Cisco live!

What You Make Possible

TOMORROW starts here.

CISCO

Communications Manager for Video Call Control

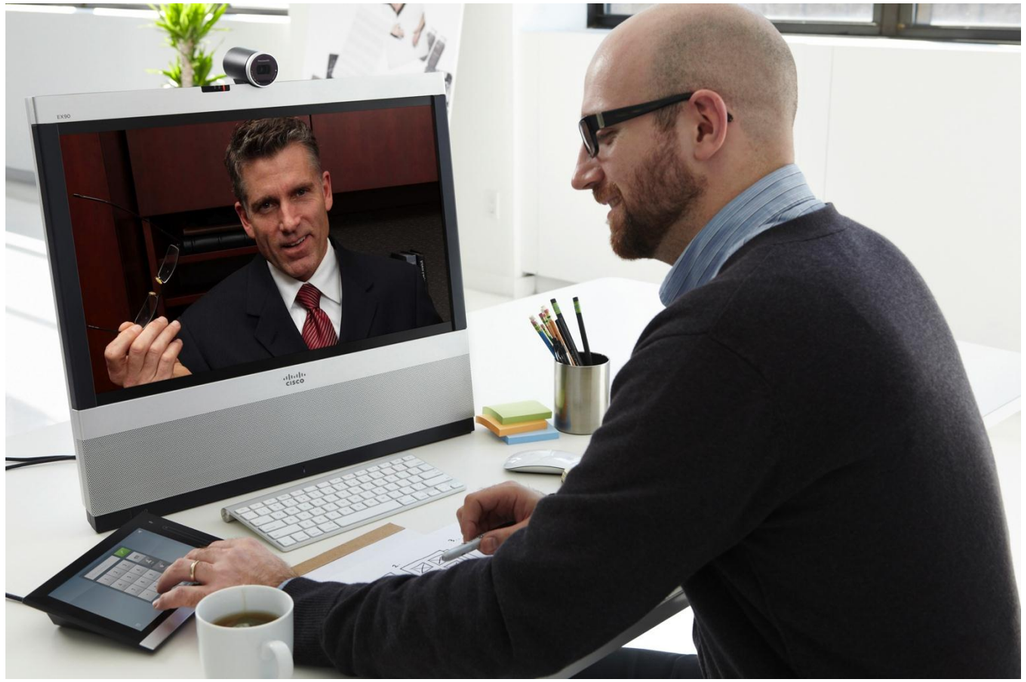
BRKUCC-2665

TOMORROW starts here.

The History

© 2013 Cisco and/or its affiliates. All rights reserved.

The History



© 2013 Cisco and/or its affiliates. All rights reserved.

Upgrading to TC6

- TC6 has two (2) .cop files for CUCM9.0.
  - Firmware/Configuration
- TC6 keys format are not supported in TC<5.1

© 2013 Cisco and/or its affiliates. All rights reserved.

Upgrading to TE6

- If upgrading from TC4.x or lower:
  - Upload sw file
  - Enter key

  or
  - Upgrade to TC5
  - Enter key
  - Upgrade to TE6
- Unified .cop file for TE6

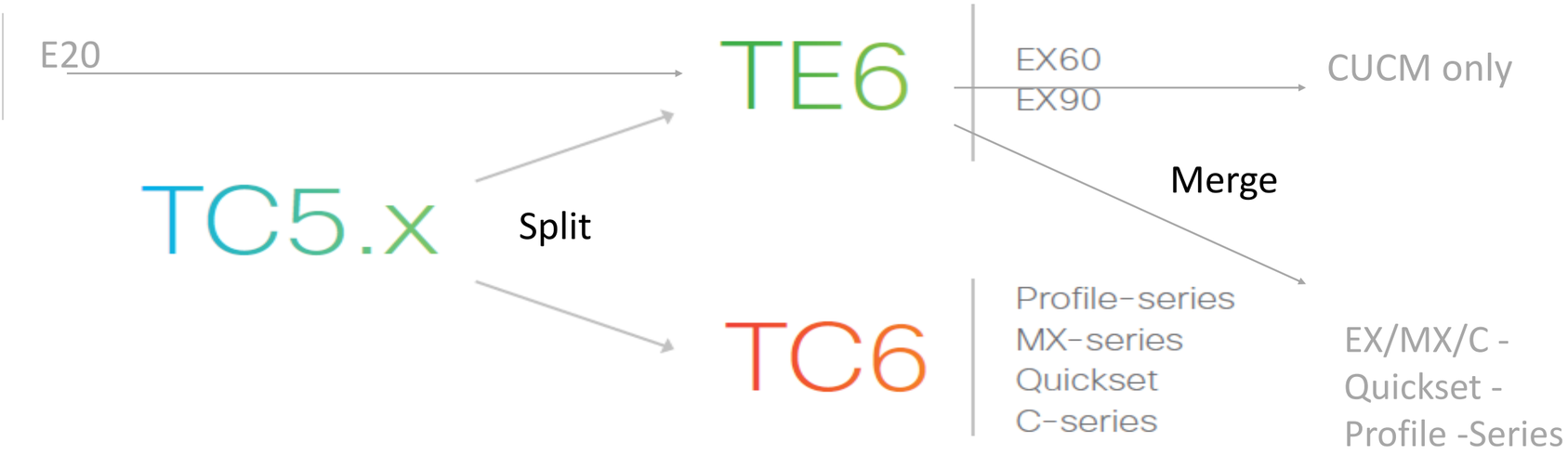
© 2013 Cisco and/or its affiliates. All rights reserved.

Provisioning

- Leverage TMS and TMS PE to manage release keys and automate software upgrades
- Purge endpoint from TMS post upgrade

© 2013 Cisco and/or its affiliates. All rights reserved.

TE 4.1



© 2013 Cisco and/or its affiliates. All rights reserved.

TC/TE software parities and imparities

- Feature parity with TC5.1.4.
- H323 and multiway is disabled
- No feature parity with TC6.
  - CTMS Encrypted calls
  - ISDN Link automatic pairing
  - Web Diagnostics
  - Web GUI and Touch UI differences
  - Diangostics
  - Multisite downspeeding

© 2013 Cisco and/or its affiliates. All rights reserved.

Common Endpoint Capabilities

- SIP URI dialling when registered to CUCM
- Encryption in CUCM Environment
- Ad hoc conferencing in CUCM
- Mediatrace
- CTI/JTAPI Support

© 2013 Cisco and/or its affiliates. All rights reserved.

TE6.0 Capabilities

- Voice mail support and message waiting indication.
- CUCM Shared Lines support
- CUCM Call Forward All

© 2013 Cisco and/or its affiliates. All rights reserved.

Registering the endpoint

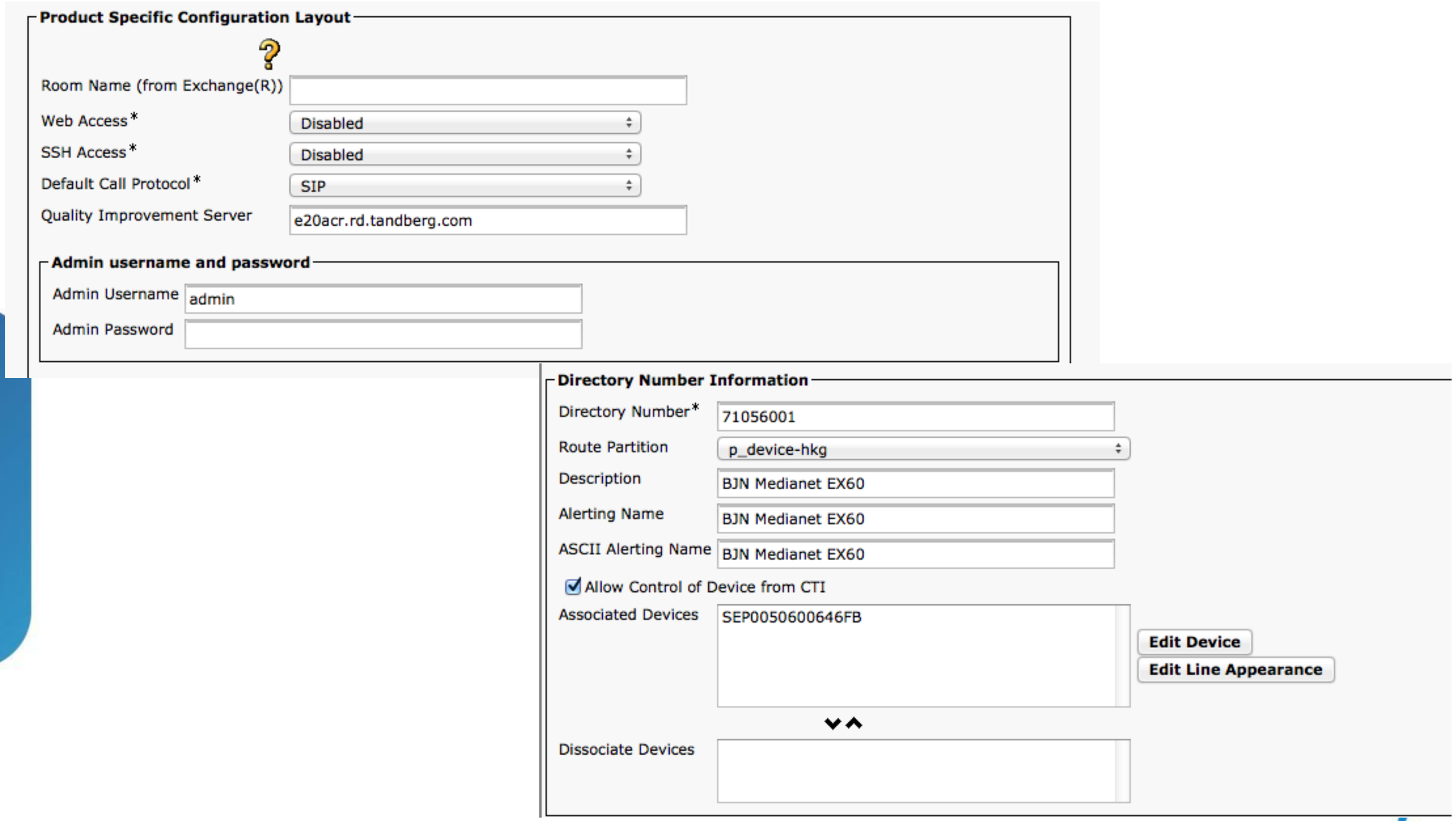
Device Information

Registration	Registered with Cisco Unified Communications Manager 10.68.37.86
IP Address	10.75.209.39
Active Load ID	TC5.1.1.288225
Download Status	Unknown
☑ Device is Active	
☑ Device is trusted	
MAC Address*	0050600646FB
Description	BJN Medianet EX60
Device Pool*	dp_apcbc-bjn — View Details
Common Device Configuration	< None > — View Details
Phone Button Template*	Standard Cisco TelePresence EX60

Protocol Specific Information

BLF Presence Group*	Standard Presence group
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco TelePresence EX60 - Standard SIP Non-Secu
Rerouting Calling Search Space	css_phone-bjn
SUBSCRIBE Calling Search Space	css_phone-bjn
SIP Profile*	Standard SIP Profile
Digest User	71056001 — Find
☐ Media Termination Point Required	
☐ Unattended Port	
☐ Require DTMF Reception	

© 2013 Cisco and/or its affiliates. All rights reserved.



© 2013 Cisco and/or its affiliates. All rights reserved.

SIP URI dialling on CUCM

- EX90 and EX60 Can now register natively to CUCM with a URI such as ‘example@cisco.com’
- Requires CUCM 9.0 or later
- Earlier CUCM versions requires numbers only (E164).
- Provisioning of alphanumeric URI is not supported in CUCM 9.0
  - DN Provisioning only via CUCM
  - Alphanumeric manually configured on endpoint

© 2013 Cisco and/or its affiliates. All rights reserved.

SIP URI Advantages

- VCS integration
- 3rd party integration
- AD integration

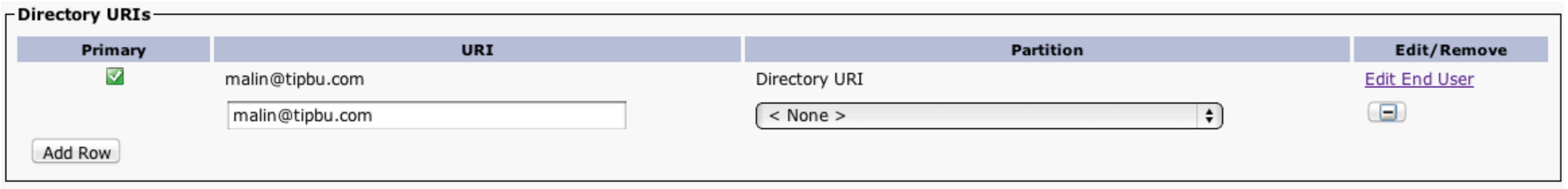
© 2013 Cisco and/or its affiliates. All rights reserved.

SIP URI Dialling

Case sensitive

myFineUri@cisco.com

- In CUCM 9.0 URIs are aliases for directory numbers (DN)
- DN registration is the main endpoint URI
  - Cisco Unified CM Administration->Device->Phone-><DEVICE>->Line [x]



© 2013 Cisco and/or its affiliates. All rights reserved.

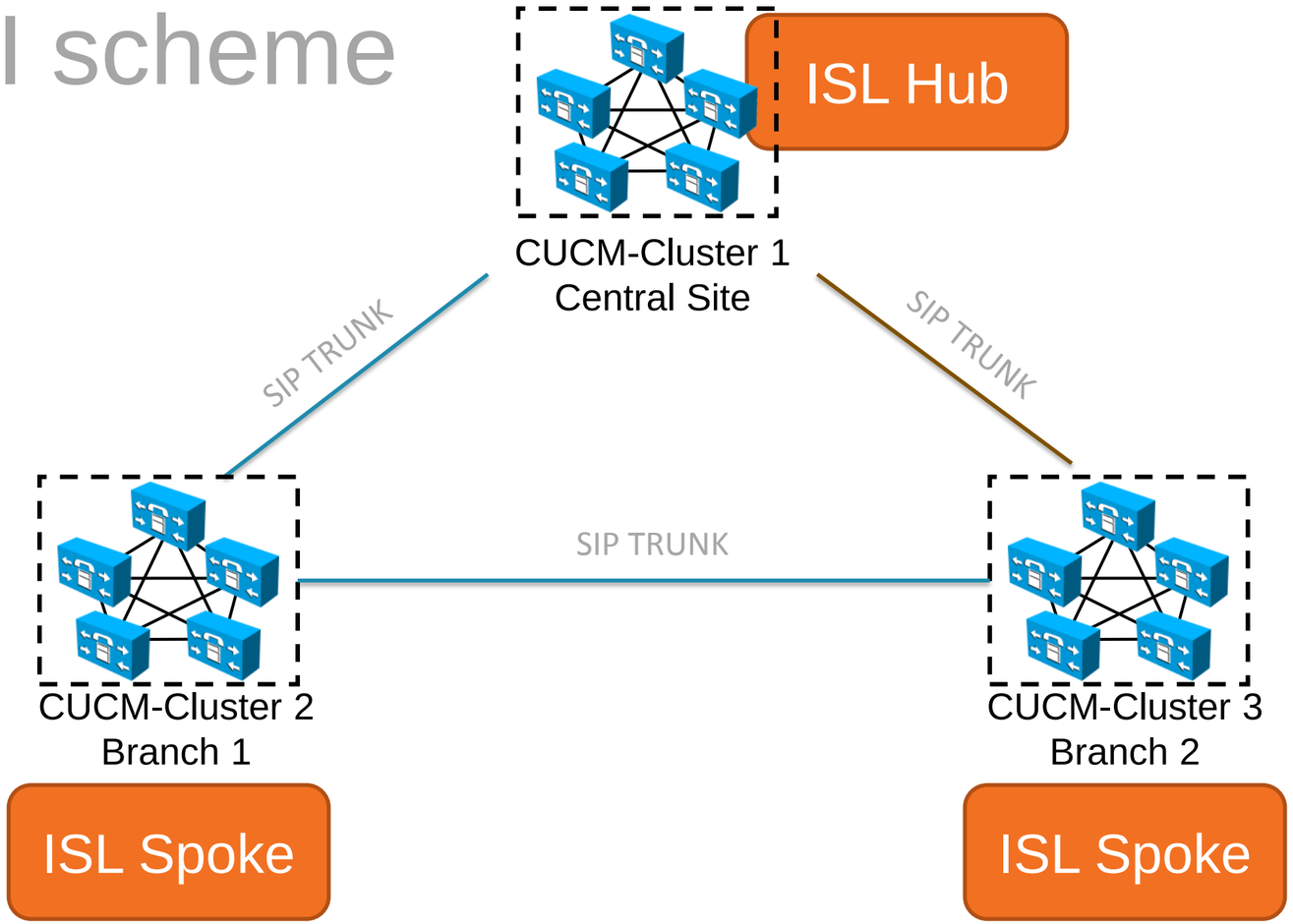
Support for URI Dialling

- URI calls between clusters can’t be routed using a prefix
- Multiple clusters can have the same domain suffix
  - No suffix based routing decisions
- Inter-Cluster Lookup Services (ILS) helps replicate respective catalog of registered URI
- ILS maps a URI to a cluster URI Route String.
  - Route the call to a SIP trunk using a SIP Route Pattern that matches the Cluster URI Route String.

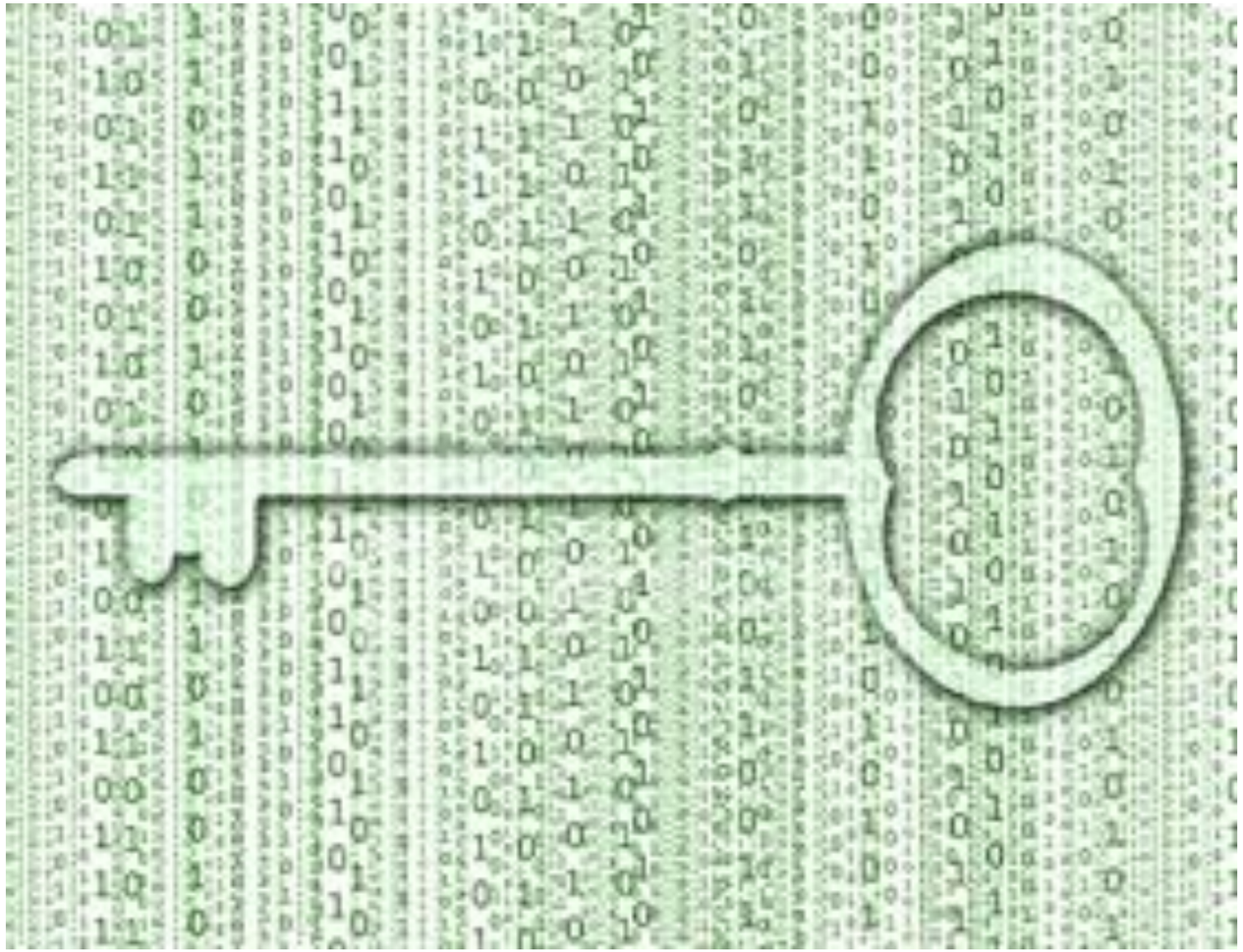
© 2013 Cisco and/or its affiliates. All rights reserved.

Support for URI Dialling

Flat URI scheme case



© 2013 Cisco and/or its affiliates. All rights reserved.



© 2013 Cisco and/or its affiliates. All rights reserved.

CUCM Encryption Refresher

- **CAPF (Certificate Authority Proxy Function):**
  - Process by which supported devices can request locally significant certificate by using Cisco Unified Communications Manager Administration. This servic runs normally in the publisher. It can also work as proxy to import certificates created by a different Certificate Authority (CA)
- **LSC (Locally Significant Certificates):**
  - A digital X.509v3 certificate that CAPF issues; installed on the end-point or JTAPI/TAPI/CTI application

© 2013 Cisco and/or its affiliates. All rights reserved.

- **CTL (Certificate Trust List):**
  - A file, which is created with the CTL Client (software installed on windows machine) and signed by the Cisco Site Administrator Security Token (USB token, order separately), that contains a list of certificates for servers that the end-point is to trust.
- **sRTP (Secure Real-Time Transport Protocol):**
  - Secure Real-Time Transport Protocol that secures voice conversation in the network and provides protection against replay attacks.

© 2013 Cisco and/or its affiliates. All rights reserved.

- **TLS (Transport Layer Security):**
  - Cryptographic protocol that provides secure and reliable data transfer between two systems or devices, by using secure ports and certificate exchange. TLS secures and controls connections among Cisco Unified Communications Manager-controlled systems, and devices. Functionally equivalent to SSL.
- **ITL (Identity Trust List)**:
  - Introduced in CUCM8.x onwards, contains the minimum list of certificates that are required by the end-point for authentication, decryption of Phone Configuration file and contacting the TVS service

© 2013 Cisco and/or its affiliates. All rights reserved.

CUCM Encryption

- The EX90 and EX60 now support encryption when registered to CUCM.
- Requires that CUCM security mode is installed and configured

Any version	Up to TE/TC 5.1	From TE 6.0
VCS	CUCM	CUCM
 	 	 
sRTP	No encryption available	CAPF/CTL, TLS/sRTP

© 2013 Cisco and/or its affiliates. All rights reserved.

Encryption in CUCM Environment

- CAPF using CTL
- Secure Real Time Protocol
- End to end security and trust
- No Configuration encryption

© 2013 Cisco and/or its affiliates. All rights reserved.

Room TelePresence

Encryption is showed on the screen (OSD)

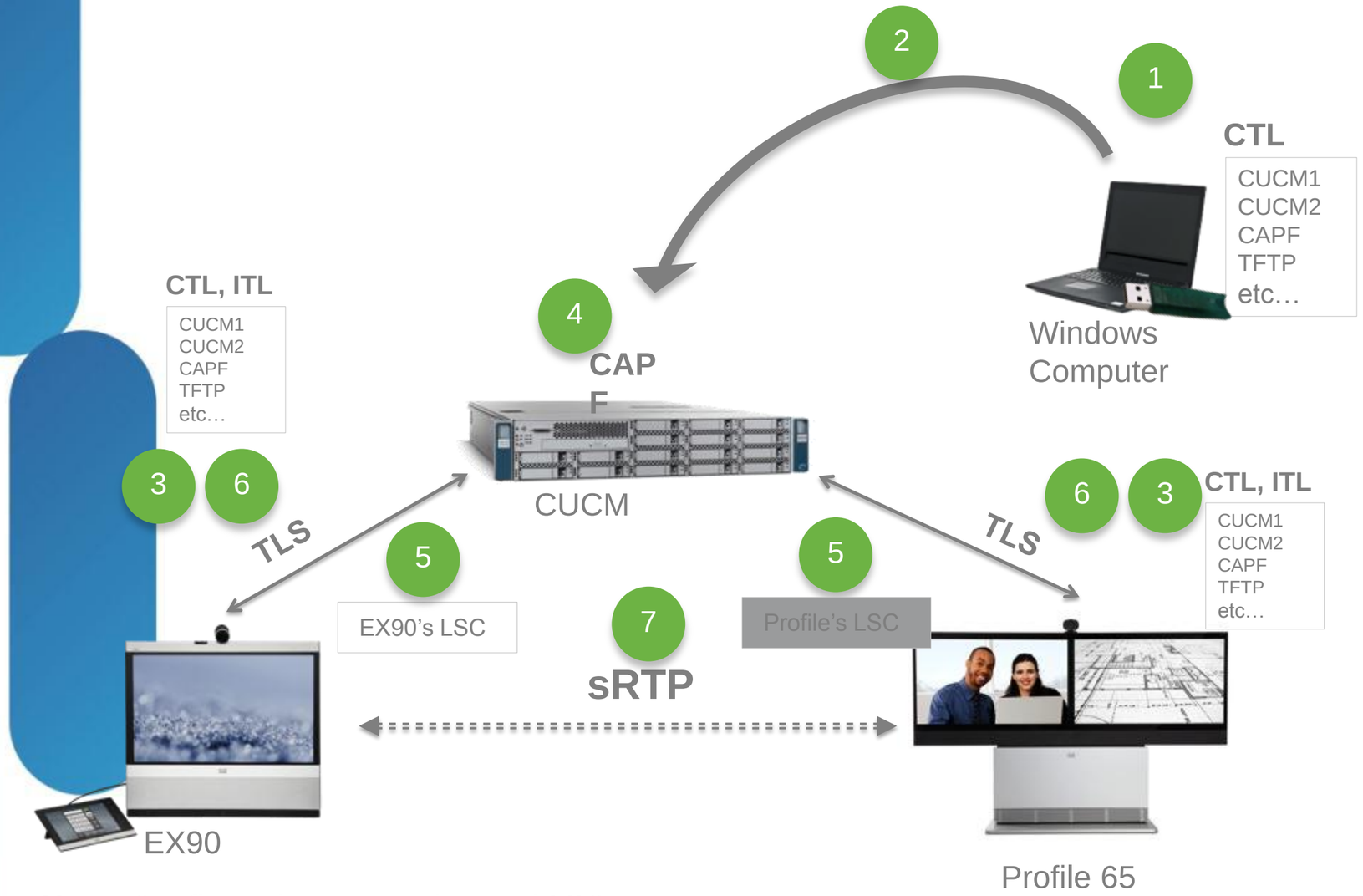
Personal TelePresence

Encryption is shown on the Touch UI

Main Benefit

A consistent encryption behaviour on all CUCM Registered Endpoints

© 2013 Cisco and/or its affiliates. All rights reserved.



Note: Configuration encryption and MIC are not available in TC/TE 6

1. Admin enables CAPF, and CTL provider on CUCM Cluster
2. Admin runs CTL app. CTL is created in CUCM and security mode set to mixed for the cluster
3. CTL, ITL and configuration are downloaded to end-point from TFTP while booting-up. Communication initiated by end-point
4. Each end-point uses CAPF Client to request a LSC from CUCM CAPF – end-point uses self signed certs– *
5. LSC downloaded to each end-point*
6. Secured communication is established between end-point and CUCM over TLS now using the LSC
7. sRTP between end-points is now possible

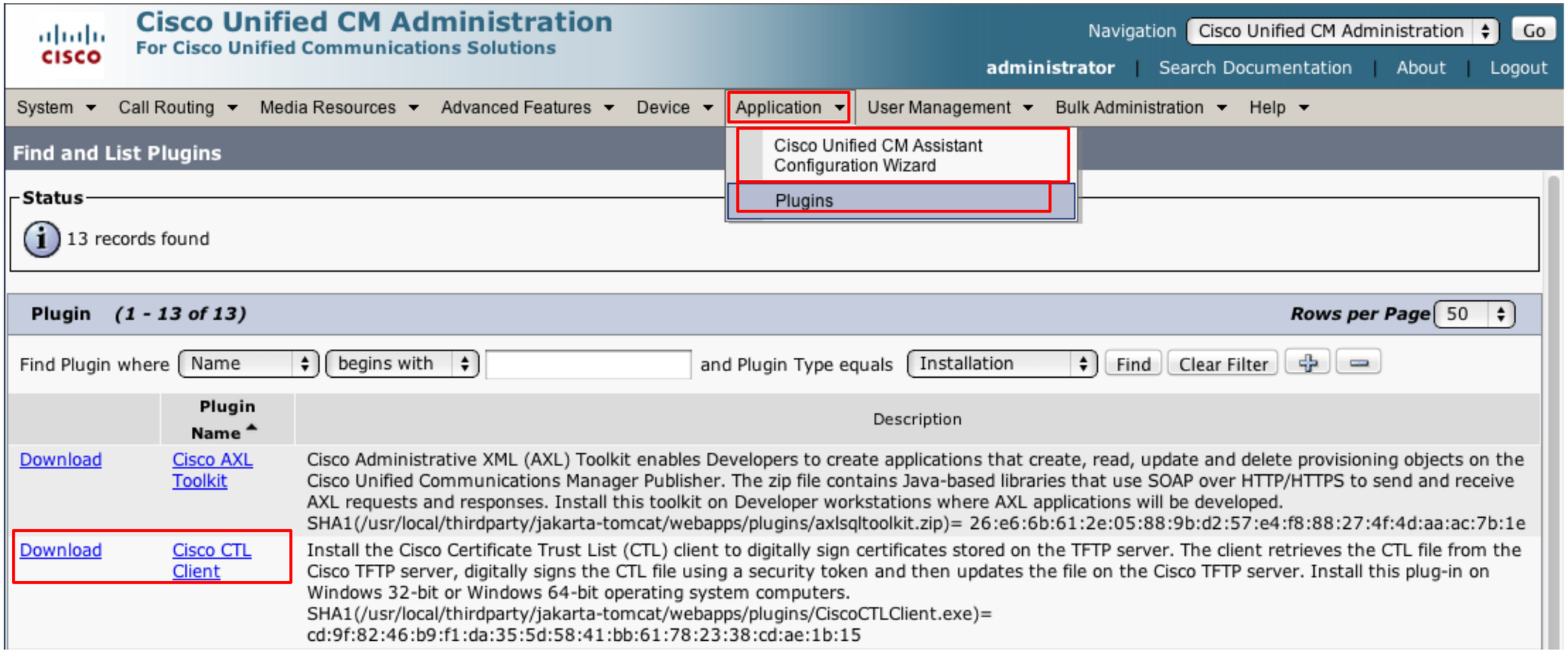
© 2013 Cisco and/or its affiliates. All rights reserved.

- When to delete the CTL/ITL?
  - Changing the CUCM IP address, or host name
  - Moving the end-point between CUCM clusters
  - Others (basically, anything that means re-generating/changing the CUCM certificate)
  - Security By Default (SBD CUCM >8.x) may cause troubles when getting the devices into secure mode the first time. In that case, delete the CTL from the end-point and try again
- You can always delete the CTL/ITL by going into the end-point configuration in the security section or by re-running the provisioning wizard*

© 2013 Cisco and/or its affiliates. All rights reserved.

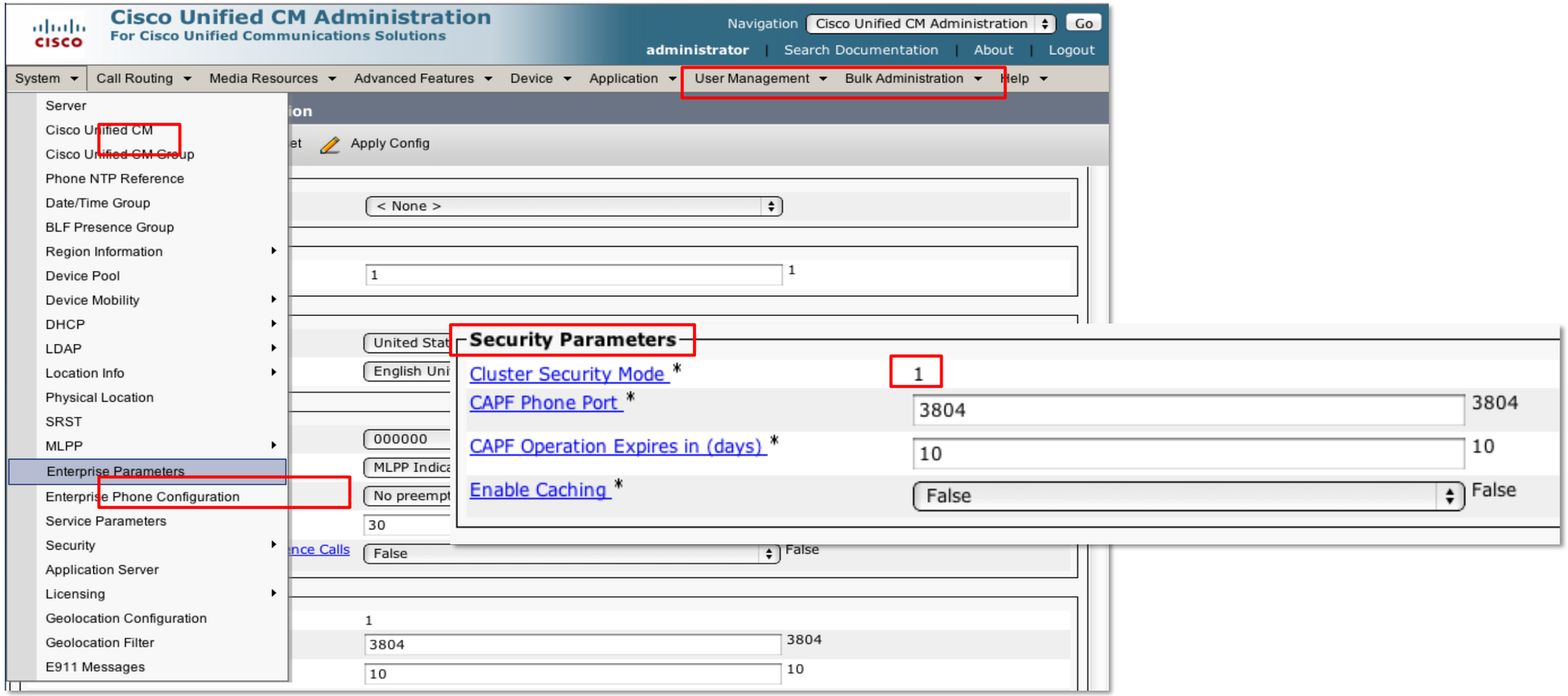
Configuring Security CUCM 9/TC6,TE6

- The CTL must be created. For this use the CTL plug-in in CM Administration->Application->Plugins



© 2013 Cisco and/or its affiliates. All rights reserved.

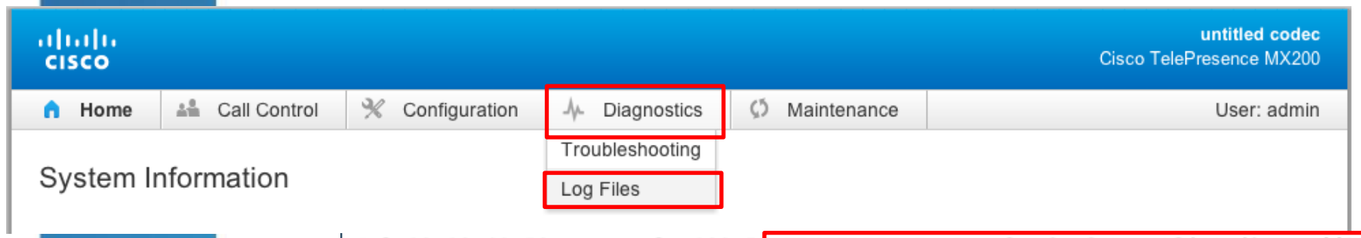
- Check mixed mode
  - CM Admin → System → Enterprise Parameters → Security Parameters.



© 2013 Cisco and/or its affiliates. All rights reserved.

- At this point any end-point connecting to the CUCM should be able to download the CTL/ITL and it’s configuration.

The best way to check if this is happening , is by looking at the logs in the end-point. The log file to look into is the application.log




```
Jul 19 10:48:59 ppc appl: 103.78 TRUSTLIST I: Download of trustlist 'http://10.1.100.12:6970/CTLSEP005060069bcf.tlv' complete
Jul 19 10:48:59 ppc appl: 103.84 DnsLocator I: recv() 0 naptr records
Jul 19 10:48:59 ppc appl: 103.85 DnsLocator I: srvQuery(s=_sips._tcp.cucm.tipbu.com)
Jul 19 10:48:59 ppc appl: 103.85 TRUSTLIST I: Download of trustlist 'http://10.1.100.12:6970/ITLSEP005060069bcf.tlv' complete
Jul 19 10:48:59 ppc appl: 103.94 PROV I: void CUCMProvision::CUCMProvisionUser::configItem() 'http://10.1.100.12:6970/SEP005060069bcf.cnf.xml.sgn'
Jul 19 10:48:59 ppc appl: 103.94 CAMERA I: CamVisca: Camera registered, noOfCameras=1
Jul 19 10:48:59 ppc appl: 103.99 CAMERA I: CamVisca::sendCAMPositionInd cameraId=1 pos=904/56/0/178
Jul 19 10:48:59 ppc appl: 104.20 MediaServerMsctrl I: Msf::localConnect(og=7,ig=3) video
Jul 19 10:48:59 ppc appl: 104.32 MediaStreamController I: MV::getVCSetting getOutputPortStatus initialized 0
Jul 19 10:48:59 ppc appl: 104.32 MediaStreamController I: MV::getVCSetting localHwCookieHint_ 32 w 704 h 576
Jul 19 10:48:59 ppc appl: 104.33 MediaStreamController I: MV::getVCSetting getOutputPortStatus initialized 1
Jul 19 10:48:59 ppc appl: 104.33 MediaStreamController I: MV::getVCSetting localHwCookieHint_ 24 w 1920 h 1080
Jul 19 10:48:59 ppc appl: 104.33 VIDEOLC-0 I: PowerManagement, request power save off
Jul 19 10:48:59 ppc appl: 104.36 VIDEOCTRL-0 I: (proxy,161) maximum number of framestorage slices 2
Jul 19 10:48:59 ppc appl: 104.45 PROV I: Ignoring upgrade to 's52000tc6_0_0_293305.pkg' (same as current)
Jul 19 10:49:00 ppc appl: 104.56 PROV I: void CUCMProvision::CUCMProvisionUser::report(bool) Provisioned Successfully
```

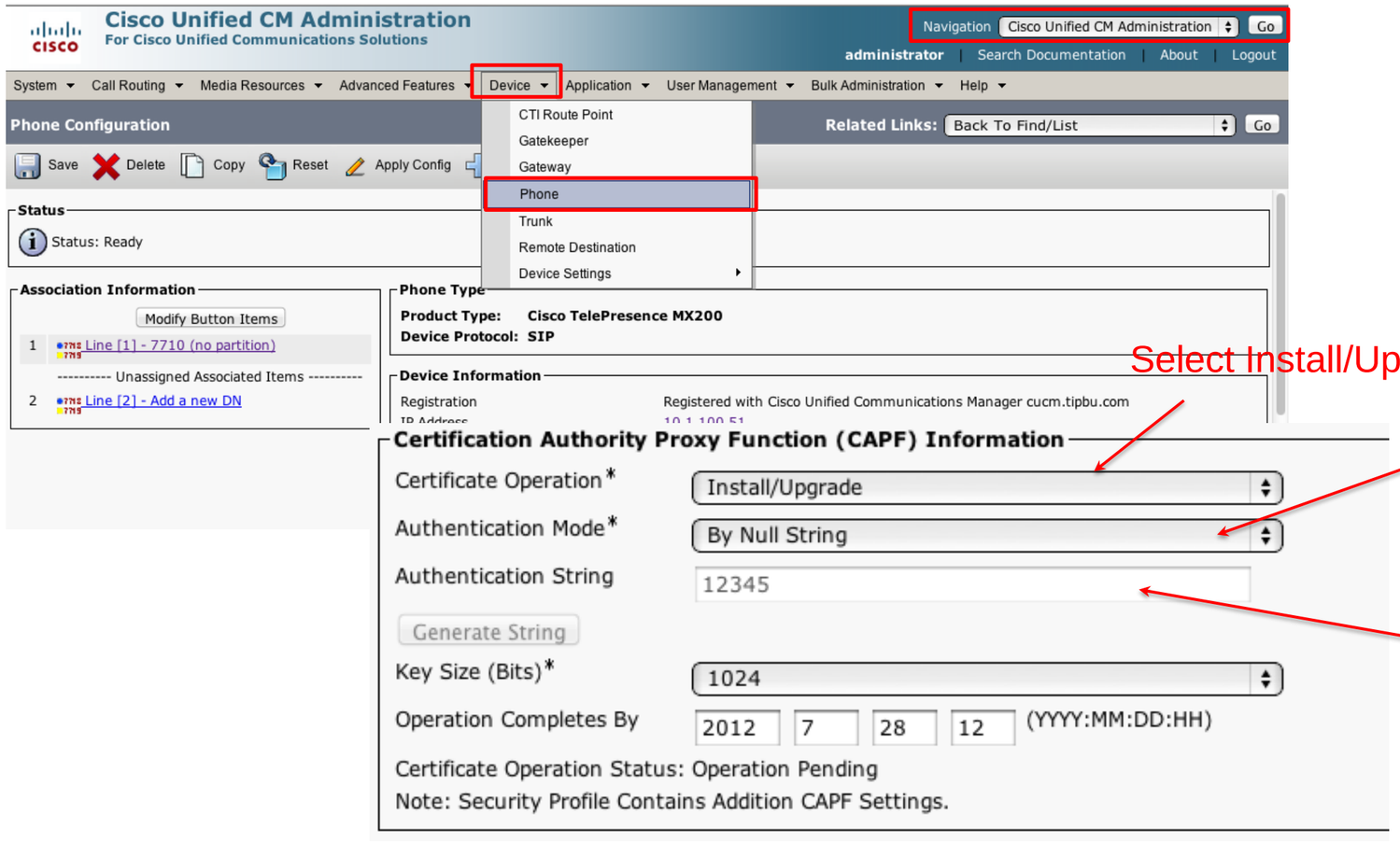
CTL

ITL

Configuration

© 2013 Cisco and/or its affiliates. All rights reserved.

- The LSC must be created by CAPF and sent to each end-point.
  - CM Administration → Device → SELECTED-ENDPOINT → CAPF Information



Select Install/Upgrade

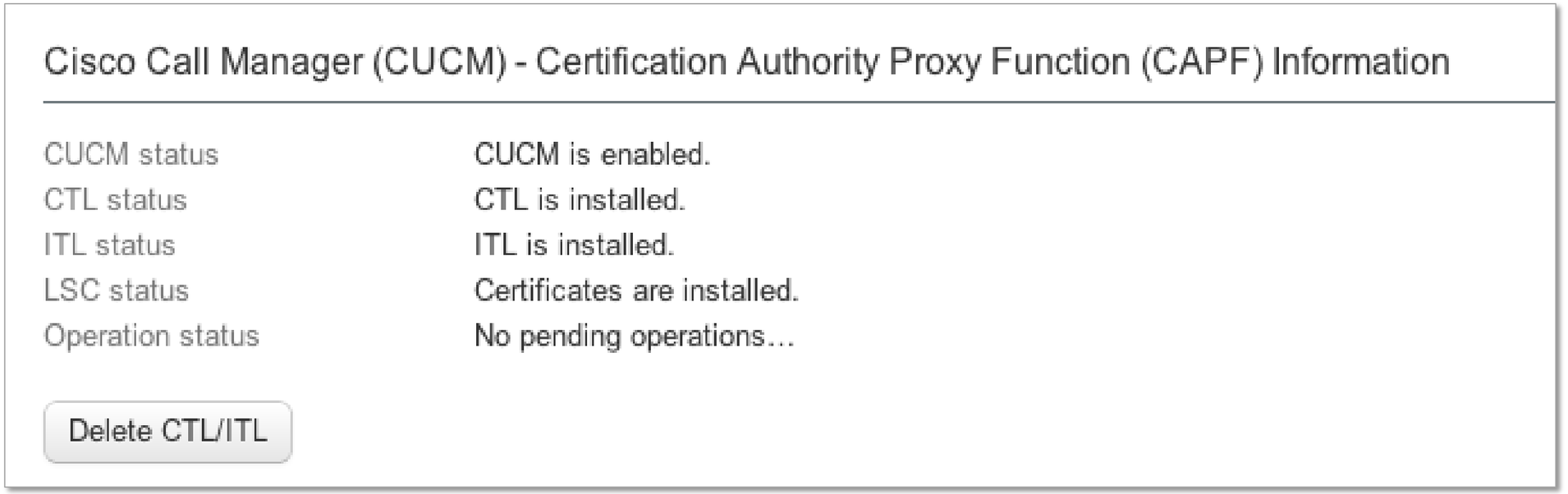
At the time of launching TE/TC 6, there is no MIC on these devices, therefore you can select only between *Null String*, or *Authentication String*

If By *Authentication String* has been chosen, you have to input a string here, and it should match the one to input in the end-point*

© 2013 Cisco and/or its affiliates. All rights reserved.

Troubleshooting CUCM Encryption

- Successful verification via web UI, Touch device or CLI

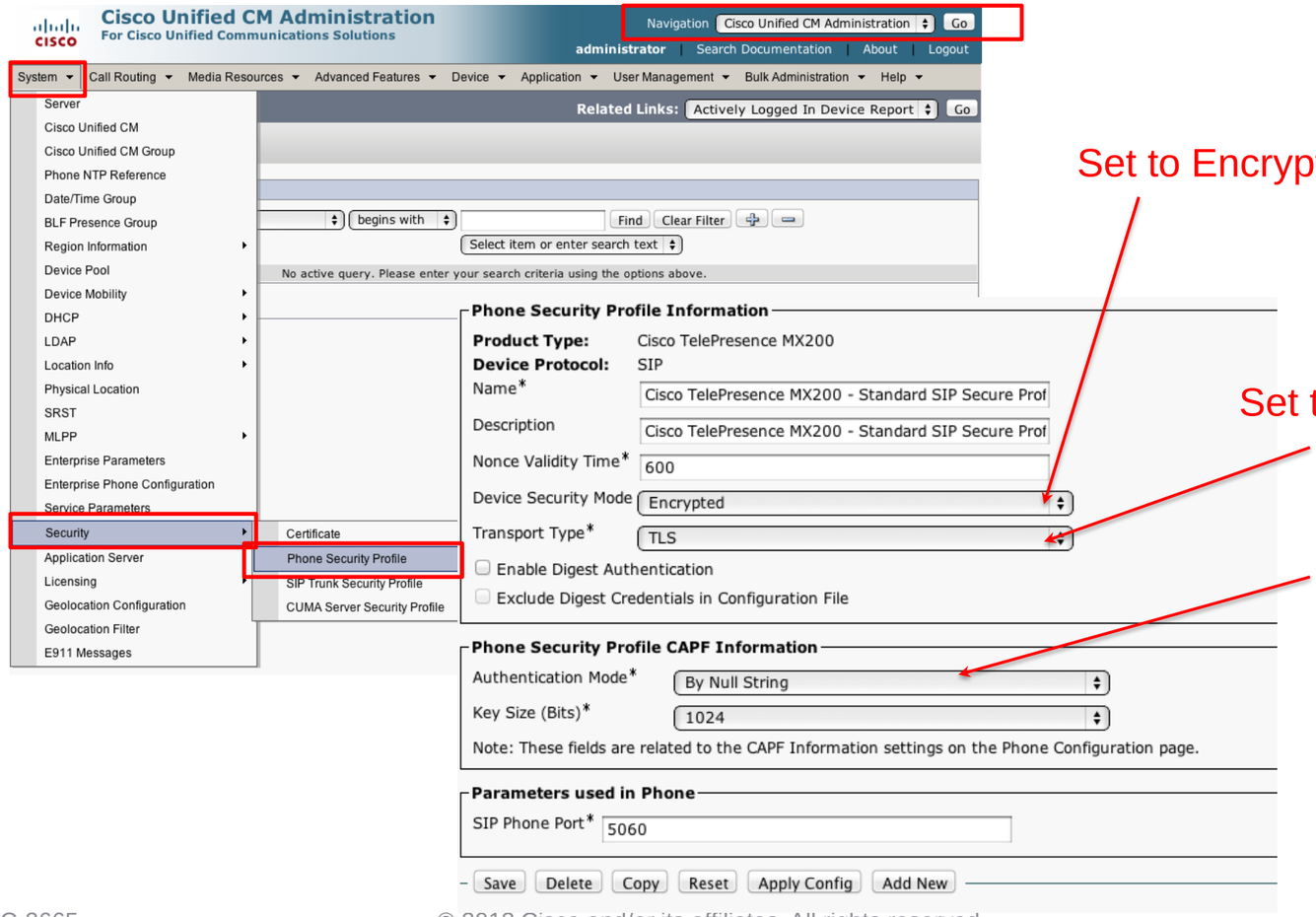


© 2013 Cisco and/or its affiliates. All rights reserved.

- CUCM encypted status can be checked using the ‘xstatus Provisioning CUCM xAPI:
  - *s Provisioning CUCM CAPF Mode: IgnoreAuth
  - *s Provisioning CUCM CAPF ServerName: "assip-cucm-3.rd.tandberg.com"
  - *s Provisioning CUCM CAPF ServerPort: 3804
  - *s Provisioning CUCM CAPF LSC: Installed
  - *s Provisioning CUCM CAPF OperationState: NonPending
  - *s Provisioning CUCM CAPF OperationResult: CAPFLSCUpdated
  - *s Provisioning CUCM ProvisionSecurity: Signed
  - *s Provisioning CUCM CTL State: Installed
- If LSC / CTL state is NOT 'Installed' the system is not able to connect securely to the CUCM

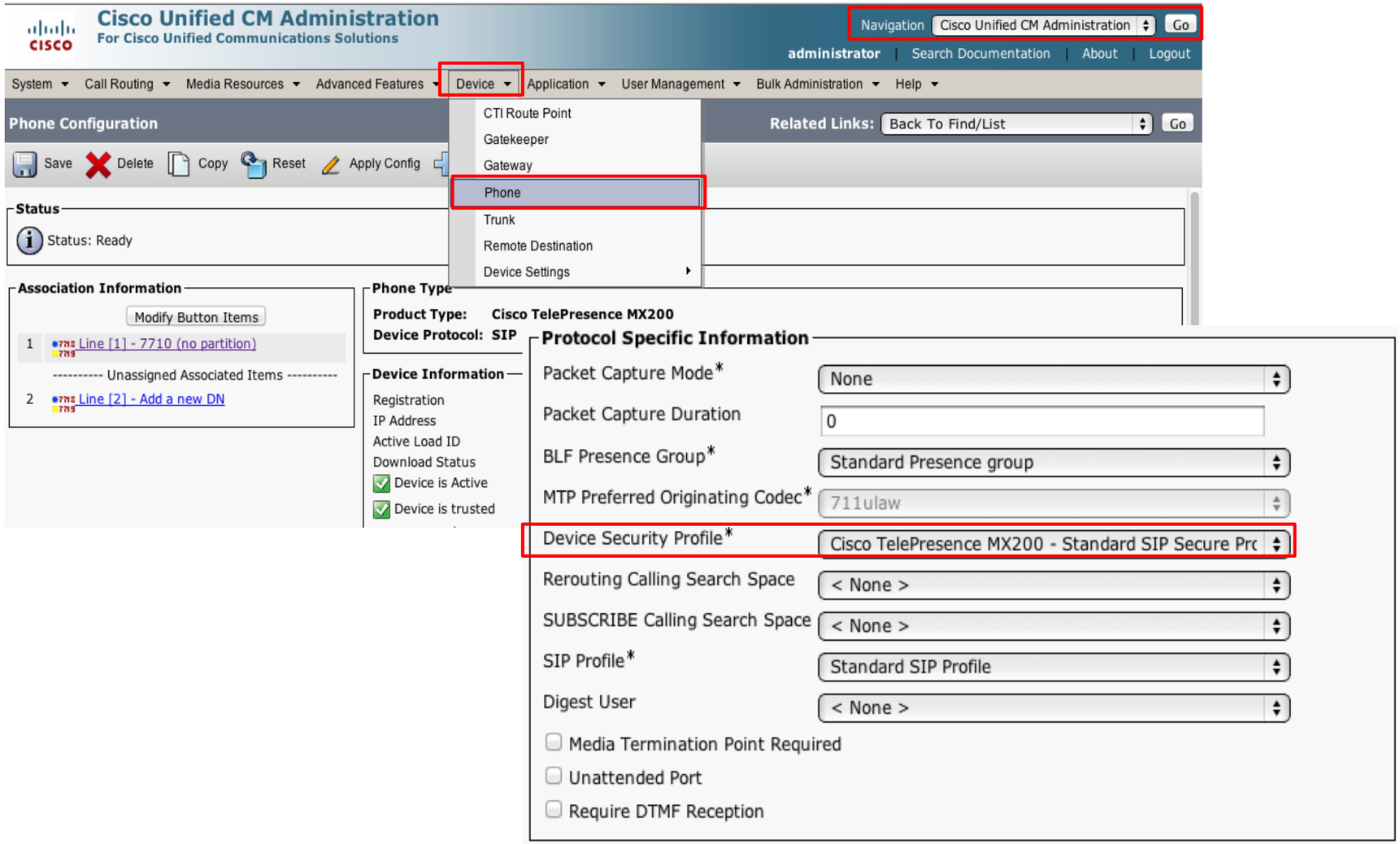
© 2013 Cisco and/or its affiliates. All rights reserved.

- Create the secured profiles



© 2013 Cisco and/or its affiliates. All rights reserved.

- Apply the secured profile to each device



© 2013 Cisco and/or its affiliates. All rights reserved.

Register the endpoint

- If endpoint is registered to CUCM in non-secure mode
  - *xConfiguration Provisioning Mode:off*
  - *xCommand Provisioning CUCM CTL Delete*
  - *xConfiguration Provisioning ExternalManager* Address: <dns/ip-address to the CUCM>
  - *xConfiguration Provisioning Mode:CUCM*

© 2013 Cisco and/or its affiliates. All rights reserved.

- CUCM and end-point communication Traces before Encryption

Source	Destination	Protocol	Info
10.1.100.53	cucm.tipbu.com	SIP	Request: REGISTER sip:cucm.tipbu.com (application/x-cisco-remotecc-request+xml)
cucm.tipbu.com	10.1.100.53	SIP	Status: 100 Trying (0 bindings)
cucm.tipbu.com	10.1.100.53	SIP	Status: 200 OK (1 bindings)
cucm.tipbu.com	10.1.100.53	SIP	Request: REFER sip:7702@10.1.100.53:59080
cucm.tipbu.com	10.1.100.53	SIP	Request: NOTIFY sip:7702@10.1.100.53:59080 (text/plain)
cucm.tipbu.com	10.1.100.53	SIP	Request: NOTIFY sip:36e6ff87-81d2-c05d-3e98-8496f30ca54d@10.1.100.53:59080;transport=tcp
cucm.tipbu.com	10.1.100.53	SIP	Request: SUBSCRIBE sip:36e6ff87-81d2-c05d-3e98-8496f30ca54d@10.1.100.53:59080
10.1.100.53	cucm.tipbu.com	SIP	Status: 200 OK
10.1.100.53	cucm.tipbu.com	SIP	Status: 481 Subscription does not exist
10.1.100.53	cucm.tipbu.com	SIP	Status: 200 OK
10.1.100.53	cucm.tipbu.com	SIP	Status: 200 OK
10.1.100.53	cucm.tipbu.com	SIP	Request: NOTIFY sip:7702@10.1.100.12:5060;transport=tcp
cucm.tipbu.com	10.1.100.53	SIP	Status: 200 OK
10.1.100.53	cucm.tipbu.com	SIP	Request: SUBSCRIBE sip:7702@cucm.tipbu.com
cucm.tipbu.com	10.1.100.53	SIP	Status: 200 OK
cucm.tipbu.com	10.1.100.53	SIP	Request: NOTIFY sip:36e6ff87-81d2-c05d-3e98-8496f30ca54d@10.1.100.53:59080;transport=tcp
10.1.100.53	cucm.tipbu.com	SIP	Status: 200 OK
10.1.100.53	cucm.tipbu.com	SIP	Request: NOTIFY sip:7702@10.1.100.12:5060;transport=tcp
cucm.tipbu.com	10.1.100.53	SIP	Status: 200 OK

cucm.tipbu.com = 10.1.100.12
MX200 = 10.1.100.53

© 2013 Cisco and/or its affiliates. All rights reserved.

- Call between two end-points traces before encryption

10.1.100.51	10.1.100.53	RTP	PT=MP4A-LATM, SSRC=0xAD49C35F, Seq=2341, Time=1713868285
10.1.100.51	10.1.100.53	RTP	PT=MP4A-LATM, SSRC=0xAD49C35F, Seq=2342, Time=1713870085
10.1.100.51	10.1.100.53	RTP	PT=MP4A-LATM, SSRC=0xAD49C35F, Seq=2343, Time=1713871885
10.1.100.51	10.1.100.53	RTP	PT=MP4A-LATM, SSRC=0xAD49C35F, Seq=2344, Time=1713873685
10.1.100.51	10.1.100.53	RTP	PT=MP4A-LATM, SSRC=0xAD49C35F, Seq=2345, Time=1713875485
10.1.100.51	10.1.100.53	RTP	PT=MP4A-LATM, SSRC=0xAD49C35F, Seq=2346, Time=1713877285
10.1.100.51	10.1.100.53	H264	PT=H264, SSRC=0xE363E6C9, Seq=39167, Time=3392998479 NAL unit - Sequence parameter set
10.1.100.51	10.1.100.53	H264	PT=H264, SSRC=0xE363E6C9, Seq=39168, Time=3392998479 NAL unit - Picture parameter set
10.1.100.51	10.1.100.53	H264	PT=H264, SSRC=0xE363E6C9, Seq=39169, Time=3392998479 FU-A
10.1.100.51	10.1.100.53	H264	PT=H264, SSRC=0xE363E6C9, Seq=39170, Time=3392998479 FU-A
10.1.100.51	10.1.100.53	H264	PT=H264, SSRC=0xE363E6C9, Seq=39171, Time=3392998479 FU-A
10.1.100.51	10.1.100.53	H264	PT=H264, SSRC=0xE363E6C9, Seq=39172, Time=3392998479 FU-A
10.1.100.51	10.1.100.53	H264	PT=H264, SSRC=0xE363E6C9, Seq=39173, Time=3392998479 FU-A
10.1.100.51	10.1.100.53	H264	PT=H264, SSRC=0xE363E6C9, Seq=39174, Time=3392998479 FU-A
10.1.100.51	10.1.100.53	H264	PT=H264, SSRC=0xE363E6C9, Seq=39175, Time=3392998479 FU-A
10.1.100.51	10.1.100.53	H264	PT=H264, SSRC=0xE363E6C9, Seq=39176, Time=3392998479 FU-A
10.1.100.51	10.1.100.53	H264	PT=H264, SSRC=0xE363E6C9, Seq=39177, Time=3392998479 FU-A
10.1.100.51	10.1.100.53	RTP	PT=MP4A-LATM, SSRC=0xAD49C35F, Seq=2347, Time=1713879085

EX60 = 10.1.100.51
MX200 = 10.1.100.53

© 2013 Cisco and/or its affiliates. All rights reserved.

- CUCM and end-point communication Traces after Encryption

10.1.100.53	cucm.tipbu.com	TCP	39322 > sip-tls [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=4294764964 TSecr=38403276
10.1.100.53	cucm.tipbu.com	TLSv1	Client Hello
cucm.tipbu.com	10.1.100.53	TCP	sip-tls > 39322 [ACK] Seq=1 Ack=262 Win=6912 Len=0 TSval=38404088 TSecr=4294765773
cucm.tipbu.com	10.1.100.53	TLSv1	Server Hello, Certificate, Certificate Request, Server Hello Done
10.1.100.53	cucm.tipbu.com	TCP	39322 > sip-tls [ACK] Seq=262 Ack=793 Win=16192 Len=0 TSval=4294765822 TSecr=38404088
10.1.100.53	cucm.tipbu.com	TLSv1	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
cucm.tipbu.com	10.1.100.53	TCP	sip-tls > 39322 [ACK] Seq=793 Ack=1922 Win=12672 Len=0 TSval=38404408 TSecr=4294766093
cucm.tipbu.com	10.1.100.53	TLSv1	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
10.1.100.53	cucm.tipbu.com	TCP	39322 > sip-tls [ACK] Seq=1922 Ack=1651 Win=17920 Len=0 TSval=4294766101 TSecr=38404412
10.1.100.53	cucm.tipbu.com	TLSv1	Application Data, Application Data
cucm.tipbu.com	10.1.100.53	TCP	sip-tls > 39322 [ACK] Seq=1651 Ack=3468 Win=15616 Len=0 TSval=38404576 TSecr=4294766263
cucm.tipbu.com	10.1.100.53	TLSv1	Application Data, Application Data
10.1.100.53	cucm.tipbu.com	TCP	39322 > sip-tls [ACK] Seq=3468 Ack=2045 Win=19616 Len=0 TSval=4294766265 TSecr=38404576
cucm.tipbu.com	10.1.100.53	TLSv1	Application Data, Application Data
cucm.tipbu.com	10.1.100.53	TLSv1	Application Data, Application Data
cucm.tipbu.com	10.1.100.53	TLSv1	Application Data, Application Data
10.1.100.53	cucm.tipbu.com	TCP	39322 > sip-tls [ACK] Seq=3468 Ack=3127 Win=21792 Len=0 TSval=4294766272 TSecr=38404584
10.1.100.53	cucm.tipbu.com	TCP	39322 > sip-tls [ACK] Seq=3468 Ack=3953 Win=23968 Len=0 TSval=4294766273 TSecr=38404584
10.1.100.53	cucm.tipbu.com	TCP	39322 > sip-tls [ACK] Seq=3468 Ack=4635 Win=26112 Len=0 TSval=4294766273 TSecr=38404584
cucm.tipbu.com	10.1.100.53	TLSv1	Application Data, Application Data
cucm.tipbu.com	10.1.100.53	TLSv1	Application Data, Application Data

cucm.tipbu.com = 10.1.100.12
MX200 = 10.1.100.53

© 2013 Cisco and/or its affiliates. All rights reserved.

- Call between two end-points traces after encryption

10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16394 Destination port: 16414
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 16416
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 1
10.1.100.51	10.1.100.53	UDP	Source port: 16396 Destination port: 1

EX60 = 10.1.100.51
MX200 = 10.1.100.53

© 2013 Cisco and/or its affiliates. All rights reserved.

Scalable Ad-hoc Conferencing

Seamless escalation to multi-party conferencing

Scalable and effective use of conferencing resources

Automatic de-escalation from multipoint to point-to-point

© 2013 Cisco and/or its affiliates. All rights reserved.

Ad-hoc Conferencing

Endpoint
Multisite

- Extra Audio Call
- Embedded Multisite (licence)

CUCM
Media Resource

- Escalate to CUCM MCU
- Dynamic deescalation
- Future platform

VCS
Multiway

- Escalate to VCS MCU
- No deescalation
- Legacy

© 2013 Cisco and/or its affiliates. All rights reserved.

UC Manager Ad Hoc Conferencing

- When configured, UCM MCU Ad Hoc Conferencing will be dominant over embedded Multisite
- “As Needed” dynamic escalation TO an MCU or de-escalation FROM an MCU (better port management)

© 2013 Cisco and/or its affiliates. All rights reserved.

UCM remote-cc

- Only supported by Cisco SCCP and SIP endpoints using Cisco-proprietary SIP remote-cc extensions
- Allows chains to occur in many circumstances
- Provides telephony-like UE including early-attended, and CTI/3PCC support
- Proper recovery handling and de-escalating back to pt-to-pt
- Centralised (per UCM cluster) policies

© 2013 Cisco and/or its affiliates. All rights reserved.

Ad Hoc Conferencing Configuration

- On the MCU, configuring settings

1. Go to **Settings > Conferences**.

2. Configure the fields on the MCU as follows:

MCU Setting	Value	Comment
Media port reservation	Enabled	
Incoming calls to unknown conferences or auto attendants	Disconnect caller	

3. Click **Apply changes**.

© 2013 Cisco and/or its affiliates. All rights reserved.

On Unified CM, configuring conference features

To configure conference features such as the maximum number of participants:

1. Go to **System > Service Parameters**.
2. Select the relevant Unified CM Server.
3. Select the **Cisco CallManager (Active)** as the service.
4. Select **Advanced** to show advanced options.
5. Configure the **Clusterwide Parameters (Feature - Conference)** section as required.

© 2013 Cisco and/or its affiliates. All rights reserved.

On Unified CM, adding the MCU

Add the MCU to Unified CM as a manageable device as follows:

1. Go to **Media Resources > Conference Bridge**.
2. Click **Add New**.
3. Select **Conference Bridge Type** as **Cisco TelePresence MCU**.
4. Enter relevant fields and click **Save**.

© 2013 Cisco and/or its affiliates. All rights reserved.

TelePresence MCU with Unified CM

Conference Bridge Information

Conference Bridge : mcu0aTTGTME (mcu0aTTGTME)
Registration: Registered with Cisco Unified Communications Manager ttgtmecucm1
IP Address: 172.19.236.207

MCU Conference Bridge Info

Conference Bridge Type*	Cisco TelePresence MCU
Device is trusted	
Conference Bridge Name*	mcu0aTTGTME
Destination Address*	172.19.236.207
Description	mcu0aTTGTME
Device Pool*	Default
Common Device Configuration	< None >
Location*	Hub_None
Use Trusted Relay Point*	Default

SIP Interface Info

Unified CM SIP Port*	5060
MCU Conference Bridge SIP Port*	5060

HTTP Interface Info

Username*	admin
Password*	•••••••••
Confirm Password*	•••••••••
HTTP Port*	80

© 2013 Cisco and/or its affiliates. All rights reserved.

- On Unified CM, configuring a media resource group list

1. Go **Media Resources > Media Resource Group**.
2. Click **Add New**.
3. Choose a name and move the MCU(s) into the **Selected Media Resources** area.
4. Click **Save**.
5. Go to **Media Resources > Media Resource Group List**.
6. Click **Add New**.
7. Choose a name and move the created Media Resource Groups into the **Selected Media Resource Groups** area.
8. Click **Save**.

© 2013 Cisco and/or its affiliates. All rights reserved.

- On Unified CM, assign a MRGL to a device

1. Go to **Device > Phone**.
2. Select a device.
3. Choose the **Media Resource Group List** that you created earlier.
4. Click **Save**.

© 2013 Cisco and/or its affiliates. All rights reserved.

- All centralised configuration
- Added as a TelePresence MCU in CUCM
- Set Multipoint settings to <<Use MRGL>>
  - Default for EX90 is «Use Endpoint»
  - Default for EX60 is «Use Media Resource Group List»
- The setup can be verified by running *xstatus Conference UseBuiltInBridge*

© 2013 Cisco and/or its affiliates. All rights reserved.

What's Cisco MediaNet – Mediatraces

Medianet is

An Architecture/Blueprint for successful deployment of multiple media and business critical applications

Medianet is **not**

A product, SKU, or a marketecture to describe just QoS/CAC

Mediatraces is

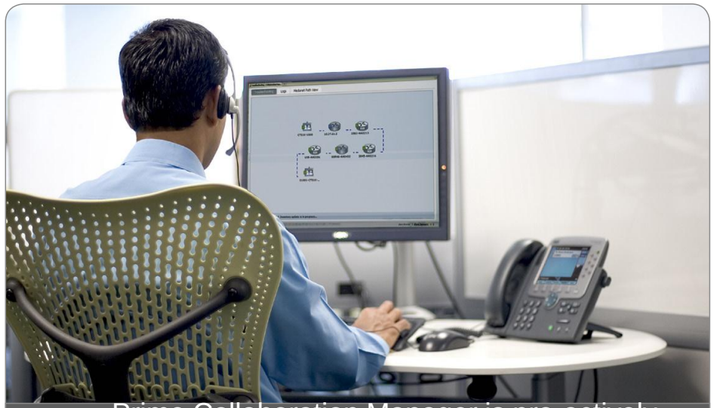
A Cisco IOS feature that discovers the routers and switches along the path of an IP flow, and collects critical information hop by hop on specific media streams as they traverse the network. It's a diagnostic tool similar to traceroute, that should be enabled on each of the network nodes you want to collect information from.

© 2013 Cisco and/or its affiliates. All rights reserved.

MediaNet – Mediatraces

1. We're having bad image, what do we do?

TP Room 1
Room with poor video quality



2. Prime Collaboration Manager is pro-actively informing that TP room 1 is suffering congestion

Administrator in front of PC detecting that there is a problem

3. With few clicks administrators can fix the routers issues remotely

Administrator fixing the problem

4. Oh!, Now it's fixed, and we didn't do anything

Great quality re-established

© 2013 Cisco and/or its affiliates. All rights reserved.

MediaNet – Mediatraces

TelePresence

Physical Security

HTTP Streams

- Video marked as “TelePresence” at origin
- Monitor only the flows that matters
- Sift through mountains of data
- No deep packet inspection (DPI)
- Works for encrypted calls

© 2013 Cisco and/or its affiliates. All rights reserved.

MediaNet – Mediatraces

- Mediatraces information collection methods
  - Exec command to perform on-demand collection of statistics (reactive method)
  - By configuring Cisco Mediatrace to start a recurring monitoring session at a specific time and on specific days (pro-active method)
- Cisco Prime Collaboration is a proactive tool

© 2013 Cisco and/or its affiliates. All rights reserved.

Medianet –Metadata

- The Medianet metadata = Application information
- OOB = Encryption friendly
- Leverages RSVP as a transport with a second 5-tuple
  - Follows same path as media

© 2013 Cisco and/or its affiliates. All rights reserved.

Medianet – Mediatrace

New in TE/TC/TX 6.0:
TelePresence end-points will include a MediaNet MSI that sends application ID/Globally Unique Session ID as part of the traffic stream and session set up

Media Services Interface (MSI): is a software component that enables end-points to consistently take advantage of intelligent network services to improve the quality of experience and reduce the cost of deployment and operations.

© 2013 Cisco and/or its affiliates. All rights reserved.

Display CDP information

- xstat network 1 CDP
  - *s Network 1 CDP Platform: "cisco WS-C3750X-48P"
  - *s Network 1 CDP Version: "Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version 15.0(1)SE2, RELEASE SOFTWARE (fc3)*Technical Support: http://www.cisco.com/techsupport*Copyright (c) 1986-2011 by Cisco Systems, Inc.*Compil Thu 22-Dec-11 00:05 by prod_rel_team"
  - *s Network 1 CDP Capabilities: "0x0029"
  - *s Network 1 CDP DeviceId: “XXXX.cisco.com"
  - *s Network 1 CDP PortID: "GigabitEthernet2/0/3"
  - *s Network 1 CDP Duplex: "Full"
  - *s Network 1 CDP VTPMgmtDomain: ""
  - *s Network 1 CDP Address: ”X.X.X.X"
  - *s Network 1 CDP PrimaryMgmtAddress: “X.X.X.X"
  - *s Network 1 CDP SysName: ""
  - *s Network 1 CDP SysObjectID: ""
  - *s Network 1 CDP VoIPApplianceVlanID: "300"
  - ** end

© 2013 Cisco and/or its affiliates. All rights reserved.

CTI/JTAPI Support

- EX90 and EX60 support JTAPI
- Cisco Remote expert 1.8 is now supported.

© 2013 Cisco and/or its affiliates. All rights reserved.

Remote Expert Support

- CTI in TE6/CUCM 9.0 is limited to the Remote Expert solution
  - CTI Monitoring of device availability
  - CTI Remote Call Control (remote-cc)
- Jabber 9 can control EX Series, however not officially supported
  - CTI basic call features supported in Experimental Mode:
  - Call, Accept, Transfer, Hold, Resume, Click to Call (websites)

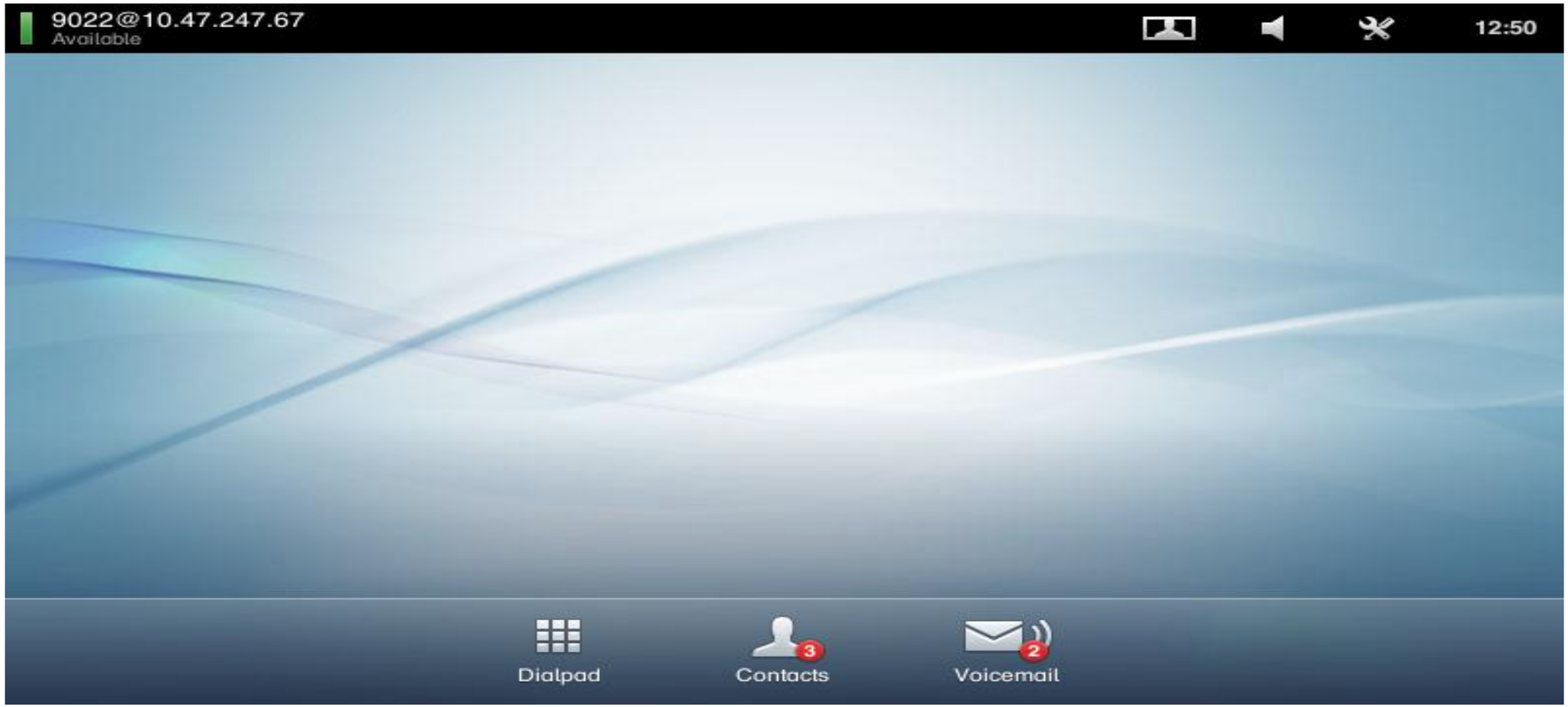
© 2013 Cisco and/or its affiliates. All rights reserved.

Voicemail

- The EX90 and EX60 support Voicemail
  - *xconfiguration SIP Profile 1 Mailbox: "voicemail@cisco.com"*
- When a mailbox is configured, a Voicemail icon will be displayed on the bottom right side of the main menu.
- Message waiting indicator badge showing number of new messages.
- Only CUCM is supported for message waiting indicator badge

© 2013 Cisco and/or its affiliates. All rights reserved.

Voicemail with MWI



© 2013 Cisco and/or its affiliates. All rights reserved.

Voicemail Integration Guiding Principles

- Unity can be integrated with UCM, or with VCS, or both (dual integration)
  - *VCS X6.1 supports direct SIP integration with Unity*
  - *VCS X7.0 adds support for receiving and responding to the diversion header sent by UCM when Unity integration is via UCM*
- Unity Voicemail does not support alpha-numeric URIs
  - *Unity voicemail pilot number must be a numeric address*
  - *Subscribers must have numeric addresses and their numeric addresses must be used in the diversion headers sent to Unity*
  - *Callers leaving a message for a subscriber must have a numeric address or else the subscriber will not be able to reply to message or call back the sender*
- Unity supports KPML and RFC 2833 DTMF
  - *VC endpoints and H.320 gateways must support either KPML or RFC 2833*
- Message Waiting Indication (MWI) is supported with TE6

© 2013 Cisco and/or its affiliates. All rights reserved.

Voicemail Integration Summary

- All UCM endpoints can be assigned a voicemail profile
- If Unity is connected to UCM, and a VCS endpoint is diverted to voicemail, VCS must be X7.0 or greater
- If Unity is directly integrated with VCS, and a VCS endpoint is diverted to voicemail, VCS must be X6.1 or greater
- VCS endpoints must have a numeric address in order to work properly with voicemail

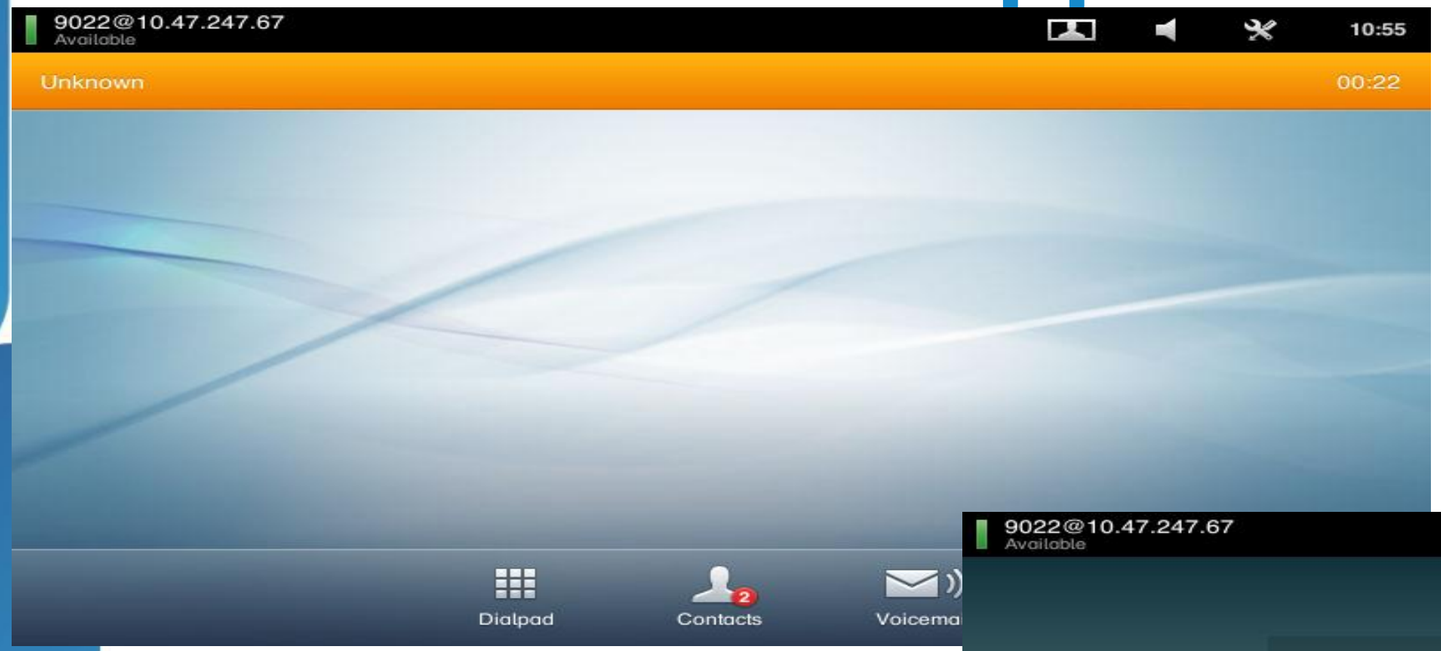
© 2013 Cisco and/or its affiliates. All rights reserved.

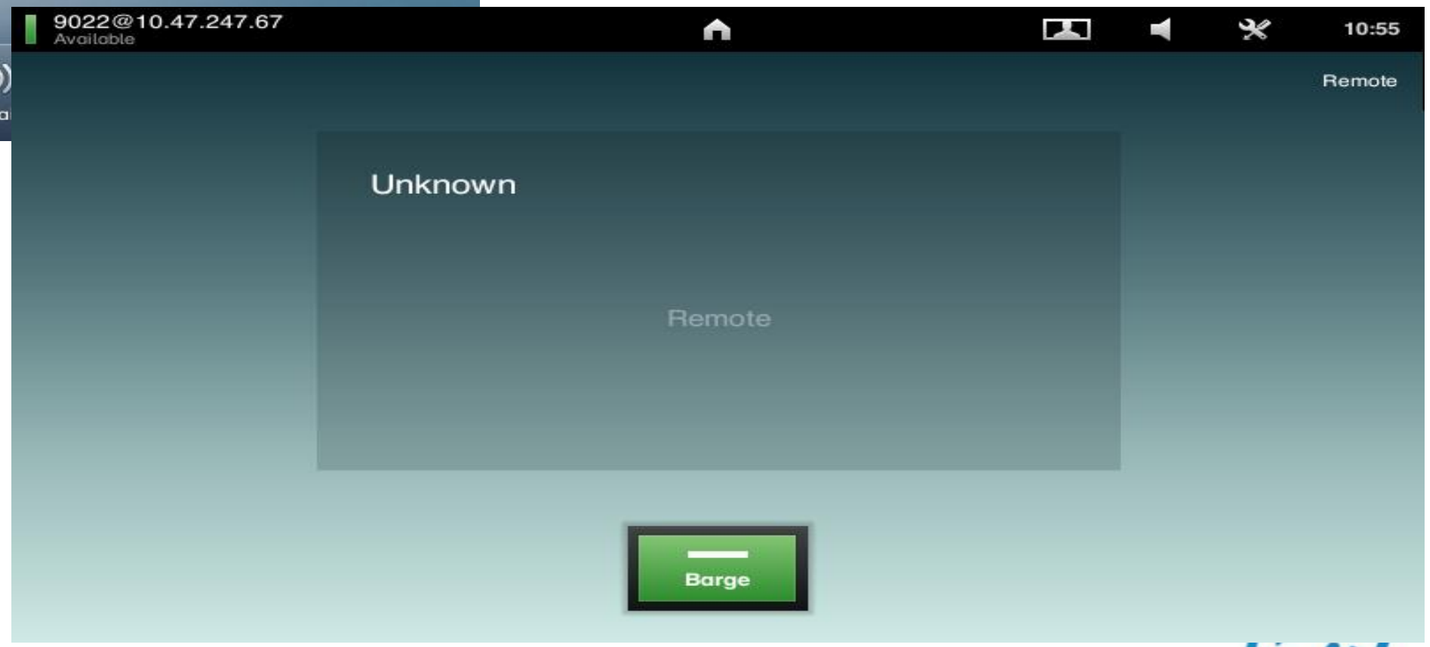
Shared Lines Support

- EX90 and EX60 now supports shared lines on CUCM.
- Barge call is supported
  - Requires TP MCU resources to support video barge
  - CUCM resources only support audio conferencing
- Supports Resume Remote.

© 2013 Cisco and/or its affiliates. All rights reserved.

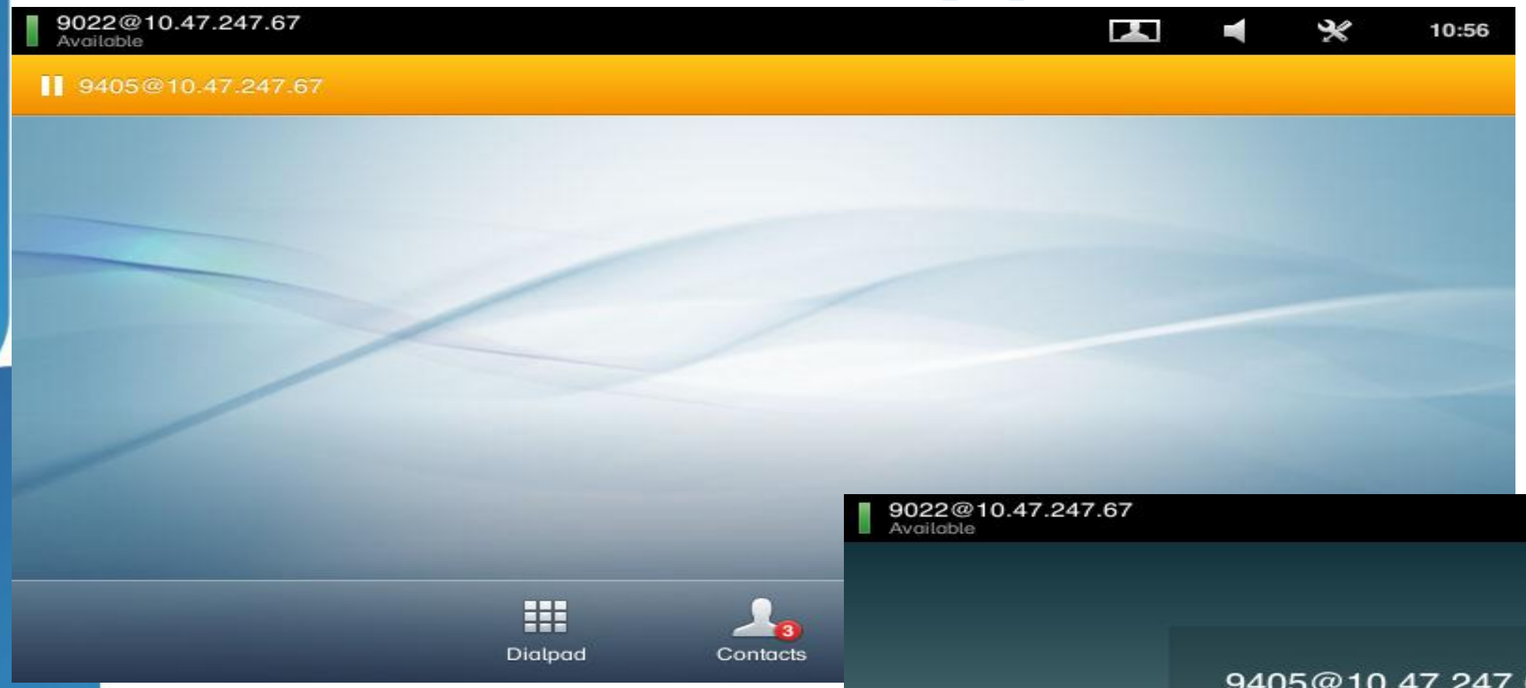
Shared Lines Support - Barge

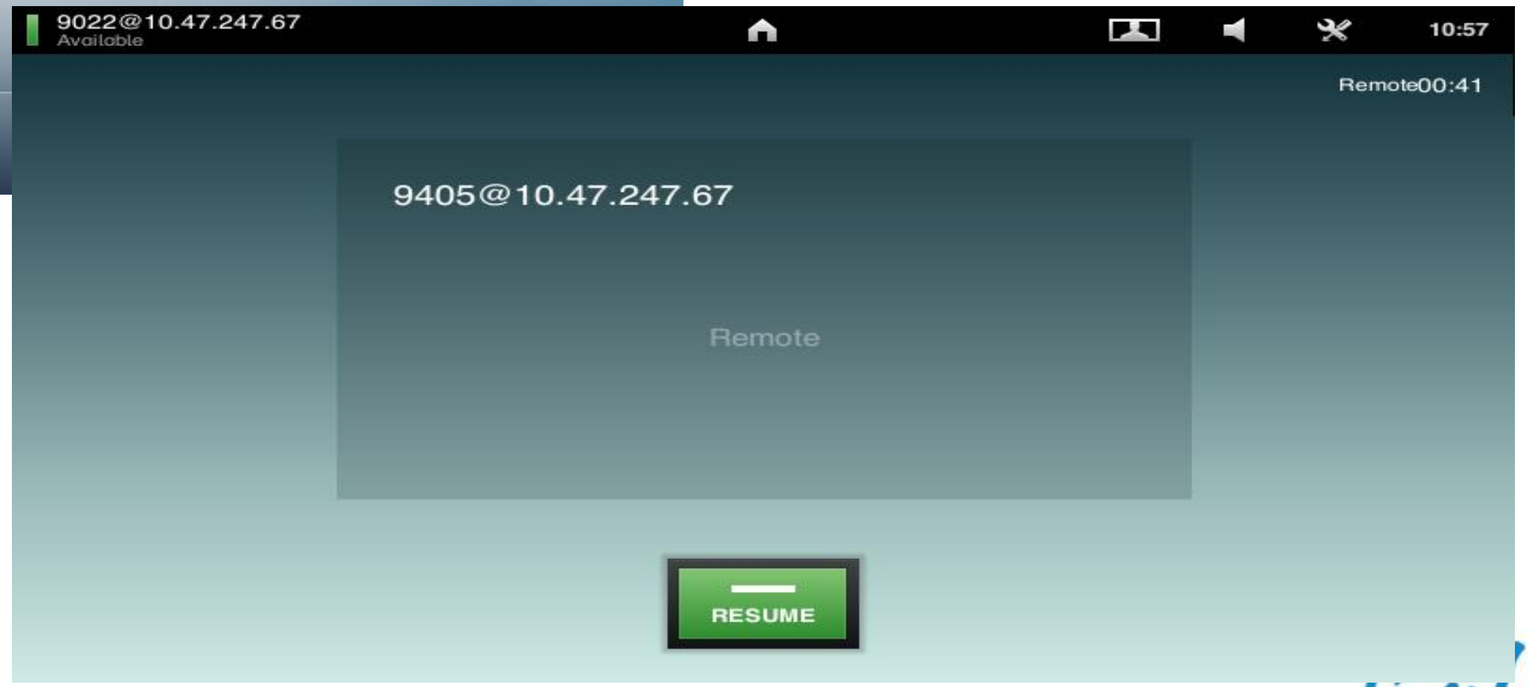




© 2013 Cisco and/or its affiliates. All rights reserved.

Shared Line Support – Remote Resume





© 2013 Cisco and/or its affiliates. All rights reserved.

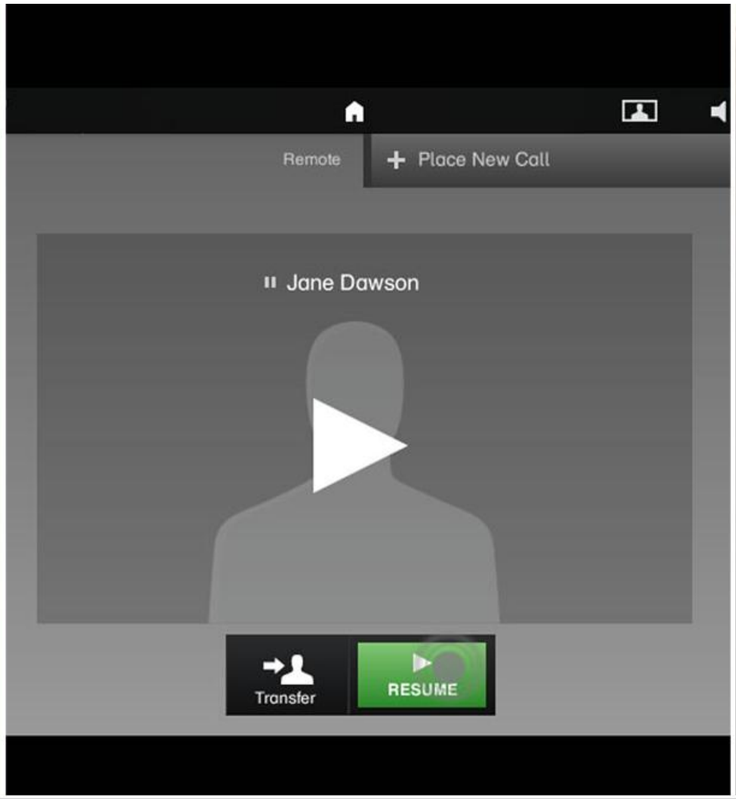
Shared Lines

- Shared Line on CUCM
  - Same DN/Partition for two or more devices
    (DN not unique, “DN + Partition” forms the unique identifier)
- Shared Line Appearances
  - Remote State Notifications
  - Hold / Resume
  - cBarge
  - Unified Mobility
    - Hand-off from mobile to desk
    - No handoff from desk to mobile

© 2013 Cisco and/or its affiliates. All rights reserved.

Seamless mobility with SNR

1. Pick up a call on mobile

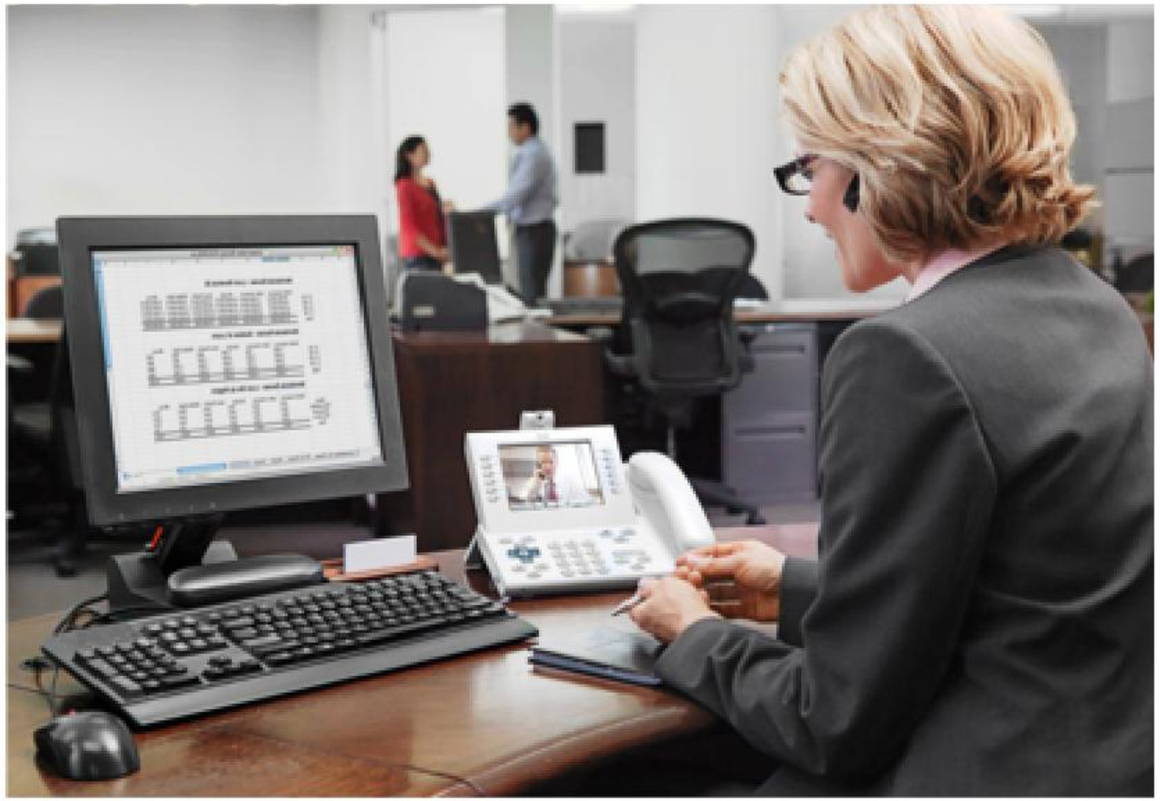


2. Resume call on the EX

3. Automatic escalation to video

© 2013 Cisco and/or its affiliates. All rights reserved.

Shared Line Support



Assisted Call handling

Admins can now fully manage calls and lines for executives using EX Systems

© 2013 Cisco and/or its affiliates. All rights reserved.

Shared lines - Helpdesk

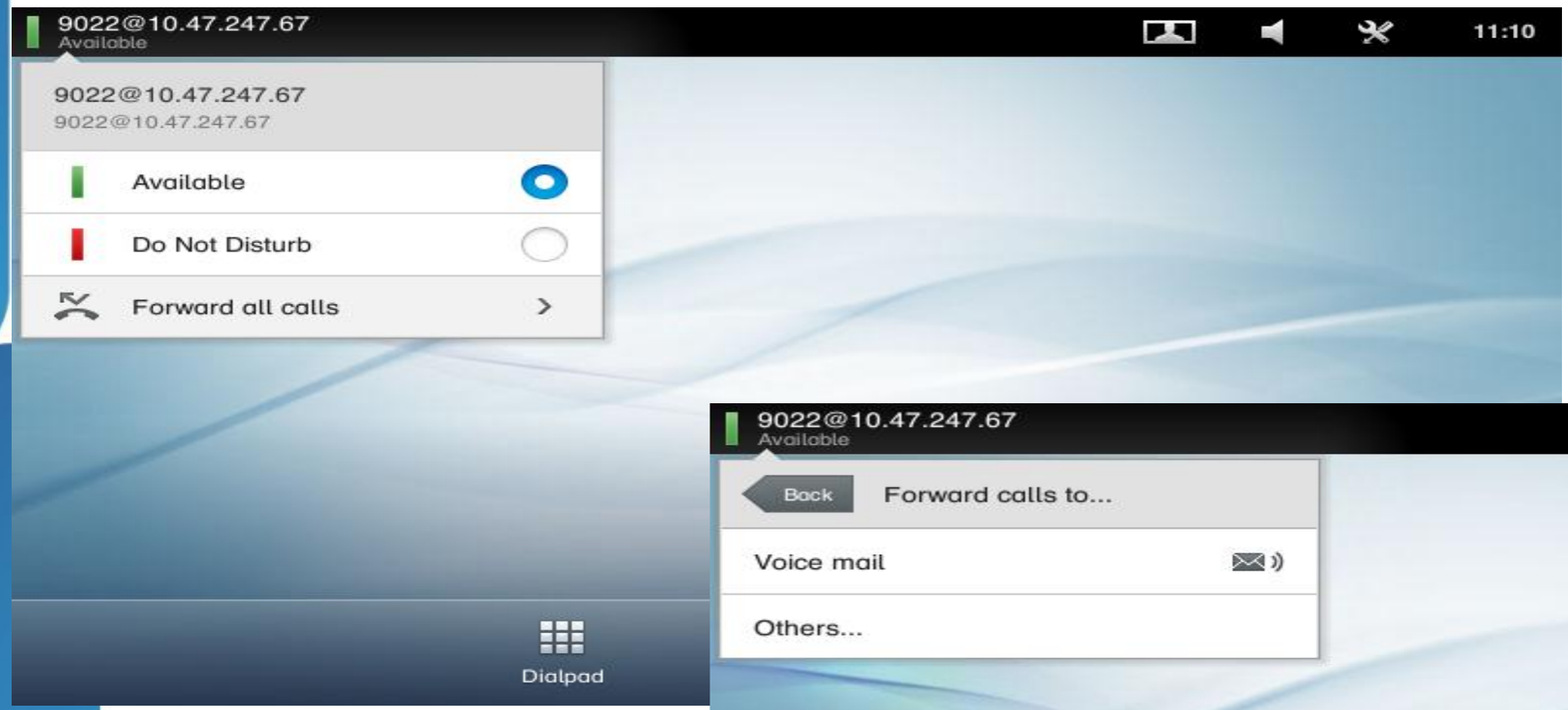
© 2013 Cisco and/or its affiliates. All rights reserved.

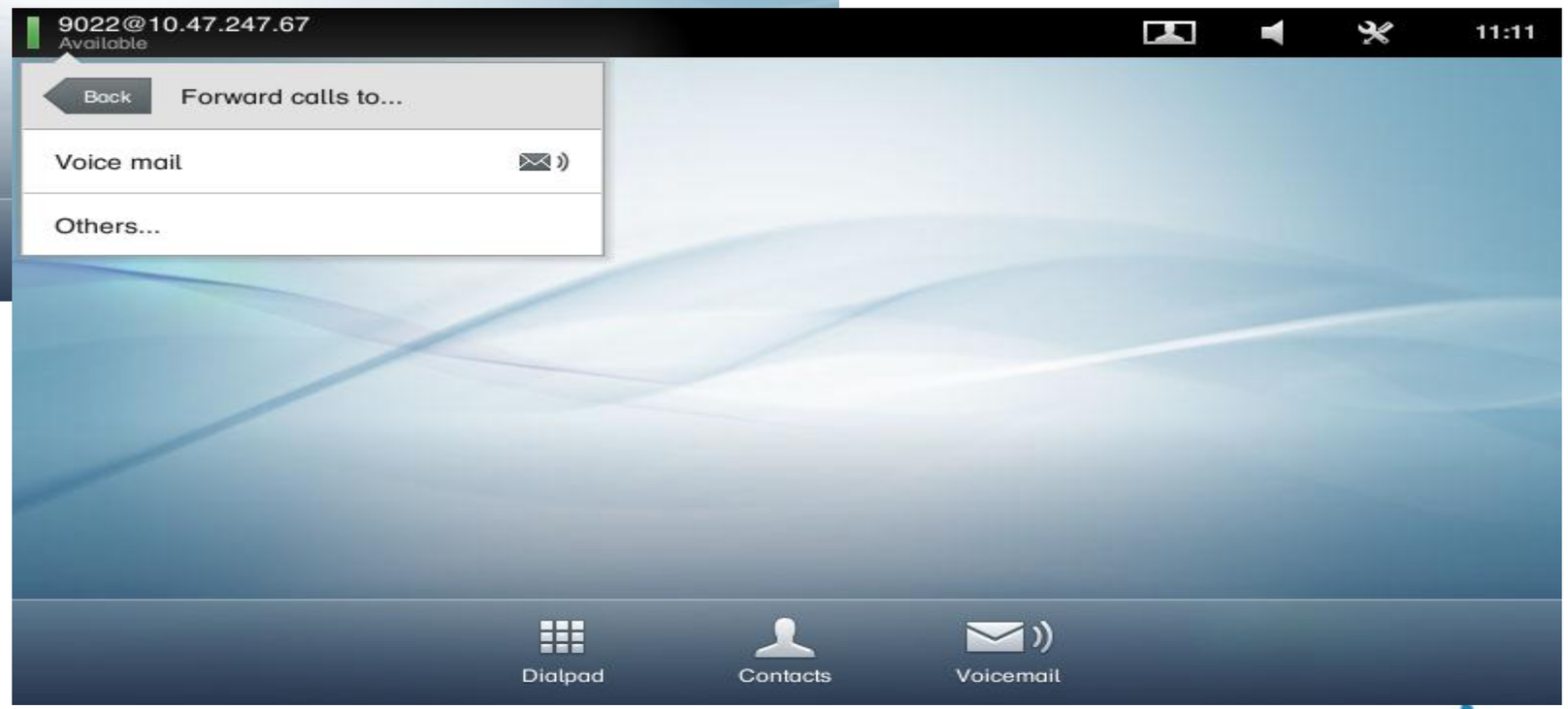
Consultative Transfer

Consultative Transfer Interaction

© 2013 Cisco and/or its affiliates. All rights reserved.

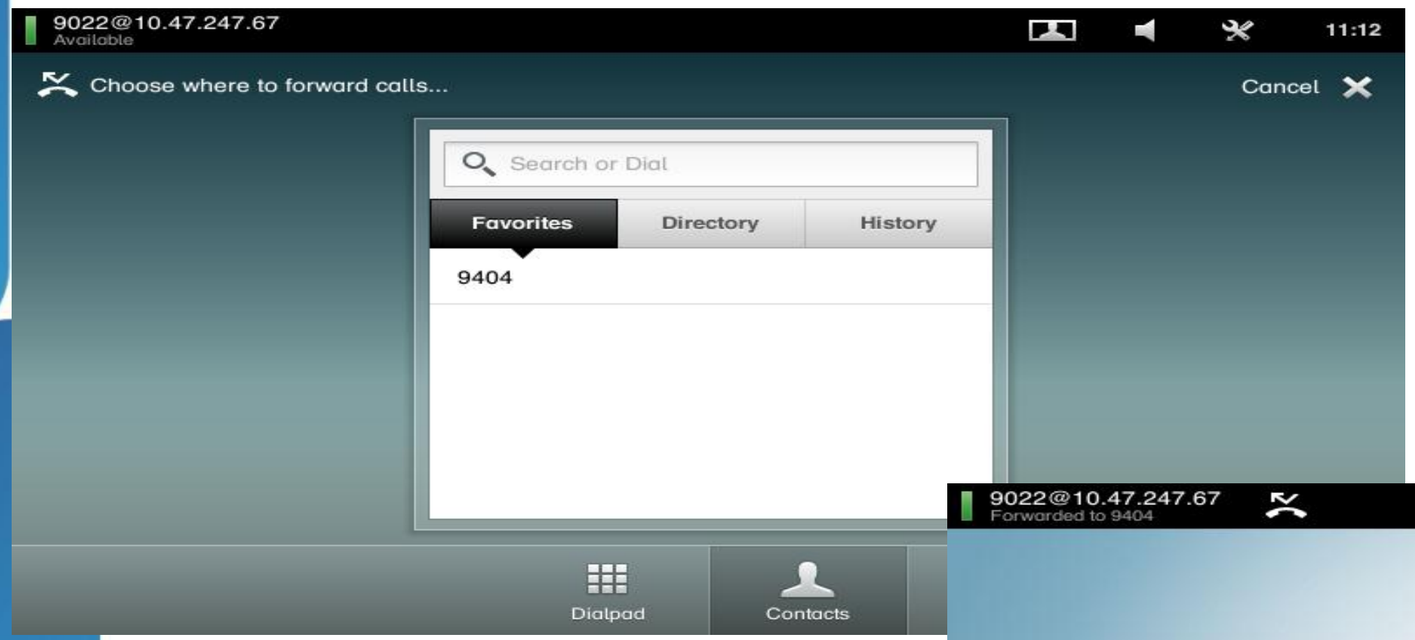
Call Forward All Calls

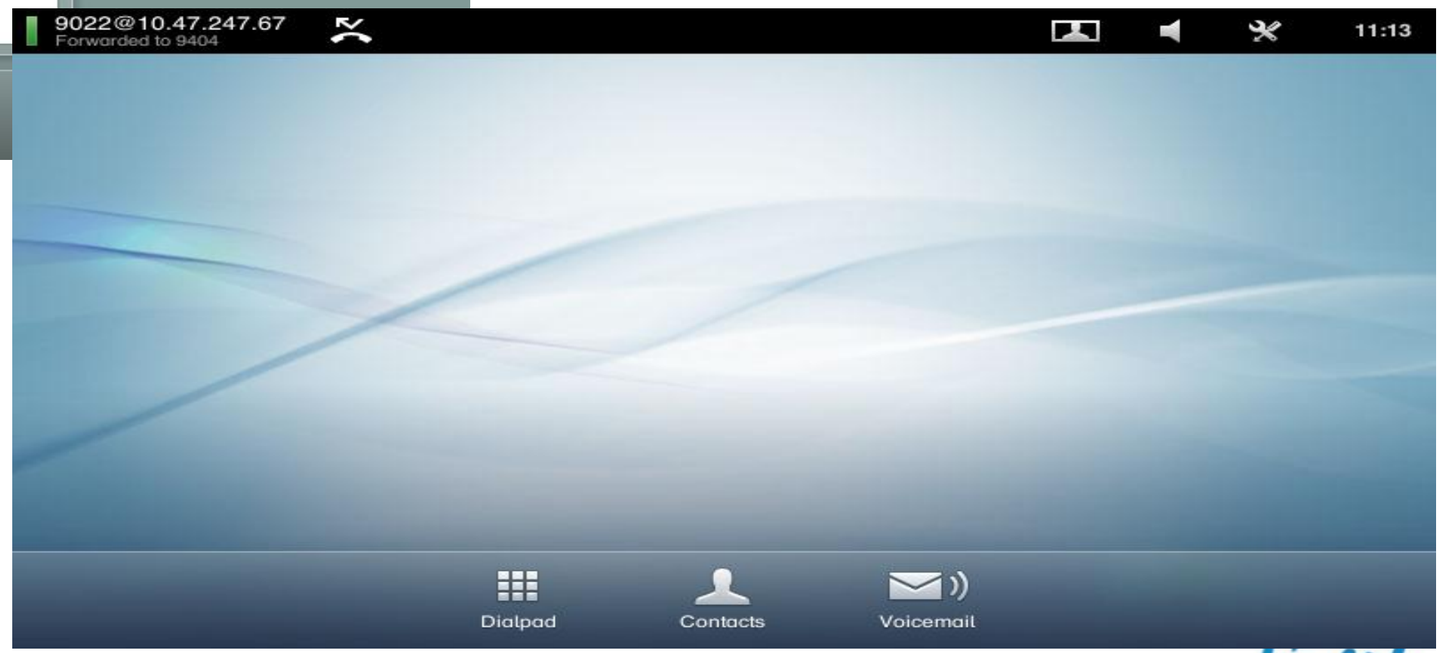




© 2013 Cisco and/or its affiliates. All rights reserved.

Call Forward All Calls, enabled





© 2013 Cisco and/or its affiliates. All rights reserved.

Other Sessions of Interest

- Orchestrate and virtualise conferencing resources
  - BRKEVT-2809
  - Understanding Cisco TelePresence Conductor
- Use TMS to schedule video endpoints
  - BRKEVT-2664
  - Video Communications Management and Scheduling
  - Learn how to deploy TelePresence CAC
- BRKUCC-2667

  Unified CM Enhanced Locations CAC Design Session and Deployment

© 2013 Cisco and/or its affiliates. All rights reserved.

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don’t forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww

Cisco live!

© 2013 Cisco and/or its affiliates. All rights reserved.

© 2013 Cisco and/or its affiliates. All rights reserved.