

# Cisco Unity Express Security

## Cisco Unity Express

### Product Overview

Cisco Unity™ Express is a Linux-based application that fits into the Cisco® 2600XM, 2691 and 3700 branch office routers, using either a Network Module (NM) or Advanced Integration Module (AIM) hardware form factor. Cisco Unity Express is a local, entry-level automated attendant (AA) and voice-mail system with 12-100 mailboxes, 4-8 sessions (“ports” or simultaneously active calls), and 8 (AIM) or 100 (Network Module) hours of storage. Cisco Unity Express R1.0 AA and voice-mail application can be deployed with Cisco CallManager Express, and Cisco Unity Express R1.1 (available in Feb 2004) can additionally be deployed with Cisco CallManager systems to provide distributed, branch-office based voice mail for the users in the branch.

### Resources

Cisco Unity Express product, configuration, presentation and design information can be found at the following links:

Cisco CallManager IP Communications Solution:

- <http://www.cisco.com/go/ccmecue>

Cisco Unity Express:

- <http://www.cisco.com/go/cue>

Send Cisco Unity Express inquiries to:

[cs-cue@cisco.com](mailto:cs-cue@cisco.com)

### Scope

The information below pertains to Cisco Unity Express R1.0 and is an extract from the Cisco Unity Express Design Guide referenced above. This information will be periodically updated as new Cisco Unity Express releases become available with improved security features.

### System and Remote Access

#### Local Access

There are no external interfaces on the Cisco Unity Express hardware (physically there is an FE interface port, but it is disabled in software and unusable)—all access must pass via the host router. The only local access to the Cisco Unity Express system is therefore via the host router’s console interface.

Access to Cisco Unity Express (via the router’s command-line interface [CLI]) is only possible by using the following command:

```
lab-2691#service-module  
service-Engine x/y session
```

This command requires Enable mode on the router and is therefore protected by the router’s enable password settings. Although there is also an “enable” mode in the Cisco Unity Express module CLI, it has no password capability.



## Remote Access—Telnet

Use the following IP configuration as reference in the text below:

```
interface FastEthernet0/0
  ip address 172.19.153.41 255.255.255.0
  no ip mroute-cache
  duplex auto
  speed auto
!
interface Service-Engine1/0
  ip unnumbered FastEthernet0/0
  service-module ip address 172.19.153.37 255.255.255.0
  service-module ip default-gateway 172.19.153.41
```

Direct Telnet access to the Cisco Unity Express module is disabled in the following configuration:

```
pc> telnet 172.19.153.37
Trying 172.19.153.37...
telnet: Unable to connect to remote host: Connection refused
```

Remote CLI access to Cisco Unity Express is via Telnet to the router (172.19.153.41) and then the session command to get access to the Cisco Unity Express module. That way, all the security aspects of Telnet to the router automatically also protect access to the Cisco Unity Express module.

```
pc> telnet 172.19.153.41
Trying 172.19.153.41...
Connected to 172.19.153.41.
Escape character is '^']'.
```

User Access Verification

```
Password:
lab-2691>en
Password:
lab-2691#service-module service-Engine 1/0 session
Trying 172.19.153.41, 2033 ... Open
```

Telnet to the router address followed by the TTY number that Cisco Unity Express uses (which depends on the slot where it is inserted) is not blocked and can provide undesirable “direct” access to Cisco Unity Express module:

```
pc> telnet 172.19.153.41 2033
Trying 172.19.153.41...
Connected to 172.19.153.41.
Escape character is '^']'.
```

User Access Verification

```
Password:
Password OK

se-cue-2691#
```



To protect against this kind of access, insert a login and password on the TTY port (in this example the Cisco Unity Express module is in slot 1/0, therefore TTY port 2033) leading to the Cisco Unity Express module.

```
line 33
 password cisco
 flush-at-activation
 no activation-character
 login
 no exec
 transport preferred none
 transport input all
```

### Secure Shell Protocol

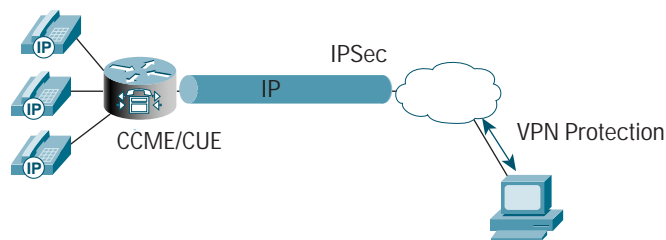
For secure CLI access to Cisco Unity Express, enable Secure Shell (SSH) on the router and use an SSH-enabled remote access application, such as the Secure Shell windows application. Cisco Unity Express itself does not support SSH (but neither does it support Telnet access), but communication between the router and Cisco Unity Express is via the router backplane and therefore not exposed to any external interfaces or IP segments. SSH access to the router is sufficient to protect Telnet access to Cisco Unity Express.

### HTTPS

Cisco Unity Express R1 does not support HTTPS—this is on the roadmap of security features to be added. Although login to the GUI is password protected, the login ID and password currently travel in clear text across the IP network.

GUI access in Cisco Unity Express R1 can be protected by using IPSec tunnels on the routers between the nearest router to where the browser is located and the Cisco CallManager Express router hosting the Cisco Unity Express module. VPN technology can be used to protect the segment between the client PC and the nearest router where IPSec is available, as shown in the figure below. Alternatively VPN technology can be used all the way from the client PC to the Cisco CallManager Express router.

Figure 1  
Secure HTTP Access



HTTPS is supported on Cisco CallManager Express and Cisco Unity Express and requires at least the 12.2(15)ZJ2 IP/FW/IDS PLUS IPSEC 3DES Cisco IOS® Software image. HTTP access for Cisco Unity Express and the IP Phones (which do not support HTTPS/SSL) continue to use port 80, while the Cisco CallManager Express GUI access uses HTTPS on port 443. For this to work, enable the following on the router:

```
ip http server
ip http secure-server
```



## Operating Environment

### Protocols/Port Numbers

As of this writing, a **netstat -ln** (on a development machine that has Linux access) shows the following ports open on Cisco Unity Express R1.0.1. CSCec16365 has been filed to close the ports that are not used. Ports legitimately in use include HTTP, NTP, syslog, and SIP.

#### TCP:

- 80: http
- 1099: rmiregistry
- 8017: ?
- 8007: jre
- 32860: ?

#### UDP:

- 123: ntp
- 514: syslog
- 800: ?
- 5060: sip
- 32769: ?

The following table lists the valid port numbers used by Cisco Unity Express.

Table 1 Valid Port Numbers

Protocol	Remote Source Port	Cisco Unity Express Destination Port	Cisco Unity Express Source Port	Remote Device Destination Port	Remote Device	Notes
SSH					Secure Shell Client	Not supported on Cisco Unity Express. Use SSH to the host router.
Telnet					Telnet Client	Not supported on Cisco Unity Express. Use Telnet to the host router.
DNS			TCP/UDP 53		DNS Servers	
TFTP			UDP 69		TFTP Server	Used for loading RAM kernel
FTP			TCP 20 (data), TCP 21 (control)		FTP Server	Used for software install; backup and restore



Table 1 Valid Port Numbers (Continued)

Protocol	Remote Source Port	Cisco Unity Express Destination Port	Cisco Unity Express Source Port	Remote Device Destination Port	Remote Device	Notes
HTTP		TCP 80			Administrator/ User Web browsers	Cisco Unity Express and Cisco CallManager Express Admin and User access
NTP		UDP 123			NTP server	Usually the Cisco CallManager Express host router
SNMP					Network Management station	SNMP hardware inventory for Cisco Unity Express is supported out of the host router. Cisco Unity Express itself does not support SNMP
Syslog		TCP 514			Syslog service	
SIP		UDP 5060			Cisco CallManager Express host router	No SIP trunking supported in Cisco Unity Express R1
RTP	UDP 16384-32767	UDP 16384-32767	UDP 16384-32767	UDP 16384-32767	Voice Media	IP Phone and GW ports

IE

### Operating System (Linux)

Although Cisco Unity Express runs on Linux, there is no access via CLI, Telnet, or any other interface into Linux. Therefore there are no HIDS or virus protections, but also no need for that because the Linux operating system is entirely embedded.

### LDAP

Although Cisco Unity Express includes an LDAP directory as part of the application, there is no access via CLI, Telnet, or any other interface or protocol into LDAP—it is an entirely embedded system.

### SQL

Although Cisco Unity Express includes an SQL database as part of the application, there is no access via CLI, Telnet, or any other interface or protocol into the database—it is an entirely embedded system.



## Application Environment

### Software Installation

Cisco Unity Express R1 uses TFTP for the initial installation step of loading the cue\_installer image (RAM-based Linux kernel). The actual software installation following that uses FTP.

TFTP is insecure and has no login/password control.

FTP access can be secured with a login/password combination even though the actual file transfer is not secure (FTPS) unless it travels over an IPSec-protected route between the FTP server and the Cisco CallManager Express router.

During the software installation, the command to start loading software from the FTP is shown in the following example:  
se-1-3-235-101installer#> s i p u ftp://1.3.61.16/cue-vm.1.0.1.pkg user ftpuser

In the example, user is the FTP account user ID, and ftpuser is the password. If the command is given exactly as above, then the password is echoed in clear text on the screen. If this operation is undesirable, omit the password from the s i p u command and the installer will prompt for it (which is not echoed to the screen or stored anywhere).

### Software Image and File Checking

All the files used during a software or license installation on Cisco Unity Express (an example list can be viewed at <http://www.cisco.com/cgi-bin/tablebuild.pl/cue-netmodule>, all files except the release notes are applicable to either a software or license install or both) have digital signatures in them that are cross-checked during software installation and start-up. This precludes rogue software from being installed or started on the Cisco Unity Express platform even in the event that a way is found to copy these files onto the hardware module.

### Backup and Restore

Cisco Unity Express uses an FTP server for backup and restore. As shown below, the FTP server's password configuration in Cisco Unity Express R1 is protected in the GUI (the field is blanked out) and the CLI show backup command (although it can be configured, it is not printed).



Figure 2  
Password Protection for Backup and Restore

IOS Telephony Services  
Configure ▾ Voice Mail ▾ Administration ▾ Defaults ▾ Reports ▾ Help ▾  
Administration > Backup / Restore > Configuration  
Apply Help  
Server URL \*: ftp://127.0.0.1/ftp  
User ID \*: test  
Password: \*\*\*\*\*  
Confirm Password: \*\*\*\*\*  
Maximum revisions \*: 20  
\* indicates a mandatory field

```
se-cue-2691# show backup
Server URL:                ftp://127.0.0.1/ftp
User Account on Server:    test
Number of Backups to Retain: 20
```

It's important to note that the backup server password is, however, printed in clear text in an sh run on the Cisco Unity Express module, as shown below. DDTS CSCec23041 is open to fix this.

```
se-cue-2691# sh run
Generating configuration:
! Timezone Settings
clock timezone America/Los_Angeles

hostname se-cue-2691

ip domain-name localhost
! DNS Servers
ip name-server 1.1.1.1

ntp server 172.19.153.41
...
...
backup revisions 20
backup server url "ftp://127.0.0.1/ftp" username "test" password "cisco"

ccn application autoattendant
description "autoattendant"
```

The workaround for this is to not configure a password for the backup server in the permanent Cisco Unity Express configuration, and to add it manually when a backup or restore procedure is run and remove it when the procedure is complete.



## User Interfaces/Passwords

Cisco Unity Express R1 has three separate user interfaces: a GUI, CLI and TUI (subscriber telephony interface). There are two types of users: administrators and end users (subscribers). Administrators can have access to the GUI and the CLI; subscribers can have access to the GUI and TUI.

The GUI and CLI login protections are referred to as a “password”, while TUI login protection is referred to as a “PIN”.

## GUI

All User IDs defined on the system are password controlled on login, regardless of whether the User ID has administrator or subscribers privileges. Passwords are mandatory and are 3 to 32 characters long, case sensitive, and allow alphabetic and numeric characters.

Passwords do not expire in Cisco Unity Express R1 (this is a roadmap feature), nor are they checked against a history of recently used passwords. When a password is changed, the following checks are done:

- Password grammar (valid characters and length)
- New password is a minimum of three characters long
- New password is different from the current password

There is an idle timeout of 10 minutes on any GUI login. Mouse movements do not count as activity, menus items must be clicked and windows must be opened/closed to reset the inactivity timer.

## Administrator

Any User ID with Cisco Unity Express administrator privileges can perform the following tasks:

- Change any user’s password or PIN, including his own
- Not see any user passwords or PINs (these are blanked out on the GUI screens), unless they have never been changed and are still set to the auto-generate password/PIN initially assigned when the account or mailbox was created
- Set the default password and PIN assignment policy for the system, as shown below

Figure 3

Options for User ID with Administrator Privileges





The random auto-generate password/PIN policy is recommended. If the blank policy is chosen, it is only the initial password/PIN that is blank. The first time the user logs into the GUI (password) or into his mailbox (TUI), the user will be forced to change his password before any access to the system is granted. At this time, the password can no longer be blank; it must be a valid password or PIN of a minimum of three characters.

#### End User (Subscriber)

Any User ID with Cisco Unity Express subscriber privileges can only change his own password and PIN. This type of user can not perform the following tasks:

- See his own password or PIN (these are blanked out on the GUI screens), but can overwrite them
- See any information on any other user
- See or change the default password/PIN assignment policy for the system

#### CLI

There is no CLI password on the Cisco Unity Express system itself. But as the Cisco IOS Software session command on the router is required to gain Cisco Unity Express CLI access, Cisco Unity Express is protected by the router CLI password protections. The Cisco IOS Software session command required Enable mode on the router.

#### TUI

All mailboxes defined on the system are PIN controlled on login. PINs are mandatory, are 3 to 19 characters long, and allow numeric characters.

PINs do not expire in Cisco Unity Express R1 (this is a roadmap feature), and are not checked against a history of recently used PIN. When a PIN is changed, the following checks are done:

- PIN grammar (valid characters and length)
- New PIN is a minimum of three characters long
- New PIN is different from the current password

There is a retry limit of three attempts on a PIN. When exceeded, an error message is logged and the user is returned to the top-level prompt (“if you have a mailbox on the system, enter it, otherwise please hold for an operator”). The mailbox is not disabled.

#### Toll Fraud

Toll fraud opportunities on Cisco Unity Express R1 are negligible as it does not support most of the voice mail features typically exploited by security breaches, including the following:

- Outdialing (calling a phone number or pager when a messages is left)
- Through-dialing (initiating a phone call from within a mailbox)
- Networking between sites (forwarding messages to unintended destinations)

Cisco Unity Express is also only a voice-mail system and does not support unified messaging; therefore there is no access to e-mail, Microsoft Exchange or any other generic message store facility.

## Best Practices

- Ensure the router hosting the Cisco Unity Express module has an enable password assigned.
- Ensure Telnet access the router is appropriately restricted.
- Ensure the router TTY connecting to Cisco Unity Express has login enabled and requires a password.
- Enable SSH on the router to protect Telnet traffic.
- Use VPN and IPSec router technology to protect HTTP access into Cisco Unity Express until it supports HTTPS in a later release.
- Use ACLs or Cisco IOS Firewall to close access to any ports not actively in use by Cisco Unity Express until CSCec16365 is fixed.
- Use ACLs to restrict SIP signaling traffic into Cisco Unity Express to be sourced only by the Cisco CallManager Express router that hosts Cisco Unity Express. No other source should be able to get into Cisco Unity Express's SIP interface.
- Ensure the FTP server used for software installation is login/password protected.
- Ensure the FTP server used for backup and restore is login/password protected.
- During a software install/upgrade, do not provide the FTP password on the install command line, let the installer prompt for it.
- Do not leave the backup and restore FTP server password configured permanently on the Cisco Unity Express module. Add it just before a backup or restore procedure is run and remove it immediately afterwards.
- Maintain the Cisco Unity Express system with the "generate random password/PIN" user access policy. This is the default policy in a newly installed system.
- Mailbox PINs do not expire, so a good practice is for the administrator to change all passwords periodically, forcing users to reset their PINs to a new setting.



### Corporate Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

### European Headquarters

Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

### Americas Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

### Asia Pacific Headquarters

Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Cisco IOS, and Cisco Unity are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R) ETMG 203246—CM 01.04