



*TOMORROW
starts here.*

**SECURITY
EVERYWHERE**



Designing and Deploying a Secure Enterprise Edge Solution for Collaboration

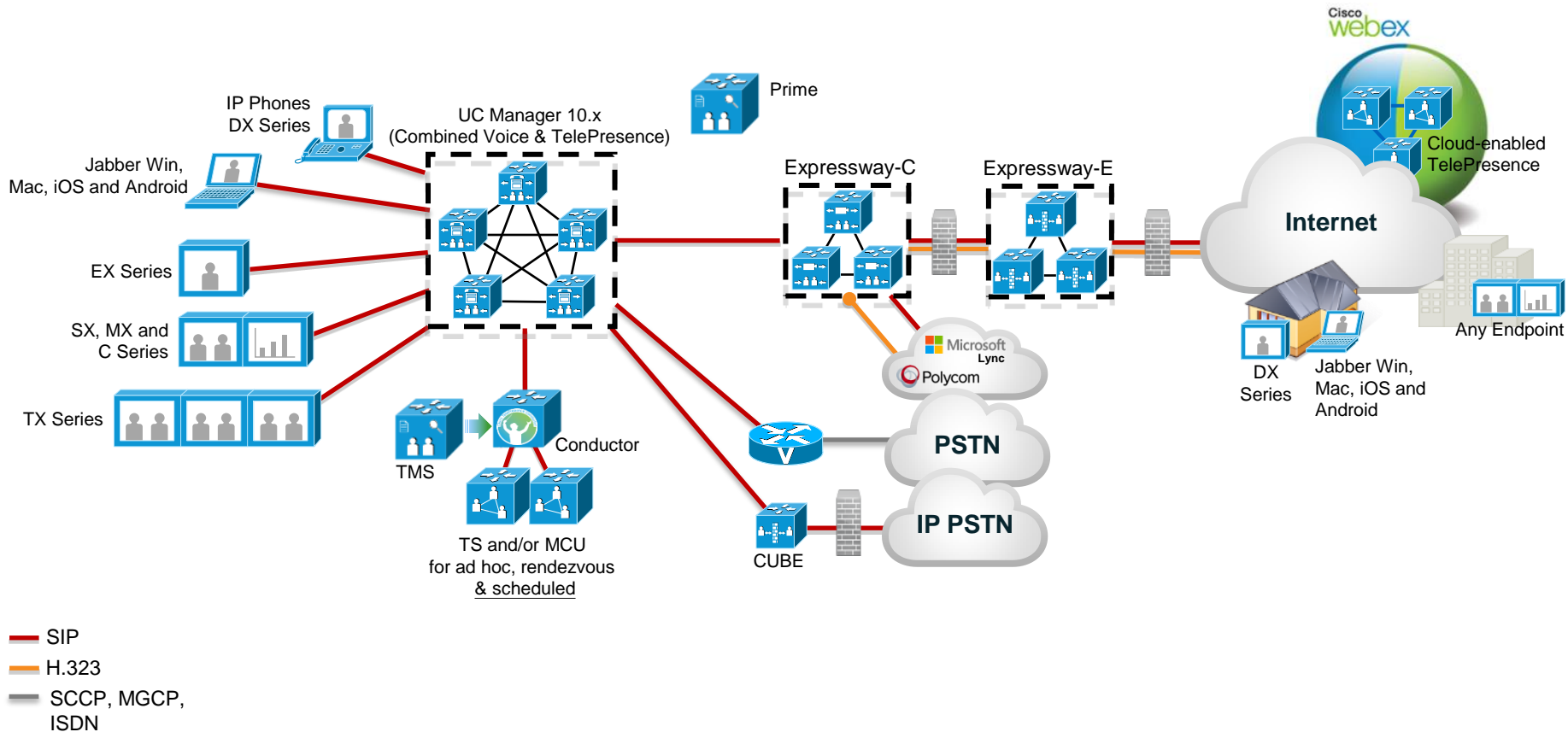
Collaboration Security

Adrian Wang

Technical Marketing Engineer, CTG

5/15/2015

Cisco Collaboration Architecture



Agenda Today

- Is your Endpoint Secure?
- Is your User Secure?
- Is your Connection Secure?

A blue-tinted image of Earth from space. The sun is in the upper left, creating a starburst effect. A satellite is visible in the upper right. The Earth's surface shows land and oceans. The text "Is your Endpoint Secure?" is overlaid on the left side.

Is your Endpoint Secure?

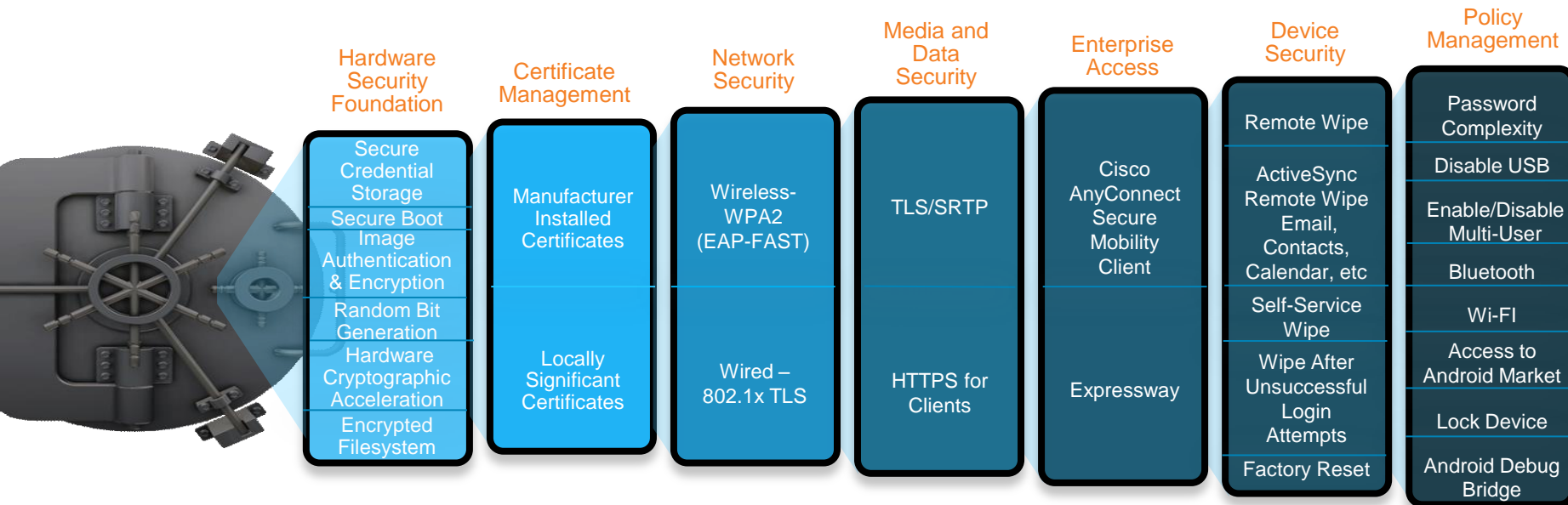
Hardware Endpoint Security

DX Series Security

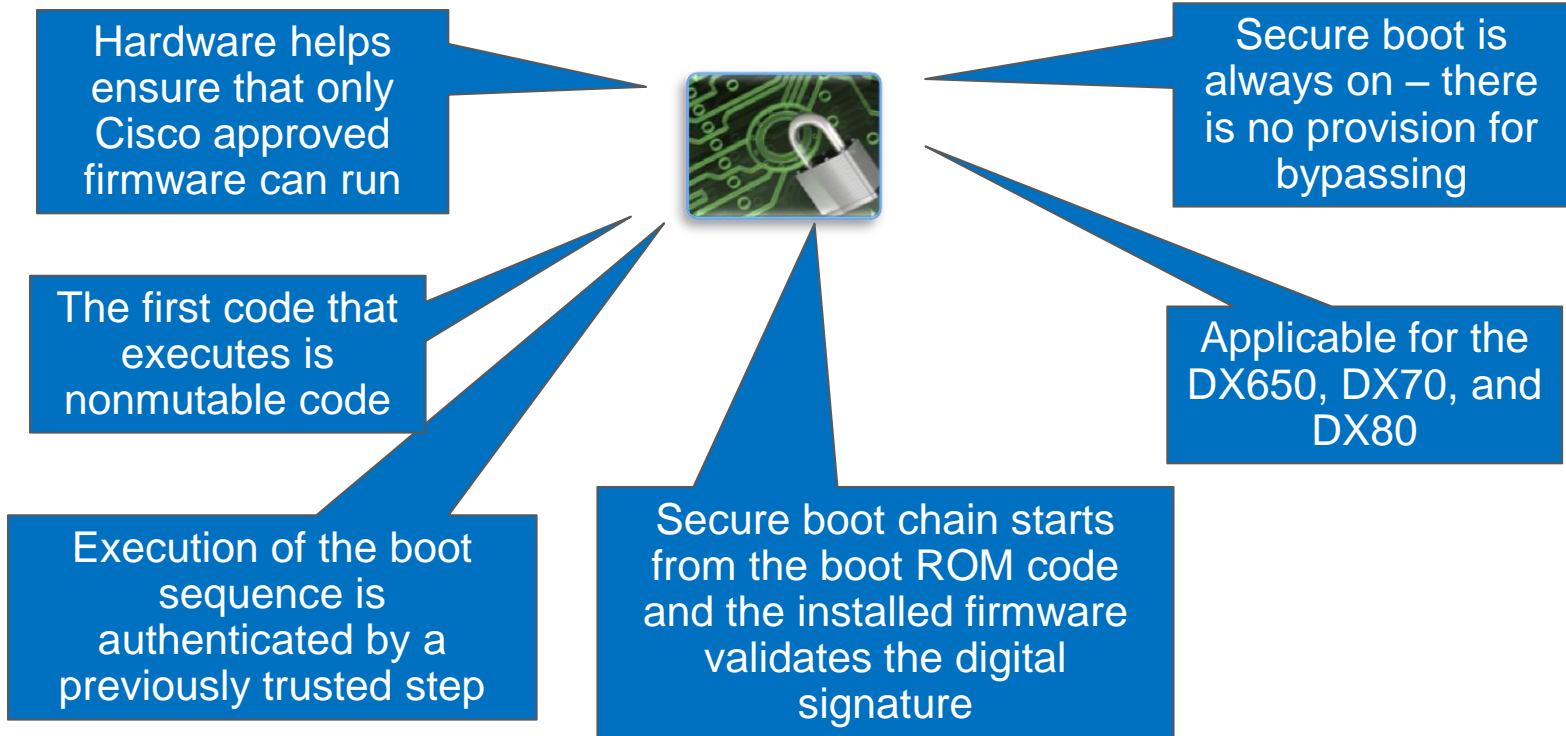
Overview



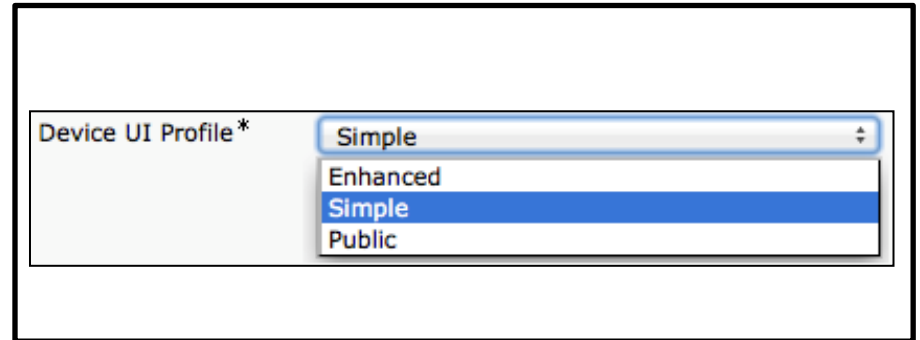
Cisco DX – Enterprise Security



Cisco DX Secure Boot



DX70 & DX80 – “Simple Mode”



- “Public Mode” is identical to Simple Mode but further restricts access to the Recent Applications list, Lock screen, PIN/password, Network configuration, and VPN. Network or VPN configuration must occur in Standard Mode prior to switching to Public Mode.

“Simple Mode” - Details

- User can not modify Wallpaper (supports admin assigned Wallpaper)
- User can not move, add shortcuts, widgets, launch applications, or long click
- No Android applications are allowed run; Google Search removed
- External USB storage is disabled
- External Monitor is only used for HD video phone
- User can create and store local contacts
- Bluetooth contacts and history sharing is also allowed
 - No other contact account types are allowed (no Exchange, Google, etc.)

Public Mode, Simple Mode, and Enhanced Mode

- Use Public Mode for public devices (requiring no hot-desking or extension mobility)
- Use “Simple Mode” for all deployments and users requiring only voice/video
- Use “Enhanced Mode” for users requiring collaboration and advanced features

	Public	Simple	Enhanced
Call Application	Yes	Yes	Yes
Recent Applications List	No	Yes	Yes
Lock Screen	No	Yes	Yes
Network Configuration	No	Yes	Yes
Visual Voicemail	No	Yes	Yes
Bluetooth	Yes	Yes	Yes
Set Date and Time	No	Yes	Yes
UDS (Cisco User Data Service)	Yes	Yes	Yes
External Storage	No	No	Yes
Jabber IM, Email, WebEx, Internet browser, and 3 rd Party Apps	No	No	Yes

Cisco DX Security – Details

Identical to other Cisco Phones

- **Image/File/Config Authentication and Encryption**
 - **Disk Encryption***
 - **Signaling Security (SSL/TLS)**
 - **Media Security (sRTP) – Both Audio and Video****
 - **CTL/ITL X.509v3 Certificates**
 - **Security by Default (SBD)**
 - **Trust List and Verification Service (TVS)**
 - **CAPF**
 - **SSH**
 - **802.1x and 802.1x PC port**
 - *Uses the standard Android disk encryption. Unlike standard Android, disk encryption will be on by default. The encryption key will be derived using the device hardware; thus, each device will have its own encryption key.
- **Secure Video requires CUCM 9.0

Overview AnyConnect VPN Client on Cisco DX

- **Complete integration with Anyconnect 3.0**
- **SCEP Proxy Support**
 - The ASA can proxy SCEP requests between AnyConnect and a third-party CA. The CA only needs to be accessible to the ASA if it is acting as the proxy.
- **Enforce Password Persistence from CUCM**
- **Enable or Disable User-Defined VPN Profiles**
- **VPN can be used over wired or wireless**



<http://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/115785-anyconnect-vpn-00.html>

Anyconnect VPN Deployment

Security (VPN)

- **Anyconnect VPN is built into the DX**
No need to download from Google Play



- Option 1 – Manually create a VPN (CUCM is unaware). This is “over the top” method.
- Option 2 – Provision VPN Profile in CUCM for DX certificate push for DX to “Phone Home” (same as 8800/8900/9900). Details below:
 - <http://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/115785-anyconnect-vpn-00.html>

Wireless Security

- **Authentication**

- **Open**
- **WEP**
- **WPA/WPA2 PSK**
- **802.1x EAP**

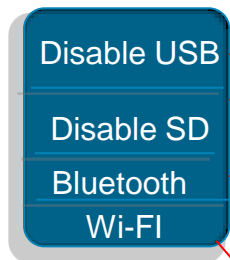
- **Encryption**

- **AES**
- **TKIP/MIC**
- **WEP 40/64 or 104/128 bit (static via open authentication only)**

- **802.1x EAP Types**

- **EAP-FAST (Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling)**
- **EAP-TLS (Extensible Authentication Protocol – Transport Layer Security)**
- **PEAP (Protected Extensible Authentication Protocol) MS-CHAPv2 and GTC with optional server validation**

Cisco DX Policy – Device Management



- **Disable USB**
- **Disable SD Card**
- **Disable Bluetooth**
- **Disable Wifi (use wired Ethernet only)**

<input type="checkbox"/> Disable USB		<input type="checkbox"/>
SDIO*	Disabled	<input type="checkbox"/>
Bluetooth*	Enabled	<input type="checkbox"/>
Wifi*	Enabled	<input type="checkbox"/>

Cisco DX Policy – Application Sources

Access to
Unknown
Sourced Apps
Access to
Android Market

Access to UC
Manager Apps

- **Disable “Side Loading” of Apps**
 - **Example: Apps from Internet or Email**
- **Disable Google Play Marketplace**
- **Disable UC Manager Provisioned Apps**



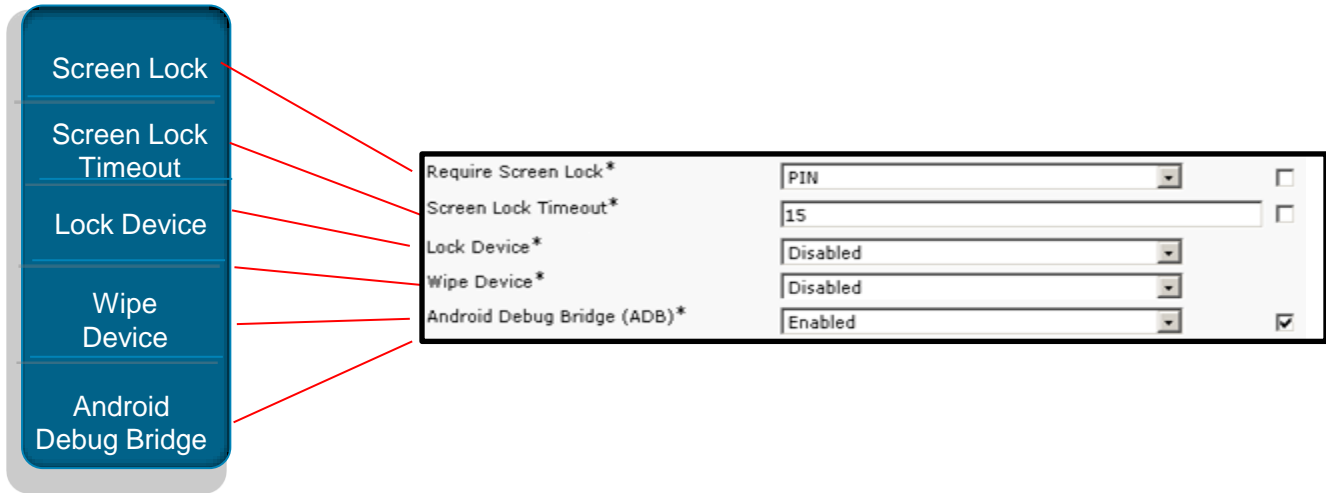
Allow Applications from Unknown Sources*

Allow Applications from Android Market

Enable Cisco Unified CM Application Client

The screenshot shows a settings interface with three rows. The first row is 'Allow Applications from Unknown Sources*' with a dropdown menu set to 'Enabled'. The second row is 'Allow Applications from Android Market' with a checked checkbox. The third row is 'Enable Cisco Unified CM Application Client' with a checked checkbox. Red lines from the left box point to each of these three rows.

Cisco DX Policy – More Security



Three Primary Methods of Application Deployment

1. Google Play

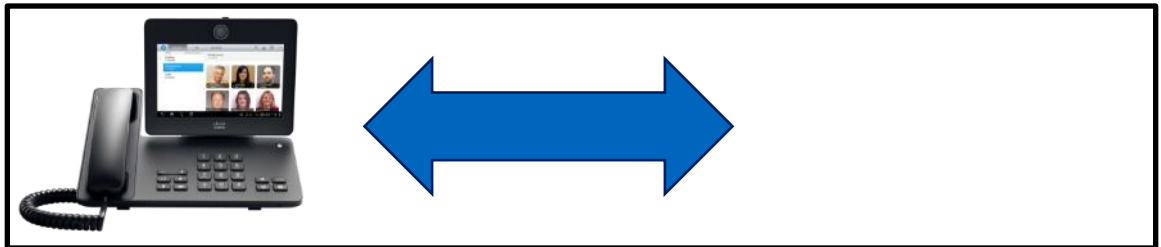
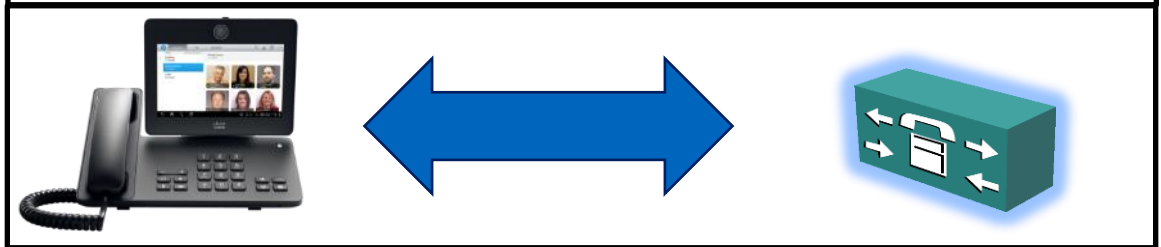
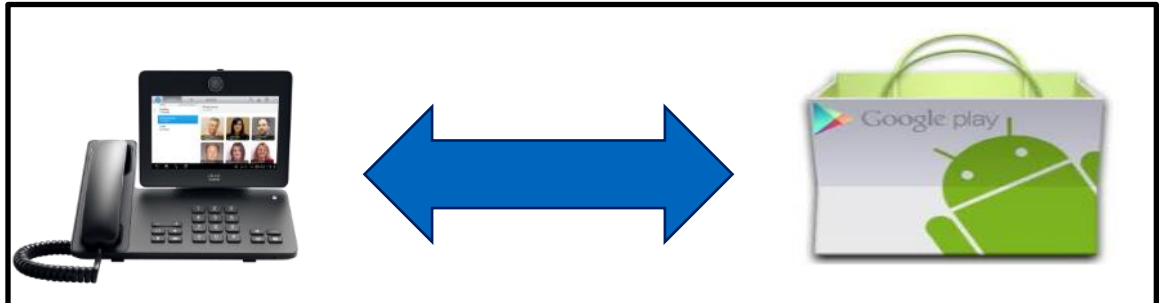
(Disabled by Default)

2. CUCM 8.5+ Push

(Disabled by Default)

3. Side Loading

(Disabled by Default)



DX Series – Application Deployment

Application Deployment with Google Play Disabled

- Example of an Android Application pushed from CUCM
- Requires local APK be on premise
- Create a CUCM IP Phone Service and subscribe DX to the service

Note: The “Service Name” requires the manifest name of the Android Application. To learn how to find the manifest name see below link:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cdce/dx600/admin/10_1_1/english/DX60_BK_CFB047D4_00_cisco-dx600-administration-guide-10_1_1/DX60_BK_CFB047D4_00_cisco-dx600-administration-guide-10_1_1_chapter_01000.html#DX60_TK_P06A3F59_00

IP Phone Services Configuration

Save Delete Update Subscriptions Add New

Status

Status: Ready

Service Information

Service Name* com.cisco.sample.techwisetv

Service Description

Service URL* http://10.10.10.10/photos/TechWiseTVv6.apk

Secure-Service URL

Service Category* Android APK

Service Type* Standard IP Phone Service

Service Vendor

Service Version

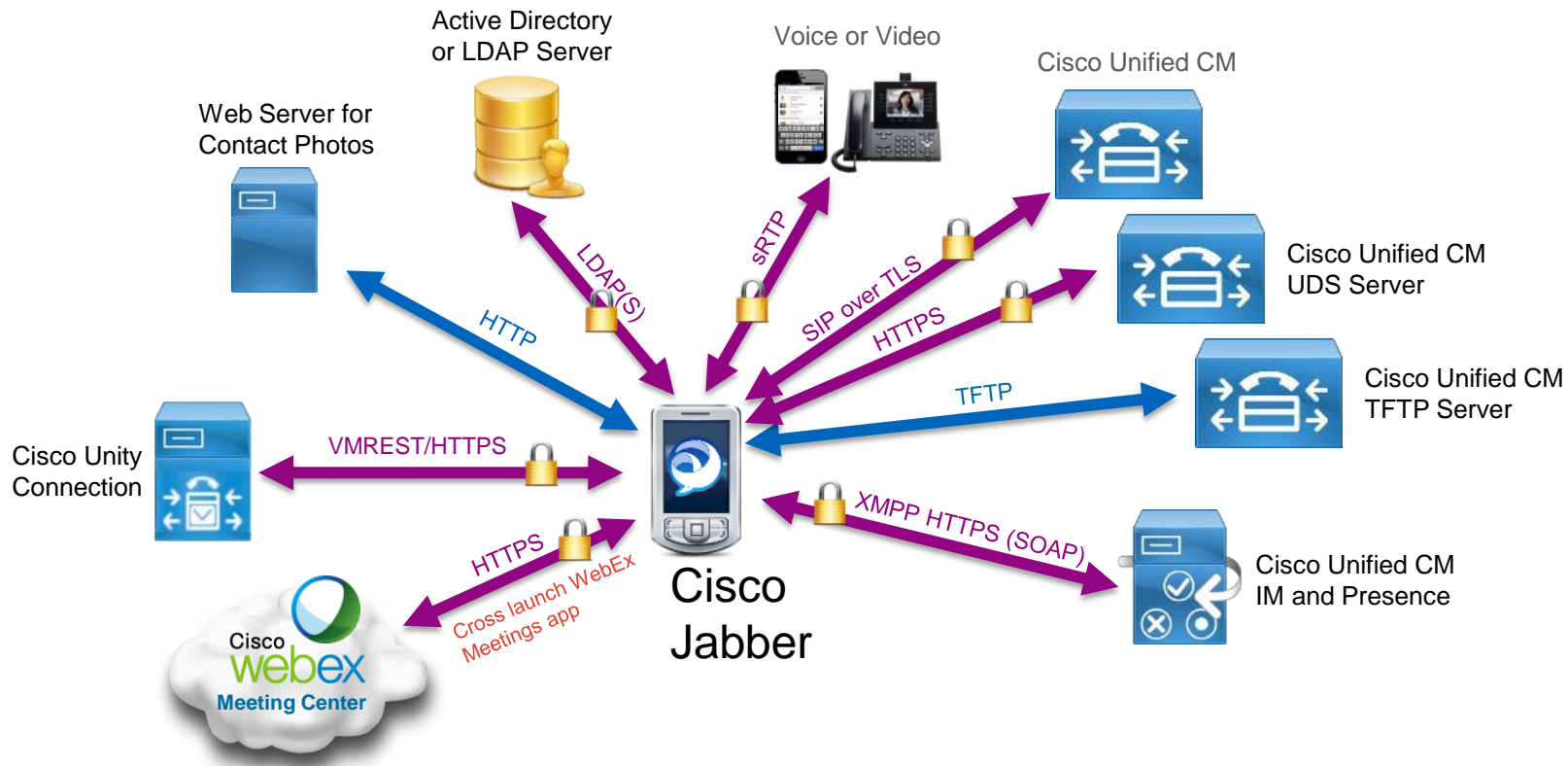
Enable

Cisco DX Multi-User Support

- User data is encrypted
- User A cannot access User B's data or applications
- Login process is identical to Extension Mobility

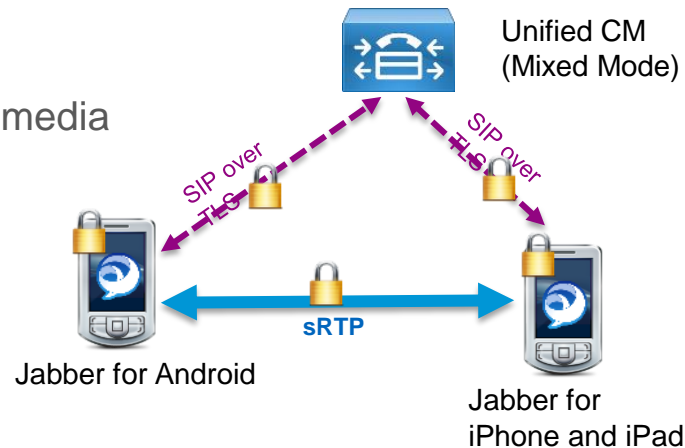


Secure Communications with UC Services



Secure Phone

- Enable security end to end from call signaling to real time media
 - SIP signaling over TLS
 - Media over sRTP
- Choice of “Authenticated” or “Encrypted”
 - Authenticated – secure signaling only
 - Encrypted – secure both signaling & media
- Supports two authentication modes in CAPF certificate operation
 - by Authentication string (recommended)
 - by NULL string
- Security must be turned on in Unified CM cluster (i.e. Mixed Mode)
 - Only supported through Unified CM CAPF* enrollment process

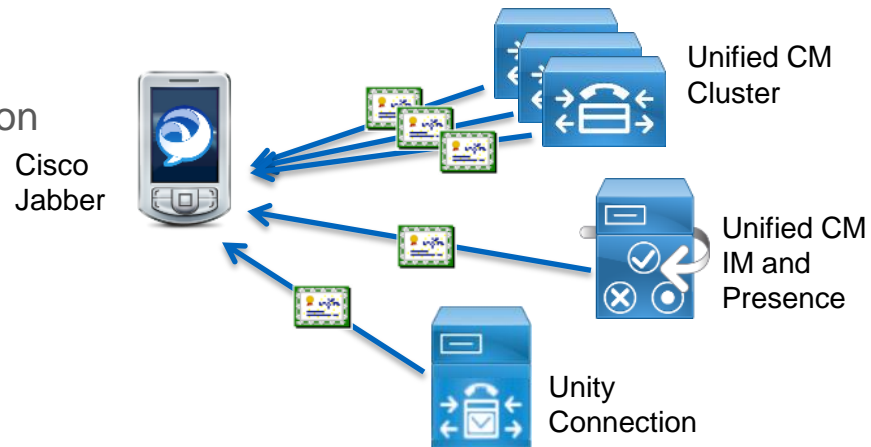


* CAPF (Certificate Authority Proxy Function)

Server Certificate Validation

- Jabber validates all certificates from UC application servers it connects to
- End user will not be prompted if either:
 - Certificate is valid (from public or private CA), or
 - Certificate matches with existing one in the cache
- End user may choose Continue or Decline when prompted if certificate validation fails
- Jabber remembers end user's choice until:
 - Jabber is signed out if Decline was chosen
 - Jabber is uninstalled if Continue was chosen

Note: CWMS requires a valid certificate to deploy. Jabber assumes the certificate is valid. If it is not, the connection fails.



<Protocols>

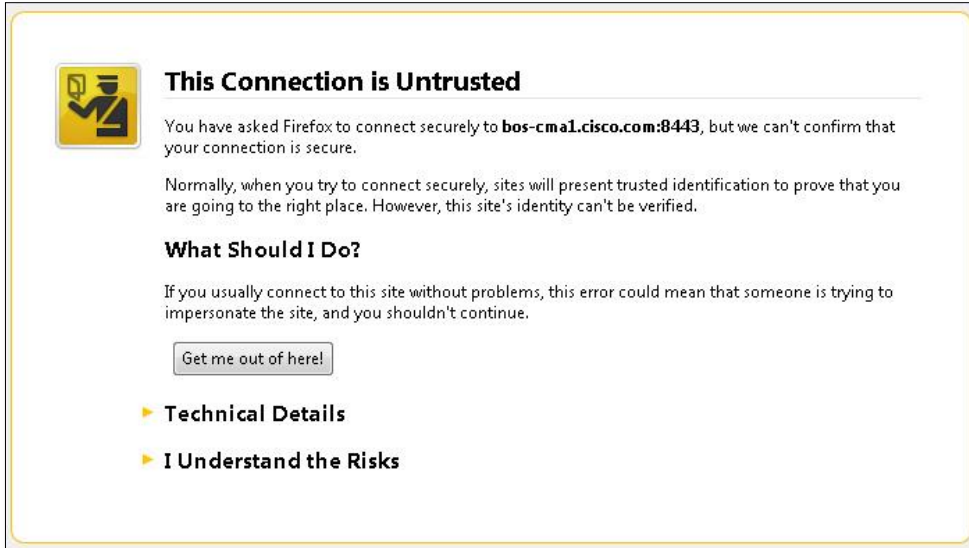
HTTPS, XMPP over TLS, LDAP over TLS

<Servers>

UCM CCMCIP, IM and Presence XMPP/SOAP
Unity Connection, LDAP

Best Practice: Tomcat Certificate signed by CA

Avoid untrusted certificate warnings in browsers and Jabber



This Connection is Untrusted

You have asked Firefox to connect securely to **bos-cma1.cisco.com:8443**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

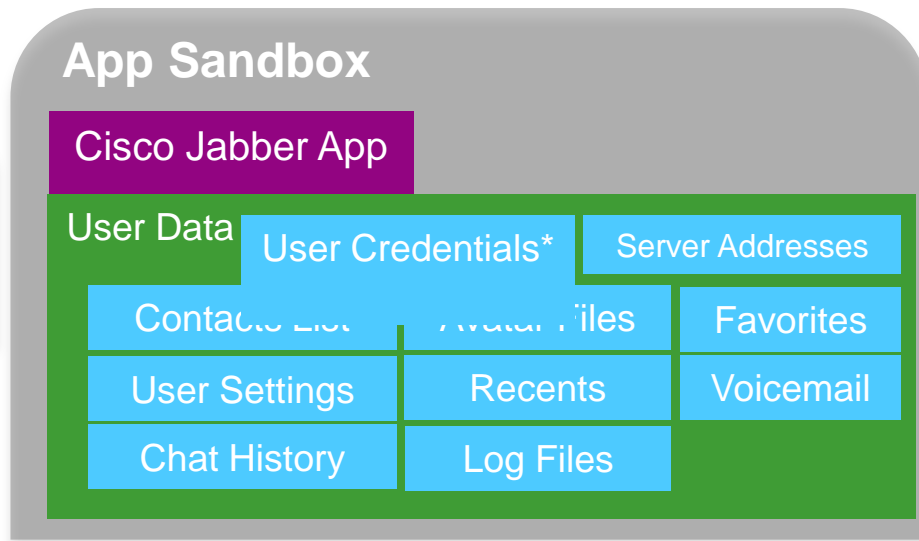
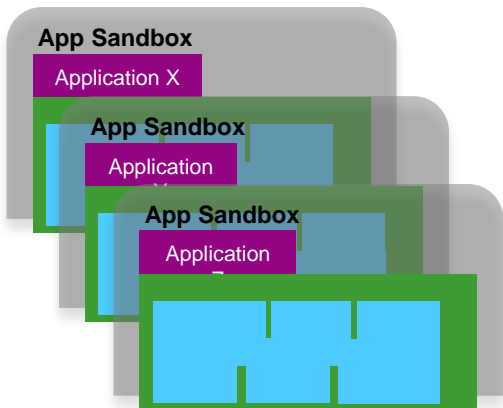
What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

- CUCM Tomcat: HTTPS certificate used for serving CUCM admin, end user self-care page, and UDS
- By default Tomcat is self signed
- Self signed certificates generate ugly security warnings and reinforce bad habits
- Use a CA signed certificate to avoid certificate errors in browser for both end users and admins
- Save time and money with multi-server Tomcat certificate

Cisco Jabber in App Sandbox



Cisco Jabber app & its user data in App Sandbox are **not encrypted but protected** by the Sandbox mechanism.

Everything in App Sandbox will be removed when Jabber is deleted by user.

* On Android, user credentials are encrypted using AES-128 before they are stored. On iOS, user credentials are secured in the iOS Keychain (encrypted container)

Jabber for Secure Environments

Jabber will provide “Best in Class” collaboration for secure environments



Federal Information Processing Standard (FIPS 140.2)

FIPS support achieved with Jabber for windows 10.5



US DoD Information Assurance (IA)

Work completed for Jabber for Windows 10.5

Currently in certification testing



Common Criteria (CC) – Voice & Video

International security standard for the US Governments

“Commercial Solutions for Classified” (CSfC)

program. Targeted for 11.0 for Windows



Relevant for
Federal customers



Relevant in Financial, Healthcare and other Security focused environments

Common Criteria For VoIP

- Common Criteria (CC) is a Standard for Information Technology Security Evaluation, used as the basis for many Government Security Certifications.
- CC is a separate certification standard from US DoD Information Assurance (IA), but efforts are underway to consolidate the two. (Both have FIPS 140.2 compliance as a base level requirement)
- CC is the security standard for the US Governments “Commercial Solutions for Classified” (CSfC) program.
- CC certification is also relevant in Financial, Healthcare and other Security focused environments
- 11.0 will Deliver Common Criteria Certification for Jabber for Windows as a VoIP (softphone only) Client. Mobile Jabber VoIP clients are planned for Jabber 11.5.
- CC VoIP specifies requirements for the Transmission of Secure (Voice) Media over a Public Network.

Common Criteria For VoIP

Jabber 11.0 content

- All Secrets (Passwords, Usernames, Keys, other Credentials, Encrypted whenever stored or being transported).
- Secrets eliminated from Logs & Memory Dumps
- Encrypt or completely Disable Logging to Disk (Admin Options)
- Encrypt PRT Files (Admin Option)
- Encrypted TFTP Traffic (Including transport of Configuration Info)
- Next Generation Encryption for SIP and SRTP interfaces:
 - TLS v1.2 Ciphers:
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 - SRTP Ciphers:
 - AEAD_AES_128_GCM
 - AEAD_AES_256_GCM
 - Elliptic Curve Certificate Generation:
 - ECDSA
 - Certificate Validation:
 - SHA-2 hashes / fingerprints
 - ECDSA certificates

Endpoint Certificates

Cryptographically assured device identity

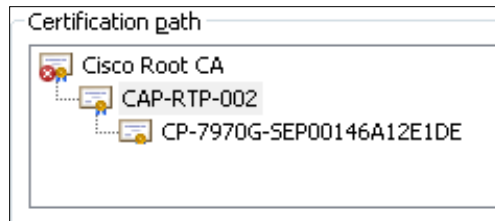
- Manufacturing Installed Certificate (MIC)
 - Cisco IP Phones ship from the factory with a unique MIC pre-installed
 - MIC is valid for 10 years
 - No certificate revocation support
- Locally Significant Certificates (LSC)
 - preferred certificate for endpoint identity
 - Endpoint support includes IP Phones, TelePresence, Jabber clients, CIPC
 - LSC signed by CAPF Service running on CUCM Publisher
 - LSC supports RSA key size 512, 1024, or 2048 bits
 - LSC can be installed, re-issued, deleted in bulk with CUCM Bulk Admin Tool
 - LSC signed by CAPF is valid for 5 years
 - Paper process required to track certificate expiration

X.509v3



Best Practice: IP Phone MIC

- Endpoints can use MICs to authenticate with CAPF for LSC installation
- Use MIC for initial endpoint provisioning of IP Phones before LSC installation is done
- Not recommended to use MIC for TLS, VPN, or 802.1x
- MIC is installed at time of manufacturing and cannot be revoked
- When both LSC and MIC are installed on a device, LSC takes preference
- MIC CA certificates included in both the CallManager and CAPF trust stores:
 - CAP-RTP-001
 - CAP-RTP-002
 - Cisco_Manufacturing_CA
 - Cisco_Root_CA_2048



Cisco Manufacturing CA SHA2

<http://www.cisco.com/security/pki/certs/cmca2.cer>

- Cisco's newest IP Phones include MIC certificates signed by this new Manufacturing SHA2 CA
- CUCM 10.5(1) includes and trusts the new SHA2 certificates
- Customers on older versions of CUCM may need to download the new Manufacturing CA certificate and
 - upload to the CAPF-trust to allow phones to authenticate with CAPF to obtain an LSC
 - upload to the CallManager-trust if customer want to allow phones to authenticate with MIC for SIP 5061



Unified CM Certificates

- Unified CM includes six certificate types:
 - Tomcat (web services)
 - CallManager (SIP/SCCP TLS, TFTP config signing, etc.)
 - CAPF (CA cert used to sign LSC, only employed on the publisher)
 - IPSEC (ipsec tunnels to gateways or other CUCM)
 - TVS (Trust Verification Service, security by default)
 - ITLRecovery (used as a trust anchor for bulk ITL recovery)
- Default to self-signed certificates, valid for 5 years
- Option to have signed by 3rd party CA
- Self-signed, 3rd party CA signed certificates, and trusted certificates managed via OS Admin page



Improved Certificate Management GUI

Including the ability to filter, sort and view certificate expiration from the list view

NEW IN 10.5

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR Download CSR

Certificate List (1 - 29 of 29) Rows per Page 50

Find Certificate List where Expiration is before 01/13/2019 Find Clear Filter

Certificate ^	Common Name	Type	Distribution	Issued By	Expiration	Description
CallManager	cucm-pub.ucdemolab.com	Self-signed	cucm-pub.ucdemolab.com	cucm-pub.ucdemolab.com	12/18/2017	Self-signed certificate generated by system
CallManager-trust	cucm-sub2.ucdemolab.com	Self-signed	cucm-sub2.ucdemolab.com	cucm-sub2.ucdemolab.com	09/10/2018	Trust Certificate
CallManager-trust	CAPF-cf683b33	CA-signed	CAPF-cf683b33	kroarty-lab	03/10/2015	Trust Certificate
CallManager-trust	CAPF-65e9c5ad	Self-signed	CAPF-65e9c5ad	CAPF-65e9c5ad	09/10/2018	Trust Certificate
CallManager-trust	CAPF-79b8b209	Self-signed	CAPF-79b8b209	CAPF-79b8b209	12/18/2017	Trust Certificate
CallManager-trust	kroarty-lab	Self-signed	kroarty-lab	kroarty-lab	07/18/2016	Signed Certificate
CallManager-trust	collabedge1.ucdemolab.com	CA-signed	collabedge1.ucdemolab.com	Cisco_SSACA2	08/27/2015	Signed Certificate
CallManager-trust	CAPF-6759db54	CA-signed	CAPF-6759db54	CAPF-6759db54	10/08/2018	Signed Certificate
CallManager-trust	CAPF-3ad253af	Self-signed	CAPF-3ad253af	CAPF-3ad253af	12/18/2017	Signed Certificate
CallManager-trust	cucm-sub1.ucdemolab.com	Self-signed	cucm-sub1.ucdemolab.com	cucm-sub1.ucdemolab.com	12/18/2017	Trust Certificate
CAPF	CAPF-cf683b33	CA-signed	CAPF-cf683b33	kroarty-lab	03/10/2015	Certificate Signed by kroarty-lab
CAPF-trust	CAPF-cf683b33	CA-signed	CAPF-cf683b33	kroarty-lab	03/10/2015	
CAPF-trust	kroarty-lab	Self-signed	kroarty-lab	kroarty-lab	07/18/2016	Signed Certificate
CAPF-trust	CAPF-6759db54	Self-signed	CAPF-6759db54	CAPF-6759db54	10/08/2018	Signed Certificate
CAPF-trust	CAPF-3ad253af	Self-signed	CAPF-3ad253af	CAPF-3ad253af	12/18/2017	Signed Certificate
ipsec	cucm-pub.ucdemolab.com	Self-signed	cucm-pub.ucdemolab.com	cucm-pub.ucdemolab.com	12/18/2017	Self-signed certificate generated by system
ipsec-trust	cucm-pub.ucdemolab.com	Self-signed	cucm-pub.ucdemolab.com	cucm-pub.ucdemolab.com	12/18/2017	Trust Certificate

Certificate Key Length & Hash Algorithm Options

Available across all server certificate types

NEW IN 10.0

Generate Certificate

Generate New Close

Status

Status: Ready

Generate Certificate

Certificate Name*	CallManager
Key Length*	1024
Hash Algorithm*	1024
	2048

Generate New Close

Generate Certificate

Generate New Close

Status

Status: Ready

Generate Certificate

Certificate Name*	CallManager
Key Length*	1024
Hash Algorithm*	SHA1
	SHA1
	SHA256

Generate New Close

Multi-Server Certificate Support

NEW IN 10.5

- Simplify certificate management in clustered environments



- New option to share a single CA signed certificate across all nodes in a cluster
- Each cluster node's FQDN included as Subject Alternative Name (SAN) in a single certificate, custom SANs can also be included
- Available for Unified CM (UCM + IM&P) and Unity Connection clusters
- Specifically for Tomcat, CallManager, CUP-XMPP & CUP-XMPP-S2S certificate types

Multi-Server CSR

NEW IN 10.5

Distribution*
cucm-pub.ucdemolab.com
cucm-pub.ucdemolab.com
Multi-server(SAN)

Distribution drop-down provides Multi-server option

Common Name can be edited, defaults to “-ms” suffix

Auto-populated domains, parent domain, and other admin supplied domain names all included in CSR as individual DNS SANs

Generate Certificate Signing Request

Generate Close

Generate Certificate Signing Request

Certificate Purpose* tomcat

Distribution* Multi-server(SAN)

Common Name* cucm-pub.ucdemolab.com-ms

Subject Alternate Names (SANs)

Auto-populated Domains
cucm-pub.ucdemolab.com
cucm-sub1.ucdemolab.com
cucm-sub2.ucdemolab.com
imp1.ucdemolab.com
imp2.ucdemolab.com

Parent Domain
ucdemolab.com

Other Domains

Browse... No file selected.

Please import .TXT file only.
For more information please refer to the notes in the Help Section

+ Add

Key Length* 2048

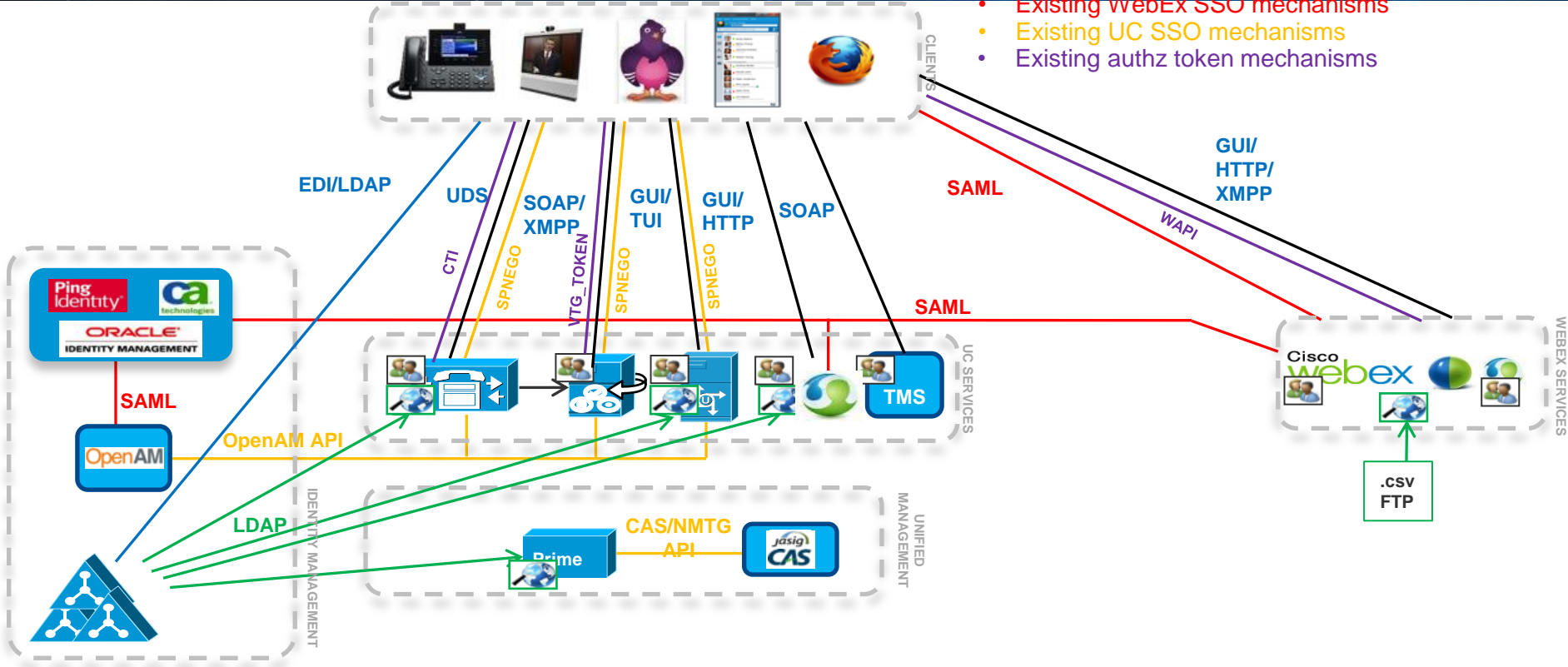
Hash Algorithm* SHA256

A blue-tinted image of Earth from space, showing the curvature of the planet and a bright sun in the upper left corner. The sun is a bright white star with a blue lens flare effect. The Earth's surface is visible in shades of blue and white, with some cloud cover. The background is a dark blue space.

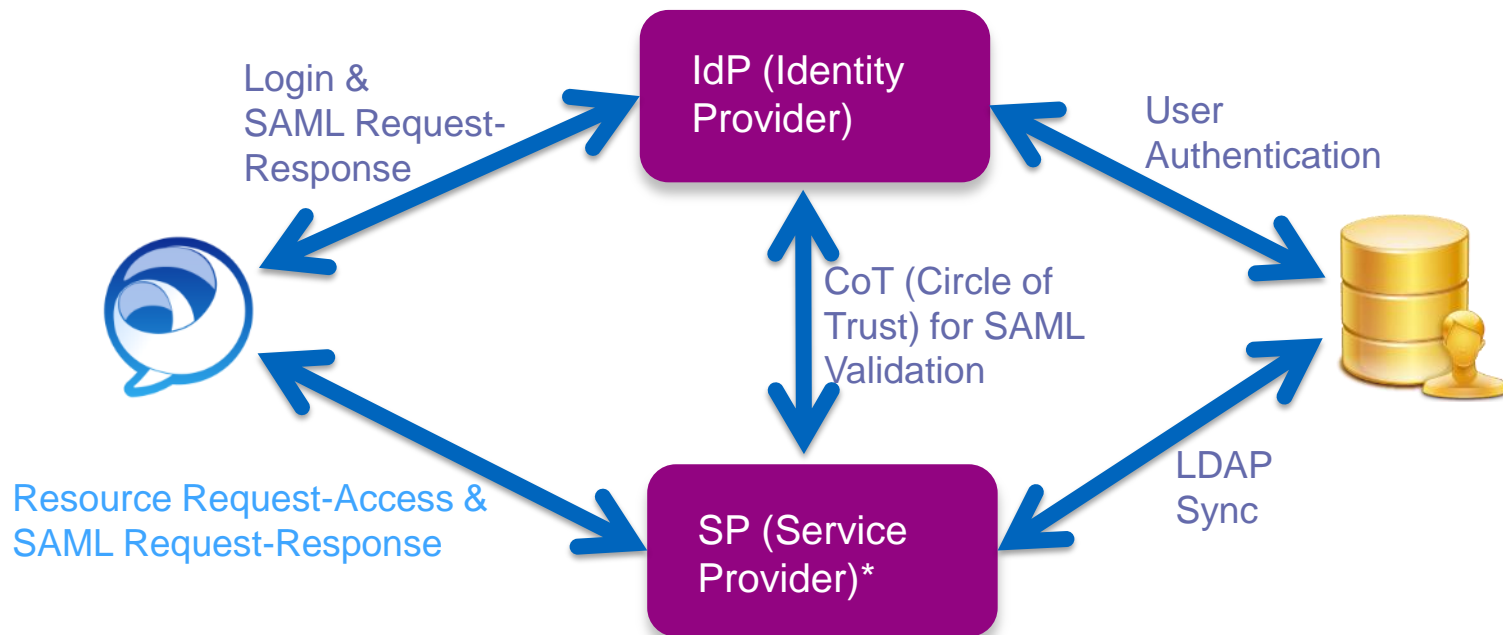
Is your User Secure?

Identity Challenge

- Existing identity stores/syncs
- Existing contact stores
- Existing contact/directory interfaces
- Existing WebEx SSO mechanisms
- Existing UC SSO mechanisms
- Existing authz token mechanisms

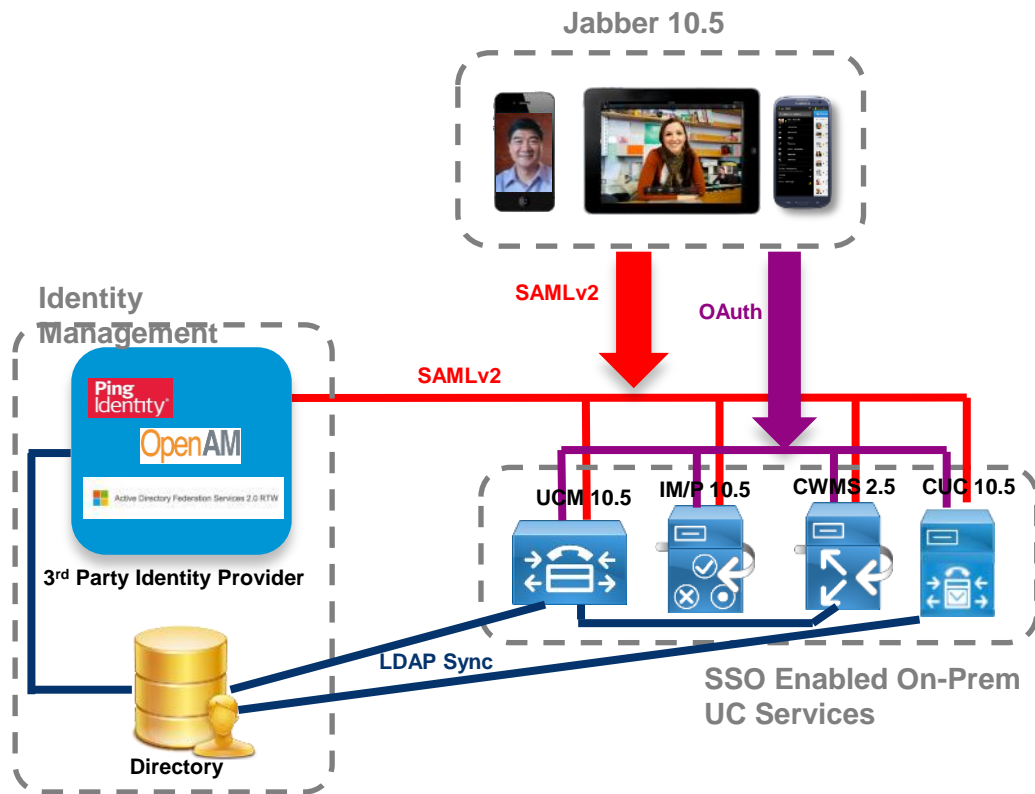


Core Elements of SAMLv2 Single Sign-On



* Service Provider: On-Premises UC Applications (10.5) such as Unified CM, IM and Presence, Unity Connection & CWMS

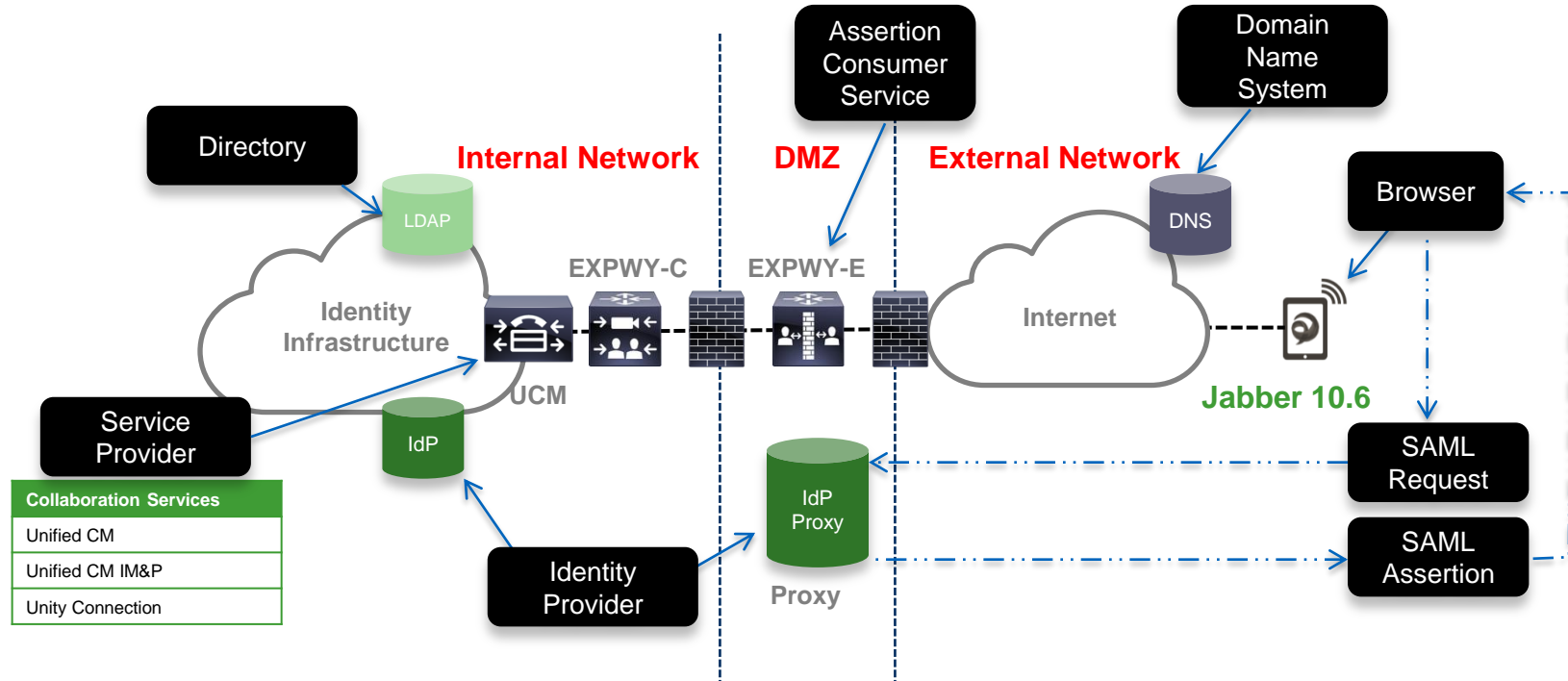
SAMLv2 SSO Architecture for On-Premises Deployment



- Same username & password to login to SSO enabled on-premises UC services
- On-premises UC services will directly integrate with IdP via SAML
- **AnyConnect** is required if **outside** corporate network (Cisco Expressway is not supported)

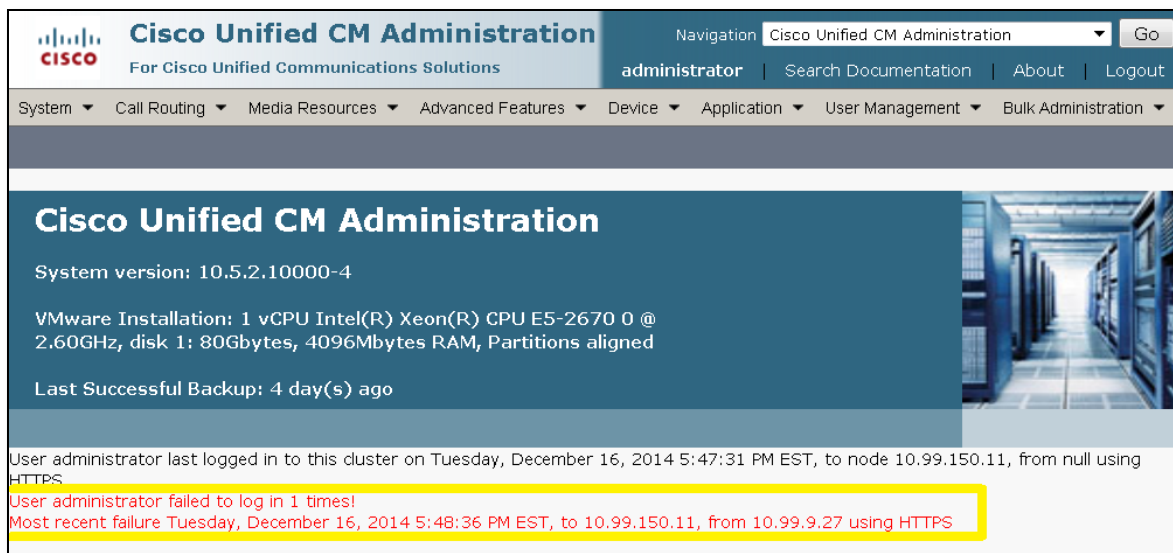
Edge SSO Solution UCM 10.5(2) + Jabber 10.6

SAML Solution Network Elements



Unified CM 10.5.2 Information Assurance Updates

- 1 of 3
- Web Admin Interfaces have been enhanced to display unsuccessful login information, including **client IP address** and **timestamp** in addition to the information provided in prior software releases



The screenshot displays the Cisco Unified CM Administration web interface. The top navigation bar includes the Cisco logo, the title "Cisco Unified CM Administration For Cisco Unified Communications Solutions", and a navigation dropdown menu set to "Cisco Unified CM Administration" with a "Go" button. Below the navigation bar, there are links for "administrator", "Search Documentation", "About", and "Logout". A secondary navigation bar contains dropdown menus for "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", and "Bulk Administration".

The main content area features a large blue header with the text "Cisco Unified CM Administration" and "System version: 10.5.2.10000-4". Below this, it lists "VMware Installation: 1 vCPU Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz, disk 1: 80Gbytes, 4096Mbytes RAM, Partitions aligned" and "Last Successful Backup: 4 day(s) ago".

At the bottom of the page, there is a section for login activity. The text reads: "User administrator last logged in to this cluster on Tuesday, December 16, 2014 5:47:31 PM EST, to node 10.99.150.11, from null using HTTPS". Below this, a yellow highlighted box contains the text: "User administrator failed to log in 1 times! Most recent failure Tuesday, December 16, 2014 5:48:36 PM EST, to 10.99.150.11, from 10.99.9.27 using HTTPS".

Unified CM 10.5.2 Information Assurance Updates

- 2 of 3

- OS Admin CLI updated to include **show login** commands
- Includes OS admin and DRS HTTPS login attempts, plus ssh and console

show logins successful

- To display the details of previous successful logins

```
admin:show logins successful
admin  https      10.77.24.78    Thu Aug  7 14:26    gone - no logout
admin  https      10.77.24.78    Thu Aug  7 14:25 - 14:26    (00:01)
admin  https      10.77.24.78    Thu Aug  7 14:25 - 14:25    (00:00)
```

show logins unsuccessful

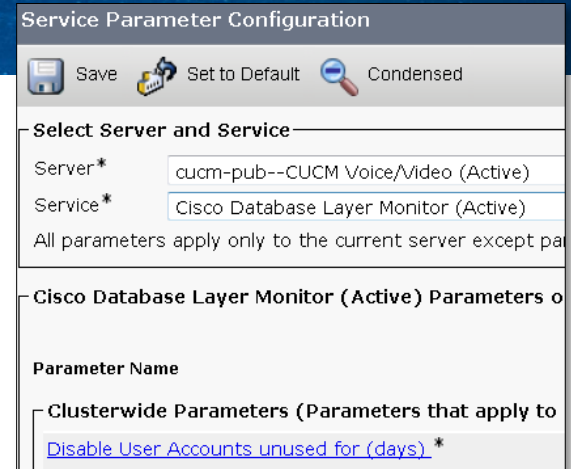
- To display the details of previous unsuccessful logins

```
admin:show logins unsuccessful
admin  https      10.77.24.62    Tue Aug  5 16:29 - 16:29    (00:00)
admin  https      10.77.24.78    Tue Aug  5 15:57 - 15:57    (00:00)
admin  https      10.77.24.62    Tue Aug  5 15:00 - 15:00    (00:00)
```

Unified CM 10.5.2 Information Assurance Updates

3 of 3

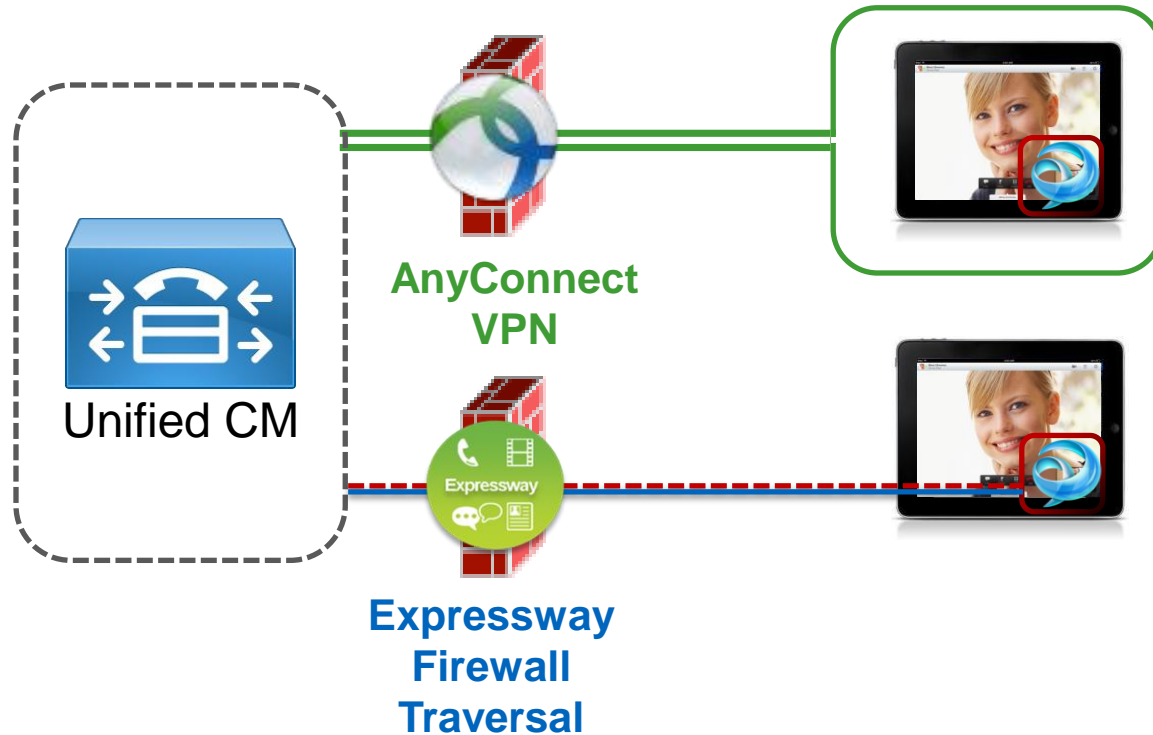
- New feature that can automatically disable inactive end user accounts
- This feature only applies to non-ldap sync'd end users, displayed in UCM as local users
- Feature is activated via Cisco Database Layer Monitor Advanced Service Parameter: “Disable User Accounts unused for (days)”
- The default value of zero days, disables the feature
- Successful end user authentication (pin or password) resets the inactivity timer
- Admin has the ability to enable/disable accounts from the end user pages only when this feature is enabled



A blue-tinted image of Earth from space. The sun is in the upper left, creating a starburst effect. A satellite is visible in the upper right. The Earth's surface shows land and oceans. The text "Is your Connection Secure?" is overlaid in white.

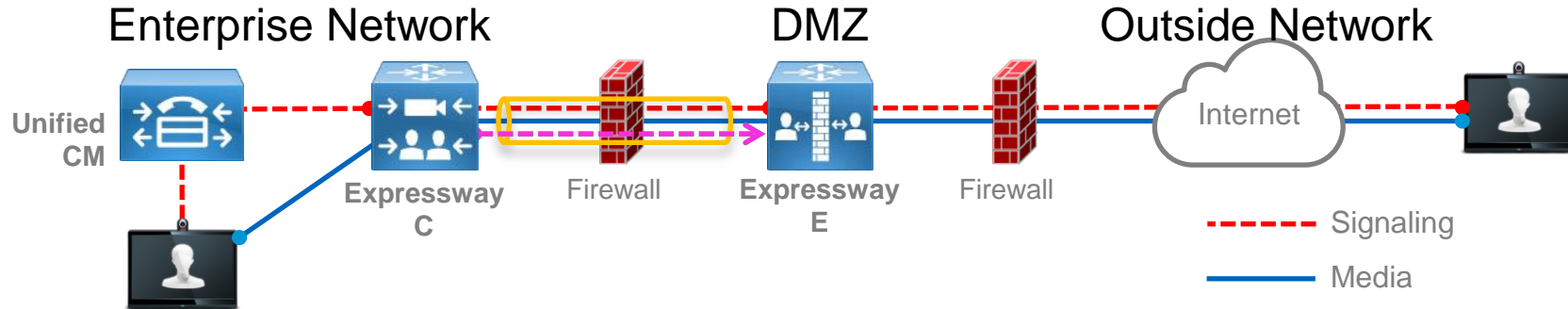
Is your Connection Secure?

Cisco Jabber Remote Access Options



- Layer 3 VPN Solution
- Secures the entire device and it's contents
- AnyConnect allows users access to any permitted applications & data
- **New Complementary Offering**
- Session-based firewall traversal
- Allows access to collaboration applications ONLY
- Personal data not routed through enterprise network

Expressway Firewall Traversal Basics

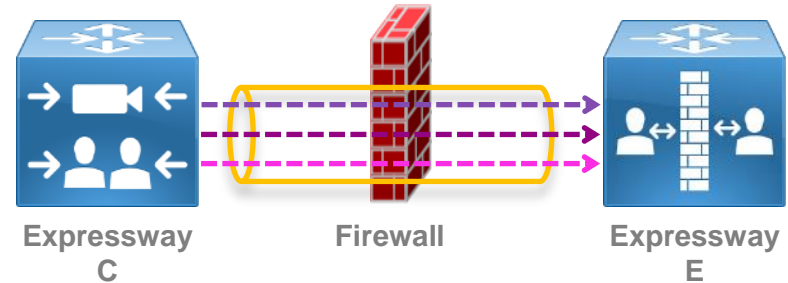


1. **Expressway-E** is the traversal server installed in DMZ. **Expressway-C** is the traversal client installed inside the enterprise network.
2. **Expressway-C** initiates traversal connections outbound through the firewall to specific ports on **Expressway-E** with secure login credentials.
3. Once the connection has been established, **Expressway-C** sends keep-alive packets to **Expressway-E** to maintain the connection
4. When **Expressway-E** receives an incoming call, it issues an incoming call request to **Expressway-C**.
5. **Expressway-C** then routes the call to **Unified CM** to reach the called user or endpoint
6. The call is established and media traverses the firewall securely over an existing traversal connection

X8.1 Firewall Traversal Capabilities Expanded

The X8.1 release delivers 3 key capabilities enabling the Expressway Mobile and Remote Access feature

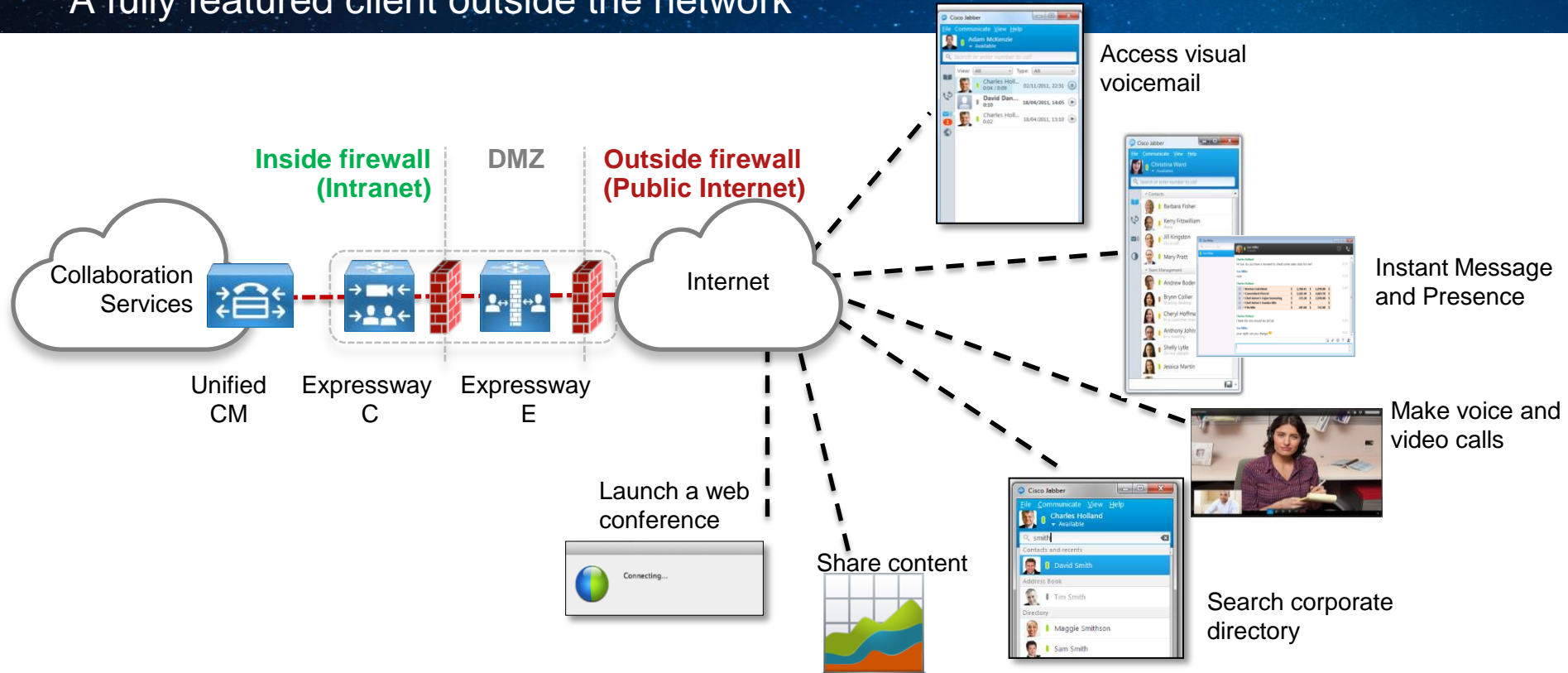
- XCP Router for XMPP traffic
- HTTPS Reverse proxy
- Proxy SIP registrations to Unified CM



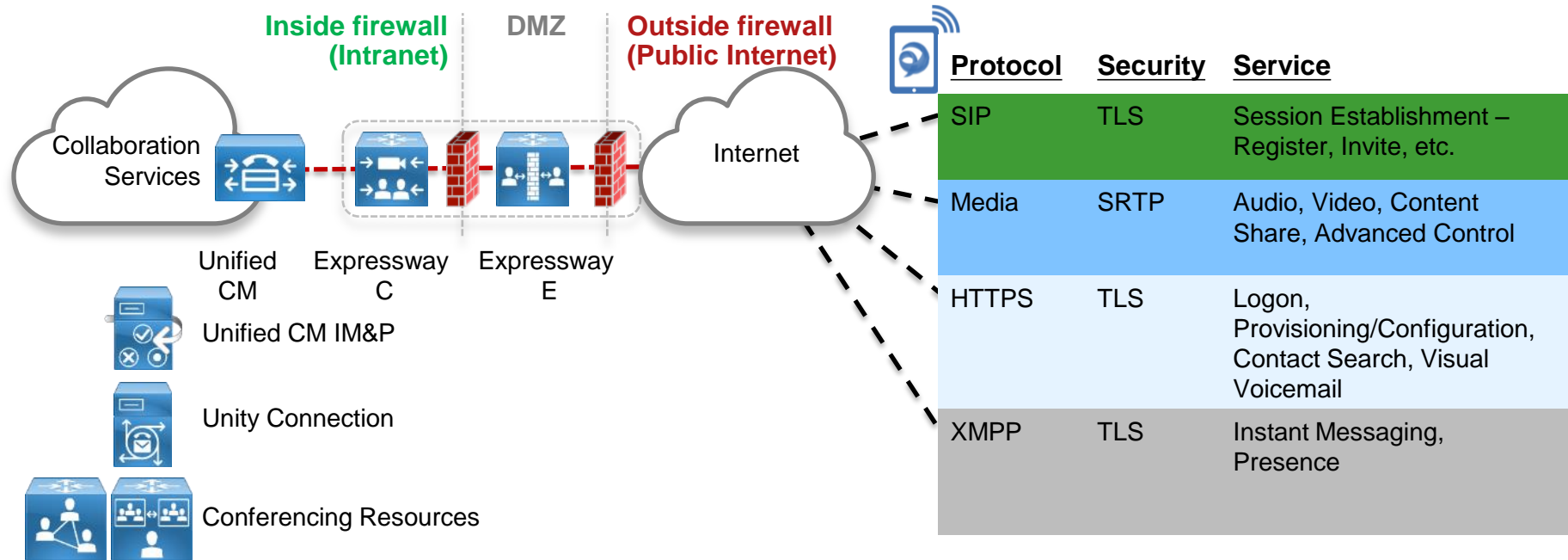
(details on new firewall port requirements covered later)

What can a Jabber client do with Expressway?

A fully featured client outside the network

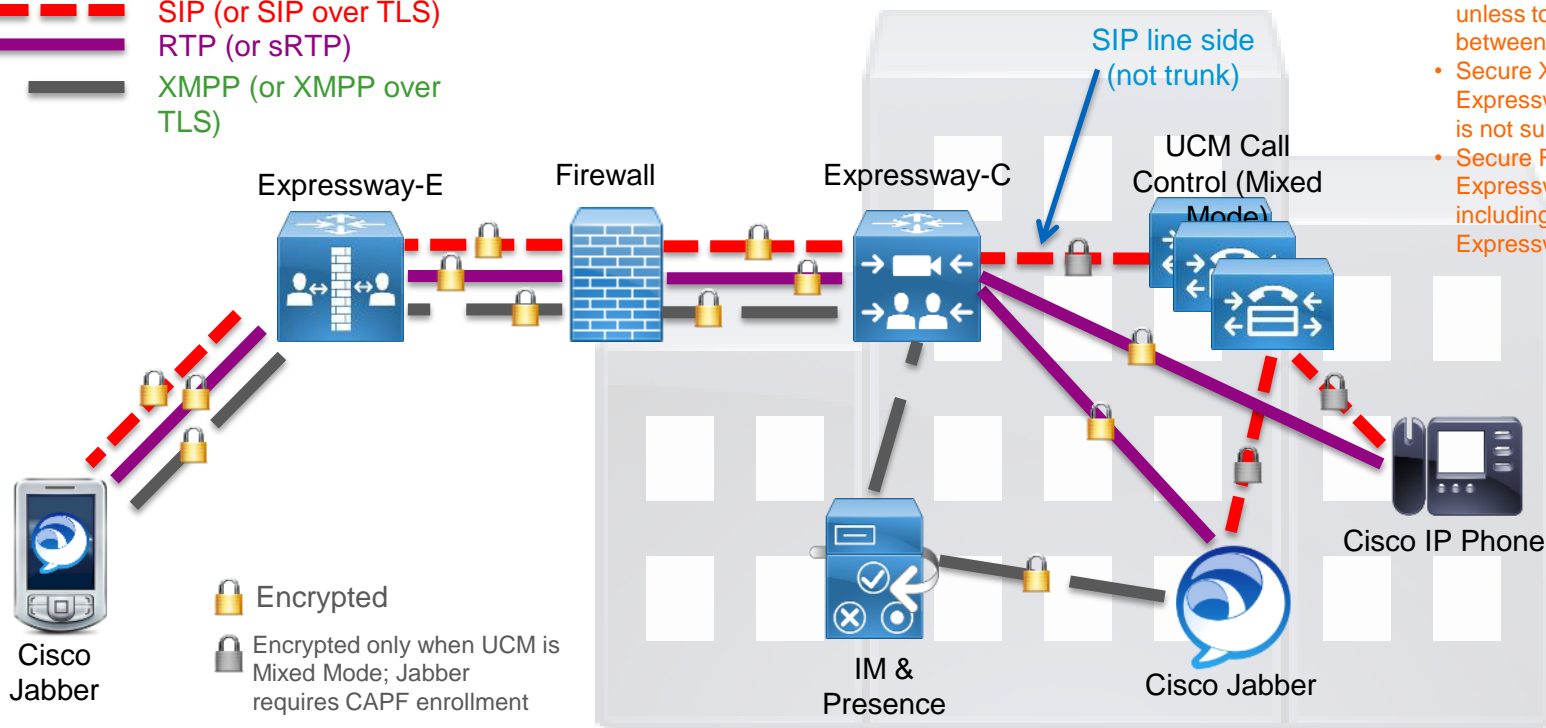


Jabber Protocol Workload Summary



Security over Expressway

- SIP (or SIP over TLS)
- RTP (or sRTP)
- XMPP (or XMPP over TLS)



- Mixed Mode not required unless to secure signaling between UCM and Jabber.
- Secure XMPP between Expressway-C and UCM IM/P is not supported.
- Secure RTP between Expressway-C and endpoints including Jabber requires Expressway X8.2 or higher

“Security is a journey.”



CISCO™