



## Starting the Prime Optical Client

---

This chapter describes how to start the Cisco Prime Optical 10.5 client and Cisco Edge Craft (CEC), which is the local craft application used to manage certain ONS 15305 NEs.



### Note

- CEC is not supported on Windows 7 client workstations.
  - CEC is an SNMP-based application. Before launching CEC, verify that the workstation performing the installation can reach the ONS 15305 devices through UDP port 161.
- 

This section contains the following topics:

- [Starting the Prime Optical Client, page 7-1](#)
- [Configuring a SOCKS Server, page 7-3](#)
- [Enable or Disable HTTP Directory Listing, page 7-3](#)
- [Customizing the Login Advisory Message, page 7-4](#)
- [Starting Cisco Edge Craft on Windows, page 7-4](#)
- [Starting Cisco Edge Craft on Linux, page 7-5](#)
- [Configuring Windows 7 to Launch Cisco Transport Controller, page 7-5](#)
- [Specifying the Default Browser to Display the Online Help, page 7-6](#)
- [Special Considerations when Proxy Server Is Enabled, page 7-6](#)
- [Setting Up Client-Server Encrypted Connections Through SSH Tunneling and SOCKS Proxy Forwarding, page 7-7](#)

## Starting the Prime Optical Client

The Prime Optical client uses Java Web Start technology. When the Prime Optical administrator updates or patches the server, the client is updated automatically.



### Note

If launching the Prime Optical client from Linux, confirm that the xterm command is installed on the host. If the xterm command is not installed, you will not be able to launch CTC or TL1 and IOS consoles from NEs.

---

To launch the Prime Optical client:

**Step 1** Open a Prime Optical-supported web browser and enter the following URL:

**https://server-hostname**

where *server-hostname* is the hostname of the Prime Optical server.

**Step 2** Accept the self-signed, untrusted security certificates.

- In Firefox, if you accept the security certificates, they do not reappear upon subsequent logins.
- In Internet Explorer, if you accept the security certificates without placing them in the trusted certificate store, they reappear upon subsequent logins.

**Step 3** The first time you log in, enter the default username and password:

- Username: **SysAdmin**
- Password: **Ctm123!**



**Note**

The username and password are case sensitive.

**Step 4** Click **OK** at the advisory message.

To customize the advisory message, see [Customizing the Login Advisory Message, page 7-4](#).

By default, for security reasons you are prompted to change the password after you log in for the first time. The password complexity is configurable through the Prime Optical UI (**Control Panel > Security Properties** pane). By default, the password must:

- Contain at least six characters, but not more than 15 characters.
- Contain at least two alphabetic characters (A–Z, a–z). Of the alphabetic characters, at least one must be uppercase and one must be lowercase.
- Contain at least one numeric character (0–9).
- Contain at least one special character (+ # % , . ; & !). The default special character set is TL1+UNIX.
- Allow a special character as the first or last character.
- Allow a numeric character as the first or last character.
- Not contain the username or any circular shift of the username. An uppercase letter and its corresponding lowercase letter are considered equivalent. For example, if the username is Arthur, the password cannot contain the string arthur, rthura, thurar, hurart, urarth, or rarthu.
- Differ from the old password by at least three characters. For example, if the old password is MikeBrady5!, the new password cannot be mikebrady5% because only the last character is different. However, the new password MikeBrady2!99 is acceptable because it differs from MikeBrady5! by three characters.

**Step 5** Change the password, and then click **OK**.

The Prime Optical Home page appears.

**Step 6** From the Prime Optical Home page menu, choose **Start** and click one of the following:

- **Domain Explorer**—Connects to the Prime Optical server directly (without going through a SOCKS server) and launches the Domain Explorer.
- **Domain Explorer (with SOCKS)**—Connects to a SOCKS server. To use this option, you must first configure a SOCKS v5 proxy server address and port value. If a SOCKS server is not configured, you will connect to the Prime Optical server directly. See [Configuring a SOCKS Server, page 7-3](#) for information on how to configure a SOCKS server.

**Note**

You can only launch the Domain Explorer from the Prime Central portal when Prime Optical is installed with Prime Central.

The Java Web Start window appears and downloads the Domain Explorer.

**Step 7**

Install the Java Runtime Engine (JRE) 1.7.0\_45 or 1.7.0\_51 on the client host. If the Domain Explorer does not start, check that Java Web Start (jnlp file type) is associated to the browser with the correct javaws application.

**Note**

Cross-launching CTC on older NE releases has not been tested with JRE 1.7. For specific CTC JRE and NE release compatibility information, see the "[PC and Unix Workstation Requirements](#)" section in the *CTC Enhancements, Operations, and Shortcuts* document.

- SSL 3.0 must be enabled in the Java Control Panel.
  - On UNIX, open a shell and change the directory to the location where JRE is installed. Then change directory to jre/bin and execute the jcontrol command.
  - On Windows, open the Control Panel and click **Java**. Navigate to the Advanced tab and make sure that the "Use SSL 3.0" check box is selected.

The Domain Explorer appears and you can begin using it.

## Configuring a SOCKS Server

To configure a SOCKS v5 proxy server address and port value to manage connectivity through network firewalls:

**Step 1**

From the Home page, select **Administration > SOCKS Table**.

**Step 2**

Click **Add Row**. Then, for the SOCKS host, enter the hostname or IP address and the TCP port number.

**Step 3**

Click **Save**.

**Step 4**

Click the radio button next to one of the rows and click **Save as Default** to save the selected SOCKS server settings for the next time you log in.

**Note**

Each user has to select a default SOCKS server.

## Enable or Disable HTTP Directory Listing

To enable HTTP directory listing for log, archive and CTC directory execute the following commands:

1. To enter in to the directory, enter the following command:  
`cd /opt/cisco/PrimeOpticalServer/bin`
2. To enable HTTP directory llisting, enter the following command:  
`./http_directory_listing.sh -enable`

To disable HTTP directory listing for log, archive and CTC directory execute the following commands:

1. To enter in to the directory, enter the following command:  
**cd /opt/cisco/PrimeOpticalServer/bin**
2. To disable the directory listing, enter the following command:  
**./http\_directory\_listing.sh -disable**

## Customizing the Login Advisory Message

An advisory message is shown both before and after a user logs into Prime Optical. By default, this message reads as follows:

```
NOTICE: This is a private computer system. Unauthorized access or use may lead to prosecution.
```

To customize the login advisory message:

- 
- Step 1** In a text editor, open the following file:  
`/cisco/PrimeOpticalServer/tomcat/webapps/OpticalPortal/lib/xwt/nts/OpticalPortalProperties.js`
  - Step 2** Update the advisory message entry with the desired text changes.
  - Step 3** Save the changes.
  - Step 4** Log out of the Prime Optical Home page, clear your browser cache, and log back in.
- 

## Starting Cisco Edge Craft on Windows



### Note

CEC supports Cisco ONS15305 with releases lower than 3.0. CTC supports Cisco ONS15305 release 3.0 or later.

---

- Step 1** Choose **Start > Programs > Accessories > Command Prompt** to open a Windows DOS Command Prompt window.
- Step 2** Change directories to the *Prime Optical-home-directory*/CiscoEdgeCraft/bin directory.
- Step 3** Double-click the **CiscoEdgeCraft.exe** file. The Cisco Edge Craft login screen appears.



### Note

It is not necessary to restart the workstation.

---

- Step 4** In the Cisco Edge Craft login window, do the following:
  - a. Enter the IP address of the NE that you want to connect to.
  - b. Ignore the User field.
  - c. Enter the Password string.

The password string represents the NE community string, which is set in the NE flash memory by using the command-line interface (CLI).

- d. Click **Logon**.
- 

## Starting Cisco Edge Craft on Linux

**Note**

CEC supports Cisco ONS15305 with releases lower than 3.0. CTC supports Cisco ONS15305 release 3.0 or later.

---

- Step 1** Depending on the option you chose during installation, execute the link that you specified, or enter the following command:

```
/cisco/Prime Optical home-directory/CiscoEdgeCraft/bin/CiscoEdgeCraft
```

- Step 2** In the Cisco Edge Craft login window, do the following:
- a. Enter the IP address of the NE that you want to connect to.
  - b. Ignore the User field.
  - c. Enter a password string. The password string represents the NE community string, which is set in the NE flash memory by using the CLI.
  - d. Click **Logon**.
- 

## Configuring Windows 7 to Launch Cisco Transport Controller

If you plan to use Cisco Transport Controller (CTC) on a Windows 7 workstation, do the following:

---

- Step 1** In Internet Explorer 10, disable the Protected Mode for a zone:
- a. Choose **Tools > Internet Options**.
  - b. Click the **Security** tab.
  - c. Select the appropriate zone, then uncheck the **Enable Protected Mode** check box.
- The Protected Mode status (“Protected Mode: On” or “Protected Mode: Off”) is visible in the bottom right corner of the IE status bar.
- Step 2** Configure the security zone level to Medium.
- Step 3** Disable automatic TCP tuning. To do this, open the CMD prompt and enter the following command:
- ```
netsh interface tcp set global autotuninglevel=disabled
```

**Note**

To reenable automatic tuning, enter:

```
netsh interface tcp set global autotuninglevel=normal
```

---

**Note**

You cannot use CTC on a Windows 7 workstation when automatic tuning is enabled.

## Specifying the Default Browser to Display the Online Help

In Windows, Prime Optical uses the default browser to display the online help. If you want to use a specific browser to launch the online help, make that the default browser for your workstation.

**Note**

During testing, Cisco uses Internet Explorer, Mozilla Firefox, and Google Chrome to display the online help; other browsers have not been tested.

The online help for Cisco Edge Craft requires Adobe Acrobat Reader. Acrobat Reader is not required in your path environment variable, but the PDF file type must be associated with Acrobat Reader.

On Solaris, the online help for Cisco Edge Craft requires Adobe Acrobat Reader to be installed and included in your path environment variable.

**Tip**

If you cannot launch the online help, open a command prompt from another window and enter the **xhost +** command (/usr/bin [Linux]) and the full path name. Also, verify that the DISPLAY variable is set correctly.

## Special Considerations when Proxy Server Is Enabled

If you are using a proxy-server enabled web browser, complete one of the following options, depending on your browser type.

For Internet Explorer, do the following:

- 
- Step 1** Choose **Tools > Internet Options**.
  - Step 2** Click the **Connections** tab.
  - Step 3** Click the **LAN Settings** button.
  - Step 4** Complete one of the following options:
    - Uncheck the **Use a proxy server for your LAN** check box.
    - If the **Use a proxy server for your LAN** check box must remain checked, click **Advanced**. Enter your server IP address in the Do not use proxy server addresses beginning with field. Separate each address with a semicolon.
  - Step 5** Click **OK**.
-

For Mozilla Firefox, do the following:

- 
- Step 1** Choose **Edit > Preferences**.
- Step 2** Expand **Advanced** and choose **Proxies**.
- Step 3** Complete one of the following options:
- If you do not want to use a proxy, click **Direct connection to the Internet**.
  - If you do not have a proxy location (URL), click **Manual proxy configuration**. In the No Proxy for field, enter the domains that you do not want to use a proxy for. Use a comma to separate domains.
- Step 4** Click **OK**.
- 

## Setting Up Client-Server Encrypted Connections Through SSH Tunneling and SOCKS Proxy Forwarding

This section describes how to configure the Prime Optical client to route all of its outbound network (TCP) connections to a SOCKS proxy server.

The proxy host must satisfy the following prerequisites:

- No firewall is present between the proxy host and the server host. In other words, the proxy host must be able to establish a connection on every port on the server host.
- A UNIX user has been created on the proxy host.



---

**Note** Cisco recommends that you avoid using the root UNIX user as the endpoint of the SSH tunnel.

---

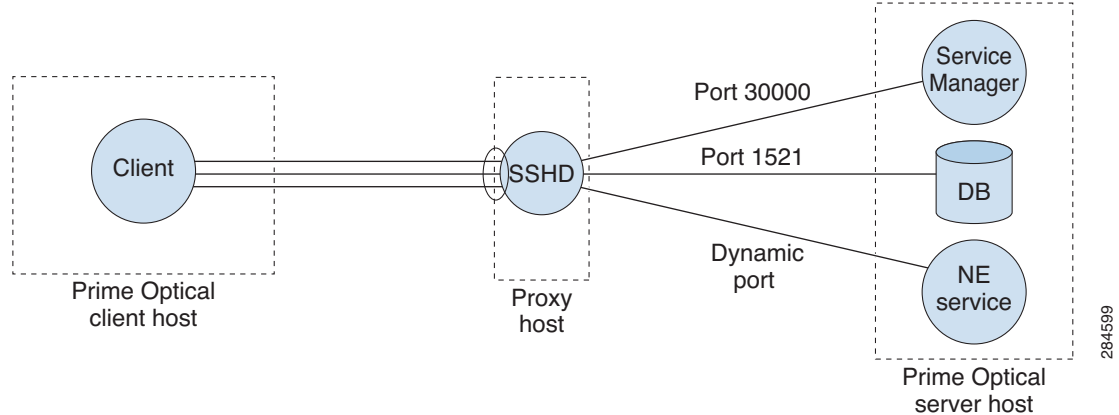
- The Proxy host is SSH-enabled.
- The Proxy host supports SOCKS5.
- You have changed the AllowTcpForwarding property value in the `/etc/ssh/sshd_config` file to **yes** and then restarted the SSH service.

The following hosts are involved:

- Proxy host
- Client host, on which the Prime Optical client runs
- Server host, on which the Prime Optical server runs

[Figure 7-1](#) shows the route of a connection. Every outbound connection of the client host, instead of being sent directly to the server host, is tunneled to the SSH port 22 of the proxy. Alternatively, you can also configure the server host to act as a proxy host. If configured, the Secure Shell Daemon (SSHD) service runs on the server host.

Figure 7-1 Route of a Connection



## Prime Optical Client on Windows (Using SSH Tunneling)

This procedure explains the steps involved in configuring the Prime Optical client route and all its outbound connections into an SSH tunnel. This SSH tunnel connection is between the client machine and the proxy host. At the end of this procedure, the client will begin to use SOCKS through an SSH tunnel.

- 
- Step 1** On the client machine, go to <http://www.putty.org> and download the plink.exe file.
- Step 2** Open a command prompt (cmd.exe), and then change directory to the location where plink.exe has been saved.
- Step 3** Execute the following command:

```
plink -N -D proxy_port proxy_user@proxy_host
```

For example:

```
plink -N -D 10080 myuser@myproxyhost
```



### Note

- The *proxy\_user* user must exist on *proxy\_host*. For security reasons, do not use root user for this purpose.
  - Ensure that the *proxy\_port* is not already in use on the client host. You can use the **netstat** command to verify if it is already in use.
- 

- Step 4** Enter the user's password when prompted.



### Caution

To avoid SSH being dropped, do not close the command prompt during the procedure or after the user has logged in.

---



- Step 5** From the Prime Optical Home page, choose **Start > Domain Explorer (with SOCKS)** after specifying a default SOCKS server. For information on how to configure the SOCKS server settings, see [Configuring a SOCKS Server, page 7-3](#).
- 

## Prime Optical Client on UNIX (using SSH tunneling)

This procedure explains the steps involved in configuring the Prime Optical client route and all its outbound connections into an SSH tunnel. This SSH tunnel connection is between the client machine and the proxy host. Use this procedure if the Prime Optical client is launched on Linux. At the end of this procedure, the client will begin to use SOCKS through an SSH tunnel.

- Step 1** On the client machine, open a terminal window and enter the following command:

```
ssh -N -D proxy_port proxy_user@proxy_host
```

For example:

```
ssh -N -D 10080 myuser@myproxyhost
```



**Note**

The *proxy\_user* user must exist on *proxy\_host*. For security reasons, do not use root user for this purpose.

---

- Step 2** Enter the user's password when prompted.



**Caution**

To avoid SSH being dropped, do not close the command prompt during the procedure or after the user has logged in.

---

- Step 3** From the Prime Optical Home page, click **Start > Domain Explorer (with SOCKS)** after specifying a default SOCKS server. For information on how to configure the SOCKS server settings, see [Configuring a SOCKS Server, page 7-3](#).
-

