuration	Displays the VoiceView Express phone authentication parameters.
show voiceview configuration	Displays all VoiceView Express configuration parameters.
show voiceview sessions	Displays all active VoiceView Express sessions.

session security

To configure the type of permitted connections from IMAP clients, use the **session security** command in IMAP configuration mode. To set the connection type to none, use the **no** or **default** form of this command.

session security {**ssl** | **none** | **mixed** | **keylabel** *labelname*}

no session security

default session security

Syntax Description

ssl	Permits only SSL connections from IMAP clients.
none	Permits only non-SSL connections from IMAP clients.
mixed	Permits both SSL and non-SSL connections from IMAP clients.
keylabel *labelname*	Associates the certificate-key pair to the SSL connection.

Defaults

The default value is none.

Command Modes

IMAP configuration

Command History

Cisco Unity Express Version	Modification
2.3	This command was introduced.
3.0	This command was implemented on the advanced integration module (AIM).
3.2	The **keyLabel** keyword was added.

Usage Guidelines

This command is not available on the AIM in version 2.3 and earlier.

Before configuring the connection type, the system must have a default security certificate and private key. Use the **crypto key generate** command to generate the pair of values.

Beginning with Cisco Unity Express 3.2, the **keyLabel** keyword is used to associate a certificate-key pair to the IMAP functionality, which uses the certificate-key pair for SSL connections. This option should be set before configuring the SSL connection. If this option is not specified, then IMAP uses the default certificate-key.

Examples

The following example sets the IMAP connection type to SSL only:

```
se-10-0-0-0#config t
se-10-0-0-0(config)# service imap
se-10-0-0-0(config-imap)# session security ssl
```

The following example associates a certificate-key pair to the SSL connection:

```
se-10-0-0-0#config t
se-10-0-0-0(config)# service imap
se-10-0-0-0(config-imap)# session security keyLabel alphakey.myoffice
se-10-0-0-0(config-imap)# session security ssl
```

Related Commands

Command	Description
crypto key generate	Generates a certificate-private key pair.
enable (IMAP)	Enables the IMAP feature.
groupname	Configures voice-mail group parameters.
maxsessions (IMAP)	Sets the maximum number of concurrent IMAP sessions.
service imap	Enters IMAP configuration mode.
show imap configuration	Displays all IMAP configuration parameters.
show imap sessions	Displays all active IMAP sessions.

show aaa accounting event

To show the AAA accounting events that are designated to be logged, use the **show aaa accounting event** command in Cisco Unity Express EXEC mode.

show aaa accounting event

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
7.0	This command was introduced.

Usage Guidelines

Table 7 describes the information displayed by this command:

Table 6 show aaa accounting event Field Descriptions

Field	Description
Event	Type of AAA accounting event.
State	Whether logging is enabled for this type of accounting event.
Description	Description of this type of accounting event.

Examples

The following example shows the output for the **show aaa accounting event** command:

```
se-10-0-0-0# show aaa accounting event
Event                  State      Description
login                  Enabled    Log accounting events for successful login
logout                 Enabled    Log accounting events for user logout
login-fail             Enabled    Log accounting events for failed login attempts
config-commands        Enabled    Log accounting events for any changes to configuration
exec-commands          Enabled    Log accounting events for execution of commands
system-startup         Enabled    Log accounting events for system startup
system-shutdown        Enabled    Log accounting events for system shutdown
imap                   Disabled   Log accounting events for all imap events
```

Related Commands

Command	Description
aaa accounting event	Enters AAA accounting submode and configures event filtering for accounting packets.

show aaa accounting service

To show the login information configured for the AAA accounting server, use the **show aaa accounting service** command in Cisco Unity Express EXEC mode.

show aaa accounting service

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
7.0	This command was introduced.

Usage Guidelines

Examples

The following example shows the output for the **show aaa accounting service** command:

```
se-10-0-0-0# show aaa accounting service
Accounting: Enabled
Address: 192.168.12.22 Port: 1813 Credentials:
woYLtSq19jEOBNL8wg+WB0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGW
TYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmP
Address: 192.168.12.57 Port: 1813 Credentials:
woYLtSq19jEOBNL8wg+WB0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGW
TYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmP
Timeout: 5 (sec)
Retries: 3
```

Table 7 describes the information displayed by this command:

Table 7 show aaa accounting service Field Descriptions

Field	Description
Accounting	Whether AAA accounting logging is enabled.
Address	IP address or DNS hostname of the AAA accounting server.
Port	Port number of the AAA accounting server.
Credentials	Credentials required to access the AAA accounting server.

Table 7 show aaa accounting service Field Descriptions (continued)

Field	Description
Timeout	Amount of time before an AAA authentication request is considered to be unanswered.
Retries	Maximum number of times an AAA authentication request is retried before the authentication fails.

Related Commands

Command	Description
aaa accounting server remote	Enters aaa-accounting submode and configures the AAA accounting server.

show aaa policy

To show the AAA policy settings, use the **show aaa policy** command in Cisco Unity Express EXEC mode.

show aaa policy

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
7.0	This command was introduced.

Usage Guidelines

Examples

The following example shows the output for the **show aaa policy** command:

```
se-10-0-0-0# show aaa policy
AAA policy:system
 authentication-order local
 merge-attributes enable
 preferred-server remote
AAA server: remote
 retries 3
 timeout 5
```

Table 8 describes the information displayed by this command:

Table 8 show aaa accounting policy Field Descriptions

Field	Description
authentication-order	The order in which to query the remote RADIUS authentication server and the local authentication database.
merge-attributes	Whether the user attributes that are retrieved from an AAA server will be merged with attributes for the same username found in the local user database.
preferred-server	Whether the preferred authentication server is local or remote.
AAA server	Whether the AAA authentication server is local or remote.

Table 8 show aaa accounting policy Field Descriptions (continued)

Field	Description
retries	Maximum number of times an AAA authentication request is retried before the authentication fails.
timeout	Amount of time before an AAA authentication request is considered to be unanswered.

Related Commands

Command	Description
show aaa accounting event	Enters aaa-policy submode and configures the system AAA policy.

show backup

To display information about the server that is used to store backup files, use the **show backup** command in Cisco Unity Express EXEC mode.

show backup

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
1.0	This command was introduced on the Cisco Unity Express network module and in Cisco Unified Communications Manager Express 3.0.
1.1	This command was implemented on the advanced integration module (AIM) and in Cisco Unified Communications Manager 3.3(3).
1.1.2	This command was implemented on the Cisco 2800 series and Cisco 3800 series routers.

Usage Guidelines

This command displays the FTP server URL, the subscriber account on the FTP server, and the number of backup file revisions that are to be stored on the server.

Examples

The following is sample output from the **show backup** command:

```
se-10-0-0-0# show backup

Server URL:                              ftp://10.12.0.1/ftp
User Account on Server:
Number of Backups to Retain:             5
```

Table 9 describes the significant fields shown in the display.

Table 9 show backup Field Descriptions

Field	Description
Server URL	IP address of the backup server.
User Account on Server	(Optional) User ID on the backup server.
Number of Backups to Retain	Number of backup files to store before the oldest one is overwritten.

Related Commands

Command	Description
show backup schedule detail job	Shows details for all recurring scheduled backup jobs.

show backup history

To display the success or failure of backup and restore procedures, use the **show backup history** command in Cisco Unity Express EXEC mode.

show backup history

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
1.0	This command was introduced on the Cisco Unity Express network module and in Cisco Unified Communications Manager Express 3.0.
1.1	This command was implemented on the AIM and in Cisco Unified Communications Manager 3.3(3).
8.0	This command was modified to show information about past backups only. Beginning with this release, past restores are shown using the **show restore history** command. In addition, new fields for showing the Schedule type and backup Version were added.

Usage Guidelines

This command displays each backup file, its backup ID, the type of data stored in the file, and the success or failure of the backup procedure.

Note If the backup/restore fails because the FTP server is not reachable, the failure is not logged in the backup/restore history.

The following is sample output from the **show backup history** command for versions 7.1 and earlier:

```
se-10-0-0-0# show backup history

#Start Operation
Category:      Configuration
Backup Server: ftp://10.100.10.215/CUE_backup
Operation:     Backup
Backupid:      2
Restoreid:     -1
Description:   test backup 1
Date:          Sun Jun 13 12:32:48 PDT 1993
Result:        Success
Reason:
#End Operation

#Start Operation
Category:      Data
Backup Server: ftp://10.100.10.215/CUE_backup
Operation:     Backup
```

```
Backupid:      2
Restoreid:     -1
Description:   CUE test backup
Date:          Sun Jun 13 12:32:57 PDT 1993
Result:        Success
Reason:
#End Operation

#Start Operation
Category:      Configuration
Backup Server: ftp://10.100.10.215/CUE_backup
Operation:     Restore
Backupid:      2
Restoreid:     1
Description:
Date:          Sun Jun 13 12:37:52 PDT 1993
Result:        Success
Reason:
#End Operation

#Start Operation
Category:      Data
Backup Server: ftp://10.100.10.215/CUE_backup
Operation:     Restore
Backupid:      2
Restoreid:     1
Description:
Date:          Sun Jun 13 12:38:00 PDT 1993
Result:        Success
Reason:
#End Operation
```

The following is sample output from the **show backup history** command for versions 8.0 and later:

```
se-10-0-0-0# show backup history

aaa# show backup history
#Start Operation
Category: Configuration
Backup Server: ftp://192.1.1.31/backups
Operation: Backup
Backupid: 7
Date: Wed Feb 17 23:19:48 EST 2010
Result: Success
Reason:
Version: 8.0.0.1
#End Operation

#Start Operation
Category: Data
Backup Server: ftp://192.1.1.31/backups
Operation: Backup
Backupid: 7
Date: Wed Feb 17 23:19:48 EST 2010
Result: Success
Reason:
Version: 8.0.0.1
#End Operation

#Start Operation
Category: HistoricalData
Backup Server: ftp://192.1.1.31/backups
Operation: Backup
Backupid: 7
```

```
Date: Wed Feb 17 23:19:49 EST 2010
Result: Success
Reason:
Version: 8.0.0.1
#End Operation

#Start Operation
Category: Configuration
Backup Server: ftp://192.1.1.31/backups
Operation: Backup
Backupid: 8
Date: Fri Feb 19 14:36:33 EST 2010
Result: Success
Reason:
Version: 8.0.0.1
#End Operation
```

Table 10 describes the significant fields shown in the display.

Table 10 show backup history Field Descriptions

Field	Description
Category	Specifies the type of file (data, configuration, or all) that was backed up.
Backup Server	Backup server location.
Operation	Type of operation performed.
Backupid	ID number of the backup file.
Restoreid	ID to use to restore this file. **Note** Beginning with Cisco Unity Express 8.0, this command no longer shows restore information. See the **show restore history** command.
Description	Optional description of the backup procedure.
Date	Date and time (in hh:mm:ss) when the operation occurred.
Result	Indication of success or failure of the operation.
Reason	If the operation failed, this field gives the reason for the failure.
Version	Specifies the scheduled backup version. This field was added in Cisco Unity Express version 8.0.

Related Commands

Command	Description
backup	Selects the backup data and initiates the backup process.
show backup server	Displays the backup file ID.
show restore history	Displays the success or failure of restore operations.

show backup schedule detail job

To display the details of the specified recurring scheduled backup job, use the **show backup schedule detail job** command in Cisco Unity Express EXEC mode.

show backup schedule detail job *job-name*

Syntax Description

job-name	Specifies the name of the scheduled backup job to display.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
7.1	This command was introduced.

Examples

The following example displays information for the specified recurring scheduled backup job:

```
se-10-0-0-0# show backup schedule detail job job-8

Name          job-8
Description   main backup
Categories   TimeCardView Configuration Data HistoricalData
Schedule      Daily at 06:00
Last Run      Jan 1, 2009 at 6:00
Last Result   Success
Next Run      Jan 2, 2009 at 6:00
Active        from Jan 01, 2000 until Dec 31, 2009
```

Table 11 describes the significant fields shown in the display.

Table 11 show backup schedule detail job Field Descriptions

Field	Description
Name	Name of the scheduled backup job.
Description	Description of the scheduled backup job.
Categories	Categories of information that will be backed up.
Schedule	When the backup job is scheduled to occur.
Last Run	Date and time the last backup occurred
Last Result	Result of the last scheduled backup job.
Next Run	Date and time the next backup will occur
Active	Time period when the scheduled backup job is active.

Related Commands

Command	Description
backup schedule	Enters commands enters backup-schedule submode.
show backup schedule detail job	Shows details for all recurring scheduled backup jobs.

show backup schedules

To display the details of all recurring scheduled backup jobs configured on the local system, use the **show backup schedules** command in Cisco Unity Express EXEC mode.

show backup schedules

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
7.1	This command was introduced.

Examples

The following example displays the details of all recurring scheduled backup jobs:

```
se-10-0-0-0# show backup schedules

Name         Schedule                 Next Run       Description   Categories
A22          NOT SET                  NEVER
backup1000   Every 1 days at 12:34    Jun 25, 2002 12:34           Data
Total: 2
```

Table 12 describes the significant fields shown in the display.

Table 12 show backup schedules Field Descriptions

Field	Description
Name	Name of the scheduled backup job.
Schedule	When the backup job is scheduled to occur.
Next Run	Date and time the next backup will occur
Description	Description of the scheduled backup job.
Categories	Categories of information that will be backed up.

Related Commands

Command	Description
backup schedule	Enters commands enters backup-schedule submode.
show backup schedule detail job	Shows details for the specified recurring scheduled backup job.

show backup server

To display the details of the most recent backup files, use the **show backup server** command in Cisco Unity Express EXEC mode.

show backup server

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
1.0	This command was introduced on the Cisco Unity Express network module and in Cisco Unified Communications Manager Express 3.0.
1.1	This command was implemented on the AIM and in Cisco Unified Communications Manager 3.3(3).
8.0	New fields for showing the Schedule type and backup Version were added.

Usage Guidelines

This command displays a list of the backup files available on the backup server. The files are grouped by category, with the date of each backup and the backup file ID. For information on the success or failure of a backup procedure, see the **show backup history** command.

Examples

The following is sample output for the **show backup server** command:

```
se-10-0-0-0# show backup server

aaa# show backup server
Category: Data
Details of last 5 backups
Backupid: 1
Date: Thu Oct 29 23:48:06 UTC 2009
Software Ver: 8.0.0.1

Backupid: 6
Date: Sat Feb 06 12:31:40 EST 2010
Software Ver: 8.0.0.1

Backupid: 7
Date: Wed Feb 17 23:19:48 EST 2010
Software Ver: 8.0.0.1



Category: Configuration
Details of last 5 backups
Backupid: 4
```

```
Date: Tue Jan 12 08:35:14 EST 2010
Software Ver: 8.0.0.1

Backupid: 5
Date: Mon Jan 25 14:10:31 EST 2010
Software Ver: 8.0.0.1

Backupid: 6
Date: Sat Feb 06 12:31:40 EST 2010
Software Ver: 8.0.0.1

Backupid: 7
Date: Wed Feb 17 23:19:48 EST 2010
Software Ver: 8.0.0.1

Backupid: 8
Date: Fri Feb 19 14:36:33 EST 2010
Software Ver: e 8.0.0.1
```

Table 13 describes the significant fields shown in the display.

Table 13 show backup server Field Descriptions

Field	Description
Category	Type of backup file.
Backupid	ID number of the backup file.
Date	Date and time (in hh:mm:ss) when the file was backed up.
Description	Optional description of the backup file.

Related Commands

Command	Description
backup	Selects the backup data and initiates the backup process.
show backup history	Displays the success or failure of backup and restore procedures.

show calendar biz-schedule

To display the business-hours schedules, use the **show calendar biz-schedule** command in Cisco Unity Express EXEC mode.

show calendar biz-schedule {*schedule-name* | **all**}

Syntax Description

schedule-name	Name of a business-hours schedule to be displayed.
all	Displays all the business-hours schedules configured on the local system.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
2.1	This command was introduced.

Usage Guidelines

Use the **calendar biz-schedule** command to create a business-hours schedule.

Examples

The following example displays the holiday-hours business-hours schedule:

```
se-10-0-0-0# show calendar biz-schedule holiday-season

******************************
Schedule: holiday-season
Day                 Open Hours
-------------------------------
Sunday              09:00 to 15:00
Monday              08:30 to 17:30
Tuesday             08:30 to 17:30
Wednesday           08:30 to 17:30
Thursday            08:00 to 21:00
Friday              08:00 to 21:00
Saturday            08:00 to 21:30
```

The following example displays all the business-hours schedules configured on the local system, including the default schedule SystemSchedule:

```
sse-10-0-0-0# show calendar biz-schedule all

******************************
Schedule: systemschedule
Day                 Open Hours
-------------------------------
Sunday              Open all day
Monday              Open all day
Tuesday             Open all day
Wednesday           Open all day
Thursday            Open all day
Friday              Open all day
Saturday            Open all day
```

```
******************************
Schedule: normal
Day                 Open Hours
-------------------------------
Sunday              None
Monday              08:30 to 17:30
Tuesday             08:30 to 17:30
Wednesday           08:30 to 17:30
Thursday            08:30 to 20:00
Friday              08:30 to 18:00
Saturday            09:00 to 13:00

******************************
Schedule: holiday-season
Day                 Open Hours
-------------------------------
Sunday              09:00 to 15:00
Monday              08:30 to 17:30
Tuesday             08:30 to 17:30
Wednesday           08:30 to 17:30
Thursday            08:00 to 21:00
Friday              08:00 to 21:00
Saturday            08:00 to 21:30
```

Related Commands

Command	Description
calendar biz-schedule	Creates a business-hours schedule.
closed day	Specifies the hours when a business is closed on a specific day.
open day	Specifies the hours when a business is open on a specific day.

show calendar holiday

To display the holidays configured on the local system, use the **show calendar holiday** command in Cisco Unity Express EXEC mode.

show calendar holiday [**all** | **year** *yyyy* [**month** *mm*] | **fixed**]

Syntax Description

year *yyyy*	(Optional) Year of the holiday list, where *yyyy* is the 4-digit year.
month *mm*	*(*Optional*)* Month of the holiday list, where *mm* is the 2-digit month.
fixed	*(*Optional*)* Display only the fixed holidays.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
2.1	This command was introduced.
3.0	This command was extended to display fixed holidays.

Examples

The following example displays all the holidays configured on the system.

```
se-10-0-0-0# show calendar holiday

********************************
           Year: 2004
********************************
February  14  FIXED  Valentine's day
September 04    Labor Day
November  01  FIXED
November  25    Thanksgiving
December  31  FIXED  New year's eve

********************************
           Year: 2005
********************************
February  14  FIXED  Valentine's day
July      04    July 4th
September 05    Labor Day
November  01  FIXED
November  24    Thanksgiving
December  25    Christmas
December  31  FIXED  New year's eve
```

The following example displays the holidays configured for a specific year.

```
se-10-0-0-0-0# show calendar holiday year 2005

********************************
           Year: 2005
********************************
February  14  FIXED  Valentine's day
July      04    July 4th
September 05    Labor Day
```

```
November  01  FIXED
November  24    Thanksgiving
December  25    Christmas
December  31  FIXED  New year's eve
```

The following example displays all the holidays for a specific month.

```
se-10-0-0-0# show calendar holiday year 2005 month 12

********************************
           Year: 2005
********************************
December  25    Christmas
December  31  FIXED  New year's eve
```

If no holidays are configured for a specific year or month, a message similar to the following appears:

```
se-10-0-0-0# show calendar holiday year 2006

No holidays found for the specified year
```

The following example displays only the fixed holidays configured on the system.

```
se-10-0-0-0# show calendar holiday year 2005 month 12

********************************
           Year: 2004
********************************
February  14  FIXED  Valentine's day
November  01  FIXED
December  31  FIXED  New year's eve

********************************
           Year: 2005
********************************
February  14  FIXED  Valentine's day
November  01  FIXED
December  31  FIXED  New year's eve
```

Related Commands

Command	Description
calendar holiday	Creates a holiday list on the local system.

show call-agent

To display the call-agent information, use the **show call-agent** command in Cisco Unity Express EXEC mode.

show call-agent

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
7.1	This command was introduced.

Usage Guidelines

This command enables you to view the call-agent information.

Examples

The following is a sample output for the **show license all** command:

```
se-10-0-0-0# show call-agent
Call-agent:         CUCM
```

Related Commands

Command	Description
call-agent	Configures the call-agent.

show ccn application

To display the currently configured applications, use the **show ccn application** command in Cisco Unity Express EXEC mode.

show ccn application

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
1.0	This command was introduced on the Cisco Unity Express network module and in Cisco Unified Communications Manager Express 3.0.
1.1	This command was implemented on the advanced integration module (AIM) and in Cisco Unified Communications Manager 3.3(3).
1.1.2	This command was implemented on the Cisco 2800 series and Cisco 3800 series routers.

Examples

The following is sample output for the **show ccn application** command:

```
cue-10-0-0-0# show ccn application

Name:                                   ciscomwiapplication
Description:                            ciscomwiapplication
Script:                                 setmwi.aef
ID number:                              0
Enabled:                                yes
Maximum number of sessions:             8
strMWI_OFF_DN:                          8001
strMWI_ON_DN:                           8000
CallControlGroupID:                     0

Name:                                   voicemail
Description:                            voicemail
Script:                                 voicebrowser.aef
ID number:                              1
Enabled:                                yes
Maximum number of sessions:             8
logoutUri:                              http://localhost/voicemail/vxmlscripts/Logout.jsp
uri:                                    http://localhost/voicemail/vxmlscripts/login.vxml

Name:                                   autoattendant
Description:                            Auto Attendant
Script:                                 aa.aef
ID number:                              2
Enabled:                                yes
Maximum number of sessions:             8
MaxRetry:                               3
```

```
operExtn:                                 0
welcomePrompt:                            AAWelcome.wav
```

Table 14 describes the significant fields shown in the display.

Table 14 show ccn application Field Descriptions

Field	Description
Name	Name of the application.
Description	Description of the application.
Script	Application script filename.
ID number	Order of configuration sequence number.
Enabled	Active status state.
Maximum number of sessions	Maximum number of concurrent calls that the application can handle.
logoutUri	Location of the logout Voice XML script to execute for the voice-mail application.
uri	Location of the login Voice XML script to execute for the voice-mail application.
MaxRetry	Number of times that the subscriber can respond incorrectly to submenu options before the application disconnects the call.
strMWI_OFF_DN	MWI off extension.
strMWI_ON_DN	MWI on extension.
CallControlGroupID	Sequence number.
operExtn	Extension dialed for the auto-attendant operator when the caller presses zero “0”.
welcomePrompt	Welcome prompt filename.

Related Commands

Command	Description
show ccn engine	Displays the application engine parameters.
show ccn scripts	Displays configured scripts.
show ccn subsystem sip	Displays configured subsystems.
show ccn trigger all	Displays configured triggers for applications.

show ccn call application

To display active calls for a specific application, use the **show ccn call application** in Cisco Unity Express EXEC mode.

show ccn call application [**all** [**subsystem** {**jtapi** | **sip**}] |
application-name [**subsystem** {**jtapi** | **sip**}]]

Syntax Description

all	(Optional) Displays active calls for all applications.
application-name	(Optional) Displays active calls for the specified application.
subsystem jtapi	(Optional) Displays active calls for the JTAPI subsystem.
subsystem sip	(Optional) Displays active calls for the SIP subsystem.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
2.1	This command was introduced.

Examples

The following are sample outputs for the **show ccn call application** command:

```
se-10-0-0-0# show ccn call application voicemail

Active Call Details for Subsystem :SIP
-----------------------------------------


 **** Details for route ID :1200 ****
 -------------------------------------


    ** Active Port #1:Call and Media info **
    ------------------------------------------

Port ID :4
Port Impl ID :16904
Port State :IN_USE
Call Id :241
Call Impl Id :FFCE47C8-669711D6-8C4BF237-80EC4A17@10.4.39.35
Call State :CALL_ANSWERED
Call active time(in seconds) :1
Application Associated :voicemail
Application Task Id :17000000122
Called Number :1200
Dialed Number :
Calling Number :1005
ANI :
DNIS :
CLID :sip:1005@10.4.39.35
Arrival Type :DIRECT
Last Redirected Number :
```

```
Original Called Number :
Original Dialed Number :

Media Id :6
Media State :IN_USE
Media Destination Address :10.4.39.35
Media Destination Port :16970
Destination Size :20
Destination Payload :G711ULAW64K
Media Source Address :10.4.39.135
Media Source Port :16904
Source Size :30
Source Payload :G711ULAW64K

se-10-0-0-0# show ccn call application promptmgmt

Active Call Details for Subsystem :SIP
-----------------------------------------


 **** Details for route ID :1202 ****
 -------------------------------------


    ** Active Port #1:Call and Media info **
    ------------------------------------------

Port ID :3
Port Impl ID :16902
Port State :IN_USE
Call Id :242
Call Impl Id :92023CF-669811D6-8C50F237-80EC4A17@10.4.39.35
Call State :CALL_ANSWERED
Call active time(in seconds) :1
Application Associated :promptmgmt
Application Task Id :17000000123
Called Number :1202
Dialed Number :
Calling Number :1005
ANI :
DNIS :
CLID :sip:1005@10.4.39.35
Arrival Type :DIRECT
Last Redirected Number :
Original Called Number :
Original Dialed Number :

Media Id :5
Media State :IN_USE
Media Destination Address :10.4.39.35
Media Destination Port :18534
Destination Size :20
Destination Payload :G711ULAW64K
Media Source Address :10.4.39.135
Media Source Port :16902
Source Size :30
Source Payload :G711ULAW64K
```

Table 15 describes the significant fields shown in the display.

Table 15 show ccn call application Field Descriptions

Field	Description
Port ID	ID number of the port.
Port Impl ID	Implementation ID for the port. This is an internally generated number.
Port State	Status of the port.
Call Id	ID number of the call.
Call Impl Id	Implementation ID of the call. This is an internally generated number.
Call State	Status of the call.
Call active time (in seconds)	Length of time for which the call has been active, in seconds.
Application Associated	Application associated with the call.
Application Task Id	ID of the application task associated with the call.
Called Number	Called number or extension.
Dialed Number	Dialed number or extension.
Calling Number	Calling number or extension.
ANI	Automatic Number Identification of the calling party.
DNIS	Dialed Number Identification Service of the called party.
CLID	Caller ID of the incoming call.
Arrival Type	Type of the incoming call.
Last Redirected Number	If this is a forwarded call, this field shows the number that forwarded the call.
Original Called Number	If this is a forwarded call, this field shows the original called number.
Original Dialed Number	If this is a forwarded call, this field shows the original number dialed by the caller.
Media Id	ID of the media.
Media State	Status of the media.
Media Destination Address	IP address of the media destination.
Media Destination Port	Port number of the media.
Destination Size	Size of the destination.
Destination Payload	Payload of the media.
Media Source Address	IP address of the media source.
Media Source Port	Port number of the media source.
Source Size	Size of the source.
Source Payload	Payload of the source.

Related Commands

Command	Description
ccn call terminate	Terminates an active call.
show ccn call route	Displays active calls for specified routes.

show ccn call fax incoming

To display active calls for incoming Cisco Unity Express IVR faxes, use the **show ccn call fax incoming** command in Cisco Unity Express IVR user EXEC mode.

show ccn call fax incoming

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express IVR user EXEC

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Examples

The following example configures a list of incoming fax calls when incoming calls are recorded:

```
se-10-0-0-0> show ccn call fax incoming
Connect Time                  Sender              Receiver
======================================================================
Mon Jan 15 12:56:26 PST 2007  1111                5000

1 incoming fax call(s)
```

Table 16 describes the significant fields shown in the display.

Table 16 show ccn call fax incoming Field Descriptions

Field	Description
Connect Time	Time when a connection is made for an incoming fax session.
Sender	Sender’s phone number for an incoming fax session.
Receiver	Receiver’s phone number for an incoming fax session.

Related Commands

Command	Description
ccn subsystem fax–IVR Only	Configures the Cisco Unity Express IVR fax settings.

show ccn call route

To display active calls for a specific route, use the **show ccn call route** command in Cisco Unity Express EXEC mode.

show ccn call route [**all** [**subsystem** {**jtapi** | **sip**}] | *route-address* [**subsystem** {**jtapi** | **sip**}]]

Syntax Description

all	(Optional) Displays active calls for all routes.
route-address	(Optional) Displays active calls for the specified route.
subsystem jtapi	(Optional) Displays active calls for the JTAPI subsystem.
subsystem sip	(Optional) Displays active calls for the SIP subsystem.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
2.1	This command was introduced.

Usage Guidelines

A route address is a trigger number configured for an application. Use the **show ccn trigger** command to display a list of configured triggers.

Examples

The following are sample outputs for the **show ccn call route** command:

```
se-10-0-0-0# show ccn call route

Active Call Details for Subsystem :JTAPI
-----------------------------------------


 **** Details for route ID :2200 ****
 -------------------------------------


    ** Active Port #1:Call and Media info **
    ------------------------------------------

Port ID :2
Port Impl ID :2225550150
Port State :IN_USE
Call Id :9
Call Impl Id :1566/1
Call State :CALL_ANSWERED
Call active time(in seconds) :12
Application Associated :voicemail
Application Task Id :17000000010
Called Number :2200
Dialed Number :
Calling Number :2001
ANI :
DNIS :
```

```
CLID :
Arrival Type :DIRECT
Last Redirected Number :
Original Called Number :2200
Original Dialed Number :

Media Id :2
Media State :IN_USE
Media Destination Address :172.16.59.11
Media Destination Port :22814
Destination Size :20
Destination Payload :G711ULAW64K
Media Source Address :10.4.14.133
Media Source Port :16388
Source Size :20
Source Payload :G711ULAW64K

    ** Active Port #2:Call and Media info **
    ------------------------------------------

Port ID :1
Port Impl ID :2225550151
Port State :IN_USE
Call Id :10
Call Impl Id :1567/1
Call State :CALL_ANSWERED
Call active time(in seconds) :12
Application Associated :voicemail
Application Task Id :17000000011
Called Number :2200
Dialed Number :
Calling Number :2003
ANI :
DNIS :
CLID :
Arrival Type :DIRECT
Last Redirected Number :
Original Called Number :2200
Original Dialed Number :

Media Id :1
Media State :IN_USE
Media Destination Address :172.16.59.12
Media Destination Port :27928
Destination Size :20
Destination Payload :G711ULAW64K
Media Source Address :10.4.14.133
Media Source Port :16386
Source Size :20
Source Payload :G711ULAW64K

Active Call Details for Subsystem :SIP
-----------------------------------------
```

The following example displays active calls for the route 1200, which is a trigger number for the voice-mail application.

```
se-10-0-0-0# show ccn call route 1200

Active Call Details for Subsystem :SIP
-----------------------------------------


 **** Details for route ID :1200 ****
 -------------------------------------
```

```
    ** Active Port #1:Call and Media info **
    ------------------------------------------

Port ID :8
Port Impl ID :16912
Port State :IN_USE
Call Id :246
Call Impl Id :E682B0A9-673311D6-8C64F237-80EC4A17@10.4.39.35
Call State :CALL_ANSWERED
Call active time(in seconds) :0
Application Associated :voicemail
Application Task Id :17000000127
Called Number :1200
Dialed Number :
Calling Number :1005
ANI :
DNIS :
CLID :sip:1005@10.4.39.35
Arrival Type :DIRECT
Last Redirected Number :
Original Called Number :
Original Dialed Number :

Media Id :1
Media State :IN_USE
Media Destination Address :10.4.39.35
Media Destination Port :18812
Destination Size :20
Destination Payload :G711ULAW64K
Media Source Address :10.4.39.135
Media Source Port :16912
Source Size :30
Source Payload :G711ULAW64K
```

Table 17 describes the significant fields shown in the display.

Table 17 show ccn call route Field Descriptions

Field	Description
Port ID	ID number of the port.
Port Impl ID	Implementation ID for the port. This is an internally generated number.
Port State	Status of the port.
Call Id	ID number of the call.
Call Impl Id	Implementation ID of the call. This is an internally generated number.
Call State	Status of the call.
Call active time (in seconds)	Length of time for which the call has been active, in seconds.
Application Associated	Application associated with the call.
Application Task Id	ID of the application task associated with the call.
Called Number	Called number or extension.
Dialed Number	Dialed number or extension.

Table 17 show ccn call route Field Descriptions (continued)

Field	Description
Calling Number	Calling number or extension.
ANI	Automatic Number Identification of the calling party.
DNIS	Dialed Number Identification Service of the called party.
CLID	Caller ID of the incoming call.
Arrival Type	Type of the incoming call.
Last Redirected Number	If this is a forwarded call, this field shows the number that forwarded the call.
Original Called Number	If this is a forwarded call, this field shows the original called number.
Original Dialed Number	If this is a forwarded call, this field shows the original number dialed by the caller.
Media Id	ID of the media.
Media State	Status of the media.
Media Destination Address	IP address of the media destination.
Media Destination Port	Port number of the media.
Destination Size	Size of the destination.
Destination Payload	Payload of the media.
Media Source Address	IP address of the media source.
Media Source Port	Port number of the media source.
Source Size	Size of the source.
Source Payload	Payload of the source.

Related Commands

Command	Description
ccn call terminate	Terminates an active call.
show ccn call application	Displays active calls for specified applications.
show ccn trigger all	Displays currently configured triggers.

show ccn document–IVR Only

To display a Cisco Unity Express IVR document, use the **show ccn document** command in Cisco Unity Express IVR user EXEC mode.

show ccn document {**all** | **generic** | **template** | **tiff**}

Syntax Description

all	Displays all types of documents.
generic	Displays generic documents.
template	Displays template documents.
tiff	Displays Tagged Image File Format (TIFF) documents.

Command Modes

Cisco Unity Express IVR user EXEC

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Examples

The following example shows sample output from the **show ccn document all** command; the output lists sample documents with .txt and .tif file extensions:

```
se-10-0-0-0> show ccn document all

Name:                         template.txt
Language:                     en_US
Type:                         Template
Last Modified Date:           Wed Jan 24 16:36:57 EST 2007
Length in Bytes:              30

Name:                         larkin.tif
Language:                     en_US
Type:                         Tiff
Last Modified Date:           Wed Jan 24 12:47:26 EST 2007
Length in Bytes:              59939

Name:                         logo.tif
Language:                     en_US
Type:                         Tiff
Last Modified Date:           Wed Jan 24 14:02:22 EST 2007
Length in Bytes:              58804

Name:                         test.txt
Language:                     en_US
Type:                         Generic
Last Modified Date:           Wed Jan 24 16:36:55 EST 2007
Length in Bytes:              21
```

The following example shows sample output from the **show ccn document generic** command; the output lists a sample generic document with .txt file extension:

```
se-10-0-0-0> show ccn document generic
```

```
Name:                         test.txt
Language:                     en_US
Type:                         Generic
Last Modified Date:           Wed Jan 24 16:36:55 EST 2007
Length in Bytes:              21
```

The following example shows sample output from the **show ccn document template** command; the output lists only the template documents:

```
se-10-0-0-0> show ccn document template

Name:                         template.txt
Language:                     en_US
Type:                         Template
Last Modified Date:           Wed Jan 24 16:36:57 EST 2007
Length in Bytes:              30

se-10-0-0-0> show ccn document tiff

Name:                         larkin.tif
Language:                     en_US
Type:                         Tiff
Last Modified Date:           Wed Jan 24 12:47:26 EST 2007
Length in Bytes:              59939

Name:                         logo.tif
Language:                     en_US
Type:                         Tiff
Last Modified Date:           Wed Jan 24 14:02:22 EST 2007
Length in Bytes:              58804
```

Table 18 describes the significant fields shown in the previous examples.

Table 18 show ccn document Field Descriptions

Field	Description
Name	Name of document file, including file extension.
Language	(Optional) Language of document file in the format *xx_YY.*
Type	Type of document file: • Generic • Template • TIFF
Last Modified Date	The date that the document was last modified, as shown in the following format: *day of the week:month:date:hour:minute:second:timezone:year*.
Length in Bytes	The size of the document in bytes.

Related Commands

Command	Description
ccn copy document–IVR Only	Copies a document from the Cisco Unity Express IVR system to a specified URL.
ccn delete document–IVR Only	Deletes an existing document from the Cisco Unity Express IVR system.

show ccn engine

To display details of the configured Cisco Unity Express software engine, use the **show ccn engine** command in Cisco Unity Express EXEC mode.

show ccn engine

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
1.0	This command was introduced on the Cisco Unity Express network module and in Cisco Unified Communications Manager Express 3.0.
1.1	This command was implemented on the advanced integration module (AIM) and in Cisco Unified Communications Manager 3.3(3).
1.1.2	This command was implemented on the Cisco 2800 series and Cisco 3800 series routers.

Examples

The following is sample output for the **show ccn engine** command:

```
se-10-0-0-0# show ccn engine

Maximum number of Tasks:                0
Maximum number of Steps:                1000
```

Table 19 describes the significant fields shown in the display.

Table 19 show ccn engine Field Descriptions

Fields	Descriptions
Maximum number of Tasks	Maximum number of tasks that the Cisco Communication Network (CCN) engine can process concurrently.
Maximum number of Steps	Maximum number of steps that can be executed in one script. If the script reaches this maximum number, the script execution is halted.

Related Commands

Command	Description
show call-agent	Displays configured applications.
show ccn scripts	Displays configured scripts.
show ccn subsystem sip	Displays configured subsystems.
show ccn trigger all	Displays configured triggers for applications.

show ccn prompts

To display the configured auto-attendant greeting prompt files, use the **show ccn prompts** command in Cisco Unity Express EXEC mode.

show ccn prompts [**language** *xx_YY*]

Syntax Description

language *xx_YY*	(Optional) Language of the prompts. See the *Release Notes for Cisco Unity Express* for a list of supported languages.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
1.0	This command was introduced on the Cisco Unity Express network module and in Cisco Unified Communications Manager Express 3.0.
1.1	This command was implemented on the advanced integration module (AIM) and in Cisco Unified Communications Manager 3.3(3).
1.1.2	This command was implemented on the Cisco 2800 series and Cisco 3800 series routers.
2.0	The **language** option was added.

Usage Guidelines

Use this command before configuring a new prompt file to verify the filenames that exist or before deleting a prompt to verify the name of the prompt file that must be removed.

If a language is not specified, **this command** displays subscriber prompts in all installed languages.

If a language is specified, this command displays subscriber prompts only for that language.

Cisco Unity Express permits only one installed language.

Examples

The following is sample output for the **show ccn prompts** command:

```
se-10-0-0-0# show ccn prompts

Name:                                   AAExtnOutOfService.wav
Language:                               de_DE
Last Modified Date:                     Thu Oct 21 a0:57:35 PDT 2004
Length:                                 25462
```

Table 20 describes the significant fields shown in the display.

Table 20 show ccn prompts Field Descriptions

Field	Description
Name	Name of the prompt file.
Language	Language of the prompt file.
Last Modified Date	Date when the prompt file was last modified.
Length	Length of the prompt file, in seconds.

Related Commands

Command	Description
ccn copy prompt	Copies prompts to a specified URL.
ccn delete prompt	Deletes the specified prompt.
voicemail default	Specifies a default voice-mail language.

show ccn reporting historical

To display the Cisco Unity Express IVR reporting historical database parameters, use the **show ccn reporting historical** command in Cisco Unity Express IVR user EXEC mode.

show ccn reporting historical

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express IVR user EXEC

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Examples

The following example output from the **show ccn reporting historical** command:

```
se-10-0-0-0> show ccn reporting historical

Database Information
--------------------
Enabled    : Yes
Location   : Local
Connection : Active
Description: ac-milan-cue.localdomain
Node ID: 0
DB Usage: 0% (Thu Jan 25  04:00:04)

Purge Schedule
--------------
Daily Time: 4:00 AM
Data older than 365 days will be purged
Date of last completed purge: Thu Jan 25  04:00:04

Purge Capacity Configuration
----------------------------
Email Address:
Warning Capacity: 85%
Purge Capacity: 90%
Oldest Days to purge: 7
```

Table 21 describes the significant fields shown in the previous examples.

Table 21 show ccn reporting historical Field Descriptions

Field	Description
Database Information	
Enabled	Indicates whether the reporting historical database is enabled.
Location	Indicates the location of the reporting historical database.
Connection	Indicates whether the database connection is active or inactive.

Table 21 show ccn reporting historical Field Descriptions (continued)

Field	Description
Description	The name of the local reporting historical database.
Node ID	The node identifier of the database.
DB Usage	The database usage in percentage as of the date indicated.
Database Purge Schedule	
Daily Time	The time of day when the daily purge starts.
Data older than 365 days will be purged	The age of the data, in number of days, that will be purged during the daily purge schedule.
Date of last completed purge	The date when the last database purge was completed.
Purge Capacity Configuration	
E-mail Address	The e-mail address to which the warning is to be sent when the database has reached its capacity.
Warning Capacity	The percentage of the database capacity that is reached or exceeded before a warning e-mail is sent.
Purge Capacity	The percentage of database capacity that is reached or exceeded before the database is purged.
Oldest Days to purge	The age, in number of days, of older data that is to be purged.

Related Commands

Command	Description
ccn reporting historical	Configures the Cisco Unity Express IVR reporting historical database settings.

show ccn scripts

To display script filenames, use the **show ccn scripts** command in Cisco Unity Express EXEC mode.

show ccn scripts

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
1.0	This command was introduced on the Cisco Unity Express network module and in Cisco Unified Communications Manager Express 3.0.
1.1	This command was implemented on the advanced integration module (AIM) and in Cisco Unified Communications Manager 3.3(3).
1.1.2	This command was implemented on the Cisco 2800 series and Cisco 3800 series routers.

Examples

The following is sample output for the **show ccn scripts** command:

```
se-10-0-0-0# show ccn scripts

Name:                                    setmwi.aef
Description:                             setmwi.aef
Name:                                    voicebrowser.aef
Description:                             voicebrowser.aef
Name:                                    aa.aef
Description:                             aa.aef
se-10-0-0-0#
```

Table 22 describes the significant fields shown in the display.

Table 22 show ccn scripts Field Descriptions

Field	Description
Name	Name of the script file.
Description	Optional description of the script file. If no description was configured, the system uses the script name for the description.

Related Commands

Command	Description
show call-agent	Displays configured applications.
show ccn engine	Displays configured application engine parameters.
show ccn prompts	Displays configured auto-attendant prompt files.

Command	Description
show ccn subsystem sip	Displays configured subsystems.
show ccn trigger all	Displays configured triggers for applications.

show ccn sip subscription mwi

To display a list of all active MWI subscriptions, use the **show ccn sip subscription mwi** command in Cisco Unity Express EXEC mode.

show ccn sip subscription mwi

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
2.3	This command was introduced on the NM-CUE and NM-CUE-EC modules.

Examples

The following is sample output for the **show ccn sip subscription** command:

```
se-10-0-0-0# show ccn sip subscription mwi

DN        Subscription Time                 Expires
5012      Mon May 24 2006 10:43:33 PDT 2006   3600
5011      Mon May 24 2006 10:43:33 PDT 2006   3600
```

The following example displays the message that appears if no subscriptions are active:

```
se-10-0-0-0# show ccn sip subscription mwi

No active subscriptions.
```

Related Commands

Command	Description
ccn subsystem sip	Enters SIP configuration mode.
dtmf-relay	Sets the SIP DTMF relay mechanism.
mwi sip	Sets the MWI notification mechanism used by Cisco Unity Express.
show ccn subsystem sip	Displays the DTMF relay mechanism.
transfer-mode	Sets the transfer mode used by Cisco Unity Express for SIP calls.

show ccn status ccm-manager

To display the status of the JTAPI subsystem, use the **show ccn status ccm-manager** command in Cisco Unity Express EXEC mode.

show ccn status ccm-manager

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
2.1	This command was introduced.

Usage Guidelines

The Cisco Unity Express JTAPI subsystem is registered with the Cisco Unified Communications Manager system indicated by the IP address shown in the output of this command.

Examples

The following example illustrates the output:

```
se-10-0-0-0# show ccn status ccm-manager

JTAPI Subsystem is currently registered with Call Manager 10.180.180.2
```

Related Commands

Command	Description
ccm-manager address	Configures the IP address or hostname of the Cisco Unified Communications Manager servers.
ccm-manager credentials	Specifies the Cisco Unified Communications Manager JTAPI username and password.
ccm-manager username	Specifies the Cisco Unified Communications Manager JTAPI user.

show ccn subsystem edbs dbprofile–IVR Only

To display the Cisco Unity Express IVR enterprise database subsystem (EDBS) profile parameters, use the **show ccn subsystem edbs dbprofile** command in Cisco Unity Express IVR user EXEC mode.

show ccn subsystem edbs dbprofile

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express IVR user EXEC

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Examples

The following example shows sample output from the **show ccn subsystem edbs dbprofile all** command:

```
se-10-0-0-0> show ccn subsystem edbs dbprofile all

Profile Name:                           msde_db
Status:                                 active
Database Type:                          MSSQL-MSDE
Database Name:                          manchester
Description:                            Manchester Test_db
Username:                               cisco
Password:                               *****
Hostname:                               myHost
Port:                                   1074
Enabled:                                yes
Maximum number of active connections:   8
```

Table 23 describes the significant fields shown in the previous example.

Table 23 show ccn subsystem edbs dbprofile Field Descriptions

Field	Description
Profile Name	Name of the database profile.
Status	Indicates whether the EDBS database is active.
Database Type	The underlying database type.
Database Name	Name of the EDBS database.
Description	Description of the EDBS database.
Username	The login username for access to the EDBS database.
Password	The login password for access to the EDBS database.
Hostname	DNS hostname or IP address of the EDBS database.
Port	Port number of the EDBS database

Table 23 show ccn subsystem edbs dbprofile Field Descriptions

Field	Description
Enabled	Indicates whether the EDBS database is enabled.
Maximum number of active connections	Indicates the maximum number of active connections to the EDBS database.

Related Commands

Command	Description
show ccn subsystem sip	Configures the Cisco Unity Express IVR EDBS profile name.

show ccn subsystem email–IVR Only

To display the Cisco Unity Express IVR *default-from* e-mail address or to display the e-mails in the queue, use the **show ccn subsystem email** command in Cisco Unity Express IVR user EXEC mode.

show ccn subsystem email [**queue**]

Syntax Description

queue	(Optional) Displays e-mail messages in the queue if the e-mail messages are sent in the queued mode.When e-mails are generated, e-mail messages can be sent synchronously or in a queued mode.

Command Modes

Cisco Unity Express IVR user EXEC

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Examples

The sample output from the **show ccn subsystem email** command lists the following *default-from* e-mail address:

```
se-10-0-0-0> show ccn subsystem email
Default From Address :                  localhost@localdomain.com
```

The following example shows sample output from the **show ccn subsystem email queue** command if the e-mail messages are sent in a queued mode:

```
se-10-0-0-0> show ccn subsystem email queue
===============================================================================
Email ID       Recipient             Subject                         Scheduled
                                                                     Send Time
===============================================================================
1196220172243  max20char@cisco.com   subject of Email - max 30 char  2007/05/30 10:52:00
```

Related Commands

Command	Description
ccn subsystem email–IVR Only	Configures the Cisco Unity Express IVR e-mail feature.

show ccn subsystem fax–IVR Only

To display the Cisco Unity Express IVR *default-from* fax address or the faxes in the fax queue, use the **show ccn subsystem fax** command in Cisco Unity Express IVR user EXEC mode.

show ccn subsystem fax [**outbound queue**]

Syntax Description

outbound queue	(Optional) Faxes are always sent in queued mode. Displays fax messages in the outbound fax queue.

Command Modes

Cisco Unity Express IVR user EXEC

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Examples

The sample output from the **show ccn subsystem fax** command lists the following fax *default-from* address:

```
se-10-0-0-0> show ccn subsystem fax
FAX Default From Address:                mqwerty@cisco.com
```

Faxes are always sent in queued mode. The following example shows sample output from the **show ccn subsystem fax outbound queue** command:

```
se-10-0-0-0> show ccn subsystem fax outbound queue
=============================================================================
Fax ID    Recipient      Subject                         Retry     Scheduled
                                                         Count     Send Time
=============================================================================
15        9784551212     subject of Fax - max 30 char    1         2007/05/30 10:52:00
```

Related Commands

Command	Description
ccn subsystem fax–IVR Only	Configures Cisco Unity Express IVR faxes.

show ccn subsystem jtapi

To display the JTAPI subsystem parameters, use the **show ccn subsystem jtapi** command in Cisco Unity Express EXEC mode.

show ccn subsystem jtapi

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
1.1	This command was introduced on the Cisco Unity Express network module (NM), advanced integration module (AIM), and in Cisco Unified Communications Manager 3.3(3).
1.1.2	This command was implemented on the Cisco 2800 series and Cisco 3800 series routers.
3.2	This command displays information for new features that enable you to specify: • A CTI port to use for MWI • The calling search space used to redirect calls from route points to CTI ports. • The calling search space used to redirect calls from CTI ports to elsewhere.

Examples

The following example displays the JTAPI parameters:

```
se-10-0-0-0# show ccn subsystem jtapi

Cisco Call Manager:                       10.30.40.50
CCM Username:                             admin
CCM Password:                             *****
Call Control Group 1 CTI ports:           7008,7009,7010
Call Control Group 1 MWI port:            4210
CSS for redirects from route points:      ccm-default
CSS for redirects from CTI ports:         redirecting-party
```

Table 24 describes the significant fields shown in the display.

Table 24 show ccn subsystem jtapi Field Descriptions

Field	Description
Cisco Call Manager	IP address of the Cisco Unified Communications Manager server.
CCM Username	JTAPI user ID.

Table 24 show ccn subsystem jtapi Field Descriptions

Field	Description
CCM Password	JTAPI user password.
Call Control Group 1 CTI ports	Cisco Unified Communications Manager CTI ports.
Call Control Group 1 MWI port	Cisco Unified Communications Manager CTI port to use for MWI. If no value is set, CTI ports are used for MWI.
CSS for redirects from route points	Specifies the calling search space used to redirect calls from route points to CTI ports. Valid values are: • ccm-default — Redirect without Cisco Unity Express specifying a calling search space. • calling-party — Use the original calling party's calling search space to redirect. • redirecting-party — Use the redirecting party's calling search space to redirect.
CSS for redirects from CTI ports	Specifies the calling search space used to redirect calls from CTI ports to elsewhere. Valid values are: • ccm-default — Redirect without Cisco Unity Express specifying a calling search space. • calling-party — Use the original calling party's calling search space to redirect. • redirecting-party — Use the redirecting party's calling search space to redirect.

Related Commandss

Command	Description
ccm-manager address	Specifies the Cisco Unified Communications Manager server.
ccm-manager username	Specifies the JTAPI user ID and password.
ccn subsystem jtapi	Enters JTAPI configuration mode.
ctiport	Specifies the Cisco Unified Communications Manager CTI ports.

show ccn subsystem sip

To display the SIP subsystem parameters, use the **show ccn subsystem sip** command in Cisco Unity Express EXEC mode.

show ccn subsystem sip

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
1.0	This command was introduced on the Cisco Unity Express network module and in Cisco Unified Communications Manager Express 3.0.
1.1	This command was implemented on the advanced integration module (AIM) and in Cisco Unified Communications Manager 3.3(3).
1.1.2	This command was implemented on the Cisco 2800 series and Cisco 3800 series routers.
2.3	This command was implemented on the NM-CUE and NM-CUE-EC modules. The output display was enhanced to include the DTMF Relay, MWI Notification, and Transfer Mode options.
3.2	This command was extended to display whether envelope information is included in SIP MWI notifications.
7.0	This command was extended to display whether sub-notify is enabled simultaneously with either outcall or unsolicited for MWI notifications.

Examples

The following is sample output for the **show ccn subsystem sip** command:

```
se-10-0-0-0# show ccn subsystem sip

SIP Gateway:        172.19.167.208
SIP Port Number:    5060
DTMF Relay:         sip-notify rtp-nte
MWI Notification:   unsolicited,sub-notify
MWI Envelope Info:  disabled
Transfer Mode:      consult (REFER)
SIP RFC Compliance: Pre-RFC3261
```

Table 25 describes the significant fields shown in the display.

Table 25 show ccn subsystem sip Field Descriptions

Field	Description
SIP Gateway	IP address of the SIP gateway.
SIP Port Number	SIP port number on the module.
DTMF Relay	Options for relaying incoming and outgoing DTMF signals.
MWI Notification	Mechanism for updating MWI status. Valid values are: • outcall • unsolicited • sub-notify • outcall, sub-notify • unsolicited, sub-notify
MWI Envelope Info	Whether envelope information is included in SIP MWI notifications.
Transfer Mode	Mode for handling transferred calls.
SIP RFC Compliance	Status of SIP RFC-3261 compliance.

Related Commands

Command	Description
ccn subsystem sip	Enters SIP configuration mode.
dtmf-relay	Sets the SIP DTMF relay mechanism.
mwi sip	Sets the MWI notification mechanism used by Cisco Unity Express.
show call-agent	Displays configured applications.
show ccn engine	Displays configured application engine parameters.
show ccn scripts	Displays configured scripts.
show ccn sip subscription mwi	Displays the active MWI subscriptions.
show ccn trigger all	Displays configured triggers for applications.
transfer-mode	Sets the transfer mode used by Cisco Unity Express for SIP calls.

show ccn trigger all

To display all the currently configured trigger types, use the **show ccn trigger all** command in Cisco Unity Express EXEC mode.

show ccn trigger all

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
1.0	This command was introduced on the Cisco Unity Express network module and in Cisco Unified Communications Manager Express 3.0.
1.1	This command was implemented on the advanced integration module (AIM) and in Cisco Unified Communications Manager 3.3(3).
1.1.2	This command was implemented on the Cisco 2800 series and Cisco 3800 series routers.

Usage Guidelines

Before deleting an application, use this command to display the triggers associated with the application. All triggers for the application must be deleted. If they are not deleted, an incoming call that is configured as a trigger will invoke the application.

Examples

The following example shows sample output from the **show ccn trigger all** command:

```
se-10-0-0-0> show ccn trigger all

Name:                         2001
Type:                         SIP
Application:                  promptmgmt
Locale:                       systemDefault
Idle Timeout:                 10000
Enabled:                      yes
Maximum number of sessions:   1

Name:                         6300
Type:                         SIP
Application:                  promptmgmt
Locale:                       systemDefault
Idle Timeout:                 10000
Enabled:                      yes
Maximum number of sessions:   8

Name:                         mwiapp
Type:                         HTTP
Application:                  ciscomwiapplication
```

```
Locale:                        systemDefault
Idle Timeout:                  1000
Enabled:                       yes
Maximum number of sessions:    1
```

Table 26 describes the significant fields shown in the previous example.

Table 26 show ccn trigger all Field Descriptions

Field	Description
Name	Telephone number used for the trigger.
Type	Type of trigger.
Application	Application assigned to the trigger.
Locale	Language used for the application prompts.
Idle Timeout	Number of seconds that the application waits for a subscriber response before disconnecting the call.
Enabled	Active or inactive state of the application.
Maximum number of sessions	Number of calls that the application can handle concurrently.

Related Commands

Command	Description
ccn trigger sip phonenumber	Configures triggers for an application.

show ccn trigger http–IVR Only

To display the configured Cisco Unity Express HTTP IVR triggers, use the **show ccn trigger http** command in Cisco Unity Express IVR user EXEC mode.

show ccn trigger http

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express IVR user EXEC

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

Before deleting an application, use the **show ccn trigger all** command to display all triggers associated with the application. All triggers for the application must be deleted. If they are not deleted, an incoming call that is configured as a trigger starts the application.

Examples

The following example shows sample output from the **show ccn trigger http** command:

```
se-10-0-0-0> show ccn trigger http

Name:                         mwiapp
Type:                         HTTP
Application:                  ciscomwiapplication
Locale:                       systemDefault
Idle Timeout:                 1000
Enabled:                      yes
Maximum number of sessions:   1
```

Table 27 describes the significant fields shown in the previous example.

Table 27 show ccn trigger all Field Descriptions

Field	Description
Name	Telephone number used for the trigger.
Type	Type of trigger.
Application	Application assigned to the trigger.
Locale	Language used for the application prompts.
Idle Timeout	Number of seconds that the application waits for a subscriber response before disconnecting the call.
Enabled	Active or inactive state of the application.
Maximum number of sessions	Number of calls that the application can handle concurrently.

Related Commands

Command	Description
ccn trigger http–IVR Only	Configures a Cisco Unity Express IVR HTTP-based URL and application trigger.

show ccn trigger jtapi

To display the currently configured Java Telephony API (JTAPI) trigger types, use the **show ccn trigger jtapi** command in Cisco Unity Express EXEC mode.

show ccn trigger jtapi

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
1.0	This command was introduced on the Cisco Unity Express network module and in Cisco Unified Communications Manager Express 3.0.
1.1	This command was implemented on the advanced integration module (AIM) and in Cisco Unified Communications Manager 3.3(3).
1.1.2	This command was implemented on the Cisco 2800 series and Cisco 3800 series routers.

Usage Guidelines

Before deleting an application, use this command to display the triggers associated with the application. All triggers for the application must be deleted. If they are not deleted, an incoming call that is configured as a trigger will invoke the application.

Examples

The following is sample output for the **show ccn trigger** command:

```
cue-10-0-0-0# show ccn trigger

Name:                        6800
Type:                        SIP
Application:                 voicemail
Locale:                      en_ENU
Idle Timeout:                5000
Enabled:                     yes
Maximum number of sessions:  8

Name:                        6700
Type:                        SIP
Application:                 autoattendant
Locale:                      en_ENU
Idle Timeout:                5000
Enabled:                     yes
Maximum number of sessions:  8
```

Table 28 describes the significant fields shown in the display.

Table 28 show ccn trigger Field Descriptions

Field	Description
Name	Telephone number used for the trigger.
Type	Type of trigger.
Application	Application assigned to the trigger.
Locale	Language used for the application prompts.
Idle Timeout	Number of seconds that the application waits for a subscriber response before disconnecting the call.
Enabled	Active or inactive state of the application.
Maximum number of sessions	Number of calls that the application can handle concurrently.

Related Commands

Command	Description
ccn trigger jtapi phonenumber	Configures triggers for an application.

show ccn trigger sip

To display the currently configured Session Initiation Protocol (SIP) trigger types, use the **show ccn trigger sip** command in Cisco Unity Express EXEC mode.

show ccn trigger sip

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unity Express EXEC

Command History

Cisco Unity Express Version	Modification
1.0	This command was introduced on the Cisco Unity Express network module and in Cisco Unified Communications Manager Express 3.0.
1.1	This command was implemented on the advanced integration module (AIM) and in Cisco Unified Communications Manager 3.3(3).
1.1.2	This command was implemented on the Cisco 2800 series and Cisco 3800 series routers.

Usage Guidelines

Before deleting an application, use this command to display the triggers associated with the application. All triggers for the application must be deleted. If they are not deleted, an incoming call that is configured as a trigger will invoke the application.

Examples

The following is sample output for the **show ccn trigger** command:

```
cue-10-0-0-0# show ccn trigger

Name:                         6800
Type:                         SIP
Application:                  voicemail
Locale:                       en_ENU
Idle Timeout:                 5000
Enabled:                      yes
Maximum number of sessions:   8

Name:                         6700
Type:                         SIP
Application:                  autoattendant
Locale:                       en_ENU
Idle Timeout:                 5000
Enabled:                      yes
Maximum number of sessions:   8
```

Table 29 describes the significant fields shown in the display.

Table 29 show ccn trigger Field Descriptions

Field	Description
Name	Telephone number used for the trigger.
Type	Type of trigger.
Application	Application assigned to the trigger.
Locale	Language used for the application prompts.
Idle Timeout	Number of seconds that the application waits for a subscriber response before disconnecting the call.
Enabled	Active or inactive state of the application.
Maximum number of sessions	Number of calls that the application can handle concurrently.

Related Commands

Command	Description
ccn trigger sip phonenumber	Configures triggers for an application.