



Cisco Content Transformation Engine (CTE) 1400 Series Configuration Note

Product Number: CTE-1400

This publication contains the procedures for configuring the Cisco Content Transformation Engine (CTE) 1400 Series.

For information on installing the CTE, refer to the *Cisco CTE 1400 Hardware Installation Guide*.



Note

Throughout this publication, the *Cisco CTE 1400 Series* is referred to as the *CTE*.

Contents

This publication consists of these sections:

- [Important Security Information, page 2](#)
- [Overview, page 2](#)
- [Configuring the CTE, page 10](#)
- [Using the CTE Administration Console, page 21](#)
- [Managing Administrative User Accounts, page 34](#)
- [Shutting Down and Restarting the CTE Server Software, page 35](#)
- [Generating a Secure Certificate for the CTE, page 35](#)
- [Recovering from a CTE Crash, page 40](#)
- [Troubleshooting a CTE, page 40](#)
- [Related Documentation, page 41](#)
- [Obtaining Documentation, page 41](#)
- [Obtaining Technical Assistance, page 43](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

Important Security Information

Improper configuration of the CTE can result in a security risk. Before you deploy the CTE, verify that it does not have access to protected intranet sites.

By default, the CTE proxies only the web pages for which it has transformation rules. As a result, the CTE prevents access to protected servers that are on the same subnet as the CTE. If you choose to override the default, do not put the CTE on the same subnet as protected servers.

**Note**

If you configure the CTE to proxy all web pages, the CTE provides access to computers on the same subnet as the web servers that are configured to work with the CTE. For example, suppose a CTE has an external IP address of 24.221.1.1 and an internal IP address of 192.168.1.31. On the same subnet, you have an intranet server protected from outside access, with an IP address of 192.168.1.20. It is possible to access all ports on the protected intranet server through the CTE by using the URL *http://24.221.1.1/http://192.168.1.20*.

Also, be aware of the following security considerations:

- IP phone/CTE connection

Because IP phones do not support Secure Sockets Layer (SSL), the connection between the IP phones and the CTE is not secure. We recommend that you locate the connection between an IP phone and the CTE behind a firewall.

- SSL to non-SSL redirects

When Design Studio is redirected to an SSL site from a non-SSL site (from HTTPS to HTTP), the connection between Design Studio and the CTE is not secure. We recommend that you locate the connection between Design Studio and the CTE behind a firewall.

Overview

The CTE transforms and delivers applications to IP phones and a variety of mobile devices, including Wireless Application Protocol (WAP) phones and Personal Digital Assistants (PDAs). The CTE is a 1U device that installs into any network infrastructure without requiring changes to the existing hardware or back-end software. The CTE sits in front of content servers and works with other networking products such as web servers, server load balancers, cache engines, firewalls, Virtual Private Network (VPN) solutions, routers, and IEEE 802.11 broadband wireless devices.

The CTE displays ScreenTop Menu, a hierarchical services menu, on connecting devices. ScreenTop Menu provides users quick access to popular destinations such as news, sports, and travel information. You can make ScreenTop Menu always available to IP phone users by using the soft switch to set a phone or phone group's idle URL to the CTE IP address. ScreenTop Menu appears on any device when the device connects to the CTE.

Design Studio is a PC-based application that you use to create transformation rules, modify the default ScreenTop Menu, and upload your changes to a CTE.

These sections describe the CTE:

- [Features, page 3](#)
- [Licensing, page 5](#)
- [Security, page 5](#)
- [Sessions and Connections, page 6](#)

- [Operation Modes, page 7](#)
- [CTE Traffic Flow, page 9](#)
- [Input and Output Encoding, page 10](#)

Features

[Table 1](#) summarizes the features of the CTE.

Table 1 CTE Features

| Feature | Description |
|---------------------------------|---|
| Performance and scalability | <ul style="list-style-type: none"> • Each CTE supports up to 1400 simultaneous connections. • Each CTE supports 1000 user sessions. • Add CTEs anywhere in your network to scale up. |
| Back-end content transformation | <ul style="list-style-type: none"> • Supports any HTML content (web server, enterprise application, etc.). • Supports raw XML data sources through XSL transformations (XSLT). • Transforms content through XSL, allowing for open standards and extensibility. • Supports advanced programming by allowing direct upload of XSL style sheets. XSL provides easy integration with existing technologies such as application servers, if needed. • Automatically removes content not supported by mobile devices or IP phones during transformation. Unsupported content includes Java Applets and Flash programs. • Prepends the CTE IP address to all links on transformed pages. You can override this operation. |
| Support for multiple devices | <p>Mobile devices and IP phones use a variety of operating system platforms, presentation languages, and screen sizes and have different bandwidth constraints. The CTE manages these requirements on many devices automatically. The CTE supports content in the following formats:</p> <ul style="list-style-type: none"> • HTML versions 4.0, 3.2, and 2.0 • XHTML versions 1.1 and 1.0 • XML version 1.0 • WML, version 1.1 • XSL¹ version 1.0 • GIF, JPEG, BMP, and WBMP image formats |

Table 1 CTE Features (continued)

| Feature | Description |
|-----------------------------|---|
| Conversion features | <ul style="list-style-type: none"> • Automatically recognizes devices and provides device-specific rendering of content. Devices send a device ID with requests; the CTE uses the device ID to determine the correct formatting for the requesting device. • Transcodes images (GIF and JPEG to BMP and WBMP) and reduces color depth for bandwidth conservation. • Provides real-time content parsing for best performance. Automatically splits pages into screen-sized chunks for small devices and adds device-appropriate navigation. • Issues pages in transit while they are still being transformed, for lower latency. • Supports dynamic content, malformed and overlapping HTML, and large forms in HTML content. • Supports web pages that use any standard encoding and transcodes web pages to the formats required by all supported wireless devices. • Supports JavaScript-dependent form manipulation, event processing, browser redirection, and cookie handling. • For XML-based IP phones, includes a preview of support for audio files that are in .au or .wav (PCM-encoded) formats. To match IP phone speaker characteristics and conserve bandwidth, the CTE converts audio files to 8-bit G.711 Mu-Law audio codecs sampled at 8 Khz. |
| Data and Session Management | <ul style="list-style-type: none"> • Works with any web server and any HTTP gateway (for example, any WAP gateway) and uses standard protocols for communication. Requires no integration effort with existing systems. • Provides load-balancing support with session stickiness. This is a high-performance solution when the CTE is used with a server load balancer. • Provides server redundancy through the server load balancer and redundancy between two CTEs. • Supports in-line operation where server load balancers are not available. Using proxy ARP, the CTE masquerades as the web server and transforms content nonintrusively. • Supports session data (virtual cookies) for devices that do not natively support cookies. • Handles timeouts automatically. A connection times out after 60 seconds of inactivity (just like clients that use HTTP keepalive). An administrator can configure the session timeout interval. • Supports Design Studio connections to the CTE through a firewall or proxy server. |

Table 1 CTE Features (continued)

| Feature | Description |
|-----------------------|---|
| Security ² | <ul style="list-style-type: none"> Fully supports Basic authentication and NTLM proxy authentication. Transcodes authentication protocols for devices that do not natively support authentication (such as Palm handheld devices). Provides SSL sessions with support for HTTP and HTTPS. Fully supports secure cookies. Supports full secure mode, where a client device is always secure to the CTE, independent of the connection to the web server. Works with VPN solutions. Supports digital certificates in PEM³ format that include a private key. Requires only three available ports: 80 (for HTTP requests from wireless devices), 443 (for HTTPS requests), 9001 (for communication with Design Studio over a secure SSL link). |

1. XSL = Extensible Stylesheet Language.

2. For more information, see the [“Security” section on page 5](#).

3. PEM = Privacy Enhanced Mail.

Licensing

The CTE includes FLEXlm licensing. All devices use floating (networked concurrent) licensing. Floating licensing limits the number of concurrent CTE users to the number of licenses purchased. Floating licensing requires no setup or administration.

To obtain additional licenses, you will need to know the host ID of your CTE, as described in the [“Host ID” section on page 34](#). You can upload a new license through the CTE Administration Console, as described in the [“Uploads” section on page 33](#).

Security

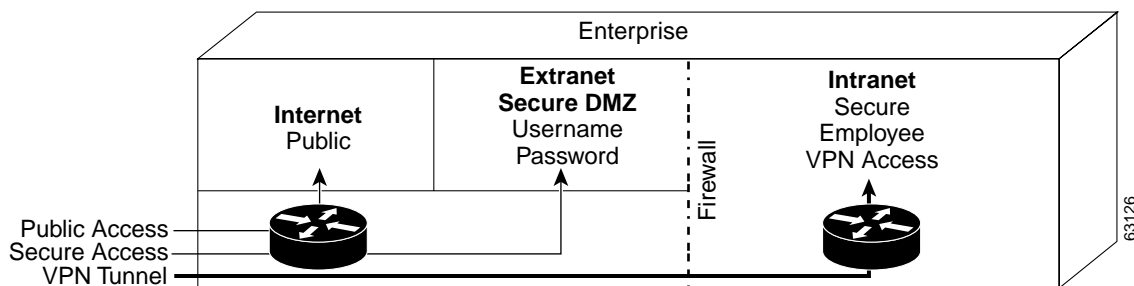
Internet, extranet, and intranet sites require different levels of security, all supported by the CTE. As shown in [Figure 1](#), those sites have the following characteristics:

- Internet sites contain external content, are public, and require no authentication for access. All wireless devices supported by the CTE can access Internet sites.
- Extranet sites also contain external content, but they require authentication for access. Extranet sites are in a secure demilitarized zone (DMZ). All wireless devices supported by the CTE can access extranet sites. (XML-based IP phones cannot authenticate, so they are unable to log in to extranet sites.)

The CTE supports Basic authentication and NTLM proxy authentication and prompts device users for authentication credentials if they are required. In addition, the CTE transcodes authentication protocols for devices that do not natively support authentication (such as Palm devices).

- Intranet sites contain internal content that resides inside the enterprise firewall. From outside the firewall, these sites require a VPN client to tunnel through the firewall. Of the wireless devices supported by the CTE, only the Palm and Pocket PC devices with a Certicom VPN client can access intranet sites.

Figure 1 Security in the Enterprise



Security Issue for WAP Phones and Palm VII Devices

The CTE terminates SSL sessions to provide an endpoint for a secure link. Some PDAs support SSL connections from the device to the CTE. However, WAP phones and the Palm VII device do not support SSL. WAP phones use Wireless Transport Layer Security (WTLS), and Palm VII devices use Elliptical Curve Cryptography (ECC). Carrier gateways usually convert WTLS and ECC to SSL; during the conversion, text is not secure.

Sessions and Connections

When a new device user makes a first request through the CTE, the CTE creates a new session for that user. The CTE must store data for each session; therefore, the number of active sessions is limited by memory.

The CTE supports two configuration options to control the cache that stores session data: maximum and minimum session-timeout thresholds. Both of these settings (Session Timeout and Minimum Session Timeout) can be set through the Advanced > General screen in the CTE Administration screens. For more information, see the [“General” section on page 27](#).

When the maximum session timeout is set and a session has not been active for the specified time period, the CTE terminates the session and wipes the data from the cache. Any session that has been inactive longer than the maximum session timeout can be removed. Data from a terminated session, which includes authentication information and other sensitive data, is physically removed from memory, preventing unauthorized access.

The minimum session timeout determines the minimum time between two requests that a session is guaranteed to be active. For example, if the minimum session timeout is set for 5 minutes, and a user requests information through the CTE every 4 minutes and 59 seconds, that session will remain active indefinitely. If the user waits more than 5 minutes between requests, the session becomes unprotected and can be replaced by a new session.

If the minimum session timeout is not set, the CTE can support the maximum number of sessions. However, not setting a minimum session timeout creates an environment in which each request initiates a new session, and there is no guaranteed stability for any session during busy periods.

The only way to increase the number of active sessions is to increase memory (RAM and/or disk) or to lower the amount of memory allocated to each user. If the memory is lowered, however, performance can suffer because the CTE must retrieve and process the data again.

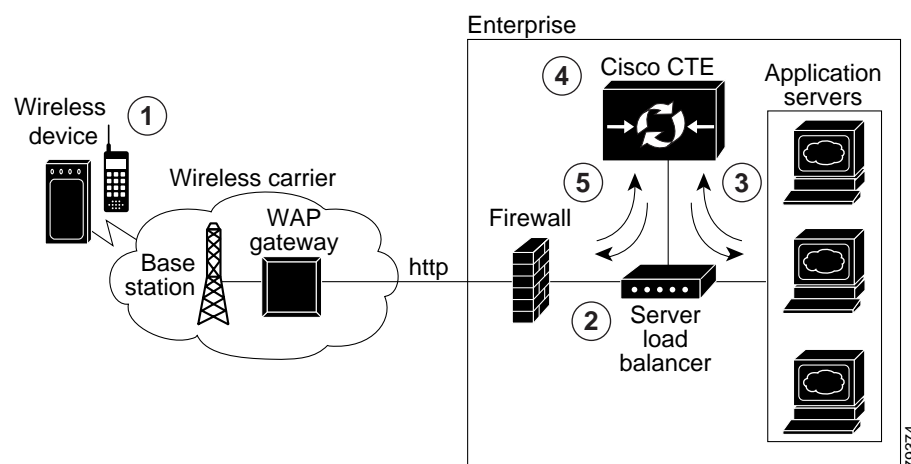
Another variable affecting performance is the number of simultaneous connections. A connection is used for each request. A session can use several simultaneous connections. For example, when a user requests a web page and that page contains images, frames, and other elements, the user's browser makes one request for each element. If a page has ten elements, the initial request makes one connection to retrieve the main page, and the browser makes ten connections to retrieve the ten elements.

Operation Modes

The CTE uses rules supplied by Design Studio to fulfill requests for wireless content. A CTE is typically installed behind a server load balancer. When a wireless device requests a web page, the CTE accepts the request from the wireless device and requests the content from the back-end servers. Functioning as a reverse-proxy, the CTE acts like a web server to the client device and acts like a client device to the web servers.

Figure 2 shows the path that a wireless user request for a web page takes when the CTE is connected to a server load balancer. This configuration is recommended for sites where most of the network traffic intercepted by the CTE uses content supplied by servers directly connected to the server load balancer.

Figure 2 CTE Connected to a Server Load Balancer



Note

The numbers in Figure 2 refer to the following process.

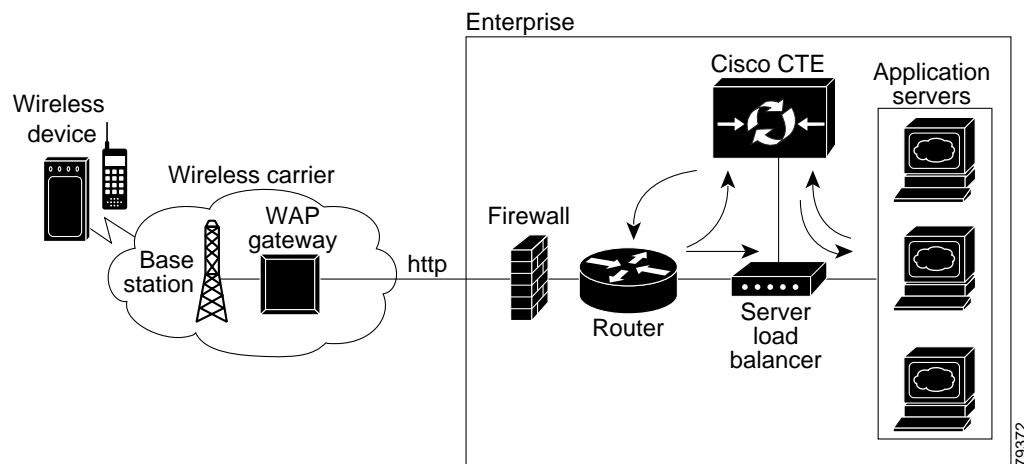
The path the wireless user request takes is as follows:

1. A wireless user requests a URL. A wireless carrier transmits the request to a communications tower, through the WAP carrier gateway, and to the Internet.
2. The server load balancer that receives the request evaluates the request header. The server load balancer directs HTML/XML requests to the web server farm and directs requests from wireless devices to the CTE.
3. The CTE terminates the request and then, acting as a proxy, sends a request to the server load balancer for the HTML/XML page.

4. When the CTE receives the page, it uses the rules in the configuration file to transform the content.
5. The CTE sends the transformed page to the server load balancer for forwarding to the wireless device.

A variation of the preceding configuration is to direct requests from the CTE through a router that sits in front of the server load balancer, as shown in [Figure 3](#). This configuration is recommended for sites where most of the network traffic intercepted by the CTE uses content supplied by servers at other locations. For example, a results page served by a search engine portal contains links to content that resides outside of the domain of the search site.

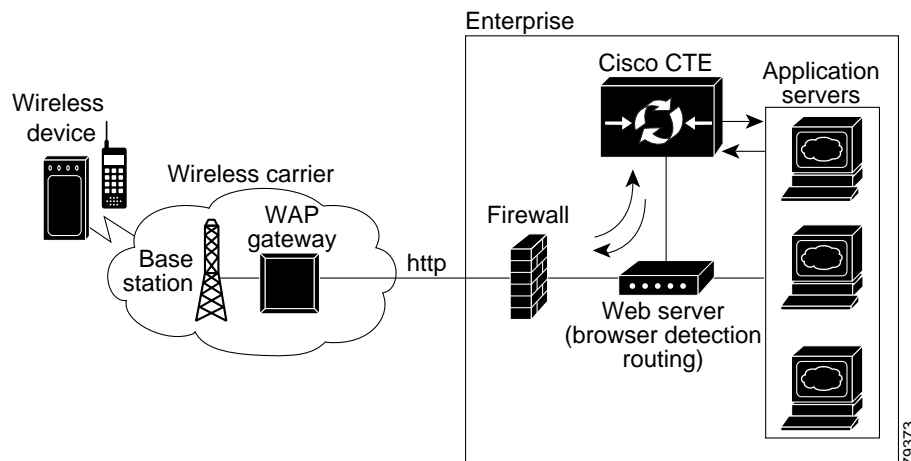
Figure 3 CTE Connected to Router and Server Load Balancer



CTE Connected to Web Server

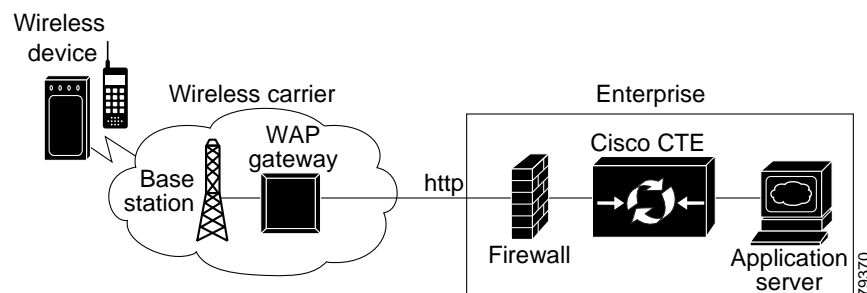
You can connect a CTE to a web server that routes traffic to the CTE or to web servers based on browser detection, as shown in [Figure 4](#).

Figure 4 CTE Connected to a Switch or Web Server That Routes



You can also connect a CTE directly to a web server, as shown in [Figure 5](#). In this case, all web traffic goes through the CTE, which passes HTML/XML requests to the web server and handles requests from wireless devices. This configuration is recommended when you designate specific IP addresses for wireless traffic.

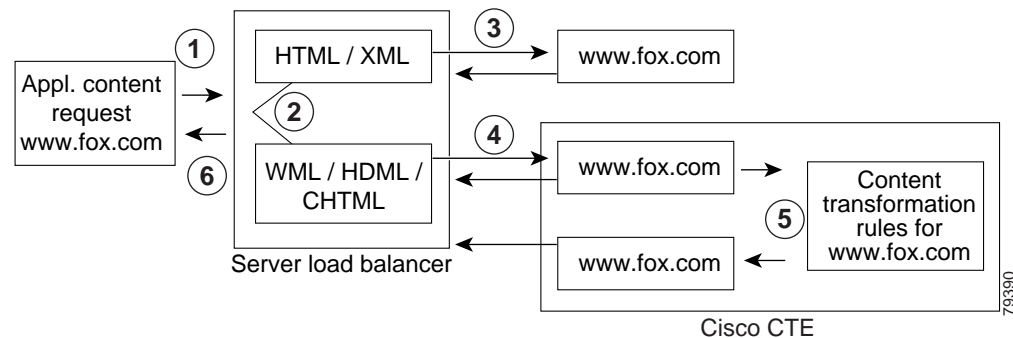
Figure 5 CTE In-line Connection



CTE Traffic Flow

[Figure 6](#) and the following procedure describe how URL requests from a wireless device are handled by the CTE and connected devices.

Figure 6 Traffic Flow for Web Page Requests



Note

The numbers in [Figure 6](#) refer to the steps in the following procedure.

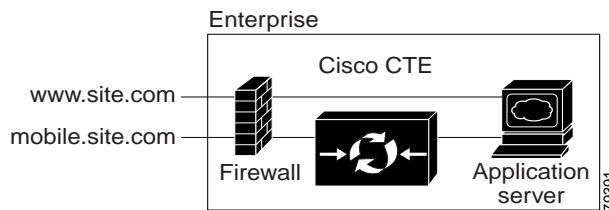
When a wireless device sends a URL to a web server, the traffic flow is as follows:

- Step 1** A wireless user enters a URL (such as `www.fox.com`). The request is transmitted to a communications tower, through the carrier gateway, and to the Internet.
- Step 2** The server load balancer that receives the request looks at the header.
- Step 3** The server load balancer directs HTML/XML requests to the web server farm.
- Step 4** The server load balancer directs requests from wireless devices to the CTE.

- Step 5** The CTE sends the new request to the server load balancer for the HTML/XML content. The CTE, acting as a proxy, sends a request to the server load balancer for the HTML/XML content. The server load balancer obtains the content from a web server and sends it to the CTE.
- Step 6** The CTE uses the rules and device definitions created in Design Studio to transform the content and then sends the transformed content to the server load balancer. The server load balancer forwards the content to the wireless device.

As shown in [Figure 7](#), you can also route requests based on a URL, so that requests from designated URLs (such as mobile.site.com) are passed directly to the CTE.

Figure 7 Requests Directed Based on a URL



Input and Output Encoding

Input encoding, the formats into which information coming to the CTE can be written, is configurable through the Administration Console. By default, input encoding is set to Western European (ISO-8859-1, Latin-1, ASCII). Only one input encoding format can be active at a time.

Output encoding, the formats into which information sent from the CTE can be written, is specified in the Device Definition File (DDF) of each device driver. If there is an error in a particular DDF file, each device driver has a hard-coded default value for output encoding. Refer to Chapter 2 of the *Design Studio User Guide* for output encoding formats.

Configuring the CTE

The configuration instructions in this publication assume the following setup:

- The CTE is installed and connected to a second computer through a serial port.
- The devices to which you are connecting the CTE, such as a server load balancer, are already part of a working configuration. This publication does not, for example, cover the steps for configuring web servers or a web server farm with a server load balancer.

The “[Operation Modes](#)” section on [page 7](#) covers typical network configurations for the CTE. Use [Table 2](#) as a guide to determining the best location for a CTE, based on network topology and website characteristics.

Table 2 CTE Network Location Guidelines

| Network Topology and Website Characteristics | Network Location of CTE |
|--|--|
| A server load balancer sits in front of one or more web servers. Most of the network traffic to be intercepted by the CTE uses website content supplied by servers directly connected to the server load balancer. | Behind the server load balancer or In front of a web server that routes traffic to one or more CTEs or to web servers based on browser detection |
| A server load balancer sits in front of one or more web servers. Most of the network traffic to be intercepted by the CTE uses website content supplied by servers at other locations. For example, a results page served by a search engine portal contains links to content that resides outside of the domain of the search site. | Behind the server load balancer with requests from one or more CTEs directed through the router |
| One web server. All traffic destined for the web server goes through the CTE. | In front of the web server |

The general process for configuring a CTE and connected devices is as follows:

1. Draw a diagram of the data flow for the CTE, including all IP addresses and VLAN numbers.
2. Physically connect the CTE to the network.
Depending on your network topology, you may need to use one or both of the CTE ports (NICs).
3. Verify that the CTE can ping the device connected to it (such as a server load balancer).
4. If you are configuring multiple CTEs, associate the various CTE network connections with a CTE server farm.
5. Configure the server load balancer so that the CTE can access web content on the web servers.
6. Configure the server load balancer so that the CTE is accessible by clients requesting web content.
7. Verify that the data flow of the CTE is as planned.
8. If a client does not require in-line data transformation by the CTE, direct its traffic to the web servers if possible.

These sections describe how to configure the CTE and connected devices:

- [Preparing to Connect and Configure the CTE, page 11](#)
- [Configuring the CTE for the First Time, page 12](#)
- [Configuring a CTE Connected Directly to a Web Server, page 13](#)
- [Configuring a CTE Connected to a Server Load Balancer, page 16](#)
- [Configuring a CTE Located Behind a Firewall or Proxy Server, page 18](#)
- [Creating and Removing Static Routes, page 19](#)

Preparing to Connect and Configure the CTE



Note

Before you deploy the CTE, verify that port 9001 is not accessible from outside of your firewall. The CTE communicates with Design Studio through port 9001 using clear-text transmissions. Only ports 80 and 443 should be visible from outside of your firewall.

Most firewalls allow administrators to deny external IP addresses access to specific ports that are set up internally. Refer to your firewall administrator guide for information on setting up rules to block specific ports.

To connect the CTE to a network, you need two network cables. Only one cable may be necessary if you connect the CTE directly to one web server. Before configuring the CTE and connected devices, plan the network information you want to use for the following, as appropriate:

- VLAN number, port numbers, and IP addresses for the client-side connections between the CTE and a server load balancer, router, or web server (directly connected to the CTE)
- VLAN number, port numbers, and IP addresses for the server-side connections between the CTE and a server load balancer



Note

The CTE does not work with Dynamic Host Configuration Protocol (DHCP). You must use static IP addresses for the CTE.

- The virtual IP address that you want to assign to a masquerade host
- CTE server farm names and their virtual IP addresses

Configuring the CTE for the First Time

The first time that you power on the CTE, you are prompted to specify login credentials and basic network settings in the serial console, a command-line interface. The CTE serial console provides access to some settings and allows you to restart or shut down the CTE.

If you completed the installation procedures described in the *Cisco CTE 1400 Series Hardware Installation Guide*, you already have a CTE serial console open on a computer that has a serial connection to the CTE. If the CTE serial console has been closed, open it by starting the terminal emulation application and opening the connection you created to the CTE. If the CTE serial console does not open, check the following:

- Verify that the CTE is powered on.
- Check the settings in the terminal emulation application. Set the serial connection to 9600 bits per second, 8 data bits, no parity, and 1 stop bit.

To configure the CTE for the first time, perform these steps:

-
- Step 1** If the serial console is prompting you for a username, enter **root**.
- Step 2** Enter a password of 8 or more characters. If prompted to verify the password, reenter it.

The CTE prompts for the following:

```
IP address [x.x.x.x] (Enter 0 to clear):
Netmask [x.x.x.x] (Enter 0 to clear):
Gateway [x.x.x.x]:
```

Step 3 Enter the IP address and netmask of the eth0 port and the IP address of the default gateway.

Step 4 The CTE prompts for the DNS server and domain name information:

```
DNS server [0] [x.x.x.x] (Enter 0 to clear): x.x.x.x
DNS server [1] [x.x.x.x] (Enter 0 to clear):
DNS server [2] [x.x.x.x] (Enter 0 to clear):
Domain Name [ ] (Enter 0 to clear):
```

The CTE requires one DNS server to resolve names and provides a default value for one DNS server. You can change the IP address or press **Enter** to accept the default value. You can also optionally set a default domain name, such as `www.fox.com`.

Step 5 If you make changes, the CTE prompts you to commit the changes. Type **yes** to commit the changes.

The Main Menu of the CTE serial console appears.

Step 6 Type **1** and then **6** to ping the connected device.

If the ping is successful, you have completed the initial configuration. If the ping is not successful, check your connections, return to the serial console Main Menu, and type **0** (Express Setup) to change settings as needed.

Configuring a CTE Connected Directly to a Web Server

You can connect a CTE directly to a web server if your site has only one web server and you want all traffic destined for the web server to pass through the CTE. The CTE determines how to handle requests for web content based on the request header, which indicates the type of device making the request. The CTE intercepts requests from supported mobile devices and passes through other requests.

Connecting a CTE directly to a web server does not require any changes to the web server configuration.

The following sections describe how to connect a CTE to a web server and configure the CTE to work with the web server:

- [Connecting a CTE to a Web Server, page 13](#)
- [Configuring CTE Network Settings, page 14](#)

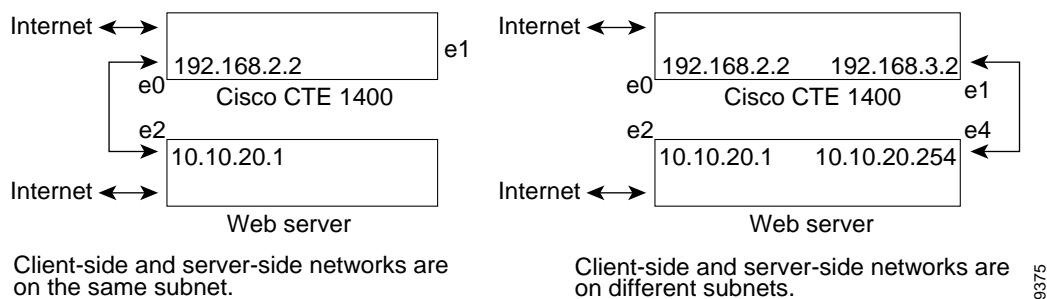
Connecting a CTE to a Web Server

Connecting a CTE to a web server requires either one or two network cables as follows:

- If the CTE can access the web server from the same subnet as it receives client requests, you can use one network cable. Connect the CTE e0 (NIC 1) port to the client-side network.
- If the web server and clients are on different subnets, you must use two network cables and connect the CTE as follows:
 - Connect the CTE e0 (NIC 1) port to the client-side network.
 - Connect the CTE e1 (NIC 2) port to the server-side network, directly or indirectly. In most cases, the gateway IP address will be on the same subnet as the web server.

Figure 8 shows how to connect a CTE to a web server.

Figure 8 CTE Connected to Web Server



Note

The IP addresses used throughout this publication are sample addresses, not actual ones.

Configuring CTE Network Settings

Use the CTE Administration Console to configure network settings. The following procedure notes the settings to use for the example configuration shown in Figure 8. This general procedure is used regardless of the CTE location in your network.

To configure network settings, perform these steps:

- Step 1 From a web browser on a PC connected to the CTE serial port, enter the following URL to connect to the Administration Console:
https://ipAddress:adminPort
 where:
 - *ipAddress* is the IP address of your CTE
 - *adminPort* is the administration port of your CTE (usually 9001)
- Step 2 Click **Yes** if a Security Alert dialog box appears.
- Step 3 Click the **Network** tab.
 You will be prompted to log in.
- Step 4 Enter **root** in the User Name field and enter the password you specified when you first logged in to the CTE.



Note

You can create additional administrative usernames and passwords from the CTE serial console. For information, see the “Managing Administrative User Accounts” section on page 34.

The Network > Interfaces screen appears.

| Main | Network | Advanced |
|-------------------|---------------------------------------|---------------------------------------|
| Interfaces | Interface 0 IP Address | <input type="text"/> |
| Ports | Interface 0 Subnet Mask | <input type="text"/> |
| DNS | Interface 0 Masq Host | <input type="text"/> |
| Routes | Interface 0 Duplex Mode | auto <input type="button" value="v"/> |
| Proxies | Interface 0 MTU | 1500 <input type="text"/> |
| Hosts | Interface 1 IP Address | <input type="text"/> |
| | Interface 1 Subnet Mask | <input type="text"/> |
| | Interface 1 Masq Host | <input type="text"/> |
| | Interface 1 Duplex Mode | auto <input type="button" value="v"/> |
| | Interface 1 MTU | 1500 <input type="text"/> |
| | Default Gateway | <input type="text"/> |
| | Gateway Interface | eth0 <input type="button" value="v"/> |
| | <input type="button" value="SUBMIT"/> | |

79385

Step 5 Specify the IP address and subnet mask for interfaces 0 and 1 as follows:

Interface 0 IP Address: **192.168.2.2**
 Interface 0 Subnet Mask: **255.255.255.0**

Interface 1 IP Address: **192.168.3.2**
 Interface 0 Subnet Mask: **255.255.255.0**

Step 6 If needed, define the Masquerade Hosts for Interface 0 and Interface 1.

The masquerade host is an IP address that can be used for Network Address Translation (NAT). NAT makes all requests appear to originate from the same client, so that the CTE sends its response to the request back on the correct network connection. If the NAT IP address is not defined, the CTE sends responses out through the NIC where the gateway is identified.

Step 7 Use the default settings for Duplex Mode and the Maximum Transmission Unit (MTU) unless you need to change them.

Step 8 Enter the Default Gateway IP address and choose the interface used for the gateway.

For this example you would enter **10.10.20.254** and choose **eth1** from the Gateway Interface menu.

Step 9 Click **Submit** to save your changes.

For help with configuring other network and operational settings, see the [“Using the CTE Administration Console”](#) section on page 21.

Configuring a CTE Connected to a Server Load Balancer

You can connect a CTE to a server load balancer. Characteristics of this configuration include the following:

- Incoming web traffic is intercepted by the server load balancer and load balanced between the CTEs (if more than one CTE is in use). All incoming client IP addresses appear as a single IP address through NAT.
- When a CTE receives a request through port 80 for a valid web page, it issues a temporary redirect to the client so that the connection uses HTTPS on port 443. The address to which the client is redirected is determined by the masquerade host IP address set for the CTE.

If multiple CTEs are in use, each CTE has a different masquerade host IP address. In addition, the CTE modifies all URLs embedded within a page to include the masquerade host IP address. This use of the masquerade host IP address ensures that the redirected client returns to the CTE it first encountered, providing session stickiness. The association between a particular request and the CTE is broken only when the client makes a new connection on port 80.

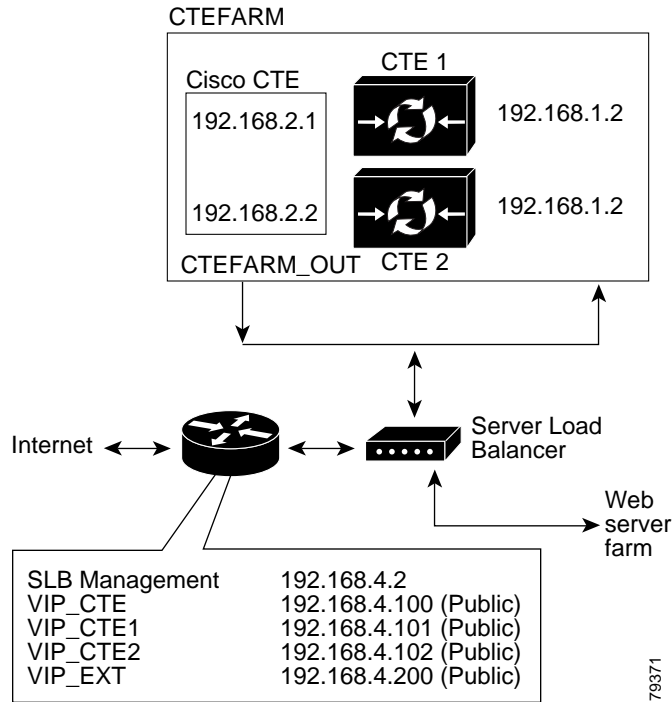
- The CTEs request content from web servers through the alias IP address set for the server-side VLAN.

The CTE farm and the web server farm are directly accessible through load-balanced virtual IP (VIP) addresses. This configuration enables you to direct traffic that originates from a wireless device to the CTE farm VIP address.

To operate with the CTE, the server load balancer must be configured to provide real-time header parsing.

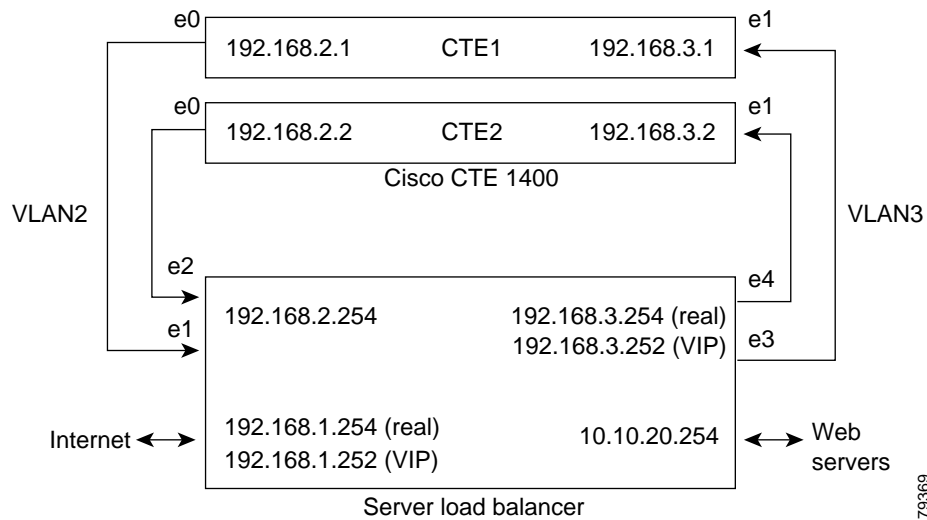
[Figure 9](#) shows a server load balancer setup in which CTE requests go to the server load balancer, rather than the router.

Figure 9 CTE Connected to a Server Load Balancer (Requests Not Directed Through Router)



This section uses the sample configuration shown in [Figure 10](#).

Figure 10 CTE Connected to Server Load Balancer



The following sequence of events occurs when a client requests content, and the SLB encounters a CTE-supported user agent string:

1. The client requests a web page from a domain.
2. The SLB forwards the request to the CTE.
3. The CTE reissues the request to the default host masquerading as the user agent.

4. The SLB receives the request and directs it to the appropriate web server.
5. The web server retrieves the content and passes it through the SLB to the CTE.
6. The CTE transforms the content and sends it back through the SLB and on to the client device.

The following sections describe how to configure a CTE with a server load balancer:

- [Configuring the CTE Connected to a Server Load Balancer, page 17](#)
- [Configuring the Server Load Balancer, page 18](#)

Configuring the CTE Connected to a Server Load Balancer

To establish the physical connection, do the following:

- Connect the CTE e0 (NIC 1) port of each CTE to the client-side network.
- Connect the CTE e1 (NIC 2) port of each CTE to the server-side network.

Use the CTE Administration Console to configure network settings. For example, specify the interfaces for CTE1 as follows:

Interface 0 IP Address: **192.168.2.1**
 Interface 0 Subnet Mask: **255.255.255.0**
 Interface 0 Masq Host: **192.168.2.1**

Interface 1 IP Address: **192.168.3.1**
 Interface 1 Subnet Mask: **255.255.255.0**
 Interface 1 Masq Host: **192.168.2.1**

Default Gateway: **192.168.3.254**
 Gateway Interface: **eth1**

Configuring the Server Load Balancer

The basic process for configuring a server load balancer is as follows:

1. Establish a serial connection to the server load balancer.
2. Define the interfaces to the VLANs.
3. Configure the circuits.
4. Define services, owners, and content rules.
5. Disable parsing of HTTP headers received on the virtual IP addresses (improves performance).
6. Check network connectivity.

Following are the general steps for configuring a server load balancer, based on the configuration shown in [Figure 10](#).

To configure a server load balancer for operation with a CTE, perform these steps:

-
- Step 1** On a computer that is connected to the console port of the server load balancer, log in to the device's command line interface.
 - Step 2** Create links between the CTE ports and the server load balancer by adding the client-side and server-side VLANs and defining the interfaces to the VLANs.

In the sample configuration in [Figure 10](#), the e1 and e2 ports are the interfaces for VLAN2; e3 and e4 are the interfaces for VLAN3.

- Step 3** Specify the IP addresses for the VLAN circuits.
- In the sample configuration, the IP address for the VLAN2 circuit is 192.168.2.254. The IP address for the VLAN3 circuit is 192.168.3.254.
- Step 4** Create services to identify the two CTEs.
- In the sample configuration, the IP address for the CTE1 service is 192.168.2.1, and the IP address for the CTE2 service is 192.168.2.2.
- Step 5** Create an owner so that you can define content rules for the CTE1 and CTE2 services.
- Step 6** Create a Layer 3 content rule for the services.
- In the sample configuration, the content rule is configured with the virtual IP address 192.168.3.252 and is added to the CTE1 and CTE2 services.
- Step 7** Disable parsing of HTTP headers received on the virtual IP addresses.
- Step 8** Check network connectivity.
-

Configuring a CTE Located Behind a Firewall or Proxy Server

If your CTE is behind a firewall or proxy server, you will need to set up CTE proxy settings through the Administration Console. For more information, see the [“Proxies” section on page 26](#).

If there is a firewall or proxy server between the computer on which Design Studio is installed and the CTE, Design Studio users will need to specify the host and port for HTTP and HTTPS connections when logging in to Design Studio.

Creating and Removing Static Routes

When setting up communication with another host or network, you will sometimes need to create a static route from the CTE to the new destination. Set up static routes on the CTE port not being used by the default gateway.

To create a static route, perform these steps:

-
- Step 1** In the CTE Administration Console, click the **Network** tab, and then click **Routes** in the left column.
- Step 2** Enter the IP address of the destination LAN.
- Step 3** Enter the subnet mask for the gateway device. The default is 255.255.255.0.
- Step 4** Enter the IP address for the default gateway. If you do not specify a gateway, the CTE can access content only on the local network.
- Step 5** Select the Interface for the static route. The default is eth0.
- Step 6** Click **Add Static Route**.
-

To test a static route, perform these steps:

-
- Step 1** From the CTE serial console, type **1** (Configure Network Interfaces).
 - Step 2** Type **6** (Ping).
 - Step 3** Enter the host IP address for the device you want to ping and press **Enter**.

If you are successfully communicating with the other machine, messages will appear saying that the same number of packets were transmitted and received, and zero packets were lost.

If you are not communicating with the other machine, the status messages indicate that zero packets were received and all the packets were lost. Return to Step 1 and recreate the static route.

To remove a static route, perform these steps:

-
- Step 1** In the CTE Administration Console, click the **Network** tab, and then click **Routes** in the left column.
 - Step 2** Click **Clear All Routes**.
-

Static Route Example

Suppose the IP address of the eth0 port on your CTE is 10.0.16.20 and there has been a request to access information at 129.6.0.20, to which you currently have no path. You can create a static route through the Ethernet port that is not set as your CTE default gateway, and out to the requested network address, as shown in [Figure 11](#).

Figure 11 Building a Static Route

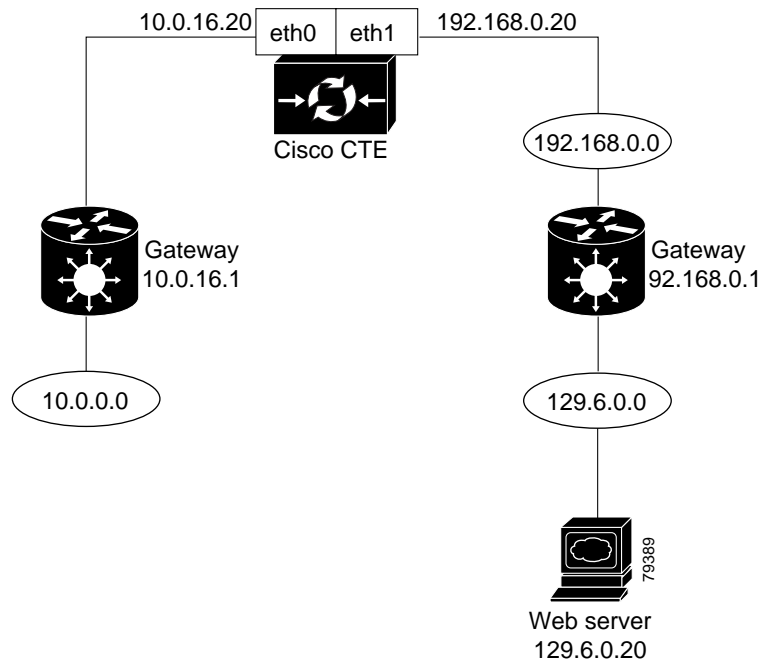


Figure 11 shows the following connections:

- The eth0 port (IP address 10.0.16.20) leads to the default gateway (IP address 10.0.16.1), which connects to the rest of the 10.0.0.0 network.
- The eth1 port (IP address 192.168.0.20) is set to communicate with the 192.168.0.0 network and its gateway (IP address 192.168.0.1). Through this gateway, the eth1 port can communicate with the 129.6.0.0 network, and the web server at IP address 129.6.0.20.

To set up this static route, you need to establish the path between the eth1 port and IP address 129.6.0.20.

To set up a static route, perform these steps:

-
- Step 1** In the CTE Administration Console, click the **Network** tab, and then click **Routes** in the left column.
- Step 2** Set the IP address of the destination LAN to **129.6.0.0**.
- Step 3** Set the subnet mask for the gateway device to the default value, **255.255.255.0**.
- Step 4** Set the IP address of the default gateway to **192.168.0.1**.
- Step 5** Choose **eth1** as the gateway device interface.
- Step 6** Click **Add Static Route**.
-

Using the CTE Administration Console

From the CTE Administration Console, you can manage the CTE with a web browser. The Administration Console provides access to all CTE configuration settings, including the following:

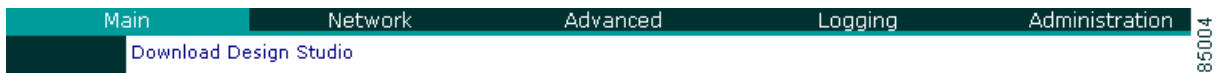
- **Network:** Configure interfaces, ports, DNS settings, static routes, and proxies.
- **Advanced:** Configure CTE operational settings such as session timeout, minimum session time, maximum buffer size, input character encoding method, and JavaScript emulation.
- **Logging:** Identify the CTE for SNMP reporting and enable the logging of SNMP, system log, and system health messages. The CTE reports only the standard MIB-II groups.
- **Administration:** Upload licenses, secure certificates, and server upgrades; manage administrative user accounts; look up the CTE host ID.

Opening the Administration Console

To open the Administration Console, perform these steps:

-
- Step 1** Make sure that the CTE is running.
- Step 2** From a web browser, connect to the CTE by entering the URL:
- https://ipAddress:adminPort**
- where:
- *ipAddress* is the IP address of your CTE
 - *adminPort* is the administration port of your CTE (9001)
- Step 3** If the Security Alert dialog box appears, click **Yes**.

- Step 4** The Main administration screen appears. From this page you can download Design Studio without logging in to the Administration Console.



- Step 5** To download Design Studio, click **Download Design Studio**, and then specify where you want to save the Design Studio installer.
- Step 6** When you select any other CTE Administration menus, the Administration Console login dialog appears.
- Step 7** Enter your administrative username and password.
The Administration screen you selected appears.

**Note**

When working with the Administration Console, click **Submit** to save changes. If a Restart Server button appears after you submit a change, click the button before making more changes.

To view information about a setting, hold the mouse over the setting and view the information area at the bottom of the screen.

Specifying Network Settings

Network settings appear on the screens described in the following sections:

- [Interfaces, page 22](#)
- [Ports, page 24](#)
- [DNS, page 25](#)
- [Routes, page 25](#)
- [Proxies, page 26](#)
- [Hosts, page 27](#)

Interfaces

To specify network interfaces, perform this step:

- In the Administration Console, click **Network** and then **Interfaces**.
The Network > Interfaces screen appears.

| Main | Network | Advanced |
|-------------------|---------------------------------------|---------------------------------------|
| Interfaces | Interface 0 IP Address | <input type="text"/> |
| Ports | Interface 0 Subnet Mask | <input type="text"/> |
| DNS | Interface 0 Masq Host | <input type="text"/> |
| Routes | Interface 0 Duplex Mode | auto <input type="button" value="v"/> |
| Proxies | Interface 0 MTU | 1500 <input type="text"/> |
| Hosts | Interface 1 IP Address | <input type="text"/> |
| | Interface 1 Subnet Mask | <input type="text"/> |
| | Interface 1 Masq Host | <input type="text"/> |
| | Interface 1 Duplex Mode | auto <input type="button" value="v"/> |
| | Interface 1 MTU | 1500 <input type="text"/> |
| | Default Gateway | <input type="text"/> |
| | Gateway Interface | eth0 <input type="button" value="v"/> |
| | <input type="button" value="SUBMIT"/> | |

79385

The Network > Interfaces screen contains the settings described in [Table 3](#).

Table 3 *Interfaces Settings*

| Setting | Description |
|-----------------------------|---|
| Interface 0 IP Address | The IP address for Interface 0. |
| Interface 0 Subnet Mask | The subnet mask for Interface 0 (usually 255.255.255.0). |
| Interface 0 Masquerade Host | The current IP address for NAT for Interface 0, which makes all requests appear to originate from the same client. All connections on interface 0 will be written with this hostname or IP address. |
| Interface 0 Duplex Mode | The duplex mode for Interface 0, which can be auto, full duplex, or half duplex. |
| Interface 0 MTU | The maximum transmission unit (MTU) for Interface 0. The MTU defines the maximum size of each transmitted packet. The default is 1500. |
| Interface 1 IP Address | The IP address for Interface 1. |
| Interface 1 Subnet Mask | The subnet mask for Interface 1 (usually 255.255.255.0). |
| Interface 1 Masquerade Host | The current IP address for NAT for Interface 1, which makes all requests appear to originate from the same client. All connections on interface 1 will be written with this hostname or IP address. |
| Interface 1 Duplex Mode | The duplex mode for Interface 1, which can be auto, full duplex, or half duplex. |
| Interface 1 MTU | The MTU for Interface 1. The MTU defines the maximum size of each transmitted packet. The default is 1500. |

Table 3 *Interfaces Settings (continued)*

| Setting | Description |
|-------------------|--|
| Default Gateway | The IP address of the default gateway device. |
| Gateway Interface | The gateway interface, which can be either eth0 or eth1. |

Ports

To specify network ports, perform this step:

- In the Administration Console, click **Network** and then **Ports**.
The Network > Ports screen appears.

The Network > Ports screen contains the settings described in [Table 4](#).

Table 4 *Ports Settings*

| Setting | Description |
|---------------------|---|
| Listen on Interface | <p>The IP address of the HTTP Listener. The CTE will listen to one or more ports, depending on how you define the HTTP Listener:</p> <ul style="list-style-type: none"> To listen to both the eth0 and eth1 ports, set the HTTP Listener IP address to 0.0.0.0. To listen to both the defined HTTP Listener and one of the Ethernet ports, set the HTTP Listener to an address that is similar to only one of the Ethernet ports. For example, if eth0 is 10.0.16.65 and eth1 is 12.4.20.8 and you want to listen on the HTTP Listener and eth0, set the HTTP Listener to 10.0.16.n. To listen to the HTTP Listener and both Ethernet ports, set the HTTP Listener to an address that is similar to both Ethernet ports. For example, if eth0 is 10.0.16.65 and eth1 is 10.0.16.98, set the HTTP Listener to 10.0.16.n. To listen only to the HTTP Listener, set it to an address that is unlike the eth0 and eth1 ports. |
| Incoming HTTP Port | The incoming HTTP port number. The default is 80. |
| Incoming HTTPS Port | The incoming HTTPS port number. The default is 443. |

Table 4 Ports Settings (continued)

| Setting | Description |
|---------------------|--|
| Administration Port | The administration port number. The default is 9001. Typically, you will not need to change this value. However, you might need to change the value to match your firewall configurations. For example, if the CTE is hosted at an ISP, and the ISP admits only a certain range of ports, you might need to change this setting. |

DNS

To specify DNS settings, perform this step:

- In the Administration Console, click **Network** and then **DNS**.
The Network > DNS screen appears.

The Network > DNS screen contains the settings described in [Table 5](#).

Table 5 DNS Settings

| Setting | Description |
|--------------|---|
| DNS Server 1 | The IP address of the first DNS server. You must define at least one DNS server because the CTE requires a DNS server to resolve names. |
| DNS Server 2 | The IP address of the second DNS server. |
| DNS Server 3 | The IP address of the third DNS server. |
| Domain | The default domain name. Do not precede the domain name with a dot ("."). For example, specify "fox.com", not ".fox.com". |

Routes

To add and remove static routes, perform this step:

- In the Administration Console, click **Network** and then **Routes**.
The Network > Routes screen appears.

The screenshot shows the 'Network' configuration page with the 'Routes' section active. The left sidebar lists navigation options: Interfaces, Ports, DNS, Routes (highlighted), Proxies, and Hosts. The main content area has tabs for 'Main', 'Network', and 'Advanced'. Under the 'Network' tab, the following fields are visible: Destination LAN IP (empty), Subnet Mask (empty), Gateway (empty), and Interface (dropdown menu showing 'eth0'). An 'Add Static Route' button is located at the bottom of the form. A vertical ID number '79384' is on the right side.

For more information, see the [“Creating and Removing Static Routes”](#) section on page 19.

Proxies

To specify proxy host settings, perform this step:

- In the Administration Console, click **Network** and then **Proxies**.
The Network > Proxies screen appears.

The screenshot shows the 'Network' configuration page with the 'Proxies' section active. The left sidebar lists navigation options: Interfaces, Ports, DNS, Routes, Proxies (highlighted), and Hosts. The main content area has tabs for 'Main', 'Network', and 'Advanced'. Under the 'Network' tab, the following fields are visible: Outbound Proxy Host (empty), Outbound Proxy Port (8080), Outbound Secure Proxy Host (empty), Outbound Secure Proxy Port (8080), and Proxy Exclusion List (empty). A 'SUBMIT' button is located at the bottom right of the form. A vertical ID number '79383' is on the right side.

The Network > Proxies screen contains the settings described in [Table 6](#).

Table 6 Proxies Settings

| Setting | Description |
|----------------------------|--|
| Outbound Proxy Host | The IP address of an outbound proxy server. This setting sets a proxy server for HTTP (nonsecure requests). If your CTE is behind a firewall or proxy server, the CTE will use these settings for HTTP requests. |
| Outbound Proxy Port | The outbound port number on the outbound proxy server. |
| Outbound Secure Proxy Host | The IP address of an outbound secure proxy server, which sets a proxy server for HTTPS (secure requests). |
| Outbound Secure Proxy Port | The outbound port number on the outbound secure proxy server. |
| Local Proxy Exclusion | If checked, specifies that the defined proxy server is ignored in the local domain (specified on the Network > Interfaces page). |
| Proxy Exclusion List | The IP addresses, hostnames, or domain names that should not use the defined proxy server. Use a space to separate items. |

Hosts

To map CTE hostnames to IP addresses, perform this step:

- In the Administration Console, click **Network** and then **Hosts**.

The Network > Hosts screen appears.

From the Hosts screen, you can map CTE hostnames to IP addresses. The host aliases that you define override DNS settings. Defined hosts appear in the Hosts Table.

After you add a host, you must click the **Restart Server** button that appears after you click **Submit**.

To clear all hosts, click **Clear Hosts Table**.

Although the CTE does not include an NIS client and thus does not support commands such as **yppbind** and **nslookup**, name resolution libraries can resolve CTE hostnames by checking the `/etc/hosts` file.

Specifying Advanced Settings

Settings that affect the overall operation of the CTE appear in the screens described in the following sections:

- [General, page 27](#)
- [IP Phone, page 30](#)

General

To specify general operational settings, perform this step:

- In the Administration Console, click **Advanced** and then **General**.

The Advanced > General screen appears.

| Main | Network | Advanced | Logging |
|----------|----------------------------------|---|---------|
| General | | | |
| IP Phone | | | |
| Date | | | |
| | Interface 0 Default URL | <input type="text"/> | |
| | Interface 1 Default URL | <input type="text"/> | |
| | Default Host | <input type="text"/> | |
| | SLB Mode | <input type="checkbox"/> | |
| | Session Timeout | <input type="text" value="0"/> | |
| | Minimum Session Time | <input type="text" value="0"/> | |
| | Max Buffer Size (bytes) | <input type="text" value="524288"/> | |
| | Security | No HTTPS <input type="button" value="v"/> | |
| | Browser Masquerade | Netscape 4.72 <input type="button" value="v"/> | |
| | Input Character Encoding | Western European (ISO) <input type="button" value="v"/> | |
| | Unrestricted Proxy | <input checked="" type="checkbox"/> | |
| | Client user-agent pass-through | <input type="checkbox"/> | |
| | Client IP pass-through | <input type="checkbox"/> | |
| | Administrator Email-To Address | <input type="text"/> | |
| | Administrator Email-From Address | <input type="text"/> | |
| | Mail Server Address | <input type="text"/> | |
| | | <input type="button" value="SUBMIT"/> | |

79379

The Advanced > General screen contains the settings described in [Table 7](#).

Table 7 General Screen Settings


| Setting | Description |
|---------------------------|--|
| Interface 0/1 Default URL | <p>The default URL that the CTE will proxy if you attempt to access the CTE directly. For example, if a device user requests <code>http://CTEIPAddress</code>, the CTE will proxy the default URL specified. You might want to set a default URL if you have your own portal page and the CTE is operating as the default gateway.</p> <p> Note If you want to deploy ScreenTop Menu, do not specify a default URL. The CTE treats ScreenTop Menu as the default URL. If you specify a default URL, it takes precedence and the CTE will not send ScreenTop Menu to devices.</p> |
| Default Host | <p>The default host that the CTE uses for requests that include a relative link. The CTE will substitute for any relative address received the IP address of the default host you specify. For example, if a device user requests <code>http://CTEIPAddress/directory/file.html</code>, the CTE will request <code>http://defaultHost/directory/file.html</code>.</p> |
| Session Timeout | <p>The amount of time a session is allowed to last. The default is 30 minutes. To disable session timeout, specify 0. For more information about sessions, see the “Sessions and Connections” section on page 6.</p> |

Table 7 General Screen Settings (continued)

| Setting | Description |
|---------------------------|--|
| Minimum Session Time | The period of time a session is guaranteed to remain active if Session Timeout is not set to "0". Setting a minimum session time protects current users when the CTE has many active sessions. When the active sessions threshold is reached, the CTE denies a new user instead of evicting a current user whose minimum session time has not elapsed. The default is 5 minutes. For more information, see the "Sessions and Connections" section on page 6 . |
| Max Buffer Size (bytes) | The maximum buffer size. The default is 524288. |
| Security | The connections method, either No HTTPS (none of the connections will be secure) or Force HTTPS (all connections will be secure). The default is No HTTPS. If the CTE must proxy secure sites, set Security to Force HTTPS. |
| Browser Masquerade | The user agent to use for transformed pages. Choose Netscape or Internet Explorer if you need the web server to use logic particular to one of those browser types when serving content to a device. Choose Cisco Content Transformation Engine if you want the CTE to act as its own user agent, which is useful for tracking device traffic for billing or other purposes. |
| Input Character Encoding | The input character encoding method used for all pages processed by the CTE. We recommend that you use Latin-1 encoding for HTML pages and UTF-8 encoding for XML pages. |
| JavaScript Emulation | Enables or disables JavaScript emulation. When this function is enabled, the CTE requires additional memory for each page, even if the page does not contain JavaScript. We recommend that you use the default value, Enabled. |
| JavaScript Exclusion List | The URLs for which you do not want JavaScript emulation to take place. This field interprets standard regular expression wildcard characters. For example, you can exclude groups of pages with a string such as <code>www.fox.com/prod?/*</code> . Design Studio users might request an exclusion if they want to use the contents of the noscript element rather than the script element for a particular page. You can list multiple space-separated URLs. |
| Outbound KeepAlive | Enables or disables outbound keepalive messaging. When enabled, outgoing keepalive holds the connection to the server open for further requests. We recommend that you use the default value, Enabled. |
| Incoming KeepAlive | Enables or disables incoming keepalive messaging. When enabled, incoming keepalive holds the connection to the client open for further requests. We recommend that you use the default value, Disabled. |
| Unrestricted Proxy | Enables or disables unrestricted proxy support. When this function is disabled, the CTE proxies only the web pages it has transformed to prevent access to protected servers that are on the same subnet as the CTE. The default is Enabled. |

IP Phone

Some IP phones require a username and password in order to accept pushed data.

To specify credentials for IP phone push operations, perform these steps:

-
- Step 1** In the Administration Console, click **Advanced** and then **IP Phone**.
The Advanced > IP Phone screen appears.
- Step 2** Specify a username to be used as the default IP phone username.
- Step 3** Specify a password to be associated with the default IP phone username.
- Step 4** Click **Submit**.
-

Date

To change the system date and time, perform these steps:

-
- Step 1** In the Administration Console, click **Advanced** and then **Date**.
The Advanced > Date screen appears.
- Step 2** Click **Update Time** to update the date and time on the CTE.
-

Specifying Logging Settings

Logging settings appear on the screens described in the following sections:

- [Configure, page 30](#)
- [System Log, page 31](#)
- [Health Log, page 32](#)
- [SNMP, page 32](#)
- [Version, page 32](#)

The logging features allow you to enable or disable the logging of system performance information and view the information collected during the logging. By reviewing the information provided, you can track unusual changes that affect the stability and performance of the CTE.

Configure

To configure logging, perform this step:

- In the Administration Console, click **Logging** and then **Configure**.
The Logging > Configure screen appears.

The Logging > Configure screen contains the settings described in [Table 8](#).

Table 8 *Configure Settings*

| Setting | Description |
|-------------------|---|
| SNMP Location | The CTE location, such as a rack, building, or network, to be monitored for SNMP messages. |
| SNMP Contact | The name of the CTE contact person. |
| SNMP Community | The password of the string that is used to read statistics from the CTE. |
| SNMP Port | The CTE port number. |
| Enable SNMP | <p>Enables or disables the logging of SNMP messages, which you can view from the SNMP screen of the Logging tab. When SNMP is enabled, the CTE reports the following standard MIB-II groups:</p> <ul style="list-style-type: none"> • MIB-II system group (1.3.6.1.2.1.1) • Interfaces group (1.3.6.1.2.1.2) • Address Translation (AT) group (1.3.6.1.2.1.3) • Internet Protocol (IP) group (1.3.6.1.2.1.4) • Internet Control Message Protocol (ICMP) group (1.3.6.1.2.1.5) • Transmission Control Protocol (TCP) group (1.3.6.1.2.1.6) • User Datagram Protocol (UDP) group (1.3.6.1.2.1.7) <p>The CTE does not support CTE-specific SNMP data.</p> |
| Enable System Log | Enables or disables the logging of system messages, which you can view from the System Log screen of the Logging tab. |
| Enable Health Log | Enables or disables the logging of health data, which you can view from the Health Log screen of the Logging tab. |

System Log



Note

Before you can view the System Log, make sure that you have enabled the logging of system messages on the Logging > Configure screen.

To view the system log, perform this step:

- In the Administration Console, click **Logging** and then **System Log**.

Health Log



Note

Before you can view health data, make sure that you have enabled the Health Log setting on the Logging > Configure screen.

To view health data, perform this step:

- In the Administration Console, click **Logging** and then **Health Log**.

The health log includes device-driver statistics, the number of requests received from each listed device, and load statistics. The load statistics displayed are as follows:

- Up Time—How long the CTE has been running in the current session; in days, hours, and minutes
- System Load Average—The average system load; measured for the past 1, 5, and 15 minutes
- Total Memory (Gb)—The total memory capacity
- Used Memory (Kb)—The amount of memory used
- Free Memory (Kb)—The amount of free memory
- Number of Connections—The number of connections serviced
- Number of Inbound Requests—The number of requests coming to the CTE
- Number of Outbound Requests—The number of requests going out from the CTE
- Number of SSL Connections—The number of Secure Sockets Layer connections
- Number of non-SSL Connections—The number of non-Secure Sockets Layer connections
- DNS lookup failures—The number of requests that failed because of DSN lookup failure
- Unknown device type—The number of requests that failed because the device type was unknown
- Bad header failures—The number of requests that failed because of bad header addresses

SNMP



Note

Before you can view the SNMP Log, be sure that you have enabled the logging of SNMP messages on the Logging > Configure screen.

To view a log of SNMP messages, perform this step:

- In the Administration Console, click **Logging** and then **SNMP**.

Version

To display the version of your installed CTE, perform this step:

- In the Administration Console, click **Logging** and then **Version**.

Specifying Administration Settings

Administration settings appear on the screens described in the following sections:

- [Users, page 33](#)
- [Uploads, page 33](#)
- [Host ID, page 34](#)

Users

To use Design Studio, a user must specify a username and password that are set up through the Administration > Users screen. You can also use that screen to delete Design Studio users and to change user passwords.

To add a Design Studio user account, perform these steps:

-
- Step 1** In the Administration Console, click **Administration** and then **Users**.
- Step 2** Type a username and password.
Usernames must be at least 6 characters. Passwords must be at least 8 characters.
- Step 3** Click **Add User**.
-

To add a Design Studio user account, perform these steps:

-
- Step 1** In the Administration Console, click **Administration** and then **Users**.
- Step 2** Click the checkbox beside the username you want to delete.
- Step 3** Click **Delete User**.
-

To reset a Design Studio user password, perform these steps:

-
- Step 1** In the Administration Console, click **Administration** and then **Users**.
- Step 2** Click the checkbox beside the username whose password you want to reset.
- Step 3** Enter a new password.
- Step 4** Click **Reset Password**.
-

Uploads

Use the Administration > Uploads screen to upload licenses and secure certificates and to upgrade the server.



Note

When you upload a server upgrade, the CTE drops the active sessions, so it is best to upgrade the server when you know that traffic is at a minimum.

To upload a file, perform these steps:

-
- Step 1** In the Administration Console, click **Administration** and then **Uploads**.
 - Step 2** Click the **Browse** button for the type of file you want to upload.
 - Step 3** Locate the file you want to upload and click **Open**.
 - Step 4** Click **Submit** to upload the file.
 - Step 5** If you uploaded a certificate, click **Network** and then **Interfaces**. Set the value for the Interface 0 Masq Host to the DNS name for which the certificate was registered.
-

Host ID

When you purchase additional licenses, a salesperson will request the host ID of the CTE for which you are purchasing licenses.

To look up the host ID:

- In the Administration Console, click **Administration** and then **Host ID**.

Managing Administrative User Accounts

The first time that you start the CTE, you must log in as root and create a password for the root account. You can create and manage additional administrative accounts through the CTE serial console.

To add, delete, and list administrative user accounts, perform these steps:

-
- Step 1** On a PC connected to the CTE serial port, start a terminal emulation application and open the connection already created for the CTE.
 - Step 2** Log in to the serial console using the root username and password.
 - Step 3** When the Main Menu appears, type **2** (Manage Administrative Users) and press **Enter**.
 - Step 4** Follow the on-screen prompts to manage administrative user accounts.
-

To change an administrative user account password, perform these steps:

-
- Step 1** On a PC connected to the CTE serial port, start a terminal emulation application and open the connection already created for the CTE.
 - Step 2** Log in to the serial console using the username whose password you want to change.
 - Step 3** When the Main Menu appears, type **2** (Manage Administrative Users) and press **Enter**.
 - Step 4** Follow the on-screen prompts to change a password.
-

Shutting Down and Restarting the CTE Server Software

Always use the CTE serial console to shut down the CTE server software. Never shut down the CTE server software by powering off the CTE.

To shut down the CTE server software, perform these steps:

-
- Step 1** In the CTE serial console, type **4** (Restart/Shutdown) and press **Enter**.
 - Step 2** Type **1** or **S** and press **Enter**.
-

To restart the CTE server software, perform these steps:

-
- Step 1** In the CTE serial console, type **4** (Restart/Shutdown) and press **Enter**.
 - Step 2** Type **0** or **R** and press **Enter**.
-

Generating a Secure Certificate for the CTE

The CTE accepts a Privacy Enhanced Mail (PEM) format certificate file. PEM is a text format that is the Base-64 encoding of the Distinguished Encoding Rules (DER) binary format. The PEM format specifies the use of text BEGIN and END lines that indicate the type of content that is being encoded.

Before you can upload a certificate to the CTE, you will need to generate a Certificate Signing Request (CSR) and private key. We recommend using Linux OpenSSL to administer any certificate activity. If Linux is not available, we recommend the Cygwin UNIX environment for Windows, which includes an OpenSSL module. Instructions for downloading, installing, and using the Cygwin UNIX environment to generate a CSR are included in this section.

If you are familiar with certificate manipulation, you can use other tools to create a PEM formatted file. The certificate that you upload to the CTE must have the following characteristics:

- It must be in PEM format and must include a private key.
- The signed certificate and private key must be unencrypted.

The following sections describe how to perform the tasks associated with generating a CSR:

- [Overview of the Certificate Signing Request, page 36](#)
- [Installing the Cygwin UNIX Environment for Windows, page 36](#)
- [Generating a CSR, page 37](#)
- [Unencrypting the Private Key, page 37](#)
- [Converting to a PEM Formatted Certificate, page 38](#)
- [Combining the Private Key with the Signed Certificate, page 38](#)
- [Generating Trusted Certificates for Multiple Levels, page 39](#)

Overview of the Certificate Signing Request

If you are unfamiliar with generating a CSR, review this section for background information.

The general process for generating a CSR and handling the signed certificate is as follows:

1. Generate a CSR (**public.csr**) and private key (**private.key**) as described in the [“Generating a CSR” section on page 37](#).
2. Send the **public.csr** file to an authorized certificate provider.
3. If you used a tool other than the Cygwin UNIX environment to generate the CSR, check the format of the private key. If it is in DER format or is encrypted, convert it to PEM format as described in the [“Unencrypting the Private Key” section on page 37](#).
4. When you receive the signed certificate file from your SSL certification company, check the file format. If it is in binary DER format, convert it to PEM format as described in the [“Converting to a PEM Formatted Certificate” section on page 38](#).
5. Combine the PEM formatted signed certificate with the PEM formatted private key (**private.key**) as described in the [“Combining the Private Key with the Signed Certificate” section on page 38](#).
6. If your certificate has more than one level, handle the intermediate certificates as described in the [“Generating Trusted Certificates for Multiple Levels” section on page 39](#).
7. Upload the certificate to the CTE as described in the [“Uploads” section on page 33](#).

Installing the Cygwin UNIX Environment for Windows

If Linux OpenSSL is not available, install the Cygwin UNIX environment for Windows. When you install Cygwin, you must choose the OpenSSL modules as described in the following steps.

To install Cygwin, perform these steps:

-
- Step 1 Use a web browser to navigate to **www.cygwin.com** and click **Install Cygwin Now**.
 - Step 2 Follow the on-screen instructions to open the setup installer.
 - Step 3 In the Cygwin Setup dialog box, click **Next**.
 - Step 4 Click **Install from Internet** and then click **Next**.
 - Step 5 Accept the default root installation directory settings and then click **Next**.
 - Step 6 Accept the default local package directory setting and then click **Next**.
 - Step 7 In the Internet Connection screen, click **Use IE5 Settings** and then click **Next**.

- Step 8** In the list of Available Download Sites, click **ftp://ftp.nas.nasa.gov** and then click **Next**.
- Step 9** In the Select Packages screen, click the **View** button (upper-right corner).
- Step 10** Scroll the packages list to locate in the Package column **openssl: The OpenSSL runtime environment** and **openssl-devel: The OpenSSL development environment**.
- Step 11** In the New column for those two entries, click **Skip**.
The current version number of Cygwin appears.
- Step 12** Click **Next** to start the installation.
After Cygwin installs, you can generate the CSR.
-

Generating a CSR

These instructions to generate a CSR assume that you are using the Cygwin UNIX environment installed as described in the [“Installing the Cygwin UNIX Environment for Windows” section on page 36](#).

To generate a CSR using the Cygwin UNIX environment, perform these steps:

-
- Step 1** Double-click the **Cygwin** icon on the desktop.
A command window opens with a UNIX bash environment.
- Step 2** To change to a particular drive, use the command: **cd driveLetter:**
- Step 3** At the \$ prompt, type the following to generate a CSR:
`openssl req -new -nodes -keyout privateKeyFilename -out certRequestFilename`
- For example:
`openssl req -new -nodes -keyout private.key -out public.csr`
- Status messages about the private key generation appear. You will be prompted for information such as country name.
- Step 4** When prompted for the Common name, enter the DNS name of the CTE.
The name that you enter will appear in the certificate and must match the name expected by PCs that connect to the CTE. Thus, if you alias DNS names, you will need to use the alias name instead.
- Step 5** Submit your CSR (**public.csr**) to an authorized certificate provider such as Verisign.
The certificate provider will return a Signed Certificate to you by e-mail within several days.
-

Unencrypting the Private Key

The following procedure is not needed if you use the Cygwin UNIX environment to generate the CSR and private key. Follow this procedure only if the method you use to generate the private key results in an encrypted key.

To unencrypt the private key, perform these steps:

-
- Step 1** Double-click the **Cygwin** icon on the desktop.
A command window opens with a UNIX bash environment.
- Step 2** To change to a particular drive, use the command: **cd driveLetter:**
- Step 3** At the \$ prompt enter the command: **openssl rsa**
If you enter this command without arguments, you will be prompted as follows:
`read RSA key`
- Step 4** Enter the name of the password to be encrypted.
You can enter the **openssl rsa** command with arguments if you know the name of the private key and the unencrypted PEM file.
For example, if the private key filename is **my_keytag_key.pvk**, and the unencrypted filename is **keyout.pem**, you would enter **openssl rsa -in my_keytag_key.pvk -out keyout.pem**.
-

For more information, refer to the following URL:

<http://www.openssl.org/docs/apps/rsa.html#EXAMPLES>

For information on downloading OpenSSL for Windows, refer to the following URL:

http://sourceforge.net/project/showfiles.php?group_id=23617&release_id=48801

Converting to a PEM Formatted Certificate

When you receive the signed certificate file from your certificate provider, check the file format. If it is in binary DER format, convert it to PEM format.

To convert a certificate to PEM format, perform these steps:

-
- Step 1** Double-click the **Cygwin** icon on the desktop.
A command window opens with a UNIX bash environment.
- Step 2** To change to a particular drive, use the command: **cd driveLetter:**
- Step 3** At the \$ prompt enter the command:
`openssl x509 -in certFile -inform DER -outform PEM -out convertedCertFile`
-

Combining the Private Key with the Signed Certificate

You must combine the signed certificate with the private key before you can upload it to the CTE.

To combine the private key with the signed certificate, perform these steps:

-
- Step 1** Use a text editor to combine the unencrypted private key with the signed certificate in the PEM file format.

The file contents should look similar to the following:

```
-----BEGIN RSA PRIVATE KEY-----
<Unencrypted Private Key>
-----END RSA Private KEY-----
-----BEGIN CERTIFICATE-----
<Signed Certificate>
-----END CERTIFICATE-----
```

Step 2 Save and name the PEM file. For example, **CTE.pem**.

Generating Trusted Certificates for Multiple Levels



Caution

Any certificate that has more than one level *must* include all intermediate certificates, or the system may become unusable.

You must determine whether your certificate has more than one level and, if it does, handle the intermediate certificates properly.

To generate trusted certificates for multiple levels, perform these steps:

Step 1 Do not exit Design Studio.

Step 2 Open Internet Explorer, and access a page through the CTE. For example, enter a URL similar to the following:

`https://ipAddress:httpPort/www.mypage.com`

where:

- *ipAddress* is the IP address of your CTE
- *httpPort* is the CTE HTTP port number

Step 3 Double-click the Lock symbol in the bottom right corner of the browser.

Step 4 Switch to the Certificate Path window pane at the top of the screen.

Step 5 Double-click the first path level to bring up the Certificate information for the first level and then go to the Details screen.

Step 6 Click the **Copy to File** button at the bottom.

Step 7 After the Certificate Export Wizard appears, click **Next**.

Step 8 Click the format **Base-64 encoded** and then click **Next**.

Step 9 Enter a filename. For example, **G:\tmp\root.cer**.

Step 10 Review the information and note the complete filename. Click **Finish**.

Step 11 Click **OK** to close the Certificate information window for the first level.

Step 12 Repeat Steps 5–11 for all levels except the last level.

Step 13 Insert all certificates into one file, and make sure that any intermediate certificates are part of any certificate file you upload.

The format of the uploaded file should be the following:

```
private key
Server Certificate
Intermediate Certificate 0
Intermediate Certificate 1
Intermediate Certificate 2
```

Recovering from a CTE Crash

If the CTE device fails, follow the instructions in the *CTE Hardware Installation Guide* for diagnosing and recovering from a hardware failure. Once the hardware is operational, reinstall the CTE server software from the CD provided with the device.

To reinstall the CTE server software, perform these steps:

-
- Step 1** Insert the installation CD in the CD-ROM drive of the CTE to start the installer.
 - Step 2** When the installation completes, power off the CTE.
 - Step 3** Power on the CTE. As the device starts, eject the CD.

The CTE serial console displays a message informing you whether the installation was successful.

Troubleshooting a CTE

The following information explains how to deal with problems you might encounter when setting up and using the CTE.

The CTE does not start and the CTE serial console is blank.

Verify that the following are correctly set up:

- The serial console is using the correct port and the physical and logical ports match.
- The cable is a null-modem cable.
- The COM settings in your serial communication software are set to 9600 bits per second, 8 data bits, no parity, and 1 stop bit.

Wireless devices or device simulators cannot communicate with the CTE.

Verify that the following are correctly set up:

- The masquerade IP address specified in the CTE Administration Console (Network tab, Interfaces screen) is available outside of your firewall.
- Any changes made in the CTE serial console have been committed.
- The devices are configured to access the correct IP address and port number.

Rules created in Design Studio are not in effect on wireless devices or device simulators.

If you are sure that the rules are correctly created and applied in Design Studio and that they have been uploaded to the CTE, verify the CTE configuration as follows:

- The server load balancer or switch connected to the CTE should be set up to recognize wireless devices.
- Wireless device traffic should be directed through the CTE.
- The CTE should be intercepting traffic from wireless devices.

I tried using Ctrl-Alt-Delete to reboot the CTE, but nothing happened.

The reboot function on the CTE is disabled. You must use the CTE serial console to start and stop the device.

The CTE does not work with European-made phones.

By default, the CTE redirects traffic from HTTP to HTTPS. European-made phones do not support those secure redirects, so if you are using this type of phone you must disable secure redirects for the CTE. To do that, go to the CTE Administration Console, and under the General screen on the Advanced tab, set the Security field to No HTTPS, and click the **Submit** button to commit the change. (Be aware that no HTTPS sites can be proxied when you set this field to No HTTPS.)

SSLV2 sessions do not work with a multi-level certificate chain

If intermediate (multi-level) certificates are part of your secure certificate upload, you need to make sure that the intermediate certificates are part of the certificate file you are uploading. SSLV2 does not support certificate chaining. Any certificate that has more than one level must include all intermediate certificates, or the system may become unusable. For information about how to add intermediate certificates to the uploaded certificate file, see the [“Generating a Secure Certificate for the CTE” section on page 35](#).

Related Documentation

For more information about the CTE, refer to the following publications:

- *CTE and Design Studio Quick Start Guide*
- *CTE Hardware Installation Guide*
- *Release Notes for CTE and Design Studio*

For information about Design Studio, refer to the *Design Studio User Guide*.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

<http://www.cisco.com>

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the **Fax** or **Email** option under the “Leave Feedback” section at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

<http://www.cisco.com/register/>

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of DUB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, First Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, SmartView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

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)

CTE Configuration Note

Copyright © 2001—2002, Cisco Systems, Inc.
All rights reserved.

