Smart Care Guide to Troubleshooting Appliance Registration

Contents

Troubleshooting Appliance Registration
  Verify the registration of the Partner CCO account
  Verify that the Customer CCO ID is valid
  Verify the HTTPS connection between the network appliance and tools.cisco.com

Registration Messages
Related Documentation
Service and Support

Troubleshooting Appliance Registration

To register your hardware or software appliance, Smart Care requires the following:

- Your partner CCO account must be registered with Smart Care. Registration of the partner CCO account must be complete before use at the customer site.

- Any customer CCO ID that is provided when the network appliance is registered must be a valid ID. The CCO ID must have been associated with the customer profile in Smart Care.

  Note

  The appliance registration process does not require the use of a customer CCO ID. However, if the customer CCO ID is not provided during the registration process, the appliance must later be manually assigned to the customer in Smart Care.

- A connection must be established over HTTPS from the appliance to tools.cisco.com. This connection must permit data to be sent and received between the appliance and tools.cisco.com.
This document describes how you can verify that these requirements were met.

**Verify the registration of the Partner CCO account**

You must be a registered Smart Care Partner before you can register network appliances for customers. Your partner CCO ID is required to register appliances at customer sites.

To verify that you are a registered Smart Care Partner:

**Step 1**
Use your partner credentials to logon to Smart Care from [https://tools.cisco.com/smartcare](https://tools.cisco.com/smartcare).

If you are a registered Smart Care Partner, your credentials will be validated and you will be redirected to the Smart Care portal.

If you are not a registered Smart Care Partner, you will be redirected to the Registration page.

**Verify that the Customer CCO ID is valid**

Before you register a network appliance, verify that any customer CCO ID that you intend to use in the registration process is shown in the profile of the customer for which you will register the appliance. This should be done before you start the appliance registration process.

Note that this step is required only if you used a customer CCO ID when you registered the appliance.

To verify the Customer CCO ID:

**Step 1**
Login to Smart Care from [https://tools.cisco.com/smartcare](https://tools.cisco.com/smartcare).

**Step 2**
Click **Add Customers**, and verify that the CCO ID is displayed for the customer.

![Customer Management page](image)

**Figure 1**  
The Customer Management page

In the Customer Management page shown in Figure 1, the customer E CIRCLES is not associated with a CCO ID. In this case, the specification of a CCO ID for this customer during appliance registration will result in a registration failure. The customer CCO account must be established in Smart Care before the customer CCO ID can be used in the appliance registration process.

If the CCO ID is valid, note that the site ID that is provided in the registration process must be the same as the site ID that was created for this customer in Smart Care.
Several factors can affect the ability of the appliance to establish an HTTPS connection to tools.cisco.com. This section describes common causes for connection failure and how to troubleshoot each of them.

Check 1 explains how to test for LAN connectivity.

### CHECK 1: LAN Connectivity

<table>
<thead>
<tr>
<th>Affected by</th>
<th>Test</th>
<th>Probable Causes of Failure</th>
<th>Corrective Action</th>
</tr>
</thead>
</table>
| Ethernet cable | Ping the default gateway from the appliance. If this test is successful, continue to Check 2. | • There is a cabling issue between the appliance and the switch port.  
• The IP address and subnet mask assignment on the appliance is not consistent with the VLAN assignment on the switch port to which it is connected.  
• A duplicate IP address assignment was made for the appliance.  
• ICMP packets are disabled in an ACL on the default gateway device. Note that there is only a low probability that this is the problem. | • Check that the link light indicator is active for both the switch port and the appliance. If the link light is not lit, either the switch port is disabled or there is a faulty cable. If the switch port is not disabled, replace the cable between the appliance and the switch port.  
• Confirm that the configuration of the IP address and subnet mask on the appliance is consistent with the configuration of the IP address and subnet mask of the default gateway.  
• Confirm that the VLAN assignment on the directly attached switch port maps to that of the subnet for the default gateway.  
• Disconnect the appliance from the switch. Perform the Check 1 test from a computer that is connected to the same switch port and that uses the same Ethernet cable and IP address, subnet mask, and default gateway assignments as the appliance. If the test fails, there is a problem outside the appliance that must first be fixed. If the test passes, there may be a problem with the appliance hardware or configuration. |
Check 2 explains how to test for DNS resolution.

**CHECK 2: DNS Resolution**

<table>
<thead>
<tr>
<th>Affected by</th>
<th>Test</th>
<th>Probable Causes of Failure</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address configuration of the DNS servers on the appliance</td>
<td>Ping tools.cisco.com from the appliance. If the ping resolves to an IP address, continue to Check 3.</td>
<td>▪ The IP address configuration of the DNS server in the appliance is incorrect.</td>
<td>▪ Confirm that the DNS configuration on the appliance matches that of the customer setup.</td>
</tr>
<tr>
<td>Connection to the DNS server</td>
<td></td>
<td>▪ Connectivity issues exist between the appliance and the DNS server for queries and responses</td>
<td>▪ Check for problems beyond the default gateway by using the <strong>traceroute</strong> command from the appliance to the DNS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Confirm that the DNS configuration on the appliance matches that of the customer setup.</td>
<td>▪ Confirm that there are no ACLs preventing DNS queries between the appliance and the DNS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Check for problems beyond the default gateway by using the <strong>traceroute</strong> command from the appliance to the DNS server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Confirm that there are no ACLs preventing DNS queries between the appliance and the DNS server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Perform the Check 2 test from a computer on the same subnet as the appliance. If the test fails, the network connection to the DNS server. If the test passes, there is a problem with the configuration of the appliance</td>
<td></td>
</tr>
</tbody>
</table>

Check 3 explains how to test for firewall issues that do not involve a proxy server.

**CHECK 3: Firewall, in cases when a proxy server is not configured on the appliance**

<table>
<thead>
<tr>
<th>Affected by</th>
<th>Test</th>
<th>Probable Causes of Failure</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>A configuration that prevents access to tools.cisco.com</td>
<td>From the command prompt, telnet on port 443 to tools.cisco.com. The computer that you use in this test should reside on the same subnet as the appliance. In a successful test, the connection is established and a Telnet window is displayed.</td>
<td>▪ The customer network includes a proxy server which is the only device that the firewall allows to access the Internet. ▪ Rules are configured in the firewall that prohibit appliance access to the Internet.</td>
<td>▪ Confirm that, for appliances registered without proxy server information, there is no proxy server in the network. For networks that include proxy servers, the firewall generally allows only the proxy server to access the Internet.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Confirm that, for appliances registered without proxy server information, there is no proxy server in the network. For networks that include proxy servers, the firewall generally allows only the proxy server to access the Internet.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ If a proxy server is the only network device that is allowed to access the Internet, be sure to obtain information about the proxy server, the proxy port for HTTPS, and the authentication credentials, from the customer and to configure the appliance to be consistent with that information. To configure the appliance with this information, use the <strong>conf ip</strong> command.</td>
<td>▪ Investigate the firewall configuration.</td>
</tr>
</tbody>
</table>
Check 4 explains how to test for firewall issues that involve a proxy server.

**CHECK 4: Firewall, in cases when a proxy server is configured on the appliance**

<table>
<thead>
<tr>
<th>Affected by</th>
<th>Test</th>
<th>Probable Causes of Failure</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>A configuration that denies HTTPS access from the appliance to the proxy server</td>
<td>From the command prompt, telnet to the proxy server on the HTTPS proxy port. The computer that you use in this test should reside on the same subnet as the appliance. In a successful test, the connection is established and the Telnet window is displayed.</td>
<td>• The IP address or HTTPS port that is configured for the proxy server is incorrect. • The network configuration prevents HTTPS packets from the LAN segment to reach the proxy server. • The authentication credentials to the proxy server are incorrect. • The proxy server disallows HTTPS inbound connections from this subnet.</td>
<td>• Confirm that a computer on the same subnet can connect to the proxy server. • Confirm the configuration of the IP address, port, and authentication credentials for the proxy server.</td>
</tr>
</tbody>
</table>

A configuration that denies HTTPS access from the proxy server to tools.cisco.com

From a browser on a computer using the configuration of the proxy server, HTTPS to tools.cisco.com. Note that the computer should be on the same subnet as the appliance. In a successful test, the connection is established and you are then redirected to www.cisco.com.

• The proxy server denies access to tools.cisco.com

• Check proxy server logs for dropped connection requests.

• Check the configuration of the proxy server for other settings that could prevent HTTPS access to tools.cisco.com.

---

**Registration Messages**

The following table explains common messages that may be displayed in the Smart Care user interface during the appliance registration process.
<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Partner CCO login/password</td>
<td>You entered an incorrect partner CCO ID or password.</td>
<td>Confirm that you can use your CCO ID and password to access your partner account on the Cisco website at <a href="http://www.cisco.com">http://www.cisco.com</a>.</td>
</tr>
<tr>
<td>Invalid Partner CCO login name</td>
<td>You entered a valid CCO ID but this ID is not registered in the Smart Care Partner program.</td>
<td>Confirm that you are a registered Smart Care Partner by logging on to Smart Care at <a href="https://tools.cisco.com/smartcare">https://tools.cisco.com/smartcare</a>.</td>
</tr>
<tr>
<td>Invalid Customer Login name</td>
<td>The customer CCO ID that you entered does not belong to a registered Smart Care customer.</td>
<td>Contact the customer to confirm that the CCO ID is correct and associated with a valid CCO account.</td>
</tr>
<tr>
<td>Partner is not associated to that customer</td>
<td>The customer login name that you entered is not associated with a registered Smart Care Partner.</td>
<td>Confirm that the customer was added to the partner account. To do so, logon to Smart Care from <a href="https://tools.cisco.com/smartcare">https://tools.cisco.com/smartcare</a> and click Add Customers. If the customer is not associated with the partner account, make the association.</td>
</tr>
<tr>
<td>Customer already has Client assigned</td>
<td>An appliance is already assigned to this customer in Smart Care. A customer is limited to the assignment of only one software or hardware appliance.</td>
<td>To replace one appliance with another, you must unassign the appliance to be replaced before you can assign the replacement appliance to the customer.</td>
</tr>
<tr>
<td>Customer already has a site. Only one site is allowed per customer</td>
<td>The site ID that you provided is different from the site ID that is assigned to the customer in Smart Care.</td>
<td>Confirm that the site that is assigned to the customer in Smart Care, is the same customer site that was specified during the registration process.</td>
</tr>
<tr>
<td>Appliance name already exists. Please retry with another name</td>
<td>The name that you tried to assign to the Smart Care appliance already exists in the system. This means that the name is not &quot;unique.&quot;</td>
<td>Assign a unique name to the appliance.</td>
</tr>
<tr>
<td>Unable to connect to server. Please make sure that server URL is correct and appliance has proper network connectivity</td>
<td>The appliance cannot connect to the server. This indicates that there is a network issue.</td>
<td>Ensure that an HTTPS connection is established between the appliance and tools.cisco.com. For more information, see “Verify the HTTPS connection between the appliance and tools.cisco.com.”</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Corrective Action</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Unable to connect to server. Please make sure that server URL is correct. | The server returned an unexpected response.                                                         | Contact CIN or TAC:  
To contact CIN from the United States or from Canada, call 1-800-GO-CISCO.  
To contact CIN from other locations, consult the list of worldwide support numbers at http://www.cisco.com/warp/customer/687/Directory/DirTAC.shtml  
For TAC, visit the TSRT online link at http://tools.cisco.com/ServiceRequestTool/create/launch.do |
| Internal Server Error occurred (10005)                       | An unexpected error occurred in the server.                                                          | Contact CIN or TAC:  
To contact CIN from the United States or from Canada, call 1-800-GO-CISCO.  
To contact CIN from other locations, consult the list of worldwide support numbers at http://www.cisco.com/warp/customer/687/Directory/DirTAC.shtml  
For TAC, visit the TSRT online link at http://tools.cisco.com/ServiceRequestTool/create/launch.do |
| Server is unable to process your request (xxxxx)              | An unexpected error occurred in the server. Note that the xxxxx value indicates the error code that was sent. | Contact CIN or TAC:  
To contact CIN from the United States or from Canada, call 1-800-GO-CISCO.  
To contact CIN from other locations, consult the list of worldwide support numbers at http://www.cisco.com/warp/customer/687/Directory/DirTAC.shtml  
For TAC, visit the TSRT online link at http://tools.cisco.com/ServiceRequestTool/create/launch.do |
Related Documentation

For answers to common questions about appliance registration, see the Q&A on the Acceleration Partner website at http://www.cisco.com/partner/services/smartcare/accelerate/documentation/index.html.

Service and Support

If you have met these requirements but remain unable to register a network appliance, contact Smart Care technical support:

- To contact CIN from the United States or from Canada, call 1-800-GO-CISCO.
- To contact CIN from other locations, consult the list of worldwide support numbers at http://www.cisco.com/warp/customer/687/Directory/DirTAC.shtml.
- For TAC, visit the TSRT online link at http://tools.cisco.com/ServiceRequestTool/create/launch.do.