ON SIGHT

APP NOTES

Onsight Connect Cisco Integration

July 2016

LIBRESTREAM

Table of Contents

Document Revision
Librestream
Onsight Connect Cisco Integration
Doc #: 400279-01
July 2016

Overview
The Onsight Connect software platform utilizes standards based SIP protocols (RFC 3261) to negotiate calls and allow users to collaborate using VOIP (G.711, GSM.610), video (H.264 and H.263+) and Onsight data channel streams. This Onsight data channel provides enhanced capabilities such as recorded video playback, still image sharing, on-screen telestration and remote control of the Onsight Devices (zoom, focus, lighting).

For the purposes of this document, Onsight Device refers to any of the following platforms running Onsight Connect:

- Onsight Rugged Smart Camera (2500, 2000, 1000)
- iOS or Android Smartphones
- iOS, Android or Windows tablet
- Windows PC

For complete details on supported platforms please refer to the Onsight Connect Release Notes for your device. (See www.librestream.com/support/knowbase.html)

There are two supported approaches for Onsight calls within Cisco infrastructure.

- Direct Onsight Device to Cisco Endpoint Calls
  - Supports Audio and Video
- Onsight Device to Onsight Device and Cisco Endpoint Calls
  - Supports Audio, Video and Data Channel capabilities

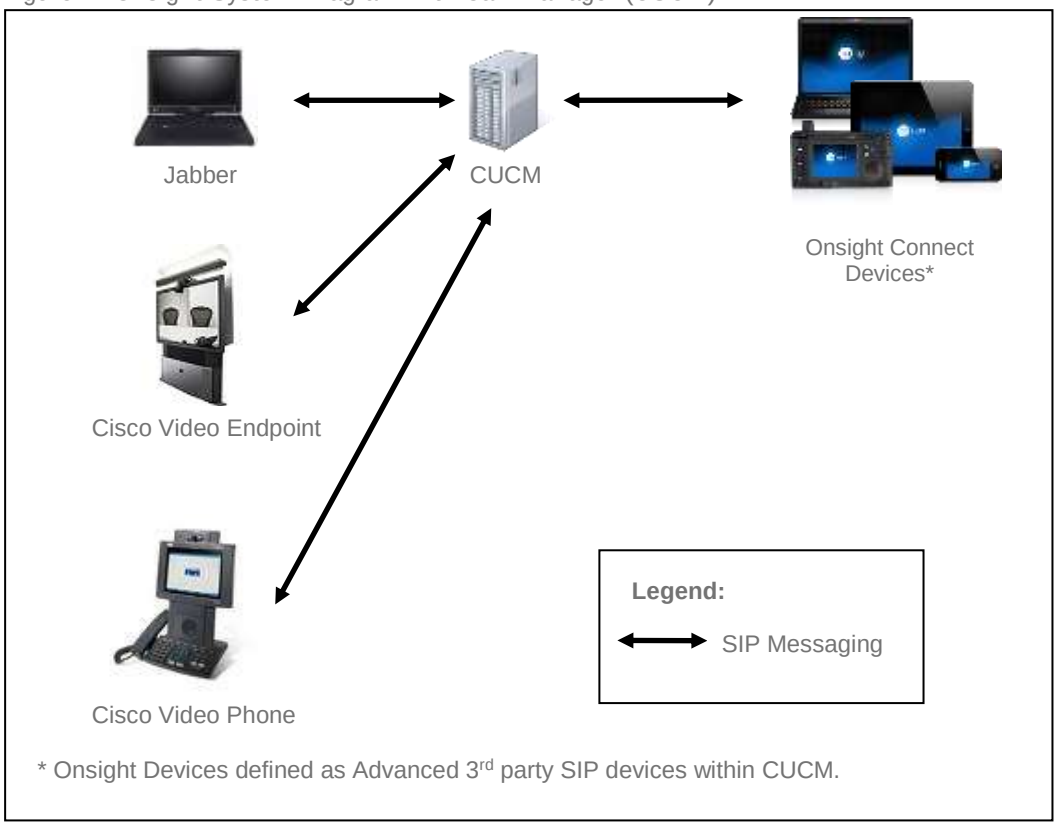
In the majority of cases, customers need to use both approaches to support various use cases. Sometimes, they need the extra capabilities supported within the Onsight data channel. Other times, audio and video are sufficient to make the decision in the field.

1. Direct Onsight Device to Cisco Endpoint Calling

For situations where audio and video is sufficient, users can call directly from an Onsight endpoint to a Cisco endpoint. In this case, the Onsight endpoint can reside within a standard Cisco Unified Communications (CUCM) environment as an Advanced 3rd Party SIP Device without the need for the Cisco VCS products. In this configuration, the Onsight 400R Collaboration Hub connects to the Onsight endpoint to share live visuals from specialized instruments or wearable cameras as part of the collaboration session.

The system diagram shows the Onsight endpoint within the Cisco Unified Communications environment in Figure 1.

Figure 1: Onsight System Diagram with Call Manager (CUCM)



Onsight Devices can register to CUCM as a Third Party SIP Device and act as a video source to other Third Party Endpoints.

Registering an Onsight Device to CUCM will disable its ability to stream video to other Onsight Devices; it will connect as an Audio only call. Onsight Devices do not accept video from 3rd Party endpoints.

Cisco Unified Communications Manager does not support Transport Layer Security (TLS) from third-party phones that are running SIP.

2. Onsight Device to Onsight Device (including Cisco Endpoint) Calling

Typically, a call includes two Onsight Devices within Cisco infrastructure for a full collaboration session. The reason that two Onsight Devices are included in a call is to support the Onsight data channel with its additional features of remote control, image sharing, telestration, etc.

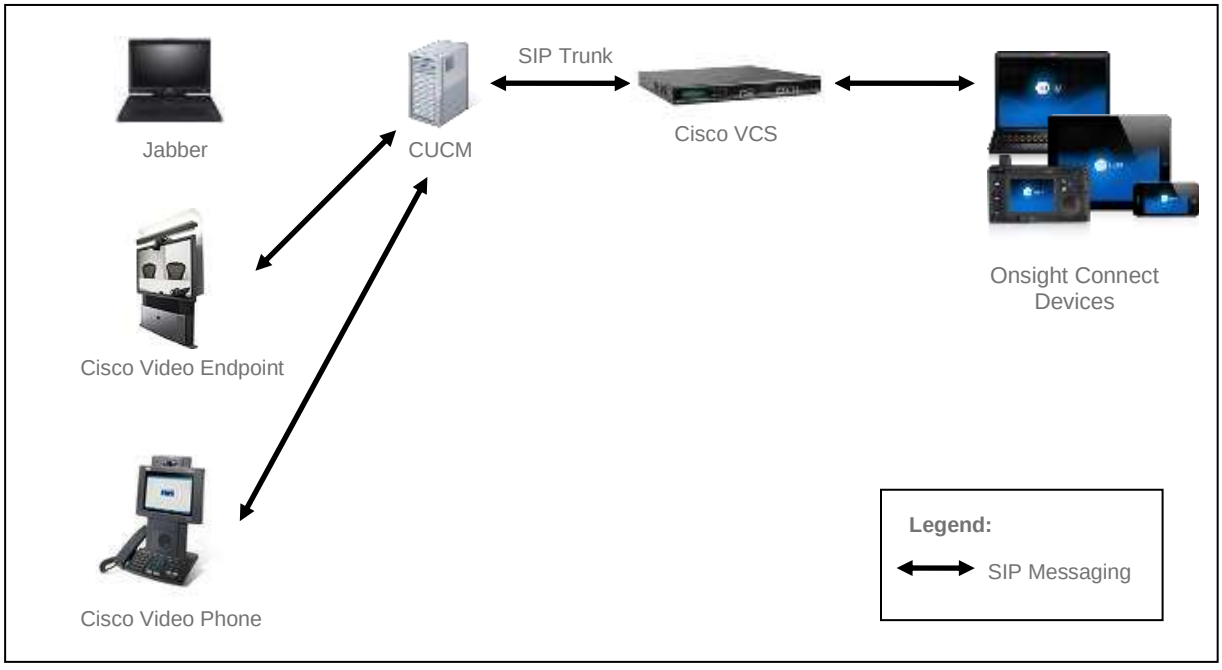
This Onsight data channel is a proprietary protocol developed by Librestream and is negotiated via the SIP INVITE SDP. This negotiation is handled properly using the Cisco VCS Control and Expressway. CUCM is currently not able to negotiate this data stream directly, as it does not support unknown SDP media description "m" lines – media types. To support this configuration, the Cisco VCS is required to act as the SIP Registrar and negotiate the SIP INVITE between Onsight Devices.

Onsight Connect Devices must register to a Cisco VCS to retain Onsight data stream capabilities such as sharing still images, telestration and remote control.

For SIP communications between Onsight Devices and Cisco endpoints, SIP INVITES pass through the VCS and to the CUCM and vice versa utilizing a SIP trunk between the two registrars. In these calls, the Onsight Devices support all the capabilities within the data stream, while the Cisco endpoints receive audio and video. In all cases, live visuals from specialized instruments or wearable cameras are shared through the Onsight 400R Hub.

The system diagram of the Onsight system and the Cisco VCS within the Cisco Unified Communications environment is shown in Figure 2.

Figure 2: System Diagram including VCS



Onsight Connect endpoints can send video and audio to any SIP enabled endpoint; however, they can only receive video from other Onsight Connect endpoints. Onsight endpoints must be registered to the Cisco VCS for this capability.

3. Cisco Unified Communications – Configuration

3.1 Logging into the CUCM Server

1. Open a web browser, e.g. Internet Explorer and type the URL of the CUCM Server e.g. "https://cisco-ucm/" in the address bar.
2. Select the "Cisco Unified Communications Manager Administration" product.
3. Enter the username and password.

3.2 Adding a Onsight Device – **"Phone Type"**

1. Login to the CUCM Server.
2. Navigate to "Device / Phone".
3. Click on the "Add New" button.
4. Select Phone Type - "Third-party SIP Device (Advanced)". Press 'Next'.
5. Enter the MAC Address.
6. For the Device Pool, choose "Default".
7. For the Phone Button Template, choose "Third-party SIP Device (Advanced)".
8. For the Device Security Profile, choose "Third-party SIP Device Advanced – Standard SIP Non-Secure Profile".
9. For the SIP Profile, choose "Standard SIP Profile".
10. Leave everything else as default and click the "Save" button.
11. On the left hand side of the Phone Configuration page click the "Add a new DN" link.
12. Enter the Directory Number (Example: if the Device Name is "UPC1007", enter "1007").
13. Leave everything else as default and click the "Save" button.
14. Now click the "Apply Config" button at the top of the page.
15. Go back to the Phone Configuration page and click the "Apply Config" button at the top of the page.
16. Navigate to "User Management / End User".
17. Click on the "Add New" button.
18. Enter a User ID (Should be the same as the Directory Number ex. "1007").
19. Enter a Password and Digest Credentials.
20. Enter a Last name.
21. Click the "Save" button.
22. Navigate back to "Device / Phone".
23. Choose the new device that was added in steps 3-10.
24. Select the new Owner User ID (the user added in steps 17-21).
25. Select the new Digest User (the user added in steps 17-21).
26. Click the "Save" and "Apply Config" buttons.
27. Navigate back to "User Management / End User".
28. Select the new user.
29. Choose the Directory Number of the device as the Primary Extension.
30. Click the "Save" button.
31. Click "Add to User Group" button.
32. Click "Find".
33. Select "Standard CCM End Users" and "Standard CTI Enabled".
34. Click "Add Selected" button.

35. Click "Save" button.

NOTE: Make sure the following are set for the End User Configuration:

- ☐ Telephone #
- ☐ Mail ID
- ☐ Digest Credentials – SIP password
- ☐ Primary Extension (add a DN for the User to get it listed as a Primary ext.)

NOTE: LDAP is required as the user database for CUCM in order to avoid the case where a user must enter 2 contacts on the CUPC to represent an Onsight endpoint. (One contact for calls, one contact for presence.)

3.3 Adding an Onsight User to CUCM

1. Login to the CUCM Server.
2. Navigate to User Management / End User.
3. Click the Add New button.
4. Enter a User ID (Should be the same as the Directory Number ex. "1102").
5. Enter a Password and Digest Credentials.
6. Enter a Last name.
7. Add a Device Association.
8. Click the Save button.

3.4 Adding a Route Pattern

1. Login to the CUCM Server.
2. Navigate to Device / Trunk.
3. Click the Add New button.
4. Select SIP Trunk as the Trunk Type and click the Next button.
5. Enter the Device Name for the trunk.
6. Choose Default for the Device Pool.
7. Enter the IP address of the neighboring sip server in the Destination Address field.
8. Choose Non Secure SIP Trunk Profile for the SIP Trunk Security Profile.
9. Choose Standard SIP Profile for the SIP Profile.
10. Click the Save and Apply Config buttons.
11. Navigate to Call Routing / Route/Hunt / Route Pattern.
12. Click the "Add New" button.
13. Enter the desired Route Pattern (Example: to route all 1100 – 1199 directory numbers, enter 11XX as the route pattern).
14. Choose the previously created sip trunk for the Gateway/Route List.
15. Click the Save button.

4. Cisco VCS Configuration

4.5 Adding an Onsight User to VCS

User accounts need to be duplicated on the VCS and the CUCM i.e. they must share the same user name and password.

1. Log on to the VCS.
2. Navigate to VCS configuration\Authentication\Devices\Local database
3. Press New to create a user with the same Username and Password as the Onsight user created for the CUCM.

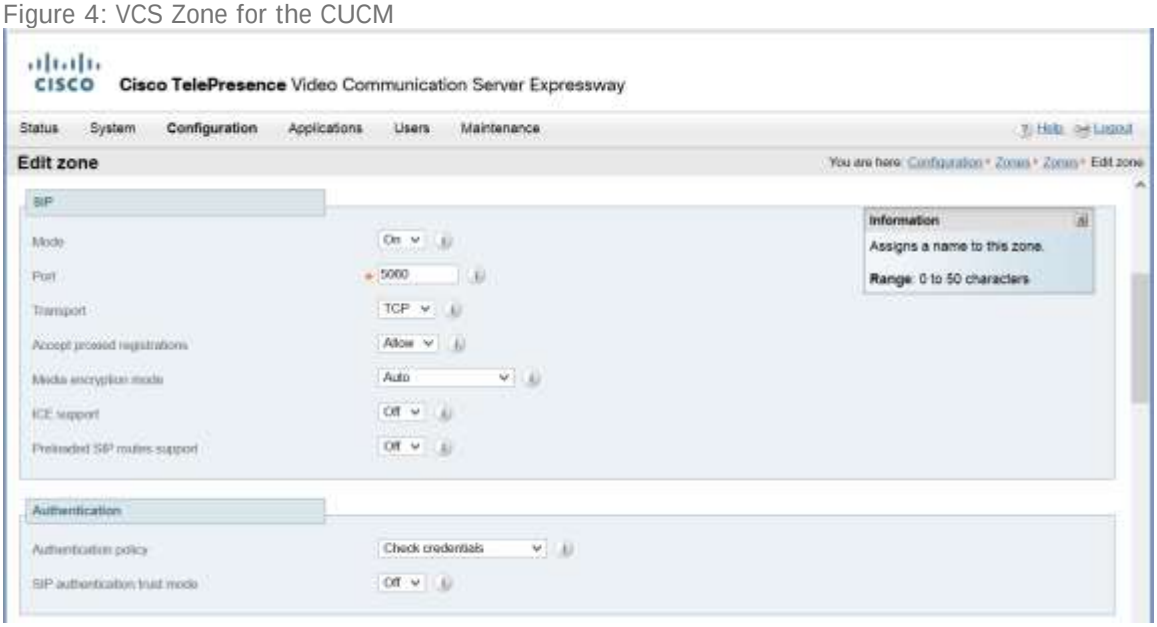
4. Save the configuration.

4.5.1 Adding a Route to the CUCM server from the VCS

A SIP Trunk route or Zone between the Cisco VCS and CUCM is required so that any calls to/from an Onsight Endpoint are correctly routed to Cisco Endpoints that are registered with the CUCM. (Note: the CUCM must have a route added for the VCS, see 'Adding a Route Pattern' under the section 'Setup on the CUCM Server'.)

1. Login to the VCS as administrator.
2. Go to VCS configuration\Zones.
3. Press New.
4. Give the Zone a name e.g, CUCM
5. Select 'Type = Neighbor'.
6. Set the following:
    a. SIP Mode: On
    b. SIP Port: 5060
    c. SIP Transport: TCP
    d. H.323: Off
    e. Peer 1 Address: 192.168.1.37 (e.g. CUCM's URL: http://cisco-ucm)
7. Press Save.
8. The Status of the connection can be viewed under Status\Zones.

Figure 4: VCS Zone for the CUCM



Adding a UCM Domain and Transform

1. Log on to the VCS.
2. Navigate to "VCS configuration" →"Protocols" →"SIP" →"Domains".
3. Click "New".
4. Enter a name (ex, vcs_ucm) that will be the SIP URI's domain.
5. Click "Create domain".
6. Navigate to "VCS configuration" →"Transforms".
7. Click "New".
8. Set the pattern string to "(.*)@<VCS_ip_address>.*".
9. Set it to a high priority (ex. 2).
10. Set the "Pattern type" to "Regex" and "Pattern behaviour to "Replace".

11. Set the replace string to "$1@<SIP_domain>" (ex. $1@vcs_ucm).
12. Click "Save".

The domain is the group to which a device is registered to. It is not necessary to have a domain specifically for the UCM. The transform changes addressed to <vcs_ip_address> to the registered device's domain.

5. Active Directory and CUCM Integration

5.6 Installing Microsoft Active Directory on Windows Server 2003

1. On the Manage Your Server window on Windows Server 2003, select Add or remove a role.
2. Click Next.
3. Select Domain Controller (Active Directory) and click Next.
4. Click Next on the Active Directory installation wizard.
5. On the Domain Controller Type window, select Domain controller for a new domain and click Next.
6. On the Create New Domain window, select Domain in a new forest and click Next.
7. Type DNS name for new domain (e.g. librestream.local) and click Next.
8. Type NetBIOS name for new domain (e.g. phoenix) and click Next.
9. Accept the default locations for the database and log and click Next.
10. Enter in a password and click Next
11. Click Finish to complete the wizard
12. Restart the server for Active Directory service to take effect.

5.7 Adding Organization Unit and/or User to Microsoft Active Directory

1. From Start>Administrative Tools on Windows Server 2003, select Active Directory Users and Computes.
2. Click the server on which Active Directory is installed.
3. From Action>New, select Organization Unit.
4. Enter a name for the organization unit (e.g. Cisco).
5. Click OK.
6. Click the organization unit.

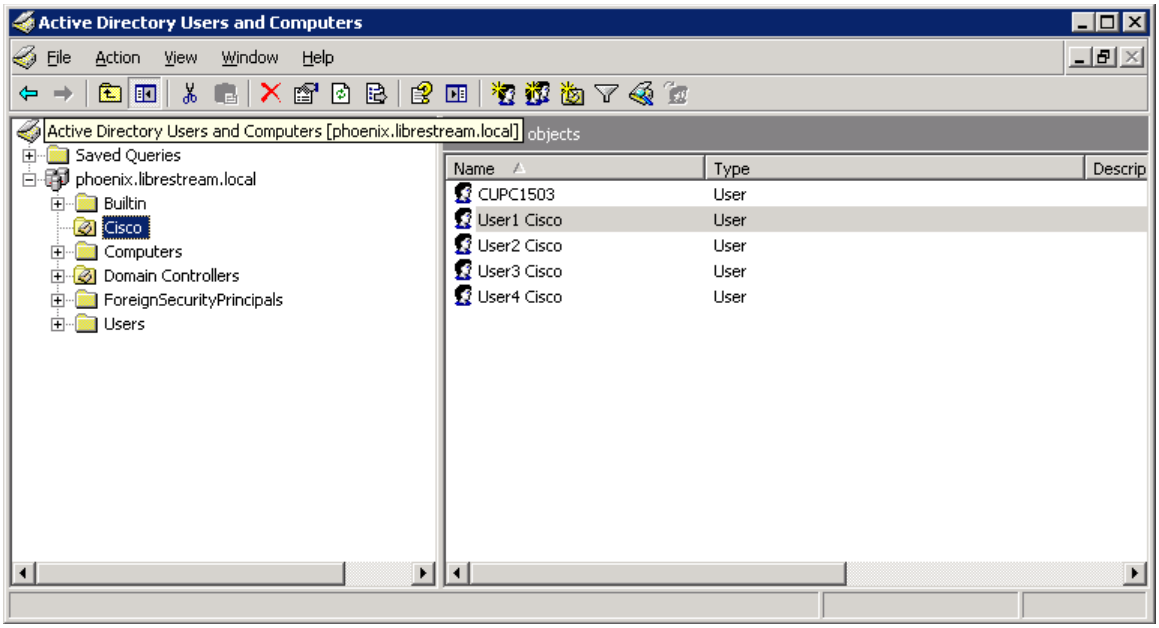


Figure 5: Active Directory User List

7. From Action>New, select User.
8. Enter first name and last name.
9. Enter a directory number in User logon name (e.g. 1551).
10. Click Next.

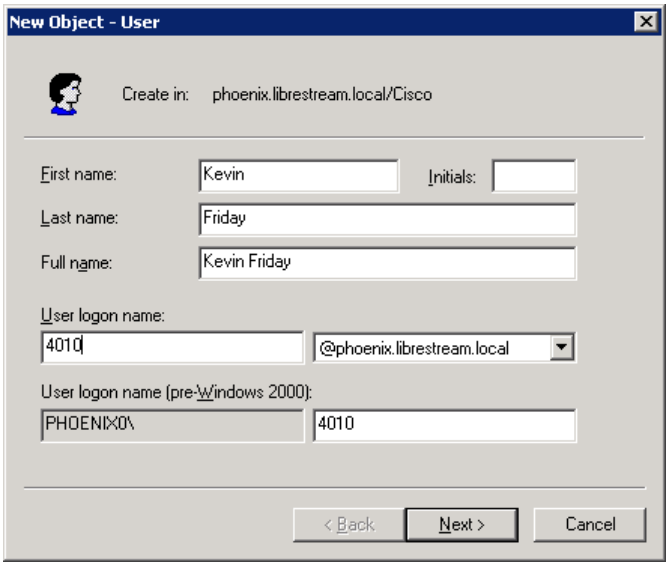


Figure 6: Active Directory New User

11. Uncheck User must change password at next logon.
12. Check Password never expires.
13. Click Next.
14. Review the user settings and click Finish.
15. Double click the user newly added.
16. Enter the directory number (User Logon name) as configured in step 9 in Telephone number (e.g. 4010).

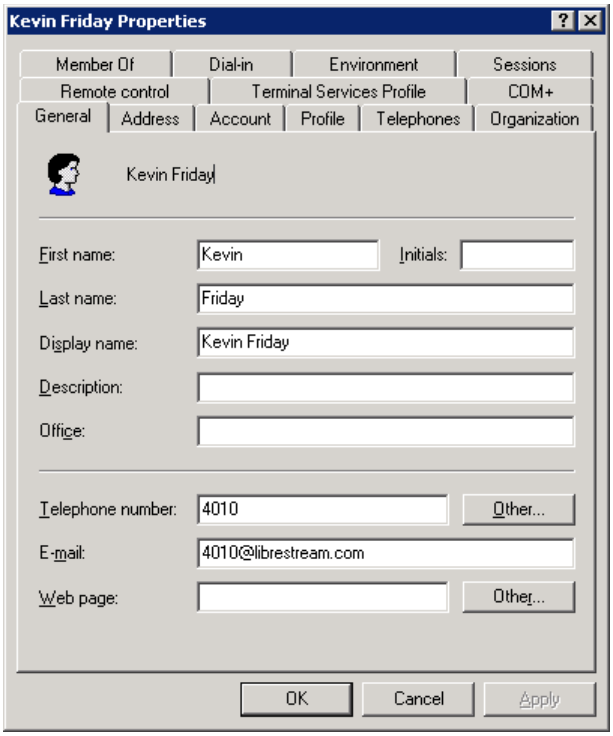


Figure 7: New User Properties

17. Enter an email address in E-mail (*CUCM requires this field*).
18. Click Apply and OK.

5.8 LDAP Configuration on CUCM

1. Login to CUCM server.
2. From System>LDAP, select LDAP System.
3. Check Enable Synchronizing from LDAP Server.
4. Select Microsoft Active Directory in LDAP Server Type.
5. Select telephoneNumber in LDAP Attribute for User ID.
6. Click "Save".
7. From System>LDAP, select LDAP Directory.
8. Click Add New.
9. Enter a name in LDAP Configuration Name (e.g. LSLDAP).
10. Enter the account information of the LDAP administrator in LDAP Manager Distinguished Name (e.g. cn=Administrator, cn=Users, dc=phoenix, dc=librestream, dc=local).
11. Enter the admin password in LDAP Password.
12. Re-enter the password in Confirm Password.
13. Enter the location where LDAP users exist in LDAP User Search Base (e.g. "cn=Users, dc= phoenix, dc=librestream, dc=local" if you use the default container for user accounts or "ou=Cisco, dc= phoenix, dc=librestream, dc=local" if you use the organization unit).
14. Leave Perform Sync Just Once and Perform a Re-sync Every fields as default.
15. Enter the host name in "Host Name or IP Address for Server" under "LDAP Server Information" (e.g. phoenix).
16. Leave the port number as default in "LDAP Port". Enter 636 if LDAP over SSL is configured.
17. Click "Save".

5.9 Performing Synchronization

1. Login to CUCM server.
2. From "System>LDAP", select "LDAP Directory".
3. Click "Find" and select the LDAP configuration.
4. Click "Perform Full Sync Now".
5. From "User Management", select "End User".
6. Note that "LDAP Sync Status" column will display "Active" if the user is successfully synced with LDAP server.
7. Follow steps in Adding an Onsight User.
8. Login to CUCM.
9. From "User Management", select "End User".
10. Select the user added above.
11. Enter password in "Password".
12. Re-enter password in "Confirm Password".
13. Enter SIP user password in "Digest Credentials".
14. Re-enter SIP user password in "Confirm Digest Credentials".

5.10 Registering to CUCM from an Onsight Device

Onsight devices can SIP register directly to CUCM and participate in calls with Cisco endpoints. Onsight endpoints are typically managed through Onsight Account Manager (OAM – onsight.librestream.com). When a user logs in to an Onsight device the configuration settings are retrieved from OAM. However, users can be granted endpoint administration privileges which allows them to manually edit settings on an endpoint.

Below is an example of how a user could configure an endpoint to connect to CUCM. For details on OAM Administration please refer to www.librestream.com/support/knowbase.html.

5.10.2 Example Manual Setup of Onsight Device with CUCM

1. Go to Settings\SIP Server\Public Server
2. Enter SIP Server Address: e.g. cisco-ucm
3. Enter URI: e..g 4004@cisco-ucm
4. Enter Authentication Name: e.g. 4004
5. Enter Authentication Password.
6. Authentication Transport: TCP

Figure 8: Onsight Device CUCM registration

6. For More Information

If you need assistance, please contact Librestream at support@librestream.com.