Cisco BroadWorks

Interoperability Testing Handbook

Document Version 1.2

Copyright Notice

Trademarks

Document Revision History

Table of Contents

Table of Figures

1 Introduction

This handbook is a companion document to the Cisco BroadWorks interoperability program and its associated test plans and applies for Cisco BroadWorks Release 23.0 and later. It contains information essential for performing interoperability testing including test platform, process, and configuration information. Cisco provides a SIP interoperability program for Cisco BroadWorks and a test platform that enables SIP device and SIP application vendors to self-test against the Cisco BroadWorks platform.

Successful completion of interoperability testing, followed by validation of the test results by Cisco, results in the device or application being validated for use with Cisco BroadWorks. It also fulfills a prerequisite for Cisco BroadCloud integration if applicable: some device or application types have applicability only to Cisco BroadWorks. For more information, see the individual test plan.

Cisco BroadWorks is a software model in which the service provider manages the software and the endpoints. Cisco BroadCloud is a cloud service model in which Cisco manages the Cisco BroadWorks software and the endpoints on behalf of the service provider. SIP and Device Management testing are prerequisites for endpoint integration with Cisco BroadCloud. After the prerequisites are met, the device is eligible for Cisco BroadCloud integration. However, Cisco BroadCloud integration is driven by customer demand and requires software development and additional testing by Cisco engineers. Because of this, only a subset of devices meeting the Cisco BroadCloud prerequisites are integrated. Cisco BroadCloud integration is outside the scope of this document and the SIP interoperability program in general.

Validation of a device or application with Cisco BroadWorks is essential as it identifies interoperability issues and determines the optimal configuration. Most service providers require validation with Cisco BroadWorks before deploying the device or application in their networks. Cisco requires validation with Cisco BroadWorks before providing technical support on issues related to the device or application in a deployment with Cisco BroadWorks.

1.1 Developer's sandbox

Cisco provides a website to facilitate the interoperability testing process: https://developer.cisco.com/docs/broadworks. The site includes everything needed for interoperability testing including test plans, interface specifications, and a forum for posting questions and obtaining help during the testing process. The site also provides an announcement blog to provide notifications for maintenance, outages, upgrades, and other topics pertaining to the test community. As a first step in the process, browse to the developer's sandbox, self-create a login, and take a look at the content.

Access to the developer's sandbox and participation in the interoperability program does not require a Non-Disclosure Agreement (NDA).

2 Test Plans

The Cisco BroadWorks test plans are available for download from the developer's sandbox. The site maintains the latest versions of the test plans including any recent corrections or updates. The site provides test plans for the current Cisco BroadWorks release.

2.1 SIP Test Plans

Table 1 maps device or application types to the applicable Cisco BroadWorks SIP interoperability test plan. Use this table to determine which test plan to use.

Table 1 SIP Test Plans

Device/Application Type	Examples	Cisco BroadWorks SIP Test Plan
SIP Phone	Desktop Phone Soft Client DECT Phone Door Phone Conference Room Phone Video Phone	Cisco BroadWorks SIP Phone SIP Interoperability Test Plan
SIP Access Device	Access Gateway ATA EMTA Integrated Access Device (IAD) Multi-Service Business Gateway (MSBG) Optical Network Terminal (ONT) Wireless Router	Cisco BroadWorks SIP Access Device SIP Interoperability Test Plan
SIP Network Device	PSTN Gateway Media Gateway E911 Gateway Peering Gateway Network Proxy	Cisco BroadWorks SIP Network Device SIP Interoperability Test Plan
SIP Trunking	IP-PBX Trunking Gateway IVR Contact Center	Cisco BroadWorks SIP Trunking SIP Interoperability Test Plan
Call Recording Server	Call Recording Server/Service	Cisco BroadWorks Call Recording Server SIPREC Interoperability Test Plan
Conference Server	Conference Server Multipoint Control Unit (MCU)	Cisco BroadWorks Conference Server SIP Interoperability Test Plan
Music/Video On Hold Server	Music/Video on Hold Server/Service	Cisco BroadWorks Music/Video On Hold Server SIP Interoperability Test Plan

Device/Application Type	Examples	Cisco BroadWorks SIP Test Plan
Voice Mail Server	Voice Mail Server/Service	Cisco BroadWorks Voice Mail Server SIP Interoperability Test Plan

2.2 Additional Endpoint Test Plans

Table 2 lists endpoint test plans for interfaces other than SIP and maps their usage to the applicable device type.

Table 2 Additional Endpoint Test Plans

Cisco BroadWorks Test Plan	Device Type	Comments
Cisco BroadWorks Device Management Interoperability Test Plan	SIP Phone SIP Access Device Enterprise SSE Trunking Gateway	Recommended for all SIP phones and SIP access devices. Prerequisite for Cisco BroadCloud integration.
Cisco BroadWorks SIP Phone Xsi and XMPP Interoperability Test Plan	SIP Phone	Required for SIP phones which have implemented the Xsi and/or XMPP interfaces.
Cisco BroadWorks SIP Phone Functional Interoperability Test Plan	SIP Phone	Optional test plan for SIP phones which exercises advanced functionality.

3 Test Platform

Cisco provide a platform for Cisco BroadWorks interoperability testing which is reachable over public internet. Cisco maintains the platform identified as Cisco BroadWorks Sandbox. The Cisco BroadWorks Sandbox platform runs the latest Cisco BroadWorks release.

It is usually sufficient to perform testing against the latest release (Cisco BroadWorks).

The test platform enables all testing required by the test plans. **However, the test platform is a closed systems. There is no PSTN access to/from the test platform.** Calls can be made only between the users and devices configured on the test platform.

SIP, HTTPS, and other interfaces are exposed with public IPs on the test platform to allow for over the top testing as shown in *Figure 1*. The SBCs fronting the platform are configured to anchor media as they would be in most deployments. The PSTN network is shown for PSTN, E911, and other PSTN testing.

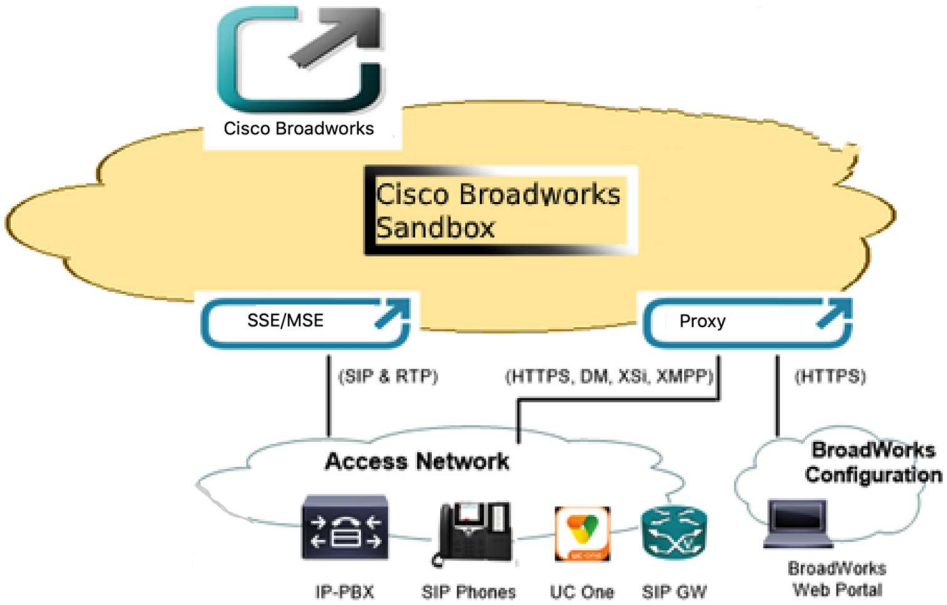

Figure 1 Cisco BroadWorks Sandbox Test Platform Network Diagram

3.1 IP Addresses and FQDNs

The IP addresses and FQDNs necessary for interoperability testing are identified in this section. TLSv1.2 is enforced when accessing Cisco BroadWorks system via Proxy server. This includes HTTPS and XMPP.

SSE and MSE are deployed in Cisco BroadWorks Sandbox system. SIP/TLSv1.2 and Secured RTP are supported via SSE/MSE.

3.1.1 Cisco BroadWorks Sandbox

3.1.1.1 FQDNs

Description	FQDN
Default System Domain	broadsoftlab.com

Description	FQDN
BroadWorks Web Portal	broadsoftsandboxxsp.cisco.com
HTTP/XMPP Proxy	ucaas01-tigase.stage.broadsoft.cloud
Signaling Service Edge (SSE)	64.103.37.43

3.1.1.2 IPv4 Addresses

Description	IPv4 Address
BroadWorks Web Portal	64.103.37.40
HTTP/XMPP Proxy	35.184.165.243
Signaling Service Edge (SSE)	64.103.37.43
DNS Server	8.8.8.8 (or other public DNS)

3.1.1.3 URIs

Description	URI
Conference URI	conference@broadsoftlab.com
Device Management URI	https://broadsoftsandboxxsp.cisco.com:443/dms
Device Management Defaults URI	https://broadsoftsandboxxsp.cisco.com:443/dms

3.2 Signaling and Media Ports

This section identifies the signaling and media ports used by the test platform.

Protocol	Port	Description
HTTPS	443/TCP	BroadWorks Web Portal, Device Management, Xsi
XMPP	5222/TLS	XMPP over TLS v1.2
SIP (UDP|TCP)	5060	SSE SIP over UDP/TCP
SIP (Failover)	8932, 8934, 8935	SSE SIP over UDP for failover testing
SIP (TLS)	5061	SSE SIP over TLSv1.2
RTP	10900 - 65535	MSE media port range

3.3 DNS SRV

The test platform FQDNs are resolvable by public DNS servers. The DNS records for the SSE FQDNs provide SRV records which the device under test must use to identify the preferred SSE address by cost/weight of the SRV record. The device under test must support DNS SRV in order to qualify as a candidate for Cisco BroadCloud integration.

If DNS SRV is not supported, alternative methods may be used for testing as follows:

- DNS A record with static order
- Hard-coded outbound proxy IP addresses on the device

4 Test Accounts

Cisco provides accounts for interoperability testing on the test platform upon request. Test accounts are provided on the Cisco BroadWorks Sandbox system. Test accounts are provided without charge. The test accounts must be used for development and interoperability testing or troubleshooting only. They are not intended for use for performance or frequent regression testing. The test platform is monitored. Misuse of the accounts will result in the account access being terminated.

4.1 Request Test Accounts

To request test accounts, navigate to the Cisco DevNet Sandbox lab site and RESERVE your account for a maximum of Five days.

One individual per company should request the test accounts. Cisco will provide an email response to the account request typically within few hours. The email will contain information on the test accounts which have been preconfigured for your use. The email may also contain special instructions or follow-up questions.

Cisco reserves the right to terminate usage of test accounts at any time for any reason.

Hi <name>,

Good News! Your Cisco BroadWorks Lab is ready. Let us get you connected to your Lab!
The BroadWorks CommPilot portal is available at
http://broadsoftsandboxxsp.cisco.com/CommPilot
And you can access it using credentials below:

Group rtolassi-Grp1:

Role	Name	Number	Password
Admin	rtolassi-Grp1		XXXXXXX
Auto Attendant	A9736722680	9736722680	
User	u9736722681	9736722681	XXXXXXX
User	u9736722682	9736722682	XXXXXXX
User	u9736722683	9736722683	XXXXXXX
User	u9736722684	9736722684	XXXXXXX
User	u9736722685	9736722685	XXXXXXX

Role	Name	Number	Password
Admin	rtolassi-Grp2		XXXXXXX

User ID	9736722681
Domain	broadsoftlab.com
Password	XXXXXXX
Display Name	u9736722681
Authorization Name	u9736722681
Outbound Proxy	64.103.37.43:5683

Your Sandbox Lab

Go directly to your Cisco BroadWorks Lab
(You need to be logged into DevNet to navigate to your lab)

We hope you find your Cisco BroadWorks Lab useful, and your reservation time productive.

If you do have questions or issues, we encourage you to engage with us in the
DevNet Sandbox Developer Community Forum
Cloud Calling community
Thanks for playing in the Sandbox with us!
--The DevNet Sandbox Team

Figure 2 Sample Cisco BroadWorks Sandbox Account Information Email

4.2 Test Account Details

The test accounts provided by Cisco for interop testing are preconfigured to facilitate much of the testing with little extra configuration required by the tester. Test cases that do require additional configuration clearly describe the necessary steps the tester must complete.

It is important to keep track of the Group administrator password because logging in as the Group admin allows you to address any issues within the group such as forgotten User passwords. Note that when you first log in as Group admin, a password change is required. If the Group administrator password is misplaced or forgotten, you must contact Cisco at devnet-broadsoft-support@external.cisco.com to request a reset.

Group services are assigned to group by default. The only group service that is preconfigured in the Group is Auto Attendant.

Most User services are pre-assigned. **User services that are not pre-assigned should only be assigned to a specific user as required by the test plan as they can conflict with other services**.

Refer to the tables in sections *0 Standard Test Account Setup* and *0* the account pre-configuration details. Replace <*Group*> with the name of your group to derive the user IDs.

Standard Test Account Setup

Refer to the tables in this section for standard test account setup which is applicable for testing most CPE, SSE, and PSTN peering.

Table 3 Standard Test Account Setup for Group 1

Group 1		
DN (Last 2 Digits)	**User ID or Group Service**	**Unique Features**
03-10	<Group>-G1U03 - <Group>-G1U10 Example: Cisco-G1U03	
11	<Group>-G1U11_Desktop Example: Cisco-G1U11_Desktop	UC-One SaaS
15-48	Unassigned	
49	Auto Attendant	

Table 4 Standard Test Account Setup for Group 2

Group 2		
DN (Last 2 Digits)	**User ID or Group Service**	**Unique Features**
50	Unassigned	
51	<Group>-G2U01 Example: Cisco-G2U01	Busy Lamp Field
52-71	<Group>-G2U02 - <Group>-G2U21 Example: Cisco-G2U02	
72	<Group>-G2U22_Desktop Example: Cisco-G2U22_Desktop	UC-One SaaS
73	<Group>-G2U23_Desktop Example: Cisco-G2U23_Desktop	UC-One SaaS
76-99	Unassigned	

Table 5 Logins and Passwords

Logins and Passwords		
Role / Service	**Username / Password**	**Additional Information**
User Login	<userID>@broadsoftlab.com / <Group>pswd Example: Cisco-G1U01_VM@broadsoftlab.com / Ciscopswd	The password can be reset via web portal by Group admin. Go to *<user>* → *Profile* → *Passwords*.
UC-One Client Login	<userID>@broadsoftlab.com / <Group>pswd Example: Cisco-G1U11_Desktop@broadsoftlab.com / Ciscopswd	The password can be reset via web portal by Group admin. Go to *<user>* → *Profile* → *Passwords*.
SIP Register Address of Record	<DN>@broadsoftlab.com Example: 2405556601@broadsoftlab.com	
SIP Authentication	Not preconfigured.	Go to *<user>* → *Utilities* → *Authentication* to configure.
Voice Management Advanced Settings	<TBD>	<TBD>
Voice Portal Passcode	User's Extension	Must be changed during initial access of the voice portal. Can be reset via web portal by Group admin. Go to *<user>* → *Profile* → *Passwords*.

Table 6 Group Services

Group Services	
Account/Authorization Codes	Hunt Group
Auto Attendant	Instant Group Call

Group Services	
Call Capacity Management	Meet-Me Conferencing
Call Park	Music On Hold
Call Pickup	Outgoing Calling Plan
Find-me/Follow-Me	Trunk Group
Group Paging	Voice Messaging Group

Table 7 User Services – Pre-assigned

User Services – Pre-assigned	
Alternate Number	Connected Line Identification Presentation
Anonymous Call Rejection	Connected Line Identification Restriction
Authentication	Customer Originated Trace
Basic Call Logs	Customer Ringback User
BroadWorks Agent	Customer Ringback User – Call Waiting
BroadWorks Anywhere	Customer Ringback User – Video
Business Communicator Desktop	Directed Call Pickup
Business Communicator Desktop - Audio	Directed Call Pickup with Barge-In
Business Communicator Desktop - Video	Do Not Disturb
Business Communicator Mobile	External Calling Line ID Delivery
Business Communicator Mobile - Audio	Fax Messaging
Business Communicator Mobile - Video	Flexible Seating Guest
Business Communicator Tablet	In Call Service Activation
Busy Lamp Field	Internal Calling Line ID Delivery
Call Center – Standard	Multiple Call Arrangement
Call Center – Premium	Music/Video On Hold
Call Forwarding Always	N-Way Call
Call Forwarding Busy	Priority Alert
Call Forwarding No Answer	Push To Talk
Calling Line ID Delivery Blocking	Remote Office
Call Park	Sequential Ring
Call Recording	Shared Call Appearance
Call Return	Silent Alerting
Call Transfer	Simultaneous Ring

User Services – Pre-assigned	
Call Waiting	Speed Dial 8

Table 8 User Services – Not Pre-Assigned

User Services – Not Pre-Assigned	Comments
Advice of Charge	Advice of Charge is not covered and should not be assigned.
Executive	Do not assign Executive and Executive Assistant to the same user.
Executive Assistant	Do not assign Executive and Executive Assistant to the same user.
Hoteling Guest	Do not assign Hoteling Host and Hoteling Guest to the same user.
Hoteling Host	Do not assign Hoteling Host and Hoteling Guest to the same user.
Voice Messaging User	Pre-assigned to Group Users 1 and 2. Otherwise, not pre-assigned. The service requires Advanced Settings which Cisco provides only for the 2 users.
Integrated IM&P	12 IM&P licenses are authorized by default (6 per group) and can be assigned to users as needed. 8 of the licenses are consumed by the preconfigured UC-One Desktop and Connect users. See section *6.10 IM&P* for configuration instructions.

5 Test Process

This section provides a step-by-step process for testing your device or application against Cisco BroadWorks and submitting your test results for validation by Cisco.

After you have completed testing and validation against the latest Cisco BroadWorks release, Cisco recommends retesting against subsequent Cisco BroadWorks releases and for new major releases of the device firmware or application software.

5.1 Get Started

This section identifies the steps to take before you start testing.

5.1.1 Log in to the Developer's sandbox

The URL for the developer's sandbox is https://developer.cisco.com/docs/broadworks. The developer's sandbox provides resources to facilitate interoperability testing including test plans, interface specification, and a forum for questions. The developer's sandbox is not the test platform.

The site requires a login which you can self-create by selecting *Sign Up* on the site's landing page. You will need to provide a valid work email address. User logins for the developer's sandbox are intended for individuals rather than organizations, so each person within your organization who will be involved with interop testing will need to create their own login.

After logging in, browse around the website to familiarize yourself with the available resources.

5.1.2 Request Test Platform Accounts

In order to perform interoperability testing, you must obtain accounts on the Cisco BroadWorks test platform. For more information, see section *4.1 Request Test Accounts*.

Unlike developer's sandbox accounts which are intended for individuals within an organization, test platform accounts are created for an organization and are intended to be shared by the individuals within the organization. Therefore, the request for test accounts must be submitted by only one member of the organization. Cisco makes exceptions to this for organizations with a range of products to test and/or with multiple teams involved in the interop process. In these cases, separate requests can be allowed.

After the test accounts are configured by Cisco, the account information will be emailed from Cisco to the requestor's email address. Cisco will also request for you to identify the SIP User-Agent header content your device(s) if we do not already have that information.

At this point, unless there are any follow-up questions in the email from Cisco, you are ready to log in to the test platform.

5.1.3 Log in to the Test Platform

The test platform account information includes a Group administrator login username and password. Use these credentials to log in to the test platform web portal. See section *3.1 IP Addresses and FQDNs* for the web portal URL.

When you first log in as Group admin, a password change is required. After changing the password, be sure to share it with those in your organization that need it and track it appropriately. If the Group administrator password is misplaced or forgotten, you must contact Cisco at devnet-broadsoft-support@external.cisco.com to request a reset. Multiple invalid password attempts will result in the login being locked out.

After initially changing the password, you will be redirected to the Group admin landing page as shown in ***Error! Reference source not found.***. There are a lot of links and information on this page. However, for the most part, you need only be concerned with the Users links as this is where you will make any configuration changes required by the test plan.

Avoid making configuration changes unless required by the test plan as this can result in unexpected behavior or affect others in your organization who are also using the accounts.

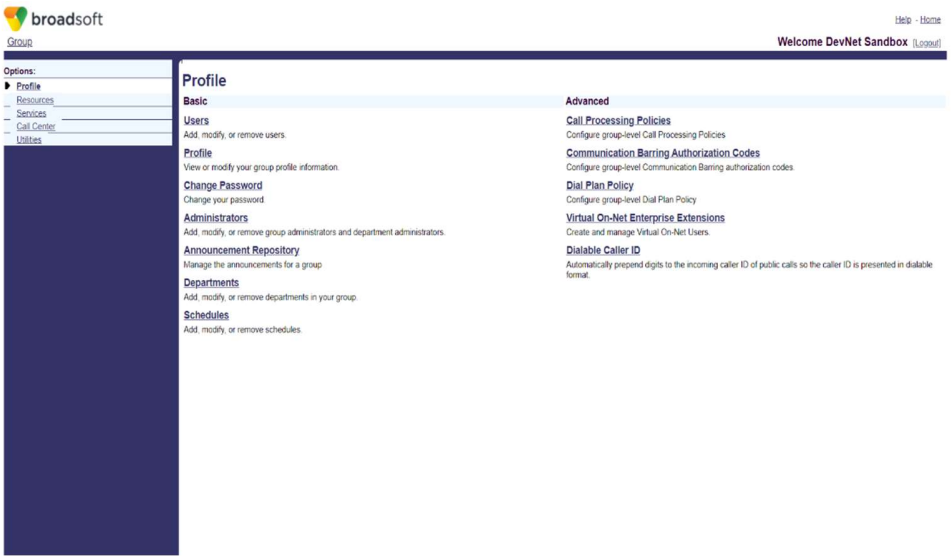

Figure 3 Group Administrator Landing Page

5.1.4 Review the Test Plan

Before starting test, download and review the applicable test plan – especially the opening sections prior to the test case sections – to understand the specific requirements for the test plan. To identify the test plans that are applicable to your device or application, see section *2 Test Plans*.

Test plans are available on developer's sandbox. Always download the test plan for the latest Cisco BroadWorks release except in cases where there is a specific need to test against the prior release.

Also download and review the accompanying test report template to understand the reporting requirements. The test report template must be used to document the test results.

5.2 Testing

This section covers the interoperability testing prerequisites and steps. Device Under Test (DUT) refers to the device or application being tested.

Types of testing:

- Interoperability Testing

  Formal interoperability testing is the focus of this document. It is the process of executing a test plan, tracking the results, and validating the results.

  For access devices, SIP interoperability testing must be completed before or in parallel with Device Management and/or Xsi/XMPP testing, if either is supported.

- Development Testing

  Development testing is necessary when adding new features unique to integration with Cisco BroadWorks or implementing standards not previously supported by the DUT. You are encouraged to use your test accounts for development testing before starting the formal interoperability testing.

- Regression Testing

  The test platform is not intended to support regular automated regression testing. Contact Cisco at devnet-broadsoft-support@external.cisco.com to request and justify a temporary exception. Automated testing that generates excessive traffic will be blocked and can result in the termination of your access to the interoperability test platform.

- Performance Testing

  Performance or capacity testing is outside the scope of interoperability testing and is not allowed. Attempts will be blocked and can result in the termination of your access to the interoperability test platform.

5.2.1 Prerequisites

5.2.1.1 DUT Firmware/Software

The DUT's firmware or software version must be either a released version or a release-candidate version. The version tested will be identified in the configuration document generated by Cisco after the testing and validation complete.

The same version should be used throughout the test iteration to ensure the integrity of the testing. If it is necessary to update the firmware/software to correct significant issues identified during testing, the testing should be restarted.

5.2.1.2 Tester Requirements

SIP testing should be performed by an engineer with expertise in the following:

- SIP protocol and relevant RFCs
- Configuring and managing the DUT

The tester should also have knowledge or understanding of the architecture as it pertains to the DUT's interface with Cisco BroadWorks.

Cisco BroadWorks expertise is not required. Test cases are written with clear instructions for any configuration that must be performed by the tester. However, familiarization with and experience testing against Cisco BroadWorks is helpful to complete the testing more quickly.

Non-SIP testing requires expertise in the following:

- HTTP – for Device Management and Xsi testing
- XMPP – for IM&P testing

5.2.2 Connect Your Device or Application to the Test Platform

This document provides the details necessary to connect your DUT – whether it be a SIP endpoint, device, or application – to the Cisco BroadWorks test platform.

The DUT, as well as other endpoints used for testing, should be on private address space behind a router that performs NAT to a public IP. This models a typical deployment and ensures the DUT is protected from internet attacks. The Cisco BroadWorks Sandbox platform SSE performs the necessary header manipulations to facilitate the NAT traversal. The DUT and other endpoints must also be enabled for symmetric SIP signaling and symmetric RTP.

The DUT's SIP signaling and media must flow directly to the SSE address without the involvement of any SIP intermediaries. SIP-aware firewalls and SIP edge devices often modify the SIP headers and/or the SDP, which can introduce signaling issues or cover them up. To request an exception to this policy, contact Cisco before testing starts.

For the SSE address to configure as the outbound proxy for the DUT and other endpoints used for testing, see section *3.1 IP Addresses and FQDNs*. After you have connected your devices to the test platform, you are ready to begin testing.

5.2.2.1 Registering Devices

For registering SIP phones and access devices, see section *4.2 Test Account Details* to identify the SIP user and domain to be populated in the *Request-URI* for REGISTER and INVITE requests send to Cisco BroadWorks. These credentials are to be used for the DUT and the other endpoints required for the testing. You can also find this information by logging in to the test platform as described in *6.6 SIP Registration and Authentication*.

If you are testing a SIP phone or other access device, it is recommend to use the Group 1 User 1 as the DUT user referred to in the test plan. Other users in Group 1 should be used for User A, User B, and so on as referred to in the test plan.

If you are testing an application such as a Call Recording or Conference server, it is recommended to use Group 1 User 1 as User A and other users in Group 1 as User B, User C, and so on.

5.2.3 Execute Test Cases

It is recommended to execute test cases in the test plan starting from the beginning and working through to the end. Some test sections take advantage of expertise the tester will have gained in previous test sections. However, for the experienced tester, it is acceptable to execute test sections in any order and/or to execute in parallel with another testing.

Cisco requires that each test case in the test plan that is supported by the DUT be executed, except those test cases or test sections identified as optional in the test plan. Cisco does not accept incomplete test results. Refer to the *Test Section Overview* section in the test plan for requirements.

All supported test cases must pass, with the following exceptions:

- The failure is due to a Cisco BroadWorks issue.

- There is a configurable workaround.
- The failure is determined by Cisco to be minor and/or not service affecting.

5.2.3.1 Capture Signaling

For most test plans, it is necessary to capture the relevant signaling for each test case, whether pass or fail, to be submitted to Cisco with the test results for review. Review the instructions in this section pertaining to the test plan or test plan type that you will be using.

Also review *5.2.3.1.6 Wireshark Guidelines for SIP UDP* to learn how to avoid problems with SIP UDP capture content.

5.2.3.1.1 SIP Test Plans

If you are executing a Cisco BroadWorks SIP interoperability test plan:

- Use Wireshark or a similar tool to capture the SIP signaling for each test case.
- **Filter the captures you submit to Cisco to contain only the SIP signaling between the DUT and Cisco BroadWorks**.
  - Do not include the RTP.
  - Filter out everything else including the SIP signaling with the remote endpoint in the test scenario.
- If there is more than one DUT model (for example, a series of SIP phones) that share the same SIP stack, capture and submit traces for one model only. It is not necessary to test each model separately. However, you must ensure that all models work the same with respect to the SIP interface with Cisco BroadWorks.
- Label each capture file name using the test number:
  - Some test plans number tests as A.1.1, A.1.2, B.1.1, and so on. Captures for these test plans must be labeled in the format *testX.X.X.pcap* or *testX.X.X.pcapng*.

    Examples:

    testA.1.1.pcap

    testA.1.2.pcap

    testB.2.14.pcap
  - Other test plans use simple numbering – 1, 2, 3, … 100, 101 and so on. Captures for these test plans must be labeled using 3 digits with leading 0's where necessary to ensure that the captures will be listed in numerical order.

    Examples:

    test001.pcap ← Include leading 0's. Do not label as "test1.pcap".

    test002.pcap

    test003.pcap

    …

    test050.pcap

    …

    test123.pcap

5.2.3.1.2 Call Recording Test Plan (SIPREC)

The requirements for *SIP Test Plans* apply for the *Call Recording Test Plan* as well. However, there is an extra requirement for Call Recording: a separate capture of the endpoint signaling is required for each test case. The endpoint traces are required to enable Cisco reviewers to establish that the test case was properly executed.

There will be two captures for each test case which must be labeled to differentiate between the call recording and the endpoint capture. Use the following format:

test001-record.pcap

test001-endpoint.pcap

5.2.3.1.3 Device Management Test Plan

Provide device logs or captures to demonstrate Device Management integration.

5.2.3.1.4 Xsi and XMPP Test Plan

Provide device logs or captures to show the commands are supported and executed correctly.

5.2.3.1.5 SIP Phone Functional Test Plan

This test plan applies to SIP phones only.

The SIP Phone Functional Test Plan is optional and it is focused on functionality rather than SIP signaling. SIP captures are not required and will not be reviewed by Cisco if submitted.

5.2.3.1.6 Wireshark Guidelines for SIP UDP

This section provides guidelines for how to avoid incomplete SIP UDP captures due to fragmentation when using Wireshark. Traces submitted to Cisco for validation must contain complete SIP captures.

When a SIP message exceeds the UDP Maximum Transmission Unit (MTU) of 1500 bytes, the message is split into two or more fragments equal to or less than the MTU. Fragmentation can occur in various scenarios with Cisco BroadWorks including Busy Lamp Field, Feature Key Sync, video, and other scenarios. The fragmented signaling must be captured and filtered properly to ensure the message can be reassembled and decoded.

To identify the Wireshark frames in a capture which contain fragmented messages, set the display filter as:

ip.flags.mf == 1

or

ip.frag_offset > 0

After the filter is applied, all fragmented frames in the captured trace will be displayed. The frames containing fragments are displayed as *Fragmented IP protocol* in the *Info* column. Each fragmented frame should have a corresponding *Reassembled in [frame number]* reference. *Figure 3* shows an example of a large SIP NOTIFY message broken into 5 frames that have been successfully decoded after reassembly at frame #11. Note that the info for each frame indicates "Reassembled in #11".

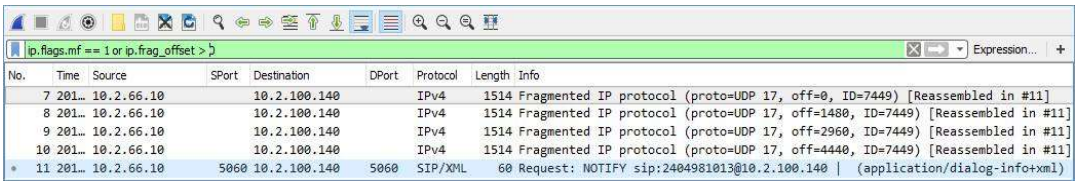

Figure 3 Wireshark Fragmented and Reassembled SIP Message

If your filtered SIP trace contains fragmented frames that do not indicate *Reassembled in [frame number]*, this typically indicates that fragments are missing and Wireshark is unable to reassemble the full message and decode as SIP. Check your pre-filtered trace to see if the fragments are properly reassembled. If so, adjust your filters to ensure that these frames are not being filtered out.

Traces submitted to Cisco for validation must contain the complete messages where all fragmented frames are present and properly reassembled.

5.2.3.2 Update the Test Report

After completing each test case, update the Test Report template marking the test case *Pass*, *Fail*, *Not Supported*, or *Not Tested*.

- Pass: The test case was executed successfully.
- Fail: There is an issue with the test case causing it to fail.
- Not Supported: The DUT has not implemented the tested functionality.
- Not Tested: The test case is optional or an exception has been granted by Cisco.

Test case failures must not be attributed to Cisco BroadWorks unless Cisco has analyzed the issue and provided a Cisco issue tracking number.

Use the Comments/Explanation column in the test report for the following or any other information necessary for the test case:

- To describe a test case issue or anomaly. If it is a Cisco BroadWorks issue, provide the Cisco issue tracking number. If it is a DUT issue, provide the DUT issue tracking number.
- To provide an explanation for why a test case was not tested.
- To identify specific models if the test case is supported by only specific models in the model series (example: video).

5.2.3.3 Asking Questions

For questions about a test case or configuration that arise during testing, go through the following steps to find an answer to the question.

1) Thoroughly review the instructions for the test case and test section. Often the test plan has the information you are looking for.
2) Search this document for an answer to your question.

3) Log in to the developer's sandbox and select the Resources - Forum tab. Search the forum to see if the same or similar question has been asked before.

4) Log in to the developer's sandbox and post a new question on the Resources - Forum tab.

Cisco interop engineers monitor the forum and provide responses on a best effort basis. Check back periodically for an answer to your question.

Alternatively, it is recommended to subscribe to the *Q&A Forum* RSS feeds to be notified of answers posted for your questions. To subscribe to the feed, right-click on *RSS Feed Answers* on the *Q&A Forum* page. Select *Copy Link Address*. Then in Microsoft Outlook or another feed reader, add a new feed with the copied link.

5.2.3.4 Troubleshooting Issues

For issues that arise during testing such as a test case failure or a server problem, go through the following troubleshooting steps. **Root cause must be determined for all issues before submitting your test results.**

1) Thoroughly review the instructions for the test case and the test section to ensure the test case was executed properly.

2) Log in to the developer's sandbox and select the Resources - Forum tab tab. Search the forum to see if the same or similar issue has been reported before and if the analysis resolves your issue.

3) Log in to the developer's sandbox and post a new question on the Forum tab. Include the following:

   – Identify the test plan name and the test case number.

   – Identify the Cisco BroadWorks group name and/or user numbers as relevant.

   – Provide a clear and complete description of the issue.

   – Attach a Wireshark capture for the issue if applicable.

> **NOTE**: Filter the capture to the relevant SIP or other signaling in order to reduce the size of the capture. Your developer's sandbox account has limited storage for attachments.

Cisco interop engineers monitor the forum and provide responses on a best effort basis. Check back periodically for response to your issue.

Alternatively, it is recommended to subscribe to the *Q&A Forum* RSS feeds to be notified of responses to your issues. To subscribe to the feed, right-click on *RSS Feed Answers* on the *Q&A Forum* page. Select *Copy Link Address*. Then in Microsoft Outlook or another feed reader, add a new feed with the copied link.

5.3 Validate Test Results

This section describes the process for submitting and validating your test results after testing has completed.

Cisco engineers review the submitted test results in order to validate that the testing has been completed properly and to ensure that the device or application is ready for deployment with Cisco BroadWorks. **The validation process typically takes at least four to six weeks**, so if your product release date or a customer commitment is dependent on completion of the validation, be sure to submit your test results well in advance.

5.3.1 Submit Test Results

To prepare your test results and submit them to Cisco, follow these steps.

1) Complete all sections of the test report template.
   - Fully document the open issues in the *Test Issues* section of the test report.

     Verify that root cause has been determined for all open issues before submitting your test results.
   - Make sure each test case is marked as Pass/Fail/Not Supported/Not Tested and annotated if necessary.
   - Do not modify the format of the test report.
2) Build test capture archive.
   - Refer to section *5.2.3.1 Capture Signaling* to determine if captures are required for the test plan type.
   - Make sure the capture files have been filtered and named as instructed in section *5.2.3.1 Capture Signaling*.
   - Use Winzip or other file compression tool to build a zip file or archive of all the capture files.
   - Do not zip the capture files individually.
   - If the capture archive is larger the 5MB, this typically indicates the required filtering has not been done. Check the larger files to ensure they are filtered as required.
3) Email Test Results to Cisco.
   - To: devnet-broadsoft-support@external.cisco.com
   - Cc: Copy only your colleagues as necessary. **DO NOT COPY customers or other third parties**.
   - Email Subject: "Cisco BroadWorks interop test results for <Company> <Product> <Version>".
   - Email Body: Provide additional comments or notes as needed.
   - Attachments: Test report, test case capture zip file.

> **NOTE**: It is also acceptable to post your test results on your ftp or file sharing site for Cisco to download from.

5.3.2 Preliminary Validation Review

After you submit your test results, Cisco will complete a Preliminary Review to ensure that the test results are ready and all requirements have been met. Cisco will typically complete this review and respond to your email within five business days. If you do no hear back within a week or so, send a follow-up email to verify that your email was received.

The Preliminary Review ensures the following:

- The test report has been completed properly.
- All required test cases have been executed.

- Traces have been captured and filtered properly.
- Trace files have been labeled as required.
- Other files (for example, Device Management configuration files) have been submitted as required.

If Cisco determines that the test results are incomplete or incorrect, Cisco will send an email response with the required corrections. The test results must then be resubmitted.

When Cisco determines the test results are complete and correct, Cisco will queue the test results for Formal Review. Cisco queues test results on a first-in first-out basis and completes the Formal Review on a best effort basis. The queue is normally three weeks or longer, meaning it is typically at least three weeks before the formal review starts.

5.3.3 Formal Validation Review

To fully validate the test results, Cisco does a Formal Review which includes the following:

- Complete review of the test report.
- Complete review of the issues and anomalies.
- Inspection of each test capture.

The time required for the Formal Review depends on a number of factors including the reviewer's workload, the number of test cases to review, and the quality of the test results. Bad captures and otherwise poor quality test results significantly increase the time required for the review, so it is imperative to adhere to the test capture requirements.

After the review completes, the Cisco engineer who has performed the review will send an email with the review results. The email will list any issues that the reviewer has identified and what corrective action must be taken. Corrective actions may require:

- Re-running test cases
- Providing explanations
- Establishing root cause for issues
- Updating documentation

Any corrective actions must be completed within a reasonable time frame – no more than three to four weeks. Cisco reserves the right to reject the test results and require a complete retest if needed.

If there were no corrective actions required or when necessary corrective actions have been completed, the Cisco reviewer will confirm the successful completion of the formal review and request input from you for the configuration guide.

5.3.4 Documentation

This section identifies the outputs from the validation process.

5.3.4.1 Partner Configuration Guide

As an output of SIP interoperability testing, Cisco creates a document called a Partner Configuration Guide (PCG) to track the test results and identify the parameter settings and configuration essential for interoperability between the DUT and Cisco BroadWorks. The Cisco reviewer will generate the initial draft for the guide and then request for you to complete specific sections in the guide pursuant to the required DUT configuration.

- The PCG should be completed by someone very familiar with the DUT configuration.

- The PCG must be completed within a reasonable time frame – no more than one to two weeks – to ensure timely completion of the validation process.
- The updated PCG must be returned to Cisco in Microsoft Word format. Do not modify the document formatting. Do not PDF.

The Cisco engineer will review your updates to the PCG and work with you on any further updates or corrections until the document is completed satisfactorily.

5.3.4.2 CPE Kit

As an output of Device Management integration testing, Cisco creates a CPE Kit using the configuration templates and other files generated as a result of the testing. The CPE Kit enables service providers to easily provision their Cisco BroadWorks platforms to enable device management of the DUT.

5.3.5 Wrap-Up

After the documentation is completed, the Cisco reviewer will send an email indicating that the validation has completed successfully.

The *Partner Configuration Guide* and the CPE Kit are posted to the Cisco/BroadSoft Xchange web site usually within two weeks after the validation completes. The Xchange site is used by service providers to download documentation and software.

Cisco also provides a SIP validation letter in PDF format which formally states that the DUT has been validated with Cisco BroadWorks. The letter also identifies the validated DUT version and models. The validation letter is usually sent within a week after the validation completes. The letter can be shared with service providers.

5.4 Next Steps

This section covers guidelines and requirements for retesting and other scenarios that can occur after the validation process has been completed.

5.4.1 Retest

Retesting should occur periodically to verify that product changes do not adversely impact interoperability. Service providers generally expect that the firmware/software versions they are using have been tested against Cisco BroadWorks. To retest, repeat the test process described in this document.

Cisco recommends the following for retesting:

- **Retest for new Cisco BroadWorks releases**

  Cisco introduces a new Cisco BroadWorks release every two years. It is recommended to retest against each new Cisco BroadWorks release.

- **Retest for DUT Major Firmware/Software Update**

  Retest is recommended for major releases of DUT firmware/software, especially those affecting the SIP and/or media stacks.

- **Do Not Retest for DUT Maintenance Firmware/Software Update**

  It is not necessary or recommended to retest maintenance firmware/software updates for minor changes and bug fixes.

- **Limit Retests**

  Retests should be limited to 1 time per calendar year. Cisco will validate a maximum of two times per calendar year. It is recommended to coordinate testing of new DUT firmware/software with new Cisco BroadWorks releases to help limit the frequency of testing.

5.4.2 Add New Models

Your company may release new models for a model series months after the validation against Cisco BroadWorks has been completed. This is most common with SIP phones and other access devices.

Cisco will facilitate updates to the PCG and the CPE Kit (if required) and provide an updated validation letter under the following conditions.

- The new model(s) must be included in a DUT firmware/software version that does not require retest, typically a maintenance version, or a version that the only change is to incorporate the new model.
- If Device Management is supported, Device Management testing must be completed to develop the configuration template for the new model and verify the integration.
- Limited to 1 update per calendar year. If you have models being added at different times throughout the year, please coordinate to limit the update requests.
- Fulfilled on a best effort basis.

To add the new model(s):

- Send an email to devnet-broadsoft-support@external.cisco.com to make the request. Identify the model(s) and the number of registering lines.
- If Device Management is supported:
  - Include the following information:
    - New model name(s)
    - Number of SIP lines for each model
    - Configuration template file name (if different from validated models)
    - Other files required (if different from validated models)
  - After Cisco completes the necessary configuration to enable Device Management testing for the new model(s), execute the Device Management test plan.
  - Submit Device Management test results to Cisco.
  - Cisco will validate the test results through the normal validation process.
- Cisco will update the PCG and CPE kit and provide an updated validation letter with the new model(s) added.

5.4.3 Add New Features

Your company may add new features to the DUT after the SIP validation against Cisco BroadWorks has been completed, such as Device Management or Xsi support.

Cisco facilitates adding new features under the following conditions.

- SIP
  - Generally, changes to the SIP stack necessitate full retest.

- Partial testing is accepted when adding support for IPv6 or TLS/SRTP.
- Contact Cisco at devnet-broadsoft-support@external.cisco.com to request other partial SIP testing exceptions.

- Device Management
  - Device Management can be added in a DUT maintenance release that does not impact the SIP interface.
  - If Device Management is already supported and additional Device Management features are being added, the Device Management test plan must still be fully executed.
- Xsi and XMPP
  - Xsi and/or XMPP supported can be added in a DUT maintenance release that does not impact the SIP interface.
  - If Xsi and/or XMPP is already supported and additional Xsi/XMPP features are being added, Cisco will accept test results for only the new features.
  - These updates can also require Device Management updates if configuration templates are affected.

5.4.4 Rename Details

If your company or DUT model name changes and you need to update the PCG accordingly, you may request a change by contacting Cisco at devnet-broadsoft-support@external.cisco.com. However, minor or unnecessary change requests will generally not be accepted, especially when CPE kit changes are also required.

5.4.5 OEM / Rebranding

Cisco will facilitate rebranding a PCG and CPE kit in cases such as an OEM where the validated device is rebranded for distribution by another company or under another company's name. Contact Cisco at devnet-broadsoft-support@external.cisco.com to request the rebranding.

The rebranded models must use the same firmware/software version and SIP stack as the previously validated models. However, the firmware/software version may be labeled differently. If the version and/or SIP stack are different than the rebranded models must be tested separately.

Rebranding requests are limited to two times per calendar year and are fulfilled on a best effort basis.

6 Cisco BroadWorks Configuration

This section provides instructions for configuration tasks commonly required or used during interoperability testing with Cisco BroadWorks.

6.1 Add Group Administrator

This section provides instructions for adding a group administrator login. A group admin login can be used to manage the users and resources in a particular group.

Follow these steps to add a group administrator:

1) Log in to the Cisco BroadWorks web portal as group admin.
2) Select *Administrators* on the group's *Profile* page.
3) Click **Add** and provide the required *Administrator ID* and *Password*.
4) Click **OK** to save the configuration.

6.2 Assign / Unassign Service

This section provides instructions for assigning / unassigning user and group services.

6.2.1 Assign User Service

Many services are pre-assigned to the users on the test platform. Some services should be assigned only if needed. For information on the user services available on the test platform, see 4.2 Test Account Details.

Follow these steps to assign a service to a user:

1) Log in to the Cisco BroadWorks web portal as group admin.
2) Browse to Users and select Search.
3) Click on the applicable user.
4) Select Assign Services on the user's Profile page.
5) Select the service(s) to assign from the Available Services column and then click Add.
6) Click OK to save the configuration.

6.2.2 Assign Group Service

Many services are pre-assigned to groups on the test platform. Other services can be assigned if needed. For information on the user services available on the test platform, see section *4.2 Test Account Details*.

Follow these steps to assign a service to a group:

1) Log in to the Cisco BroadWorks web portal as group admin.
2) Select Assign Group Services on the group's Profile page.
3) Select the service(s) to assign from the Available Services column and then click Add.
4) Click OK to save the configuration.

6.2.3 Unassign User Service

Follow these steps to unassign a service from a user:

1) Log in to the Cisco BroadWorks web portal as group admin.
2) Browse to Users and select Search.
3) Click on the applicable user.
4) Select Assign Services on the user's Profile page.
5) Select the service(s) to unassign from the Assigned Services column and then click Remove.
6) Click OK to save the configuration.

6.2.4 Unassign Group Service

Follow these steps to unassign a service from a group:

1) Log in to the Cisco BroadWorks web portal as group admin.
2) Select Assign Group Services on the group's Profile page.
3) Select the service(s) to unassign from the Assigned Services column and then click Remove.
4) Click OK to save the configuration.

6.3 Configure Services

This section provides general instructions for configuring group and user services.

6.3.1 Configure User Service

The Cisco BroadWorks test plans provide explicit instructions for user service configuration where required for specific test cases. General guidelines for configuring user services are included here, but in most cases, just follow the instructions in the test plan.

To configure a user service, log in to Cisco BroadWorks with group admin credentials or with the user's login credentials. However, for some services, the user has limited access to the configuration.

1) Log in to the Cisco BroadWorks web portal as group admin or as the user.
2) If you logged in as an admin, browse to Users and select Search. Then click on the applicable user.
3) Find the service you want to configure using one of the following links in the left column:
   - The *Incoming Calls* link is used to configure services that trigger when the user receives a call.
   - The *Outgoing Calls* link is used to configure services that trigger when the user makes a call.
   - The *Call Control* link is used to configure services that pertain to call control such as Call Waiting, Call Transfer, Call Recording, Three-Way Call, BroadWorks Anywhere, Remote Office, Shared Call Appearance, Hoteling, Flexible Seating, Call Centers, and so on.

- The *Client Applications* link is used to configure non-call applications such as Busy Lamp Field and BroadWorks Agent.
- The *Messaging* link is used to configure messaging services such as Voice Management, Fax Messaging, and Integrated IM&P.
- The *Collaborate* link is used to configure the collaborate room settings.
- The *Utilities* link is used to configure SIP Authentication and to view basic call logs and registrations.

4) Configure the service. Use the *Help* link for assistance.

5) Click **OK** to save the configuration.

6.3.2 Configure Group Service

The Cisco BroadWorks test plans provide explicit instructions for group service configuration where required for specific test cases. General guidelines for configuring group services are included here, but in most cases, just follow the instructions in the test plan.

To configure a group service, log in to Cisco BroadWorks with either group admin credentials.

1) Log in to the Cisco BroadWorks web portal as group admin.
2) Find the service you want to configure using one of the following links in the left column:
   - The *Services* link is used to configure group service including Auto Attendant.
   - The *Call Centers* link is used to add call centers to the group.
3) Configure the service. Use the *Help* link for assistance.
4) Click **OK** to save the configuration.

6.4 Add / Delete User

In some cases it may be necessary or useful to add more users to pre-provisioned users in your test accounts. This section provides instructions for adding a user to the group and for deleting a user from the group. Deleting users should rarely be necessary. The pre-provisioned users should never be deleted.

6.4.1 Add User

Follow these steps to add a user to a group:

1) Log in to the Cisco BroadWorks web portal as group admin.
2) Browse to *Users* and select *Add*.
3) Configure all required fields (indicated by *) on the *User Add* page. Remaining fields may be left as default or blank.
   - User ID

     The user ID must be unique on the system.
   - Name fields

     The name fields do not need to be unique. However, it is recommended to make them unique within your group.

     Use the same setting for *Last Name*, *Calling Line ID Last Name*, and *Hiragana Last Name*.

Use the same setting for *First Name*, *Calling Line ID First Name*, and *Hiragana First Name*.

4) Click **OK** to add the user.

5) Browse to *Users* and select *Search*.

6) Click on the new user.

7) Select *Addresses* to go to the user's *Addresses* configuration page.

8) On the *Addresses* page, configure the following:

- Select a *Phone Number* from the drop-down. The *Extension* is populated automatically.

  If there are no numbers available in the drop-down, this means that you have used all of the numbers assigned to the group. You may either free up a number from another user in the group or request additional numbers for your group by contacting Cisco at devnet-broadsoft-support@external.cisco.com.

- Select *Identity/Device Profile* toggle, if not already selected.

- From the *Identity/Device Profile* drop-down menu, select the new device profile.

  The device profile you select should be one that you created by following the steps in *6.5.1 Create Device Profile*.

  Alternatively, scroll to the bottom of the drop-down menu, select *New Identity/Device Profile* and create the device profile instantly.

- Configure the *Line/Port* user portion to a unique value such as the user's phone number.

- The *Line/Port* domain portion must be set to the test platform's default domain.

  Example: broadsoftlab.com

4) Click **OK** to save the changes.

6.4.2 Delete a User

1) Log in to the Cisco BroadWorks web portal as a group admin.

2) Browse to *Users* and select *Search*.

3) Click on the applicable user.

4) Select *Profile* under the *Basic* column.

5) Click *Delete* on the user's *Profile* page and then click **OK** on the confirmation popup.

6.5 Device Profiles

A device profile represents the endpoint that is associated with the Cisco BroadWorks user. A device profile is derived from a device profile type which serves as a template for a device profile and has settings specific to the endpoint type (for example, Cisco MPP, Polycom VVX, Yealink T4x). Device profile types are developed as a result of SIP interoperability and Device Management testing.

In order for a Cisco BroadWorks user to make and receive calls, the user must have a device profile assigned. Test accounts are pre-provisioned with device profiles. However, you may find a need to change a user's device profile so this section provides instructions for creating and changing device profiles.

6.5.1 Create Device Profile

Follow these steps to create a new device profile:

1) Log in to the Cisco BroadWorks web portal as group admin.
2) Select *Resources* in the left column.
3) Select *Identity/Device Profiles* on the *Resources* page.
4) Click **Add** on the *Identity/Device Profiles* page.
5) On the *Identity/Device Profile Add* page, complete the following. Other fields not identified here should be left blank.
   - **Identity/Device Profile Name**

     Provide a unique name for the device profile.

     Example: Cisco_MPP
   - **Identity/Device Profile Type**

     Select a device type from the drop-down menu.

     Examples: Cisco-CP-78xx-88xx-68xx-3PCC, PolycomVVX_350, Yealink-T46G

     If your endpoint is not in the drop-down list, then select a Generic device type.

     SIP Phone: Generic SIP Phone – IOP

     SIP Access Device: Generic SIP Access Device – IOP
   - **IP Address / Port**

     Do not fill this in unless the endpoint does not register.
   - **MAC Address**

     If MAC authentication is used for Device Management, provide the MAC address of the endpoint.
   - **Use Custom Credentials**

     If Device Management is supported by the endpoint, select *Use Custom Credentials* and provide a user name and password.
6) Click **OK** to save the changes.

6.5.2 Modify Device Profile

Follow these steps to modify an existing device profile:

1) Log in to the Cisco BroadWorks web portal as a group admin.
2) Select *Resources* in the left column.
3) Select *Identity/Device Profiles* on the *Resources* page.
4) Click **Search** on the *Identity/Device Profiles* page and then select the Device Profile to modify from the list.
5) On the *Identity/Device Profile Modify* page, make the necessary changes.
6) Click **OK** to save the changes.

6.5.3 Change User's Device Profile

1) Log in to the Cisco BroadWorks web portal as a group admin.

2) Browse to *Users* and select *Search*.
3) Click on the applicable user.
4) Select *Addresses* to go to the user's *Addresses* configuration page.
5) On the *Addresses* page, configure the following:
   - Select *Identity/Device Profile* toggle (if not already selected).
   - From the *Identity/Device Profile* drop-down menu, select the new device profile.

     The device profile you select should be one that you created by following the steps in section *6.5.1 Create Device Profile*.

     Alternatively, scroll to the bottom of the drop-down menu, select *New Identity/Device Profile* and create the device profile instantly.
   - Configure the *Line/Port* user portion to a unique value such as the user's phone number.
   - The *Line/Port* domain portion must be set to the test platform's default domain.

     Example: broadsoftlab.com
6) Click **OK** to save the changes.

6.6 SIP Registration and Authentication

Settings on Cisco BroadWorks for SIP registration and authentication must match the settings on the endpoint. This section identifies how to configure these parameters on Cisco BroadWorks.

6.6.1 SIP Register

The SIP register address-of-record is configured on the Cisco BroadWorks user's *Addresses* page. Follow these steps to configure the register address-of-record:

1) Log in to the Cisco BroadWorks web portal as a group admin.
2) Browse to *Users* and select *Search*.
3) Click on the applicable user.
4) Select *Addresses* to go to the user's *Addresses* configuration page.
5) On the *Addresses* page, configure the following:
   - Configure the *Line/Port* user portion to a unique value such as the user's phone number.
   - The *Line/Port* domain portion must be set to the test platform's default domain.

     Example: broadsoftlab.com
6) Click **OK** to save the changes.
7) Make sure the endpoint's register address-of-record matches the Cisco BroadWorks settings.

6.6.2 SIP Authentication

The Cisco BroadWorks SIP test plans require that SIP authentication is enabled throughout the testing. Follow these steps to configure SIP authentication for a Cisco BroadWorks user:

1) Log in to the Cisco BroadWorks web portal as a group admin.
2) Browse to *Users* and select *Search*.
3) Click on the applicable user.
4) Select *Utilities* to access the *Utilities* page.
5) The *Authentication* service should be listed at the top of the *Utilities* page. If it is not there, follow the steps in section ***Error! Reference source not found. Error! Reference source not found.*** to assign the *Authentication* service to the user.
6) Select *Authentication* to access the *Authentication* data page.
7) On the *Authentication* page, configure the following:

   - Authentication user name (does not have to be unique)
   - Authentication password

8) Click **OK** to save the changes.
9) Make sure the endpoint's SIP authentication username and password match the Cisco BroadWorks settings.

6.7 Trunk Groups

6.7.1 Add Trunk Group

6.7.1.1 Create Device Profile

The concept of trunk groups to be associated with device profiles is similar to associating device profiles to users. Cisco requires that the DUT sends a single (pilot) registration for the trunk as recommend by the SIP Connect specification. Contact Cisco to request an exception as this may require alternative configuration on the Cisco BroadWorks platform.

Create a device profile based on *Generic SIP Trunk – IOT Pilot* device profile type in the test group by following the same instructions as detailed in section *6.5.1 Create Device Profile*.

6.7.1.2 Create Trunk Group with Pilot User

Follow these steps to create a new Trunk Group:

7) Log in to the Cisco BroadWorks web portal as an group admin.
8) Select *Services* from the left column.
9) On the *Services* page, select *Trunk Group*.

Click the **Add** button.

On the *Trunk Group Add* page, configure the following. Remaining fields may be left as default or blank.

- Configure the Trunk Group Name.
- Set the Maximum Active Call Allowed to "10".
- Select the Identity/Device toggle under Device Category.

- In the Identity/Device Profile Name drop-down box, choose the device profile type created in the previous section.

Select the *Add Pilot User* check box.

In the *Pilot User* configuration section, configure the required fields as indicated by the "*" symbol.

- User ID

  The user ID must be unique in the system.

- Name fields

  The name fields do not need to be unique. However, it is recommended to make them unique within your group.

  Use the same setting for *Last Name*, *Calling Line ID Last Name*, and *Hiragana Last Name*.

  Use the same setting for *First Name*, *Calling Line ID First Name*, and *Hiragana First Name*.

10) Click **OK** to save the changes.

6.7.2 Add New User to Trunk Group

The initial steps of adding a user to a trunk group are identical to adding a user to Cisco BroadWorks. Follow these alternate steps to continue trunk group user provisioning from section *6.4.1 Add User*.

1) On the *Addresses* page, configure the following:

- Select a *Phone Number* from the drop-down. The *Extension* is populated automatically.

  If there are no numbers available in the drop-down, this means that you have used all of the numbers assigned to the group. You may either free up a number from another user in the group or request additional numbers for your enterprise by contacting Cisco at broadsoft-validation@cisco.com.

- Select *Trunking* toggle.
- From the *Identity/Device Profile* drop-down menu, select the new Trunk Group.

  The device profile you select should be one that you created by following the steps in section *6.7.1.2 Create Trunk Group with Pilot User*.

- Configure the *Line/Port* user portion to a unique value such as the user's phone number.
- The *Line/Port* domain portion must be set to the test platform's default domain.

  Example: broadsoftlab.com

2) Click **OK** to save the changes.

6.7.3 Migrate Existing User to Trunk Group

1) Follow these steps to move an existing User into a Trunk Group:

2) On the user's *Profile* page, select *Addresses*.

3) On the *Address* page, select the *Trunking* toggle.

4) From the *Trunk Group* drop-down box, choose the destination Trunk Group to move the user. Then, provide the line/port configuration as follows:

- Configure the Line/Port user portion to a unique value such as the user's phone number.
- The Line/Port domain portion must be set to the test platform's default domain.
- Example: broadsoftlab.com
- (Optional) If the user was previously assigned to an Identity/Device Profile, the device profile can be removed if it is no longer in use by other users.

6.7.4 Unassign User from Trunk Group

1) Follow these steps to unassign a User from a Trunk Group:

2) On the user's *Profile* page, select *Addresses*.

3) On the *Address* page, select one of these two following toggles:

- Identity/Device Profile

4) Choose Identity/Device Profile if the user is to be assigned to an existing or newly created access device. After selection, continue by following the Identity/Device Profile create/assignment steps detailed in section *6.4.1 Add User* to complete the migration.

- None
- Choose *None* if the user does not have a device assignment or a new trunk ready for assignment.

6.7.5 Configure SIP Authentication for Trunk Group

Follow these steps to enable and configure SIP authentication for a trunk group:

1) Log in to the Cisco BroadWorks web portal as a group admin.
2) Select *Services* from the left column.
3) On the *Services* page, select *Trunk Group*.
4) On the *Trunk Group* page, select the *Trunk Group* you want to configure.
5) Select *Profile* to modify the trunk group parameters.
6) On the *Profile* page, configure the following:
   - Select *Enable Authentication*.
   - Configure the Authentication User Name.
   - Configure the Authentication password.

Note that the authentication settings apply to all users assigned to the trunk group.

7) Click **OK** to save the changes.
8) Make sure the trunking device's SIP authentication username and password match the Cisco BroadWorks settings.

6.7.6 Change Device Profile for Trunk Group

The device profile of a Trunk Group is associated with all users that are included in the Trunk Group. Therefore, changing the device profile of a Trunk Group is an involved process that requires migrating all users away from the Trunk Group, changing the device profile, and then migrating the users back to the Trunk Group.

As an alternative, it may be more practical to create a new Trunk Group with the desired device profile and then migrate the users from the old Trunk Group to the newly created one.

Whichever approach is chosen to replace the device profile, reference the required instructions in the previous parts of this section.

6.8 Shared Call Appearance

Shared Call Appearance is a desktop phone feature that enables a line to be shared by two or more phones. The Cisco BroadWorks test plan provides complete instructions for configuring Shared Call Appearance as needed for testing. The basic configuration steps are also provided here.

Figure 4 provides a Shared Call Appearance example in which Phone 1 shares a line with Phone 2.

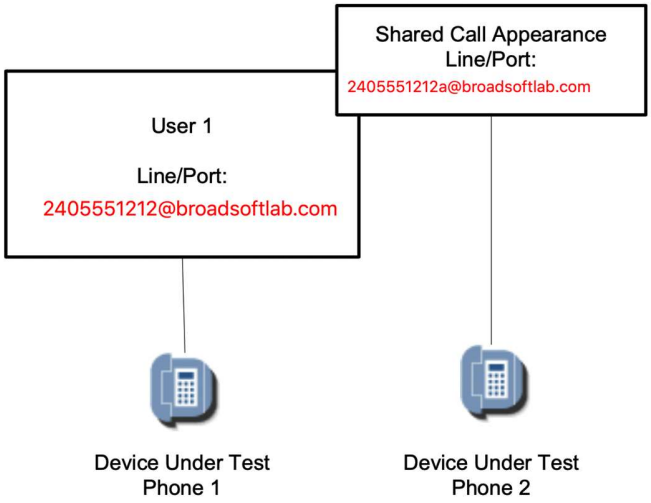

Figure 4 Shared Call Appearance Example

Follow these steps to configure Shared Call Appearance as shown in *Figure 4*.

1) Log in to the Cisco BroadWorks web portal as a group admin.
2) Browse to *Users* and select *Search*.

3) Click on the applicable user.
4) Select *Call Control* from the left column.
5) From the *Call Control* services page, select *Shared Call Appearance*. If *Shared Call Appearance* is not listed, follow the steps in section ***Error! Reference source not found. Error! Reference source not found.*** to assign the service to the user.
6) Select *Add* to add a shared line.
7) From the *Shared Call Appearance Add* page, configure the following:

   – From the *Identity/Device Profile* drop-down menu, select a device profile.

     The device profile you select should be one that you created by following the steps in section *6.5.1 Create Device Profile*.

     Alternatively, scroll to the bottom of the drop-down menu, select *New Identity/Device Profile* and create the device profile instantly.

   – Configure the *Line/Port* user portion to a unique value such as the user's phone number+extension to distinguish the shared line from the primary line.

     Examples: 2405551212a, 2405551212-1

   – The *Line/Port* domain portion must be set to the test platform's default domain.

     Example: broadsoftlab.com

   – Select *Enable this location*.
   – Select *Allow Origination from this location*.
   – Select *Allow Termination to this location*.

8) Click **OK** to save the changes.
9) The shared line phone must register with the Shared Call Appearance line/port and the same SIP authentication settings as the primary line.

6.9 Custom Ringback

The Custom Ringback service is recommended or required for use in certain test cases. For this purpose, there are sample audio and video ringback files that can be downloaded from the developer's sandbox. Download the *customRingbackSamples.zip* file. You can then upload the file(s) to Cisco BroadWorks for the user's Custom Ringback service as directed in the test plan.

6.10 IM&P

Test accounts are limited to 12 IM&P user licenses due to backend resource limitations. 8 of the licenses are consumed by preconfigured UC-One SaaS users. The IM&P service is otherwise not necessary unless you are testing a SIP phone's XMPP integration with Cisco BroadWorks.

NOTE: The Device Management template file for your device must be used to obtain the IM&P login credentials. It is not possible to manually configure your device for IM&P.

The following Device Management tags must be used:

%BW_USER_IMP_ID-x%

```
%BW_USER_IMP_PWD-x%
```

Follow the steps below to assign the IM&P service to a user:

1) Log in to the Cisco BroadWorks web portal as a group admin.
2) Browse to *Users* and select *Search*.
3) Click on the applicable user.
4) Select *Assign Services* on the user's *Profile* page.
5) Select the *Integrated IM&P* service to assign from the *Available Services* column then click **Add**.
6) Click **OK** to save the configuration.
7) Browse to *<user>* → *Messaging* → *Integrated IM&P* and set to "On".
8) Browse to *<user>* → *Profile* → *Addresses* and select *Configure Identity/Device Profile*.
   - Select the *Files* tab.
   - Select *Rebuild the files* so that the IM&P credentials will be updated in the device configuration file.
9) Restart your phone to obtain the updated configuration file with IM&P credentials.

NOTE: The error message "*Failed to modify: [Warning 4400] Could not assign service/service pack: Integrated IMP*" when assigning the IM&P service to a user indicates that the available licenses have been used up.

In this case, either perform your testing with a user that already has the service assigned, or browse to *<group>* → *Resources* → *Existing User Services* to identify which users have the Integrated IM&P service assigned and follow the steps in section 6.2.3 *Unassign User Service* to unassign the service from one or more users.

7 UC-One Client

The UC-One SaaS client are used in some test plans for test cases such as third-party call control, video, and XMPP.

Your Cisco BroadWorks test accounts include Cisco BroadWorks users that are preconfigured for use with the clients as the primary endpoint.

7.1 Client Download and Install

- UC-One SaaS

  The UC-One SaaS client can be downloaded from the below sites,

  For MAC: Storage site

  For Windows: Storage site

  After downloading the client, open the installer file and click through the queries to install. In most cases, accept the default settings.

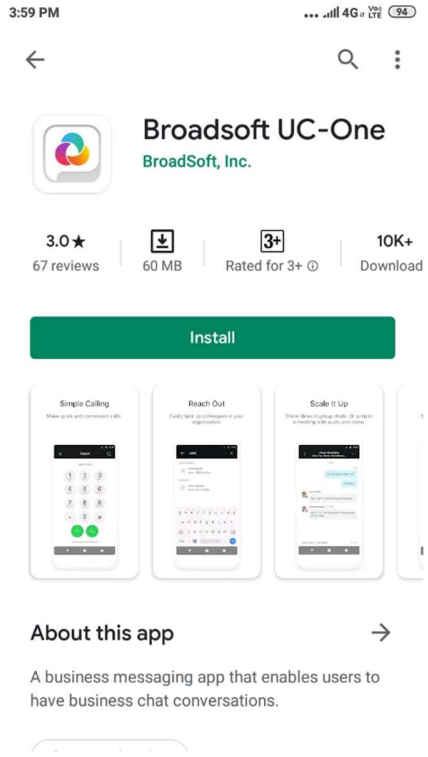

Figure 8 UC-One Connect App

7.2 Client Login

Test groups provided on the Cisco BroadWorks Sandbox systems include preconfigured users that are enabled for the UC-One SaaS client as the primary endpoint. These users contain “UC-One” in the username. Naming convention:

- UC-One SaaS: <Company Name>-GxUyy_SaaS

See section *4.2 Test Account Details* or log in to the web portal as a group administrator to view the users in the group.

After the client is installed, start the client and enter the Access Code corresponding to the Cisco BroadWorks Sandbox system on which you are testing.

Example: Access Code: ADGU6B

Then supply the web portal login username and password for the Cisco BroadWorks user. See ***Error! Reference source not found.***, ***Error! Reference source not found.***, and ***Error! Reference source not found.*** for examples of the UC-One SaaS client at login and the dial tab after login.

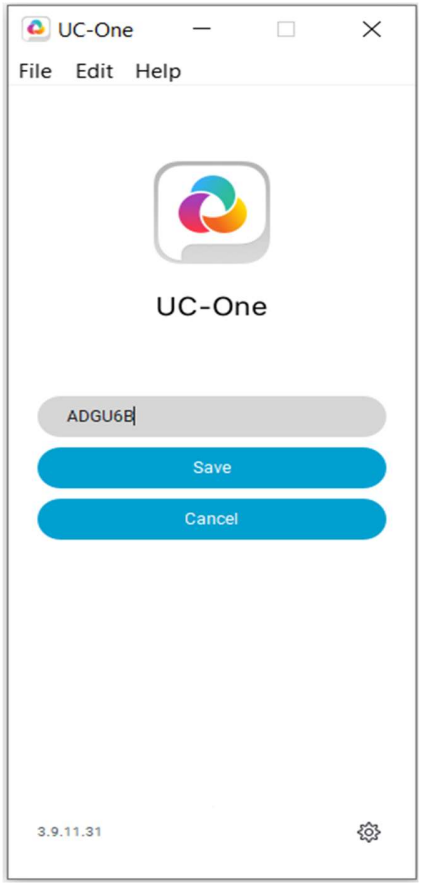

Figure 9 UC-One SaaS Client Login Step 1

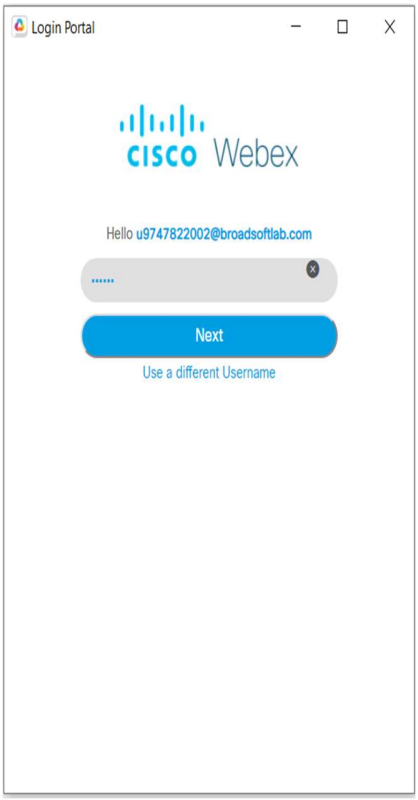

Figure 10 UC-One SaaSClient Login Step 2

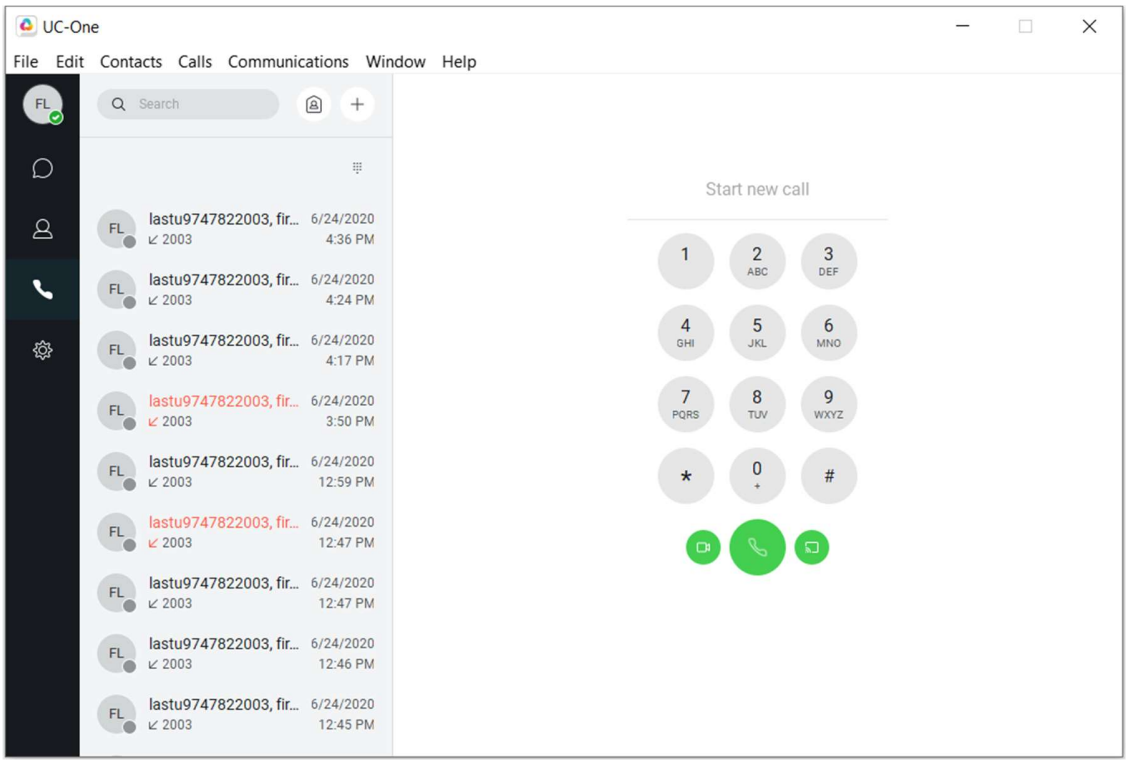

Figure 11 UC-One SaaS Client Dial Tab After Login

7.3 Configure UC-One SaaS as Call Control Client

The UC-One SaaS client can also be configured as a third-party call control client. This enables the client to remotely control a SIP desktop phone or other endpoint. This configuration is necessary for *Basic* and *Advanced Call Control* test cases which require use of a third-party call control client.

As a Cisco BroadWorks group administrator, check the following configuration for the Cisco BroadWorks user selected to perform third-party call control:

- Browse to *<user>* → *Addresses*. Select the *Configure Identity/Device Profile* link. On the subsequent web page, make sure that Identity/Device Profile Type is not any of the following: *Business Communicator – PC*, *Business Communicator – Mobile*, *Business Communicator – Tablet*. The client does not work as a call control client if the primary endpoint is also a UC-One client. The Identity/Device Profile Type should match the device profile type for the device you are testing.
- Browse to *<user>* → *Call Control* → *Shared Call Appearance*. Make sure that *Alert all appearances for Click-to-Dial calls* is not selected.
- Browse to *<user>* → *Profile* → *Assign Services* and make sure that the *Business Communicator Desktop* service is assigned to the user.

After the client is installed (see section *7.1 Client Download and Install*), start the client, and enter the Access code corresponding to the Cisco BroadWorks Sandbox system on which you are testing. This *Login details* specifically applies to call control mode.

Then supply the web portal login username and password for the Cisco BroadWorks user performing the call control. See ***Error! Reference source not found.***, ***Error! Reference source not found.***, and *Figure 5* for examples of the UC-One SaaS client at login and the dial tab after login. Note that in *Figure 5* only the phone icon is shown at the bottom of the client screen. This indicates that the client is correctly configured for call control only.

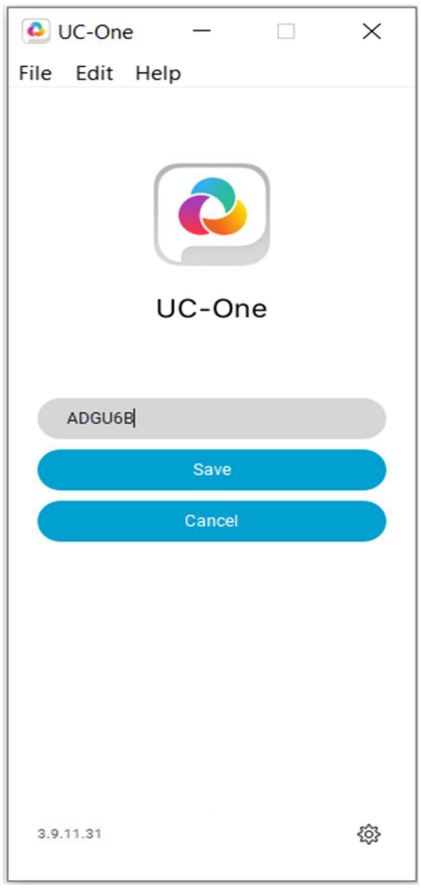

Figure 12 UC-One SaaS Client Call Control Only Login Step 1

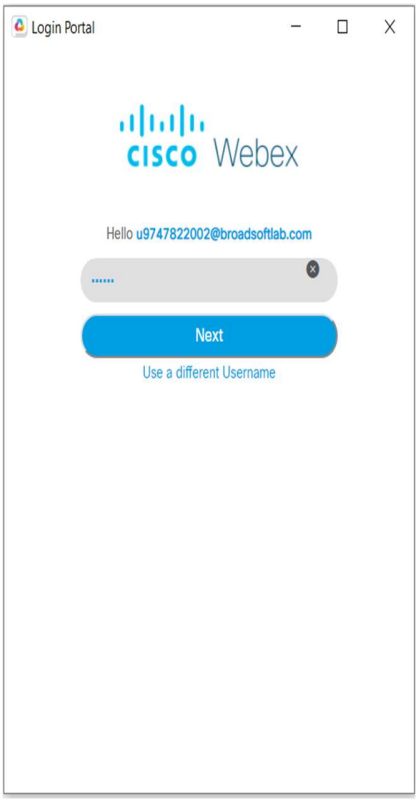

Figure 13 UC-One SaaS Client Call Control Only Login Step 2

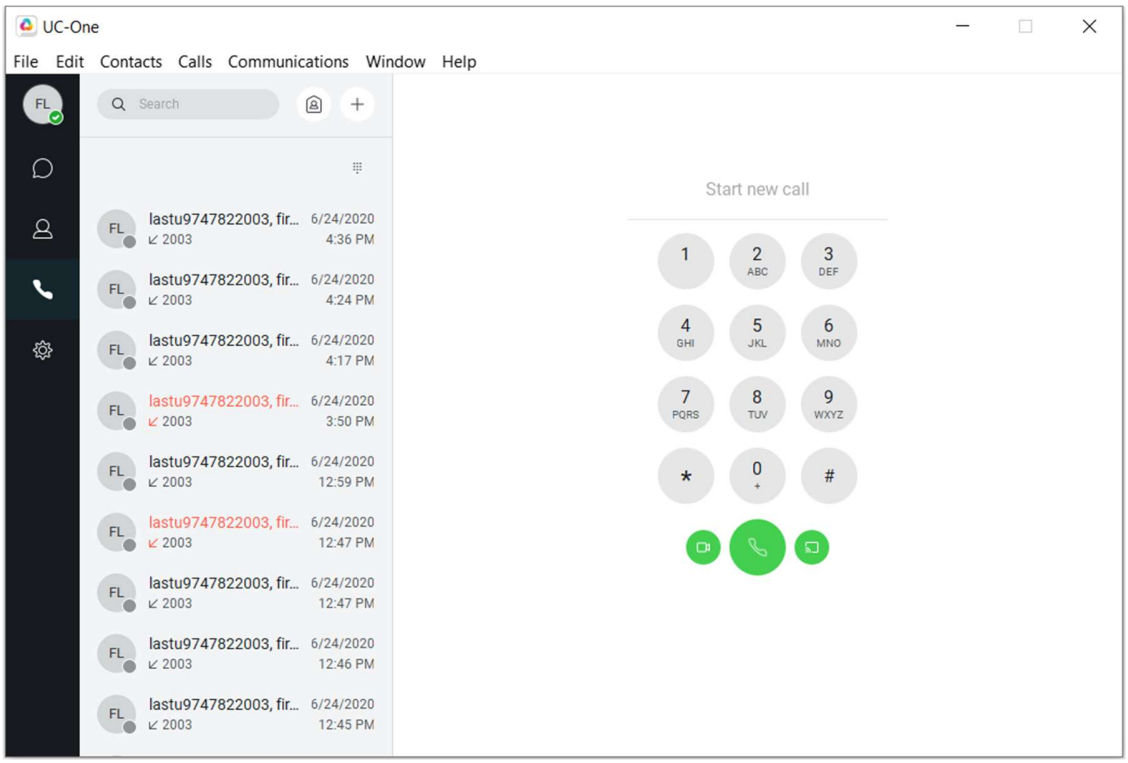

Figure 5 UC-One SaaS Client Call Control Only After Login

7.4 Manually Configure UC-One SaaS as Primary Endpoint

It is recommended to use the accounts preconfigured with UC-One as the primary endpoint, but in some cases it may be necessary or useful to configure additional users with UC-One SaaS as the primary endpoint.

Follow these steps to manually configure a user with UC-One SaaS as the primary endpoint:

1) As the group administrator, add a new user. See section *6.4.1 Add User*.
2) Assign the services in *Table 7 User Services – Pre-assigned* to the new user. Also, assign the *Integrated IM&P* service to the user. See section ***Error! Reference source not found. Error! Reference source not found.***.
3) Browse to *<user>* → *Messaging* → *Integrated IM&P* and set to "On".
4) Browse to the user's *Profile* page and click on **Passwords**. Then set the *web access password.* This web access password and user ID are the credentials required when launching the UC-One client.
5) Browse to the user's *Utilities* page and click on **Authentication**. Provide a SIP authentication username and password. For convenience, these credentials may be the same as the web access credentials.
6) Browse to the user's *Profile* page and click on **Addresses**. Select an available *Phone Number* from the drop-down box on the *Addresses* page. If the drop-down box is empty, then all phone numbers assigned to your group have been used. Free (unassign) a number from another user in the group to continue.
7) On the *Addresses* page, select the *Identity/Device Profile* radio button. In the *Identity/Device Profile Name* drop-down box, scroll to the bottom and select *New Identity / Device Profile (Group)*.
   - Provide a name for the new device profile in the *New Identity/Device Profile Name* field. The name must be unique to the group.

     Example: UCOneSaaS3.
   - In the *Identity/Device Profile Type* drop-down box, select *Business Communicator – PC* as the device profile type.
   - Use the Phone Number as the user portion of the *Line/Port.* Leave the domain portion of the *Line/Port* as the default setting.
8) Click **OK** to complete the device profile addition and assignment.
9) On the user's *Profile* page, click on **Addresses**, and then select the *Configure Identity/Device Profile* link.
   - On the *Identity/Device Profile Modify* page, at the bottom of the *Profile* tab, set the *Device Access User Name* and *Device Access Password*. For convenience, these credentials may be the same as the user's web access credentials.
10) Launch the UC-One SaaS client and use the user's web access credentials to login.

7.5 Manually Configure UC-One SaaS as Shared Call Appearance

It may be necessary to configure UC-One SaaS as a Shared Call Appearance with the DUT configured as the primary device. A specific scenario where this is required is for XMPP testing.

Follow the steps below to manually configure a user with UC-One SaaS as a Shared Call Appearance.

1) As the group administrator, browse to the user's *Profile* page and click on **Addresses**. Make sure that the Identity/Device Profile Name indicates the primary device is the DUT.

2) Make sure the services in *Table 7 User Services – Pre-assigned* are assigned to the user. Also, assign the *Integrated IM&P* service to the user (see section ***Error! Reference source not found. Error! Reference source not found.***).

3) Browse to *<user>* → *Messaging* → *Integrated IM&P* and set to "On".

4) Browse to *<user>* → *Profile* → *Addresses* and select *Configure Identity/Device Profile*.

   – Select the *Files* tab.

   – Select *Rebuild the files* so that the IM&P credentials will be updated in the device configuration file.

5) Restart the DUT to obtain the updated configuration file with IM&P credentials.

6) Browse to the user's *Profile* page, click on **Passwords**, and then set the *web access password.* This web access password and user ID are the credentials required when launching the UC-One client.

7) Browse to the user's *Call Control* page and click on **Shared Call Appearance**. On the *Shared Call Appearance* page, select **Add**.

8) On the *Shared Call Appearance Add* page, in the *Identity/Device Profile Name* drop-down box, scroll to the bottom, and select *New Identity / Device Profile (Group)*.

   – Provide a name for the new device profile in the *New Identity/Device Profile Name* field. The name must be unique to the group.

     Example: UCOneSaaS3.

   – In the *Identity/Device Profile Type* drop-down box, select *Business Communicator – PC* as the device profile type.

   – For the Line/Port setting, provide a unique user portion (for example, <DN>-1). Leave the domain portion of the *Line/Port* as the default setting.

9) Click **OK** to complete the device profile addition and assignment.

10) On the *Shared Call Appearance* page, click the **Edit** link on the newly added Shared Call Appearance.

11) On the *Shared Call Appearance Modify* page, select the *Configure Identity/Device Profile* link.

   – On the *Identity/Device Profile Modify* page, at the bottom of the *Profile* tab, set the *Device Access User Name* and *Device Access Password*. For convenience, these credentials can be the same as the user's web access credentials.

12) Launch the UC-One SaaS client and use the DUT user's web access credentials to login.

7.6 UC-One SaaS Parameter Customization

For some test scenarios, there may be the need to alter the UC-One client settings. An example is changing the outbound proxy setting when using the UC-One client for testing behind an enterprise SSE. Customization is accomplished by use of Device Management tags.

Follow these steps to customize a UC-One client tag:

1) Log in to the Cisco BroadWorks web portal using the group administrator's credentials.

2) As the group administrator, browse to *<group>* → *Resources* and select *Identity/Device Profile*.

3) On the *Identity/Device Profiles* page, click **Search** to show a list of the device profiles in the group.

4) From the list of device profiles, select the UC-One SaaS device profile that you need to customize.

5) On the *Identity/Device Profile Modify* page, select the *Custom Tags* tab.

6) Add or modify the custom tag as required.

7) If the UC-One client is currently logged in, log out.

8) Log in to the UC-One client to obtain the modified configuration.

8 Frequently Asked Questions

8.1 Connectivity

8.1.1 I used to be able to log in to the web portal. Now I cannot log in anymore. Has my account been disabled?

It is unlikely that your account has been disabled. This usually indicates that the wrong password was entered too many times and the account has been automatically locked out. Follow these instructions pertaining to the type of account that is locked out.

- User Account

1) Log in to the Cisco BroadWorks web portal as a group admin.

2) Browse to *Users* and select *Search*.

3) Click on the applicable user.

4) Browse to *Profile* → *Passwords* and reset the *Web access password*.

- Group Admin

Contact Cisco at devnet-broadsoft-support@external.cisco.com to request a reset. Identify the group admin in your request.

8.1.2 I cannot ping or traceroute to the Cisco BroadWorks Sandbox test platform SSE IP addresses. There is no response.

Internet Control Message Protocol (ICMP) requests (ping or trace route commands) are blocked, so ping is not a reliable indicator of a problem. If your SIP requests or responses are not getting through, then you may have a network or firewall issue.

8.1.3 Is there PSTN access?

No, there is no PSTN access to/from the test platform. Calls can be made only between the users and devices configured on the test platform.

8.1.4 When I attempt to call my assigned user numbers from my work or mobile phone I get a recording or a wrong number.

See section *8.1.2*.

8.1.5 When I call from one user in my group to another user in my group, the call does not complete to the remote endpoint. Instead I hear an announcement like "*Your call cannot be completed at this time.*"

This typically indicates one of the following:

- The terminating endpoint is not registered. To check the user's endpoint registrations, log in to the Cisco BroadWorks web portal as a group admin and browse to *<user>* → *Utilities* → *Registrations* to check the registrations.
- The INVITE does not correctly identify the originator. The FROM, P-Asserted-Identity, and any other identity headers in the INVITE from the DUT must match the SIP REGISTER address-of-record. See section *6.6 SIP Registration and Authentication*.

  If this is the problem, then a call to a user's extension will not work, but a call to a user's full phone number will work.

8.1.6 How can I verify that my endpoint is registered?

Follow these steps to check if an endpoint or application is registered with Cisco BroadWorks:

1) Log in to the Cisco BroadWorks web portal as a group admin.
2) Browse to *Users* and select *Search*.
3) Click on the user that you want to check to see if the endpoint is registered.
4) Select *Utilities* in the left column.
5) Select *Registrations*. The *Registrations* page shows the user's current registrations.

8.1.7 Which IP addresses and ports should I tell my IT department to prepare the firewall for?

The IP addresses and ports used by the Cisco BroadWorks test platform are listed in *3.1 IP Addresses and FQDNs*.

8.2 Process

8.2.1 How do I get help?

This document provides most of the essential information. Check the frequently asked questions and other resources in this document.

Cisco provides troubleshooting help and assistance via the developer's sandbox forum. Search the forum first to see if your question has been asked before. If you post a new question, use the RSS feed for answers to monitor for updates to your question or otherwise check back periodically for a response. Cisco responds to questions on a best effort basis. Most questions are answered within a few days.

8.2.2 If I have several device models that share the same SIP stack and code base, do I need to submit separate test results for each model?

No. Submit one set of test results using one or more of the models. This covers all models that share the same SIP stack.

If there are models with features that other models do not have, such as video, note in the test report the list of models that support the feature.

8.2.3 The test case result does not match the test case expected outcome. How do I resolve this?

Before submitting a question to the Q&A forum for analysis, review the test section, test group, and test case to make sure all test setup instructions have been followed. If the results are still the same after reviewing and re-executing the test case, then research the Q&A forum to see if others have experienced the same issue and an explanation is available. If no similar posts are found, then post a new question to the forum and include a SIP capture if applicable.

For some test cases, there may be minor differences between the DUT's implementation and the expected result as specified for the test case. Minor differences are identified as those that are non-service affecting. These differences should be documented in the test report.

8.2.4 The test case does not work as written. What should I do?

Carefully review all setup instructions in the test section, test group, and test case and rerun the test case if necessary. Most test cases have been successfully executed many times.

Temporary outages may be the cause. Check the Announcements on the developer's sandbox to see if any outages have been reported.

Otherwise, report the issue on the Q&A forum.

8.2.5 Can I perform other types of testing besides interop testing, such as development, regression, or performance testing?

See section *5.2 Testing*.

8.2.6 The test plan includes *Administrator Reference Only* notes for some test cases. What is the purpose for these? How do I check them?

Administrator Reference Only notes are for Cisco internal usage only. These notes enable Cisco to track the required test platform configuration to enable the various test scenarios. For the tester, these notes should be disregarded.

8.3 Cisco BroadWorks Services

8.3.1 Voice Messaging deposit/retrieve does not work.

If Voice Messaging is not working, you will likely hear an audio error message such as "*This operation cannot be completed at this time"*. This typically indicates a misconfiguration.

Your test accounts include two users preconfigured with Voice Messaging. Make sure that you are using one of those users for the test. The users preconfigured for Voice Messaging are identified by "_VM" at the end of the Cisco BroadWorks user ID. The configuration must not be modified.

For more information, see *6.8* .

8.3.2 Where do I find the conference-URI for Network Ad Hoc Conference?

If you are testing Network Ad Hoc Conference, you will need to configure the test platform conference-URI on your endpoint.

See section *3.1 IP Addresses and FQDNs*.

8.3.3 How do I change or reset a user's web portal password or voice portal passcode?

Log in to the Cisco BroadWorks web portal as a group admin. Select the User, then browse to *<user>* → *Profile* → *Passwords*. From there you can set the web access password (which is used for web portal login) or the portal password (which is used for the voice portal and voice mail).

8.4 SIP

8.4.1 My device is sending SIP REGISTER or INVITE to the IOP SBC address, but there is no response.

Verify that your firewall is not blocking SIP traffic to/from the IOP address.

If it was working before and recently stopped working, temporary outages may be the cause. Check the Announcements on the developer's sandbox to see if any outages have been reported.

8.4.2 Why is my device receiving a 404 response for a REGISTER request?

A 404 response indicates that the address-of-record (username@domain) in your REGISTER request does not match the configured value on Cisco BroadWorks. Make sure the FROM/TO URI matches the Line/Port configured on Cisco BroadWorks for that user. The address-of-record is identified in section *4.2 Test Account Details*.

See also section 5.2.2.1 Registering Devices.

8.4.3 Why is my device keep receiving a 401 responses for a REGISTER request?

If Cisco BroadWorks keeps responding with *401 Unauthorized* response to a REGISTER request, this indicates that SIP authentication is failing. Make sure that the authentication username and password configured on the DUT match those configured on Cisco BroadWorks.

Also, see section *6.6.2 SIP Authentication*.

8.4.4 How can I avoid fragmented packets in my Wireshark captures?

Instead of using "sip" as the display filter, consider using "tcp.port==5060 or udp.port==5060". Another possibility is to identify the fragmented packets and use "sip or frame.number==<fragmented packet number 1> or frame.number==<fragmented packet number 2>…".

See also section 5.2.3.1.6 Wireshark Guidelines for SIP UDP.

8.5 Media

8.5.1 The voice quality for a call is poor or garbled.

Garbled voice typically indicates a codec or packetization interval (ptime) mismatch or interoperability issue. Review the capture for the call to verify. Other voice quality issues may be a result of the traffic on the test network.

8.5.2 There is one-way voice for my call.

One-way voice indicates a routing or firewall issue. This may occur if there is a SIP-aware firewall or other intermediary device in the signaling path.

8.6 UC-One Clients

8.6.1 I am trying to use UC-One SaaS for call control but see an error: "Connection to server failed".

Make sure that you are using the full URL as specified in section *7.3 Configure UC-One SaaS as Call Control Client*.

Acronyms and Abbreviations

CPE	Customer Premises Equipment
DN	Directory Number
DUT	Device Under Test
EMTA	Embedded Multimedia Terminal Adaptors
FQDN	Fully Qualified Domain Name
HID	Human Interface Device
HSS	Home Subscriber Server
HTTPS	Hypertext Transfer Protocol Secure Sockets
IAD	Integrated Access Device
ICMP	Internet Control Message Protocol
IM&P	Instant Messaging and Presence
IMS	IP Multimedia Subsystem
IVR	Interactive Voice Response
MAC address	Media Access Control Address
MCU	Multipoint Control Unit
MPP	Multiplatform Phone (Cisco phone)
MSBG	Multi-Service Business Gateway
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NDA	Non-Disclosure Agreement
OEM	Original Equipment Manufacturer
ONT	Optical Network Terminal
PBX	Private Branch Exchange
PCG	Partner Configuration Guide
PSTN	Public Switched Telephone Network
Q&A	Question and Answer
RSS	Really Simple Syndication
RTP	Real-Time Transport Protocol
S-CSCF	Serving – Call Session Control Function
SBC	Session Border Controller
SDP	Session Definition Protocol
SIP	Session Initiation Protocol
SIPREC	SIP Recording
SRTP	Secure Real-time Transport Protocol
TCP	Transmission Control Protocol

TLS	Transport Layer Security
UC	Unified Communications
UDP	User Datagram Protocol
UE	User Equipment
VM	Voicemail
VoLTE	Voice over Long-Term Evolution
XMPP	Extensible Messaging and Presence Protocol
Xsi	Xtended Services Interface