



Cisco Patient Connect Troubleshooting Guide

Release 1.6

Last Revised: July 28, 2017

Overview

This guide is intended for customers, partners, and the field team who will troubleshoot the Cisco Patient Connect solution.

This document discusses and solves the most common problems that have been reported during testing and from customers.

Topics in this guide include:

- [Troubleshooting Patient Connect - Patient View](#)
 - [TV/Monitor/Touchscreen is blank or dark](#)
 - [Touch Screen function is not working correctly](#)
 - [Virtual Keyboard is displayed](#)
 - [IEC Does Not Detect Connected Peripherals](#)
 - [IEC Does Not Reflect The Applied Policy](#)
 - [IEC's Profile Configuration Is Not Active](#)
 - [Patient View Home Page is not Displayed](#)
 - [IEC is Rebooting Unexpectedly](#)
 - [Network Error Message](#)
 - ['Management failure: Product VEP is not found' Error Message](#)
 - ['Management Server is not reachable' Error Message](#)
 - ['Startup URL is not configured' Error Message](#)
 - ['Cannot register' Error Message](#)
 - ['Server is down' Error Message](#)
 - ['Service Temporarily Unavailable' Error Message](#)
- [Troubleshooting Tools](#)
 - [Cache Refresh](#)

- [Sample IEP Policies for Cisco Patient Connect Administrators](#)
- [Events Tab in the IEM](#)
- [Configuring an IEC to Use a Static IP Address](#)
- [Basic Troubleshooting Steps for Rebooting the IECs](#)
- [Troubleshooting the Issues While Accessing the CPC Solution](#)
 - [Images and Icons are Blank When Loading the Application](#)
 - [User Gets Locked out After Attempting to Login With Incorrect Password](#)
 - [The CPC Solution Works Better on Chrome Browser](#)
 - [Monitoring Feature for the CPC Solution](#)

Troubleshooting Patient Connect - Patient View

This section provides details of the issues and errors that customers might encounter with the Patient View application, Cisco Interactive Experience Clients (IECs), and connected peripherals.

TV/Monitor/Touchscreen is blank or dark

Do the following:

1. Check whether the TV/monitor/touchscreen is working and the power is connected to it.
2. If TV/monitor/touchscreen was connected after the IEC was booted up, reboot the IEC.
3. Try connecting the TV/monitor/touchscreen to the IEC's alternate video port (VGA/miniDisplayport or HDMI).

Touch Screen function is not working correctly

Perform the following steps to troubleshoot if a touch screen is connected to Patient View and is not working correctly:

Step 1 Ensure that the USB interface cable is plugged into the IEC and the touch screen.

Step 2 Use the calibration utility to recalibrate the screen.

- Press **Ctrl+Alt+S**.
- Enter the **DMC** (Device Maintenance Code).
- Click **Calibrator**.

Step 3 Reboot the system if the touch screen USB cable was not connected before boot time.

Virtual Keyboard is displayed

If a touchscreen is connected to the IEC and displays a virtual keyboard on the Patient View app. This is due to an incorrect policy applied to the IEC. Disable the following configuration settings in the policy that is applied to the IEC. If there is no policy applied to the IEC, then these changes should be set in the IEC profile configuration.

Step 1 Log into the IEM.



Note Refer to the *Interactive Experience Manager (IEM) documentation* for more details.

Step 2 Go to the policy that is applied to the IEC or the IEC's profile.

Step 3 Go to **keyboard > virtual > enabled property**.

Step 4 Set enabled value to **false**.

Step 5 Go to **browser > input > popup > keyboard > enabled property**.

Step 6 Set enabled value to **false**.

Step 7 Save the policy by clicking the **Apply** button.

Step 8 Reboot the IEC to activate the policy on it.

IEC Does Not Detect Connected Peripherals

Peripherals such as a printer, scanner, keyboard, or mouse must be connected to the IEC before it is booted up in order for the IEC to detect them. If you connect a peripheral after the IEC has booted up, reboot the IEC to detect that peripheral.

IEC Does Not Reflect The Applied Policy

After applying the policy, IEC needs to be rebooted to have the policy enforced. Also check the IEM to ensure that the IEC has the proper policy applied to it.

IEC's Profile Configuration Is Not Active

If there is a policy assigned to the IEC, its configuration takes precedence over the IEC's profile configuration. If the IEC's profile configuration is required instead, remove the applied policy.

Patient View Home Page is not Displayed

Home page display issues could happen due to the following reasons:

- The IEC does not have the policy with the startup URL pointing to the CPC applied to it. Apply that policy to the IEC in the IEM.

- If IEC does not have a policy but using its profile in the IEM for the startup URL, verify that the startup URL in the profile is pointing to the CPC server.

**Note**

Use of policies is the preferred method for configuring IEC properties.

- If the IEC was updated recently but not rebooted, the IEC needs to be rebooted.
- Check if CPC Server is reachable and web services are accessible.

IEC is Rebooting Unexpectedly

The following are some of the scenarios in which reboot is initiated from the IEM:

- Whenever there is a power failure, the IEM reboots the IEC to identify all peripherals that are connected.
- If Patient View-side video endpoint goes down and comes up, the IEM reboots the IEC.
- If the Cobra application is not working normally, the IEM reboots the IEC.

Network Error Message

If LAN cable was connected after the IEC was booted, reboot the IEC. Check the network connection. If it is DHCP-based, check whether the DHCP server is correctly leasing an IP address to the IEC.

'Management failure: Product VEP is not found' Error Message

The IEC has an older version of firmware. Upgrade the IEC's firmware.

'Management Server is not reachable' Error Message

The message "Management Server is not reachable" indicates that the IEM IP Address is not correct or inaccessible. This message may also appear due to a network problem, a proxy server configuration error, or an incorrect IEM URL. Check if the firewall policy is blocking access.

If the IEM is down but the IEC has accessed the startup URL previously, it will load the startup URL from its cache. In other words, the failure of the IEM does not prevent the IEC from functioning. If any configuration changes are needed, then the IEM has to be active for pushing the new policy configurations to the IEC.

'Startup URL is not configured' Error Message

The following are the possible reasons and resolutions for the message "Startup URL is not configured":

- IEC does not have a policy (initial configuration that includes startup URL) enforced in IEM. Verify the IEC has the correct policy applied and the IEC has been rebooted.
- Another possibility is that the IEC is not registered in the IEM, instead it is in standalone mode. Check the IEM to ensure that the proper serial number is added for the IEC.

- If the IEC is not rebooted after configuration changes, reboot the IEC.

'Cannot register' Error Message

Click the **Show Details** button to reveal information about the service that is disabled.

Complete the following steps to enable the IEM for registration:

-
- | | |
|---------------|--|
| Step 1 | Log into the IEM as root/administrator user. Otherwise, users cannot see the Maintenance link. The Maintenance link is not shown to regular users. |
| Step 2 | Click the Maintenance link. |
| Step 3 | Click Server Settings . |
| Step 4 | Check the Device gateway enabled check box. |
| Step 5 | Click Apply . |
-

'Server is down' Error Message

Check the IEC's Policy or Profile settings in the IEM with respect to startup URL configuration.

'Service Temporarily Unavailable' Error Message

This error occurs when the IEC cannot pull the home page because the startup URL configured in the IEM is not reachable or the CPC server or services are down. To resolve this error:

-
- | | |
|---------------|---|
| Step 1 | Verify CPC is up and functioning. |
| Step 2 | Check the IEC's event log in the IEM. |
| Step 3 | Verify that the correct IP address of the CPC server is used as the startup URL. |
| Step 4 | Verify that the IEM policy that is applied to the IEC or the IEC's profile is configured correctly. |
-

Troubleshooting Tools

This section explains how to use tools to troubleshoot and fix issues with the solution.

Cache Refresh

The Cache Refresh feature in the Admin View application allows Cisco Patient Connect administrators to clear old data and pull the latest data for a particular feature. It also helps to apply new code or configuration changes to a feature.

Refer to the *Cisco Patient Connect Admin View Guide* for the description of the cache refresh buttons.

Perform cache refresh if any code or configuration is changed for a feature in the application, a particular feature is nonfunctional, or a particular feature hangs without pulling latest data properly.

Refreshing the cache may affect the smooth functioning of a feature. Choose a time for cache refresh that will impact as few patients as possible.

**Note**

Before performing cache refresh on a feature that is displayed on Patient View, consider broadcasting a message prior to the refresh in order to inform patients that the feature will not be available for a few minutes.

Sample IEP Policies for Cisco Patient Connect Administrators

Cisco Patient Connect administrators can create policies in IEP to troubleshoot and to perform administrative tasks.

Clear Cache

the administrator creates and applies a Clear Cache policy to clear a device's cache from the IEM, when the server is being updated. Once a policy is created, it appears in the **Custom Actions** menu.

To create a Clear Cache policy, complete the following steps:

-
- Step 1** Name the policy "ClearCache".
 - Step 2** Set the browser cached media clear property to 'true':
browser > cache > media > clear = **true**
 - Step 3** Set the browser cached media clear property to 'true':
browser > cache > web > clear = **true**
-

Restart and Clear Cache

When there is a server update and you want to ensure that the application loads all new content from the server on restart, create and apply the Restart and Clear Cache policy. Applying this policy is the same as applying the [Clear Cache](#) policy and then restarting the application.

To restart and clear cache, complete the following steps:

-
- Step 1** Name the policy "RestartAndClearCache"
 - Step 2** Set the browser application restart property to 'true':
browser > application > restart = **true**
 - Step 3** Set the browser cached media clear property to 'true':
browser > cache > web > clear = **true**
-

Debug Panel

Create and apply a Debug Panel policy to an IEC to watch its CPU performance during the operation and view the scripts which runs on the device. The policy can be accessed from the **Custom Actions** menu of the IEM.

To create and apply a Debug Panel policy, complete the following steps:

-
- Step 1** Name the policy “DebugPanel”.
 - Step 2** Enable the debug panel enabled property:
browser > debug > panel > enabled = **true**
-

Virtual Network Computing

An administrator creates and applies the Virtual Network Computing policy to use Virtual Network Computing (VNC) or to remotely view an IEC.

To create and apply the policy, complete the following steps:

-
- Step 1** Name the policy “VNC”.
 - Step 2** Enable the remoteview property:
remoteview > enabled = **true**
-

Events Tab in the IEM

The IEM allows you to do view all the IECs registered with the IEM. Follow these steps to view the Event tab:

-
- Step 1** Click **Devices** on the left navigation pane.
All the IECs registered with the IEM in your account are visible in both the left and center panes.
 - Step 2** Click the **Show screenshots** button on the top right corner of the display view to view the screenshot of each of the IECs registered with the IEM.
 - Step 3** Default polling time for each IEC image is 10 minutes. The most recent image for the specific IEC can be obtained by clicking the Refresh button beneath the IEC’s screen shot.
 - Step 4** In order to enlarge the screen shot of the IEC, click the **Zoom** button.
 - Step 5** In the Devices menu (left pane), choose the IEC by double-clicking on the icon for that particular IEC.
 - Step 6** Click the **Events** tab.
 - Step 7** You can filter the logs by checking the browser check box in the Facilities list. Click **Apply**.
-

Configuring an IEC to Use a Static IP Address

This section provides instructions on how to configure an IEC to use a static IP address.

To configure an IEC to use a static IP address, complete the following steps:

-
- Step 1** From the keyboard, press **Ctrl-Alt-S** and enter the maintenance code. The **System Settings** window appears. Select the **Network** icon. The **Network** window appears.
 - Step 2** In the Network window, press tab to the **Use DHCP** check box. Tap on the spacebar to uncheck the **Use DHCP** check box, and enter the network settings.
 - Step 3** Enter the IP Address, Subnet Mask, Gateway Address, Primary DNS Server IP Address, and Secondary DNS Server IP Address in the respective text fields.
 - Step 4** Click **Apply** and then click **Close** to exit the **Network** window.
 - Step 5** Click **Reboot** to restart the IEC.
-

Basic Troubleshooting Steps for Rebooting the IECs

This section provides information on the basic troubleshooting steps for the Cisco Interactive Experience Clients (IECs).

IEM Main Screen

From the left menu, click **Devices** to view a list of all the devices registered on the IEM.

Click a device to bring up the device status screen in the center frame. Double-click a device to see specific information about that device.

IEC States in the IEM

Table 1 *IEC States in the IEM*

Status	Description
The IEC displays red OFF on 'icon view' or red dot on 'screenshot view'.	The IEC is offline.
The IEC displays green ON on 'icon view' or content on 'screenshot view'.	The IEC is online and is reachable from the IEM and SSH.
The IEC displays a black screen in the IEM 'screenshot view'.	The IEC is online, but the application is powered off. The application can be powered off from the pillow speaker and must be powered on in the same way.
The IEC is online, but displays in an improper resolution in the IEM 'screenshot view'.	The IEC is online, but the television is off. Therefore, the IEC does not know the proper resolution. The television must be powered on in the room.

The Events Screen

On the 'Event's screen, you can see information messages, warning messages, and error messages from the IEC. This can be a crucial tool in troubleshooting an IEC. For each message you can see the Event time, the Message sent, the Severity, and the Facility (where the message is located).

On the left side of the screen, you can filter messages by Severity or by Facility. Click the check boxes to select, or de-select, an option. Click the check mark to apply the changes, or click the circle to revert them. You can also change the number of events displayed under the 'Max number of events' option.

If you would like to download a copy of the event logs to your machine, click **Save As** and attach the report to the ticket.

Rebooting an IEC

Reboot the IEC to troubleshoot the following common issues:

- Volume stops working on the pillow speaker for the patient.
- Phone number for the room does not appear on the TV screen and video call does not work.
- Distorted picture on the TV.
- Slow transition between TV channels.
- Incorrect TV line up display and the patient unable to choose directions with the pillow speaker such as up, down, left, or right.

Troubleshooting the Issues While Accessing the CPC Solution

This section provides details of the issues and errors that can be experienced while accessing the CPC solution.

Images and Icons are Blank When Loading the Application

When the Cisco Patient Connect Content Management System (CPC CMS) is unable to handle the load, images and icons are shown as blank while loading the CPC solution. An optional cache mechanism feature has been introduced to share the load of CPC CMS. The calls made from TV, now go to the CPC CMS through the cache mechanism, which enables the system to display the icons and images from the cache tool locally. The cache mechanism feature helps download and cache the URLs, videos, images, and icons and get them populated to reduce the load and lag of CPC CMS. Refer *Appendix-D* of the *Cisco Patient Connect Admin View Guide* for more details on the cache feature.



Note The cache mechanism feature is optional for the customers.

If the images and icons are still blank, do the following workaround:

1. Restart IEM.
2. Reboot IEC.
3. Check the CPC CMS to see if it is down.

User Gets Locked out After Attempting to Login With Incorrect Password

The openLDAP server that comes along with the CPC solution has a pre-configured list of users. When these users attempting to log in with incorrect password for 10 times, they are locked out and will not be able to login for one hour. After one hour they can try login again with their correct password. If there is an emergency situation where user, whose account has been locked out, needs to log in the workaround is you need to log into the wso2 user console and change the password for the user. Now the lock is released for the user and the user can login with the new password.

The CPC Solution Works Better on Chrome Browser

If an administrator or a nurse dashboard user tries to access the CPC solution on a different browser other than Chrome, the solution may not work properly. Chrome browser has been certified for the better performance of the CPC solution.

Monitoring Feature for the CPC Solution

At times, any process or service of the CPC solution may stop working because of unexpected reasons, such as, out of memory issue. To overcome such issues, it is recommended to implement the monitoring feature to monitor the different services that are installed. In such situations, the monitoring feature notifies the interested parties to take appropriate action immediately.

Refer *Cisco Patient Connect Monitoring Guide* for more details on the monitoring feature.