



# **Brooktrout SR140 Fax Software with Cisco Unified Communications Manager 14.0**

Installation and Configuration Integration

## **IMPORTANT NOTE**

This document is not to be shared with or disseminated to other third parties, in whole or in part, without prior written permission from Enghouse. To seek such permission, please contact your Enghouse Sales Representative

---

## Copyright

Enghouse Interactive is a wholly owned subsidiary of Enghouse Systems Limited. Enghouse Systems Limited is a publicly traded Canadian based software and services company founded in 1984. Enghouse shares are traded on the Toronto Stock Exchange (TSX) under the symbol "ESL".

The information contained in this document represents the current view of Enghouse Interactive on the issues discussed as of the date of publication. Because Enghouse Interactive must respond to changes in market conditions, it should not be interpreted to be a commitment on the part of Enghouse Interactive and Enghouse Interactive cannot guarantee the accuracy of any information presented after the date of publication. The user assumes the entire risk as to the accuracy and the use of this document.

INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND FREEDOM FROM INFRINGEMENT.

This product and related documentation are protected by copyright and distributed under licenses restricting its use, copying, distribution, and recompilation. No part of this product or related documentation may be reproduced in any form by any means without prior written authorization by Enghouse Systems Limited.

---

## 1. Scope

This document is intended as a general guide for configuring a basic installation of the Cisco Unified Communications Manager Version 14.0 (CUCM 14.0) for use with Brooktrout SR140 Fax over IP (FoIP) software platform. The interoperability includes SIP call control and T.38/T.30 media.

The specific version of CUCM tested was 14.0.1.100000-20

For ease of reference, the Brooktrout SR140 Fax Software and Brooktrout TR1034 Fax Boards will sometimes be denoted herein, respectively, as SR140 and TR1034. The Cisco Unified Communications Manager will be denoted herein as CUCM 14.0 or Cisco CUCM 14.0, or some other form thereof. All references to the SDK herein refer to the Brooktrout Fax Products SDK.

This document is not intended to be comprehensive and thus does not replace the manufacturer's detailed configuration documentation. Users of this document should already have a general knowledge of how to install and configure the CUCM 14.0.

The sample configuration shown and/or referred in the subsequent sections was used for lab validation testing by Enghouse Interactive /Dialogic. As the lab system did not have an external PSTN or SIP trunk interface the testing was done between two different SR140 systems. Each system was configured with its own SIP trunk interface configured within the CUCM environment. The CUCM was then configured to route calls based on the numbers that were dialed to either of the two systems. Therefore, it is possible and even likely that the example configuration will not match the exact configuration and versions that would be present in a deployed environment. However, the sample configuration provides a possible starting point to work with the equipment vendor for configuring your device. Please consult the appropriate manufacturer's documentation for details on setting up your specific end user configuration.

## 2. Prerequisites

No special requirements to note.

## 3. Summary of Limitations

No special limitations to note.

---

## 4. SIP / SIP Configuration Details

The following systems were used for the sample configuration described in the document.

### 4.1 Cisco Unified Communication Manager 14.0 –SIP / SIP Configuration

<b>Vendor</b>	Cisco
<b>Model</b>	Cisco Unified Communication Manager
<b>Software Version</b>	14.0.1.100000-20
<b>Protocol to SR140 (1)</b>	SIP
<b>Protocol to SR140 (2)</b>	SIP

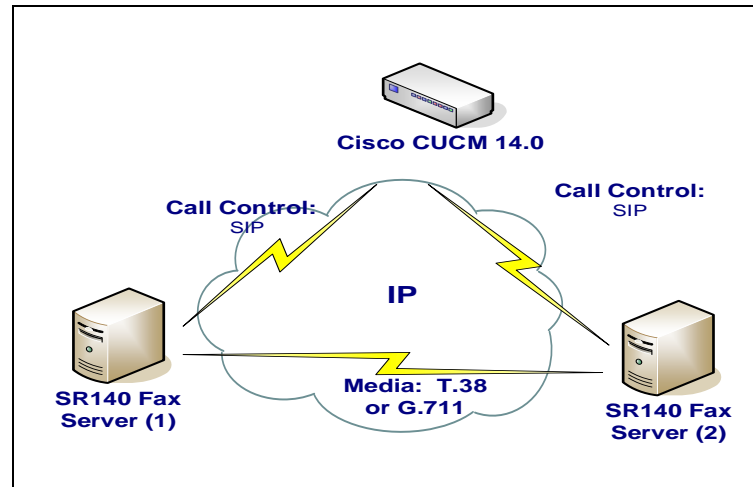
### 4.2 Brooktrout SR140 Fax Software

<b>Vendor</b>	Enghouse Interactive/Dialogic
<b>Model</b>	Brooktrout SR140 Fax Software
<b>Software Version</b>	SDK 6.15
<b>Protocol to CUCM</b>	SIP
<b>callctrl.cfg file</b>	SDK 6.15 – with recommended settings for SIP_From and SIP_Contact

---

## 5. Network System Configuration – SIP / SIP Configuration

The diagram below details the sample configuration used in connection with the SIP / SIP Configuration.



### Diagram Notes:

- SR140 Fax Server = Fax Server including Brooktrout SR140 Fax Software and third party fax application. In this test, two different fax servers were used to route calls between them through the CUCM.

### 5.1 Network Addresses

Device #	Device Make, Model, and Description	Device IP Address
1	Brooktrout SR140 (1)	10.51.42.7
2	Cisco Unified Communication Manager 14.0	10.51.53.177
3	Brooktrout SR140 (2)	10.51.42.8

### 5.2 Dialing Plan Overview

To call the SR140 (1) from SR140 (2), dial 21021XXX, where x is a number between 0 and 9.

To call the SR140 (2) from SR140 (1), dial 21022XXX, where x is a number between 0 and 9.

---

## 6. Brooktrout SR140 Fax Software Setup Notes

The manuals for the SR140 are available from the following site:  
<http://www.dialogic.com/manuals/brooktrout/default.htm>

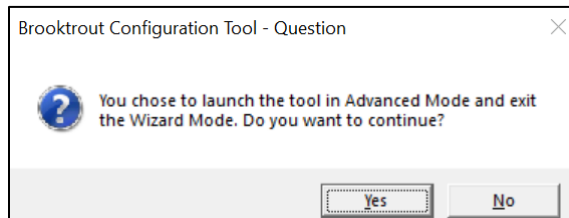
### 6.1 Test Configurations

The following SR140 Setup Wizard screen shots illustrate how the test configurations were set up to interop with the CUCM 14.0 system. Both of the SR140 servers were configured the same except for the IP address in the From Value filed.

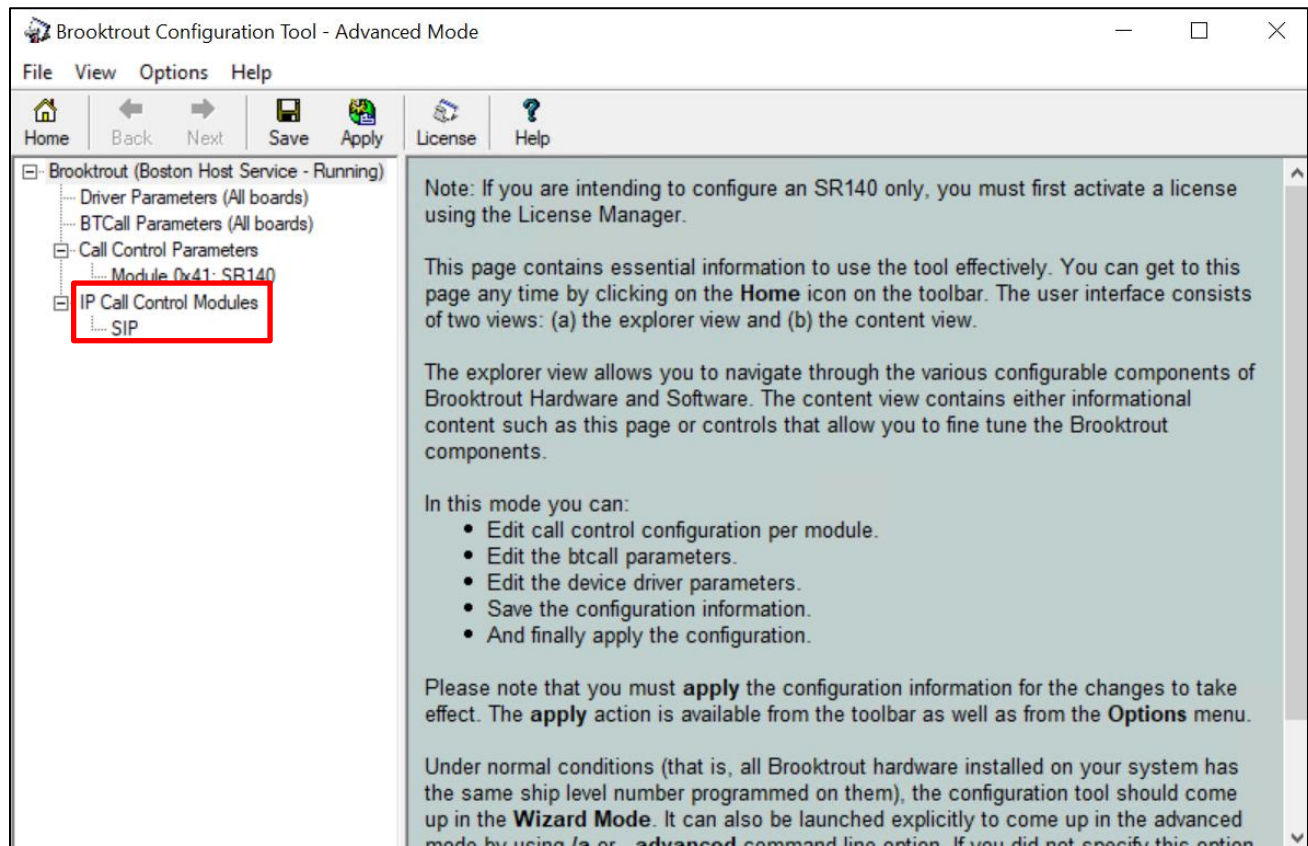
Launch the Config Tool (Start->Programs->Brooktrout->Brooktrout Configuration Tool)



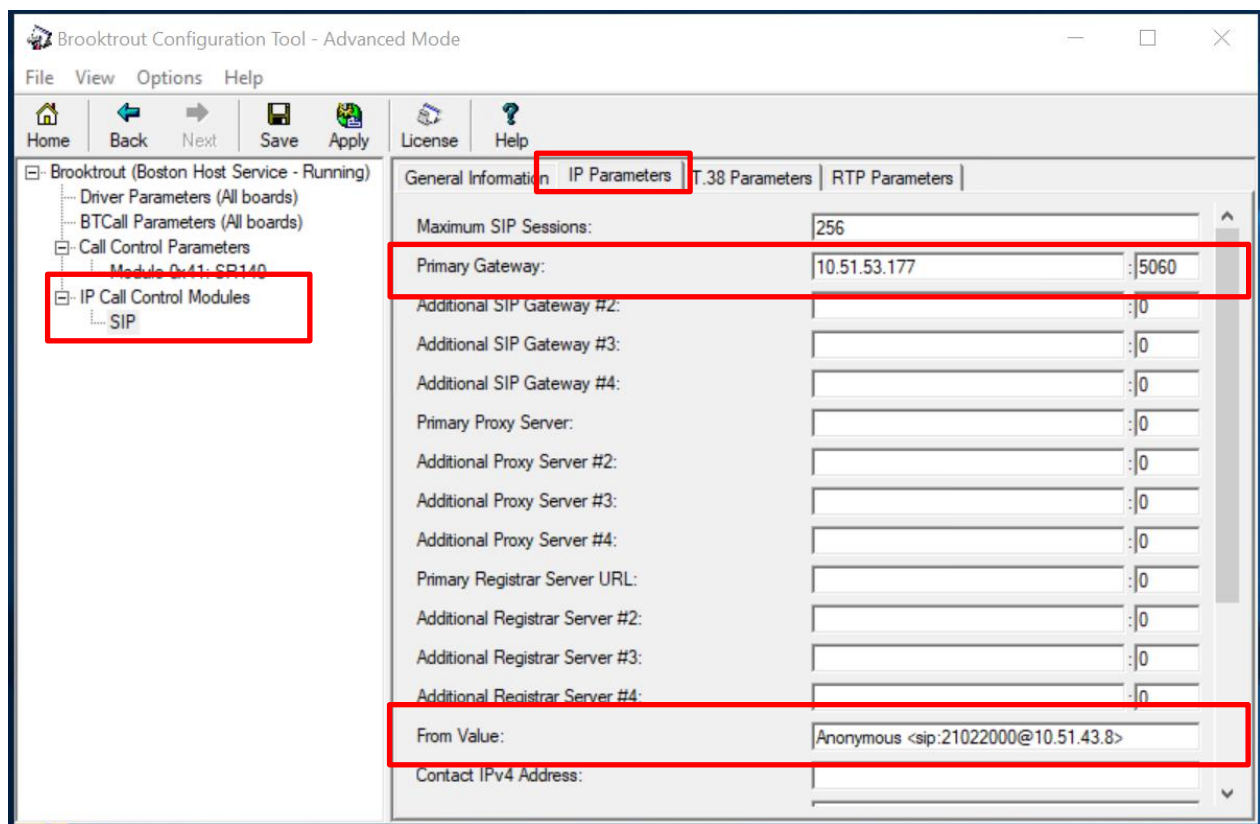
Select **Advanced Mode**.



Select **Yes** to enter Advanced Mode.



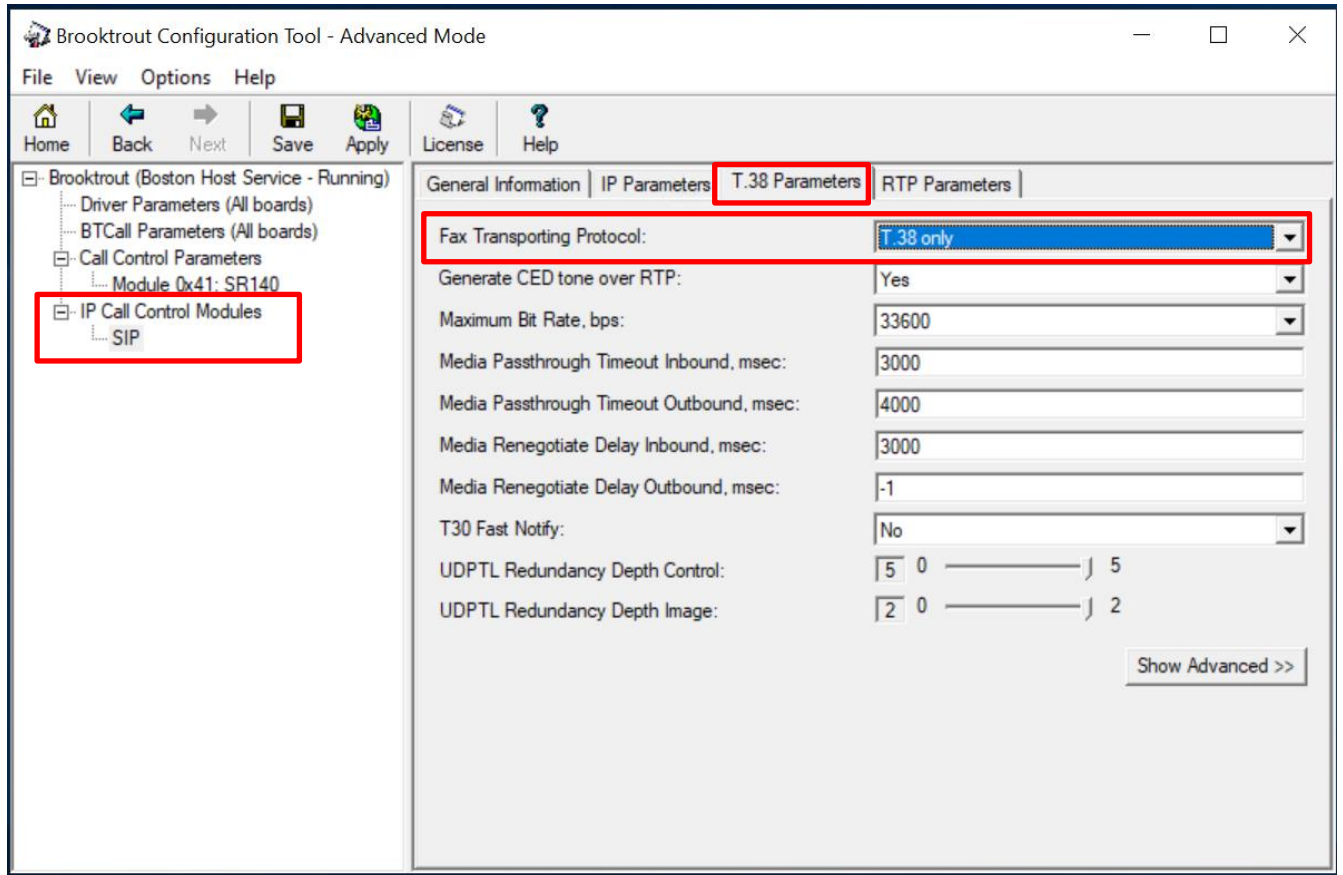
Select **SIP** under **IP Call Control Modules** and open the **IP Parameters** tab.



- In the **Primary Gateway** parameter enter the **IP address** and **signaling Port** of the Cisco UCM signaling port received from the Cisco administrator.
- Change **From Value** to **Anonymous <sip:PhoneNumber@SR140 server IP>** where the “**PhoneNumber**” is either specified by your Cisco Administrator, or one of the valid phone numbers in your inbound fax numbers. The **SR140 server IP** is the internal IP address of the SR140 server. For example: Anonymous [sip:21021xxx@10.51.43.8](mailto:sip:21021xxx@10.51.43.8) Note. This is the IP address that changes between the two SR140 servers used in this test scenario.



Select **SIP** under **IP Call Control Modules** and open the **T.38 Parameters** tab



- Confirm that **Fax Transporting Protocol** is set to **T.38 only**

Click **Save** then **Apply**. After the Apply is done, close the Configuration Tool.

---

## 6.2 SR140 callctrl.cfg File

The SR140 callctrl.cfg file used in the sample test configuration is shown below for reference.

```
l3l4_trace=none
l4l3_trace=none
api_trace=none
internal_trace=none
host_module_trace=none
ip_stack_trace=none
# Most of the time a path should be used for this file name.
trace_file=..\logs\ecc.log
max_trace_files=1
max_trace_file_size=10
[module.41]
model=SR140
virtual=1
exists=1
vb_firm=C:\Users\Administrator\Desktop\FDTool_PACKAGE 6.15-GA\FDTool_PACKAGE\bin\bostvb.dll
channels=2
[module.41/ethernet.1]
ip_preference=ipv4_only
ip_interface={A961EF98-A943-4706-92B5-F2FBDE015011}:0
ip_interfaceV6=
ip_address=0.0.0.0
ip_addressV6=
media_port_min=56000
media_port_max=56999
[module.41/host_cc.1]
host_module=1
number_of_channels=2
[host_module.1]
module_library=brktsip.dll
enabled=true
[host_module.1/t38parameters]
t38_fax_rate_management=transferredTCF
fax_transport_protocol=t38_only
t38_fax_udp_ec=t38UDPRedundancy
rtp_ced_enable=true
t38_max_bit_rate=33600
t38_fax_version=3
media_passthrough_timeout_inbound=3000
media_passthrough_timeout_outbound=4000
media_renegotiate_delay_inbound=3000
media_renegotiate_delay_outbound=-1
t38_fax_fill_bit_removal=false
t38_fax_transcoding_jbig=false
t38_fax_transcoding_mmr=false
```

---

```
g711_fallback_rtp_reinvite=false
t38_stream_renegotiation=single
t38_t30_fastnotify=false
t38_UDPTL_redundancy_depth_control=5
t38_UDPTL_redundancy_depth_image=2
t38_fax_max_buffer=200
t38_fax_max_datagram_send=72
t38_fax_max_datagram_rcv=125
[host_module.1/rtp]
rtp_frame_duration=20
rtp_jitter_buffer_depth=100
rtp_codec=pcmu
rtp_silence_control=inband
t38_offer_as_ced=true
rtp_voice_frame_replacement=0
[host_module.1/parameters]
sip_max_sessions=256
sip_default_gateway=10.51.53.177:5060
sip_gateway2=
sip_gateway3=
sip_gateway4=
sip_proxy_server1=
sip_proxy_server2=
sip_proxy_server3=
sip_proxy_server4=
sip_registration_server1=
sip_registration_server1_aor=
sip_registration_server1_username=
sip_registration_server1_password=
sip_registration_server1_expires=3600
sip_registration_server2=
sip_registration_server2_aor=
sip_registration_server2_username=
sip_registration_server2_password=
sip_registration_server2_expires=3600
sip_registration_server3=
sip_registration_server3_aor=
sip_registration_server3_username=
sip_registration_server3_password=
sip_registration_server3_expires=3600
sip_registration_server4=
sip_registration_server4_aor=
sip_registration_server4_username=
sip_registration_server4_password=
sip_registration_server4_expires=3600
sip_registration_interval=60
sip_registration_interval_delta=5
sip_registration_proxied=false
sip_Max-Forwards=70
```

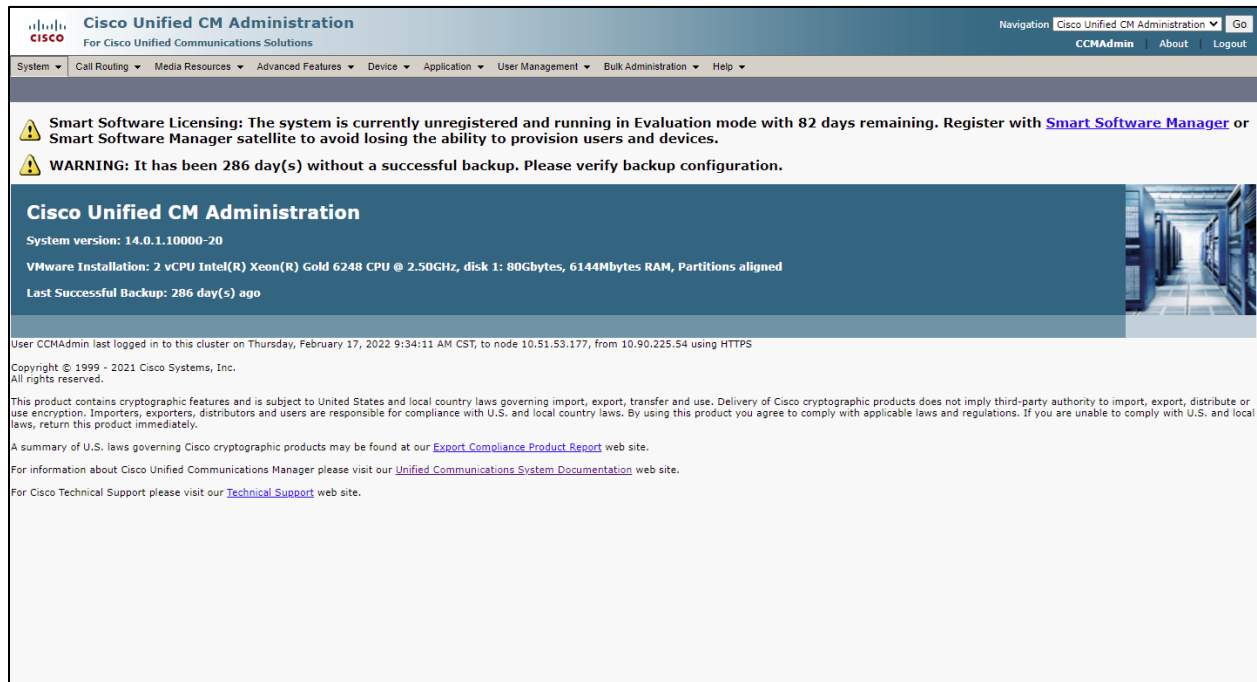
---

---

**sip\_From=Anonymous <sip:21022000@10.51.43.8>**

sip\_Contact=  
sip\_ContactV6=  
sip\_username=  
sip\_session\_name=no\_session\_name  
sip\_session\_description=  
sip\_description\_URI=  
sip\_email=  
sip\_phone=  
sip\_Route=  
sip\_session\_timer\_session\_expires=0  
sip\_session\_timer\_minse=-1  
sip\_session\_timer\_refresh\_method=0  
sip\_ip\_preference=ipv4\_only  
sip\_ip\_interface=  
sip\_ip\_interfaceV6=  
sip\_ip\_interface\_port=5060  
sip\_ip\_interface\_portV6=5060  
sip\_redirect\_as\_calling\_party=0  
sip\_T1\_timeout=500  
sip\_max\_invite\_retransmissions=7  
sip\_redirect\_as\_called\_party=0  
sip\_tcp\_enable=false  
sip\_user\_agent=Brktsip/6.15.0B2 (Dialogic)  
sip\_RFC3325\_identity=0  
sip\_transport\_protocol=udp  
sip\_reject\_call\_not\_answered=486  
sip\_reject\_unsupported\_media=488  
sip\_reject\_t38\_renegotiation=488  
sip\_100\_call\_not\_answered=true  
sip\_RFC6913\_enable=false  
sip\_options\_up\_interval=120  
sip\_options\_down\_interval=60  
sip\_tls\_enabled=false  
tls\_config\_filename=sip\_tls.cfg  
sip\_tls\_port=5061  
block\_udp\_port=true  
block\_tcp\_port=true  
srtp\_enabled=false  
srtp\_config\_filename=srtp.cfg  
fips\_enable=false  
sip\_use\_any\_reg\_contact\_expire=true  
ignore\_non\_initial\_record\_route=false  
sips\_sip\_uri\_scheme=sips  
nat\_sip\_address=  
nat\_media\_address=

## 7. CUCM 14.0 Setup Notes – SIP / SIP Configuration



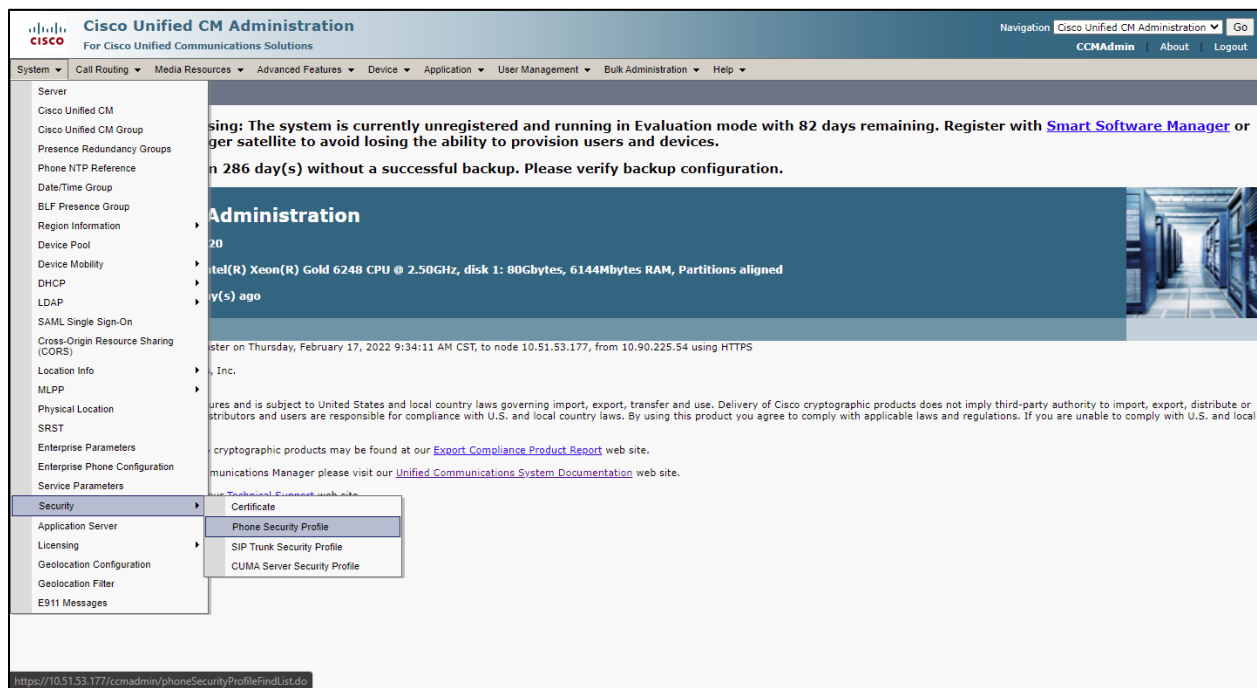
The CUCM 14.0 configuration values that were used in the sample configuration involve configuring the following items:

- Configure SIP Trunk Security Profile
- Configure SR140 (1) Trunk
- Configure SR140 (2) Trunk
- Configure Call Routing

### 7.1 Configure SIP Trunk Security Profile

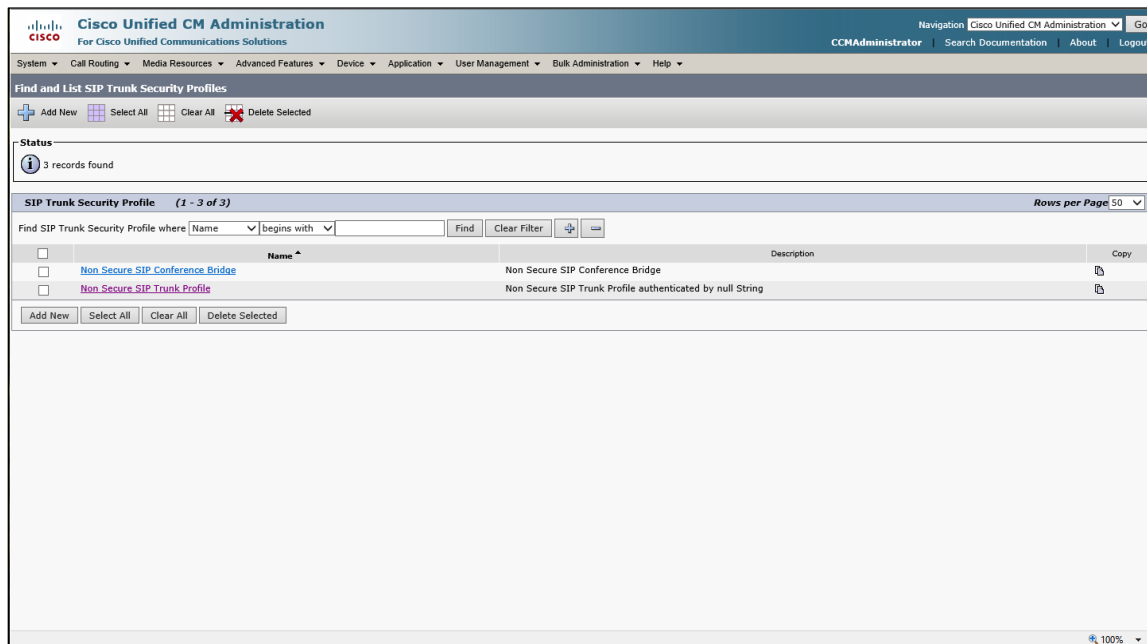
Using a web browser, log into CUCM 14.0. The following Cisco Unified CM Administration screen appears.

From the menu select System | Security | SIP Trunk Security Profile



The following screen will appear.

Click **Add New**.



Enter a Description: Dialogic Brooktrout SR140 (for example)  
Change **Outgoing Transport Type** to **UDP**

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go  
CCMAdministrator | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

**SIP Trunk Security Profile Configuration** Related Links: Back To Find/List | Go

Save

**Status**  
Status: Ready

**SIP Trunk Security Profile Information**

Name \* Dialogic Non Secure SIP Trunk Profile

Description Dialogic Brooktrout SR140

Device Security Mode Non Secure

Incoming Transport Type \* TCP+UDP

Outgoing Transport Type UDP

☐ Enable Digest Authentication

Nonce Validity Time (mins) \* 600

Secure Certificate Subject or Subject Alternate Name

Incoming Port \* 5060

☐ Enable Application level authorization

☐ Accept presence subscription

☐ Accept out-of-dialog refer \*\*

☐ Accept unsolicited notification

☐ Accept replaces header

☐ Transmit security status

☐ Allow charging header

SIP V.150 Outbound SDP Offer Filtering \* Use Default Filter

Save






Click **Save**.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go  
CCMAdministrator | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

**SIP Trunk Security Profile Configuration** Related Links: Back To Find/List | Go

Save     

**Status**  
Status: Ready

**SIP Trunk Security Profile Information**

Name \* Dialogic Non Secure SIP Trunk Profile

Description Dialogic Brooktrout SR140

Device Security Mode Non Secure

Incoming Transport Type \* TCP+UDP

Outgoing Transport Type UDP

☐ Enable Digest Authentication

Nonce Validity Time (mins) \* 600

Secure Certificate Subject or Subject Alternate Name

Incoming Port \* 5060

☐ Enable Application level authorization

☐ Accept presence subscription

☐ Accept out-of-dialog refer \*\*

☐ Accept unsolicited notification

☐ Accept replaces header

☐ Transmit security status

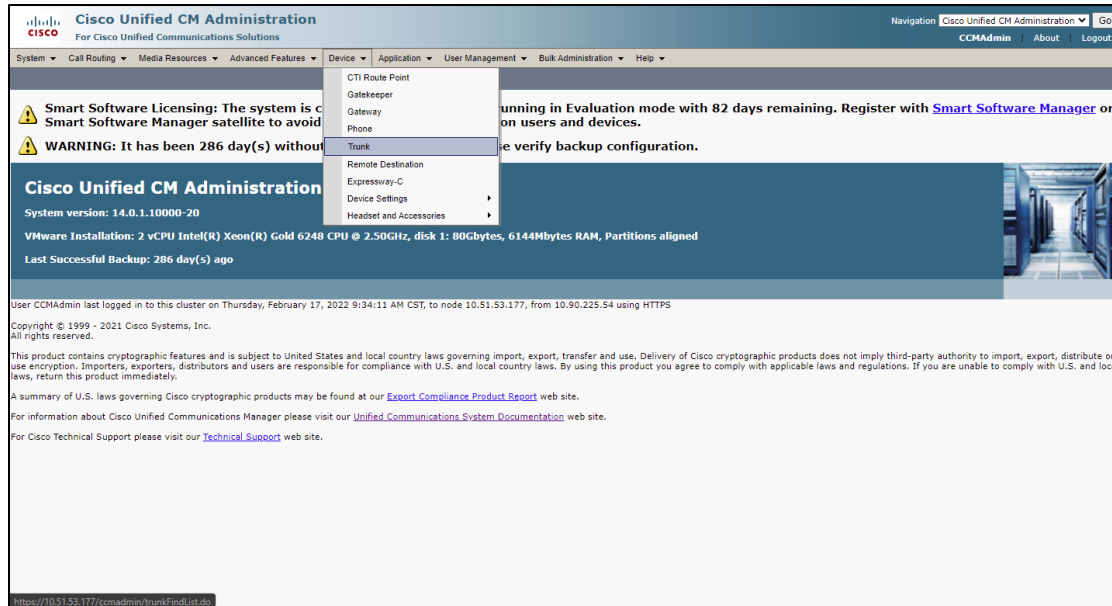
☐ Allow charging header

SIP V.150 Outbound SDP Offer Filtering \* Use Default Filter

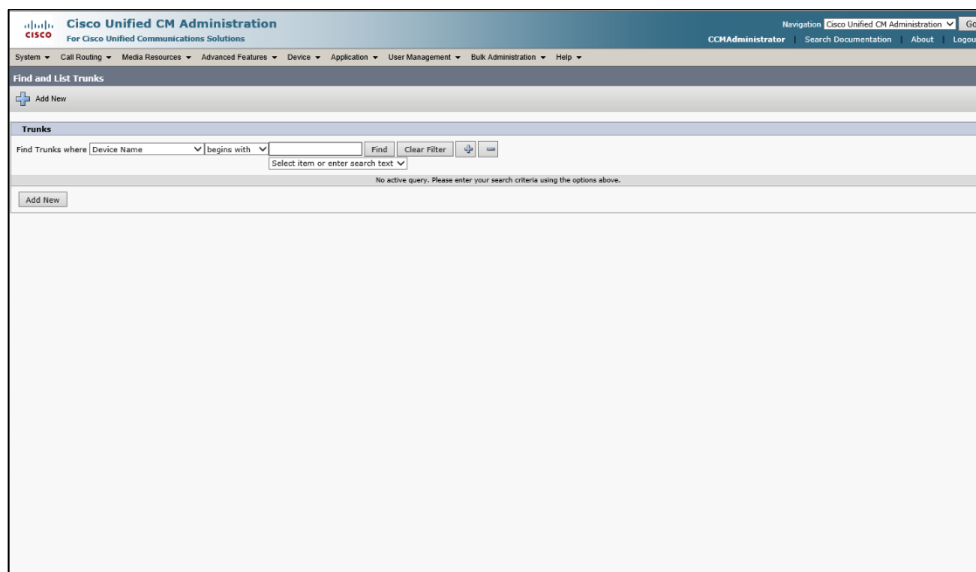
Save Delete Copy Reset Apply Config Add New

## 7.2 Configure SR140 (1) Trunk

Using a web browser, log into the Cisco Unified CM Administration screen  
From the menu select Device | Trunk



The following screen will appear. Press **Add New** to add a new SIP Trunk



Select **SIP Trunk** for the Trunk Type. Click **Next**.



**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go  
CCMAdministrator Search Documentation About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

Trunk Configuration Related Links: Back To Find/List Go

Next

*i*
Status: Ready

Trunk Information

Trunk Type \* -- Not Selected --  
Device Protocol \* H.225 Trunk (Gatekeeper Controlled)  
Inter-Cluster Trunk (Gatekeeper Controlled)  
Inter-Cluster Trunk (Non-Gatekeeper Controlled)  
SIP Trunk

Next

*i* \* indicates required item.

Accept the default Trunk Service Type. Click **Next**.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go  
CCMAdministrator Search Documentation About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

Trunk Configuration Related Links: Back To Find/List Go

Next

*i*
Status: Ready

Trunk Information

Trunk Type \* SIP Trunk  
Device Protocol \* SIP  
Trunk Service Type \* None(Default)

Next

*i* \* indicates required item.

Select **SIP** for the Device Protocol and press **Next**.

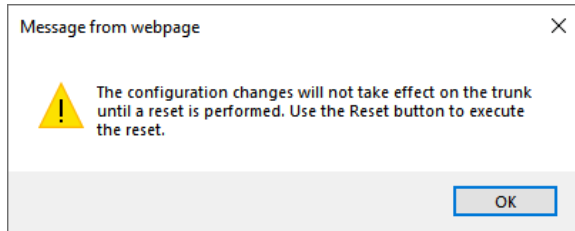
Set the following:

- Device Name: SR140-SIP (for example)
- Device Description: SR140-SIP (for example)
- Device Pool: Default
- Call Classification: OffNet
- Destination Address: 10.50.50.101 (Use the IP address of your SR140 server)
- SIP Trunk Security Profile: Dialogic Non Secure SIP Trunk Profile (for example)
- SIP Profile: Standard SIP Profile

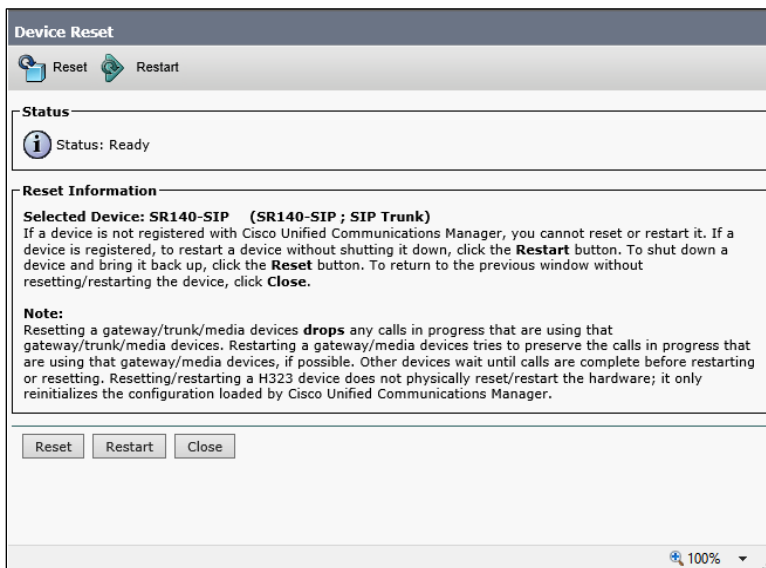
---

Click **Save**.

A reset message will appear. Click **OK**.



Press **Reset**, then click **Close**.

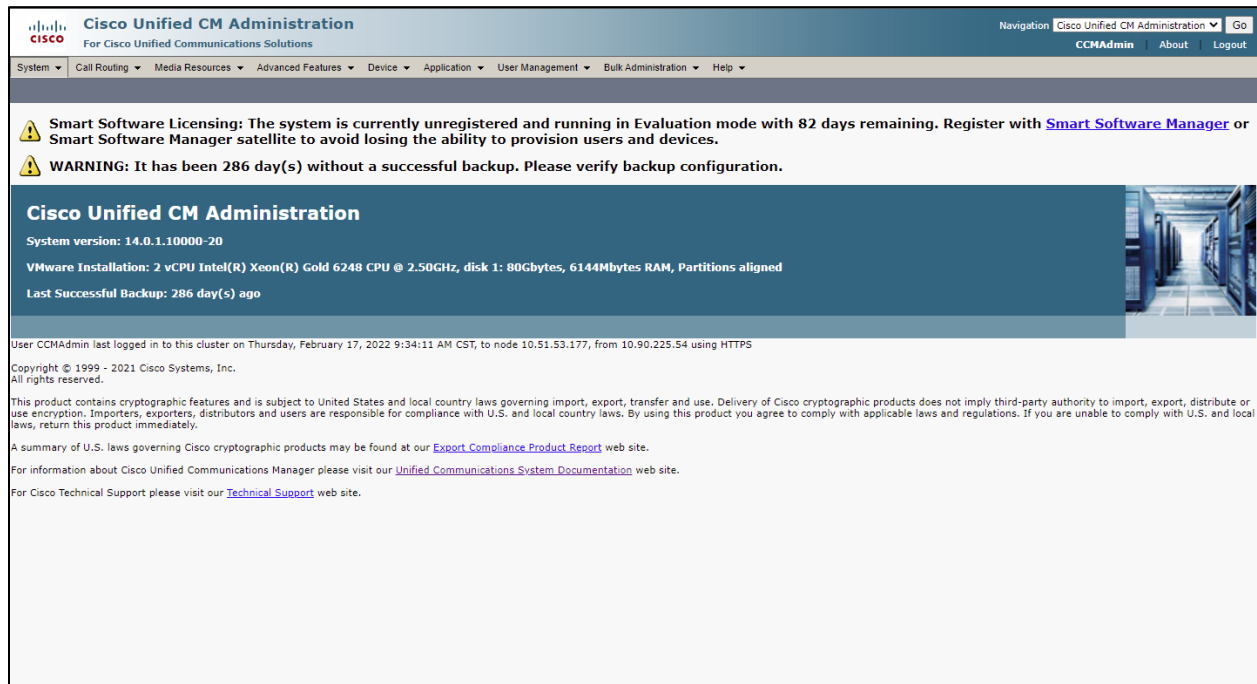


## 7.3 Configure SR140 (2) Trunk

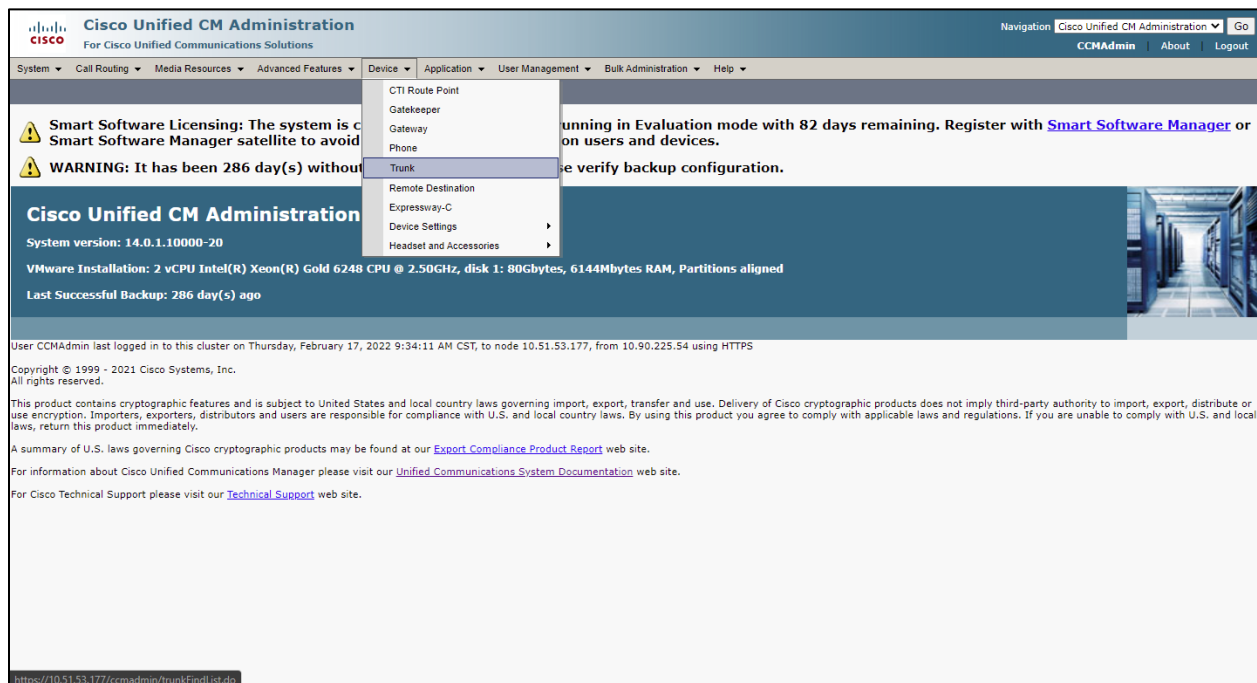
Under normal deployments the second trunk will be used to bring in a PSTN connection either through a SIP trunk using an SBC like the Cisco CUBE, or through a PRI through a Cisco voice router. In most cases this will already be configured for your voice usage. You will want to confirm that the following setting are set to support fax.

The following section describes how the second trunk was configured for this testing. It is similar to the previous trunk configuration but with a different IP address and a different route pattern that will be configured to route to this trunk versus the first one.

Using a web browser, log into the Cisco Unified CM Administration screen.



From the menu select Device | Trunk.



The following screen will appear. Click **Add New** to add a new SIP Trunk.

The screenshot shows the 'Find and List Trunks' page in the Cisco Unified CM Administration interface. The page has a header with the Cisco logo and navigation tabs. Below the header, there is a section titled 'Find and List Trunks' with an 'Add New' button. A search bar is present with a dropdown menu for 'Device Name' and a 'Find' button. Below the search bar, there is a message: 'No active query. Please enter your search criteria using the options above.' The main content area is empty.

Select **SIP Trunk** for the Trunk Type. Click **Next**.

The screenshot shows the 'Trunk Configuration' page in the Cisco Unified CM Administration interface. The page has a header with the Cisco logo and navigation tabs. Below the header, there is a section titled 'Trunk Configuration' with a 'Next' button. A 'Status' section shows 'Status: Ready'. Below this, there is a 'Trunk Information' section with a dropdown menu for 'Trunk Type'. The dropdown menu is open, showing the following options: 'Not Selected --', 'H.225 Trunk (Gatekeeper Controlled)', 'Inter-Cluster Trunk (Gatekeeper Controlled)', 'Inter-Cluster Trunk (Non-Gatekeeper Controlled)', and 'SIP Trunk'. The 'SIP Trunk' option is highlighted. Below the dropdown menu, there is a 'Next' button. At the bottom, there is a note: '\* - indicates required item.'

Accept the default Trunk Service Type. Click **Next**.

Cisco Unified CM Administration  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go  
CCMAdministrator Search Documentation About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

Trunk Configuration Related Links: Back To Find/List Go

Next

Status  
Status: Ready

Trunk Information  
Trunk Type \* SIP Trunk  
Device Protocol \* SIP  
Trunk Service Type \* None(Default)

Next

\* indicates required item.

Set the following:

- Device Name: SR140-SIP-2 (for example)
- Device Description: SR140-SIP-2 (for example)
- Device Pool: Default
- Call Classification: OffNet
- Destination Address: 10.50.50.102 (Use the IP address of your SR140 server)
- SIP Trunk Security Profile: Dialogic Non Secure SIP Trunk Profile (for example)
- SIP Profile: Standard SIP Profile

Cisco Unified CM Administration  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go  
CCMAdministrator Search Documentation About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

Trunk Configuration Related Links: Back To Find/List Go

Save

Status  
Status: Ready

Device Information  
Product: SIP Trunk  
Device Protocol: SIP  
Trunk Service Type: None(Default)  
Device Name: SR140-SIP-2  
Description: SR140-SIP-2  
Device Pool: Default  
Common Device Configuration: < None >  
Call Classification: OffNet  
Media Resource Group List: < None >  
Location: Hub\_None  
AAR Group: < None >  
Tunneled Protocol: None  
QSIG Variant: No Changes  
ASN.1 ROSE OID Encoding: No Changes  
Packet Capture Mode: None  
Packet Capture Duration: 0  
☐ Media Termination Point Required  
☒ Retry Video Call as Audio

**SIP Information**

☐ Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port	Status	Status Reason	Duration
1* 10.50.50.102		5060	N/A	N/A	N/A

NTP Preferred Originating Codec\* 711ulaw

BLF Presence Group\* Standard Presence group

SIP Trunk Security Profile\* Dialogic Non Secure SIP Trunk Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile\* Standard SIP Profile [View Details](#)

DTMF Signaling Method\* No Preference

**Normalization Script**

Normalization Script < None >

☐ Enable Trace

Parameter Name	Parameter Value
1	

**Recording Information**

☒ None

☐ This trunk connects to a recording-enabled gateway

☐ This trunk connects to other clusters with recording-enabled gateways

**Geolocation Configuration**

Geolocation < None >

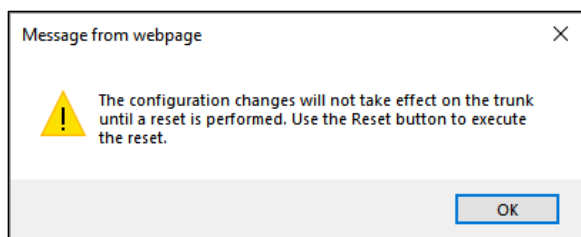
Geolocation Filter < None >

☐ Send Geolocation Information

[Save](#)

Click **Save**.

A reset message will appear. Click **OK**.



Press **Reset**, then click **Close**.

**Device Reset**

[Reset](#) [Restart](#)

**Status**

Status: Ready

**Reset Information**

**Selected Device: SR140-SIP-2 (SR140-SIP-2; SIP Trunk)**

If a device is not registered with Cisco Unified Communications Manager, you cannot reset or restart it. If a device is registered, to restart a device without shutting it down, click the **Restart** button. To shut down a device and bring it back up, click the **Reset** button. To return to the previous window without resetting/restarting the device, click **Close**.

**Note:**  
Resetting a gateway/trunk/media devices **drops** any calls in progress that are using that gateway/trunk/media devices. Restarting a gateway/media devices tries to preserve the calls in progress that are using that gateway/media devices, if possible. Other devices wait until calls are complete before restarting or resetting. Resetting/restarting a H323 device does not physically reset/restart the hardware; it only reinitializes the configuration loaded by Cisco Unified Communications Manager.

[Reset](#) [Restart](#) [Close](#)

100%

## 7.4 Configure Call Routing

Using a web browser, log into the Cisco Unified CM Administration screen.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

CCMAdmin About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

**Smart Software Licensing:** The system is currently unregistered and running in Evaluation mode with 82 days remaining. Register with [Smart Software Manager](#) or Smart Software Manager satellite to avoid losing the ability to provision users and devices.

**WARNING:** It has been 286 day(s) without a successful backup. Please verify backup configuration.

**Cisco Unified CM Administration**  
System version: 14.0.1.10000-20  
VMware Installation: 2 vCPU Intel(R) Xeon(R) Gold 6248 CPU @ 2.50GHz, disk 1: 80Gbytes, 6144Mbytes RAM, Partitions aligned  
Last Successful Backup: 286 day(s) ago

User CCMAdmin last logged in to this cluster on Thursday, February 17, 2022 9:34:11 AM CST, to node 10.51.53.177, from 10.90.225.54 using HTTPS

Copyright © 1999 - 2021 Cisco Systems, Inc.  
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

From the menu select Call Routing | Route / Hunt | Route Pattern.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

CCMAdministrator Search Documentation About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

**Smart Software Licensing:** The system is currently unregistered and running in Evaluation mode with 69 days remaining. Register with [Smart Software Manager](#) or Smart Software Manager satellite to avoid losing the ability to provision users and devices.

**WARNING:** It has been 286 day(s) without a successful backup. Please verify backup configuration.

**Cisco Unified CM Administration**  
System version: 14.0.1.10000-20  
VMware Installation: 2 vCPU Intel(R) Xeon(R) Gold 6248 CPU @ 2.50GHz, disk 1: 80Gbytes, 6144Mbytes RAM, Partitions aligned  
Last Successful Backup: 286 day(s) ago

User CCMAdmin last logged in to this cluster on Tuesday, August 11, 2020 2:14:15 PM CDT, to node 10.51.53.175, from 10.90.247.26 using HTTPS

Copyright © 1999 - 2021 Cisco Systems, Inc.  
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.



The following screen will appear. Click **Add New**.

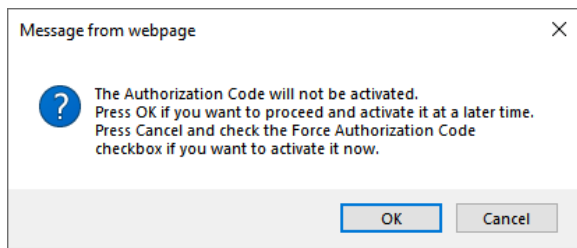
The screenshot shows the 'Find and List Route Patterns' page in the Cisco Unified CM Administration interface. The page has a header with the Cisco logo and navigation tabs. Below the header, there is a section titled 'Find and List Route Patterns' with an 'Add New' button. A search bar is present with a dropdown menu set to 'Pattern' and a 'Find' button. Below the search bar, there is a message: 'No active query. Please enter your search criteria using the options above.' The main content area is empty.

Set the following:

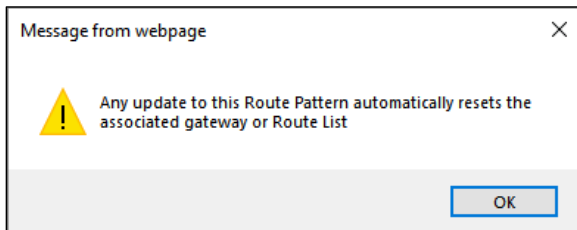
- Route Pattern: 21021XXX
- Description: SR140-SIP 21021XXX
- Gateway/Route List: SR140-SIP
- Call Classification: OffNet

The screenshot shows the 'Route Pattern Configuration' page in the Cisco Unified CM Administration interface. The page has a header with the Cisco logo and navigation tabs. Below the header, there is a section titled 'Route Pattern Configuration' with a 'Save' button. The page displays the configuration for a route pattern. The 'Status' is 'Ready'. The 'Pattern Definition' section includes the following fields: 'Route Pattern' (21021XXX), 'Route Partition' (< None >), 'Description' (SR140-SIP 21021XXX), 'Numbering Plan' (Not Selected), 'Route Filter' (< None >), 'MLPP Precedence' (Default), 'Apply Call Blocking Percentage' (unchecked), 'Resource Priority Namespace Network Domain' (< None >), 'Route Class' (Default), 'Gateway/Route List' (SR140-SIP), 'Route Option' (Route this pattern), 'Call Classification' (OffNet), 'External Call Control Profile' (< None >), 'Allow Device Override' (unchecked), 'Provide Outside Dial Tone' (checked), 'Allow Overlap Sending' (unchecked), 'Urgent Priority' (unchecked), 'Require Forced Authorization Code' (unchecked), 'Authorization Level' (0), and 'Require Client Matter Code' (unchecked).

Click **Save**.



Press **OK**.



Press **OK**.

Repeat the same steps and set the following to route to the SR140-2:

- Route Pattern: 21022XXX
- Description: SR140-SIP-2 21022XXX
- Gateway/Route List: SR140-SIP-2
- Call Classification: OffNet

Click **Save**.

---

## 8. References

- Brooktrout Fax Products Installation and Configuration Guide  
<http://www.dialogic.com/manuals/brooktrout/default.htm>
- CUCM Documentation Roadmaps  
[http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_documentation\\_roadmaps\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html)

## 9. Frequently Asked Questions

- ***I'm configured as near as possible to the sample configuration described in this document, but calls are still not successful; what is my next step?***

If you have confirmed your configuration is correct, you should open a support case with your Fax Server Application provider or Brooktrout technical support and provide the following information:

- The LAC (License Activation Code) for the SR140 license that is covered by a support contract
- A network capture showing the failed call attempts (see below for information on collecting a network capture)
- A copy of your callctrl.cfg and btcall.cfg files
- A set of debug logs (see below for information on collecting debug logs)

For Brooktrout Technical Support, email [Brooktrout.support@enghouse.com](mailto:Brooktrout.support@enghouse.com).

- ***How do I obtain network captures?***

There are two options: Wireshark and Brooktrout Capture Tool.

### Wireshark

Traces can be captured and viewed using the Wireshark network analyzer program, which can be freely downloaded from <http://www.wireshark.org>. Instructions for using this program can also be found on that site.

Select "Capture->Options" and select the Network Interface that the fax server is set up to use. Select "Start" and place a test call

To view the call flow in Wireshark, open the desired network trace file and select "Statistics->VoIP Calls" from the dropdown menu. Then highlight the call and click on the "Graph" button.

---

## Brooktrout Capture Tool

Information on running the Brooktrout Packet capture utility can be found at:

<https://ei-brooktrout.smartsupportapp.com/articles/132-New-Features-in-Brooktrout-SDK-6-15-Command-Line-Packet-Capture-Tool>

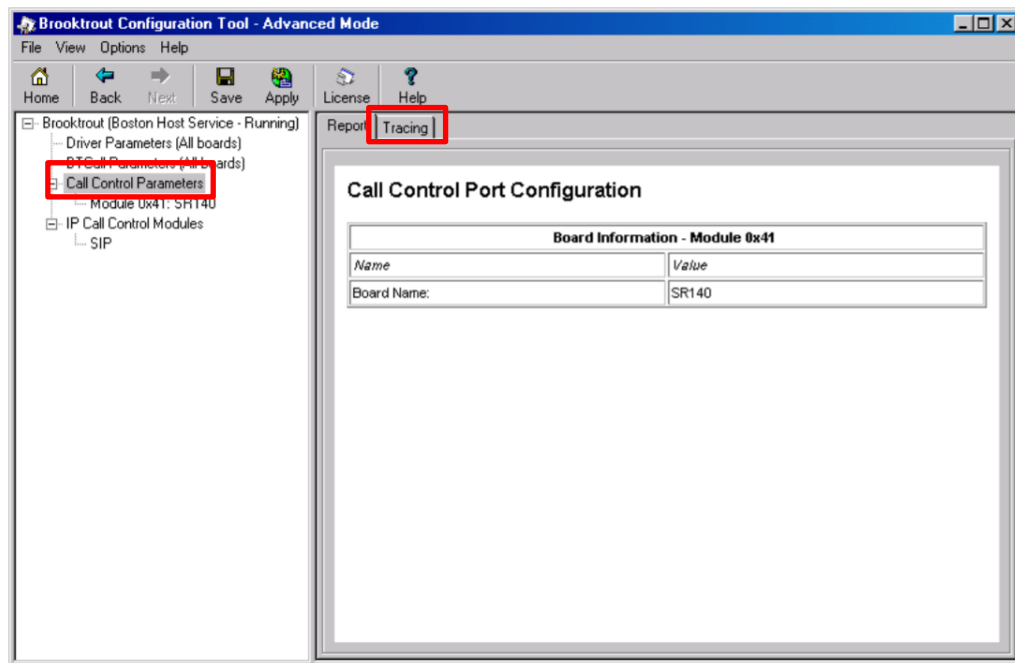
- ***How do I enable and gather debug logs?***

### ECC Logs

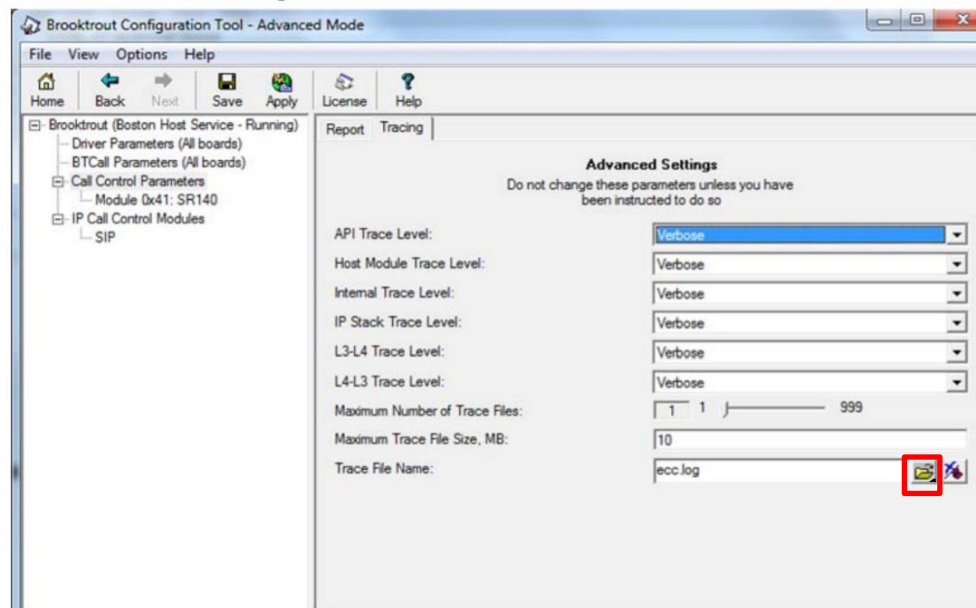
1. Open the Config Tool in Advanced Mode. This is done by clicking the "Advanced Mode" button on the lower left when/if the tool opens by default in Wizard Mode.



2. Highlight "Call Control Parameters." On the right side click "Tracing."



3. For all "\_trace" values, choose "Verbose."



4. For the "trace\_file" select a file name with an \*absolute\* path, that's important. You do this by clicking the open folder icon and going from there.

- 
5. If you wish to create multiple call trace logs and/or set another maximum size in megabytes, please do so where indicated.
  6. When done, hit "Save" then "Apply". Among other things this will restart the Boston Host Service.
  7. To turn off ECC logging later, go back into the config tool and set all "trace" values to "none", and click the blue cross/red flag icon by "trace\_file" to wipe everything out of that field to give it a null value. Then hit Save/Apply again.

### **API Debug Logs**

API debug logs need to be configured by the Fax Server application providers. Please follow their directions on enabling their logging including Brooktrout API logs.

If using the Brooktrout FDTool sample application API debug logs can be enabled by selecting: "Tools->Debug".

The resulting logs will be stored in "logs" directory of the folder where FDTool was installed.