cisco

You make **possible**

Cloud Security Unveiled - All aspects of Network, Data-Security, Compliance and Data Leakage Prevention in Cisco Webex Meetings and Teams

Marc Dionysius - Technical Solution Architect
Paulo J. Correia - Technical Solution Architect
Tobias Neumann- Technical Solution Architect

TECCOL-3033

Barcelona | January 27-31, 2020

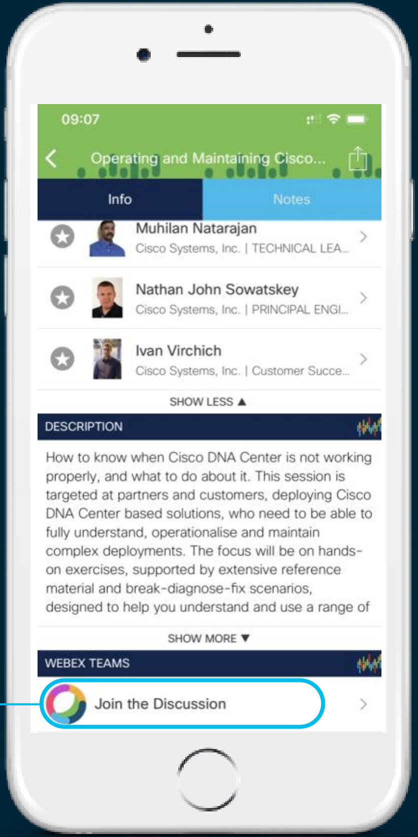
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat
with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click "Join the Discussion"
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



09:07

Operating and Maintaining Cisco...

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

WEBEX TEAMS

Agenda

- Introduction to Cloud Security Challenges
- Legislation and regulation for cloud service
- Data Locality
- Cloud Collaboration architecture
  - Micro Service Architecture
  - Cisco Webex Teams Architecture
- Identity management

Webex service connection to the Cloud

Media Types for Cisco Webex Teams Service

Media Types for Cisco Webex Meetings Service

Media Types for Cisco Webex Calling Service

Firewall support

Hybrid Services connections considerations

- Enterprise security feature for Cloud

Content Ownership

ECM

Device security

DLP, Legal Hold/Retention Policy, Archival

Hybrid Data Security

Roundtable Discussion

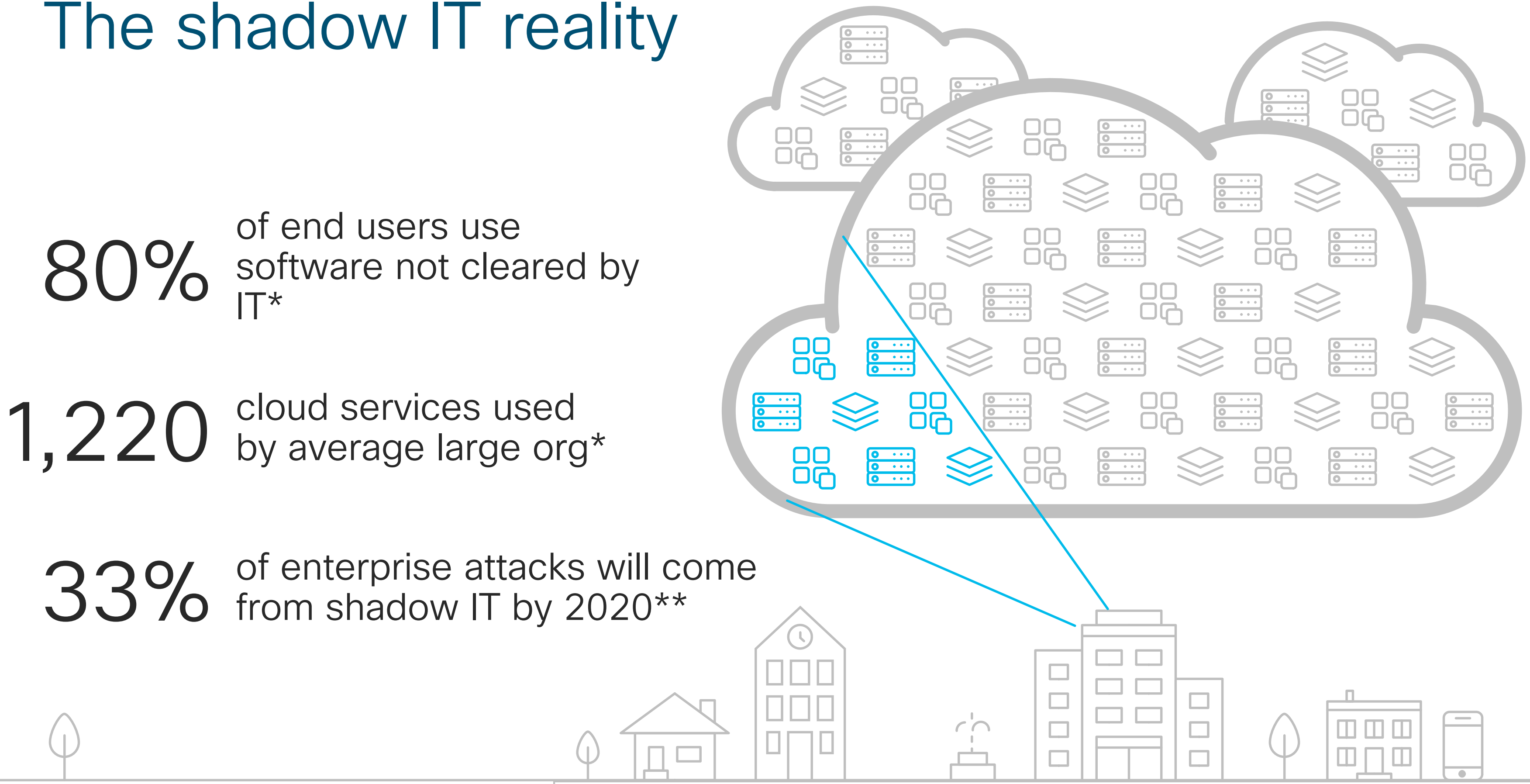
Introduction to Cloud Security Challenges

The shadow IT reality

80% of end users use software not cleared by IT*

1,220 cloud services used by average large org*

33% of enterprise attacks will come from shadow IT by 2020**



*Cisco Cloudlock CyberLab ** Gartner's Top 10 Security Predictions (ref)

Gartner

“Shadow IT is growing and is an unstoppable force”

“If governed, managed and guided appropriately to mitigate the risks, shadow IT can create a lot of value for the organization. But the opposite is also true, in that, left unguided and controlled, it can destroy value.”

Gartner: Embracing and Creating Value From Shadow IT, Simon Mingay, refreshed 5 January 2017

Users and apps have adopted the cloud...

49%
of the workforce is mobile[1]

82%
admit to not using the VPN[2]

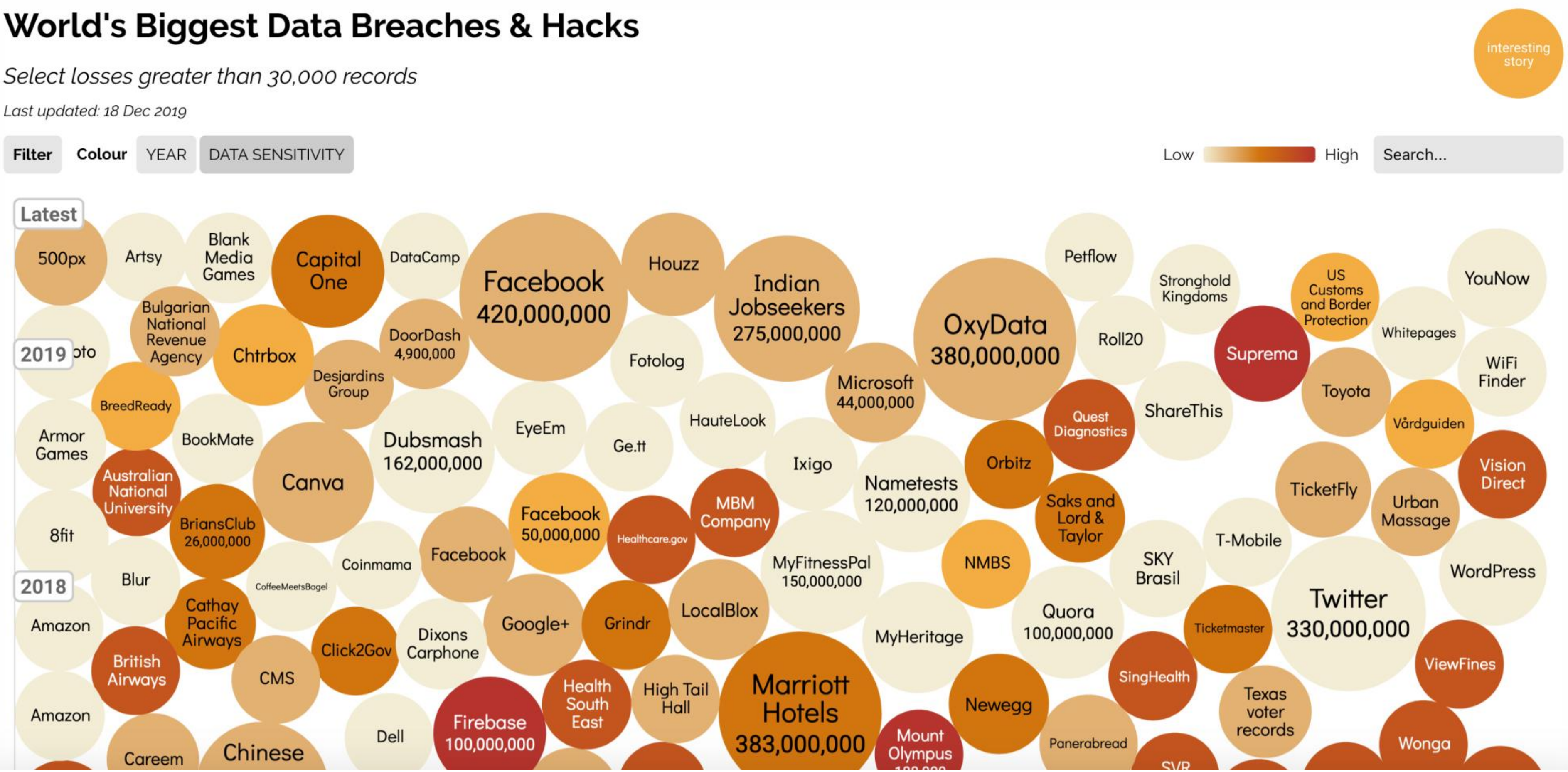
70%
increase in SaaS usage[3]

70%
of branch offices have DIA[4]

...security must, too.

Sources:

1. “Securing Portable Data and Applications for a Mobile Workforce” SANS, 2015
2. “Your Users Have Left the Perimeter. Are You Ready?” IDG, 2016
3. “Keeping SaaS Secure” Gartner, 2016
4. “Securing Direct-To-Internet Branch Offices: Cloud-Based Security Offers Flexibility and Control,” Forrester, 2015



World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

Last updated: 18 Dec 2019

Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

What do we need to know ?

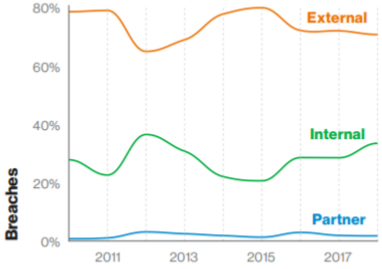
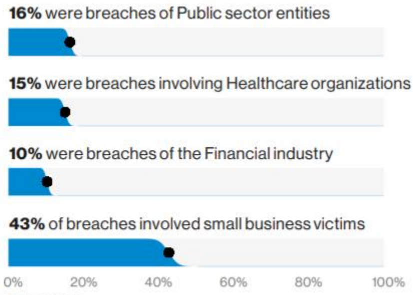


Figure 6. Threat actors in breaches over time



16% were breaches of Public sector entities

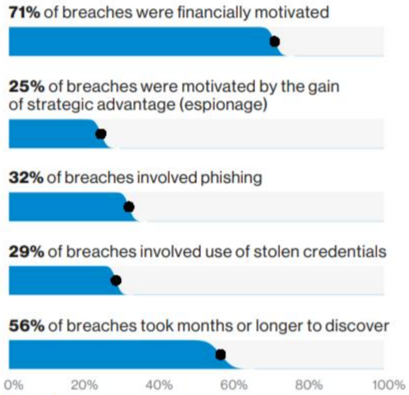
15% were breaches involving Healthcare organizations

10% were breaches of the Financial industry

43% of breaches involved small business victims

Breaches

Figure 2. Who are the victims?



71% of breaches were financially motivated

25% of breaches were motivated by the gain of strategic advantage (espionage)

32% of breaches involved phishing

29% of breaches involved use of stolen credentials

56% of breaches took months or longer to discover

Breaches

Figure 5. What are other commonalities?

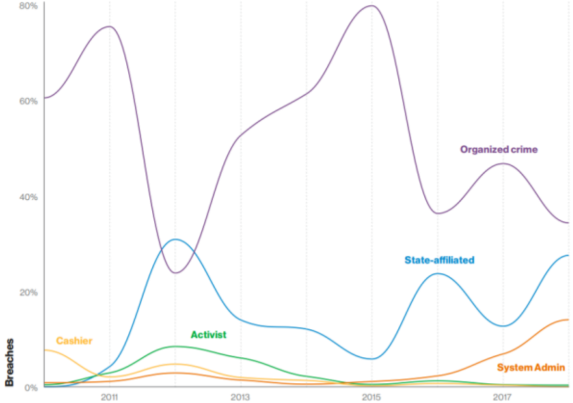
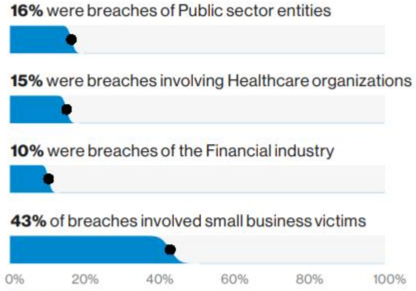


Figure 8. Select threat actors in breaches over time



16% were breaches of Public sector entities

15% were breaches involving Healthcare organizations

10% were breaches of the Financial industry

43% of breaches involved small business victims

Breaches

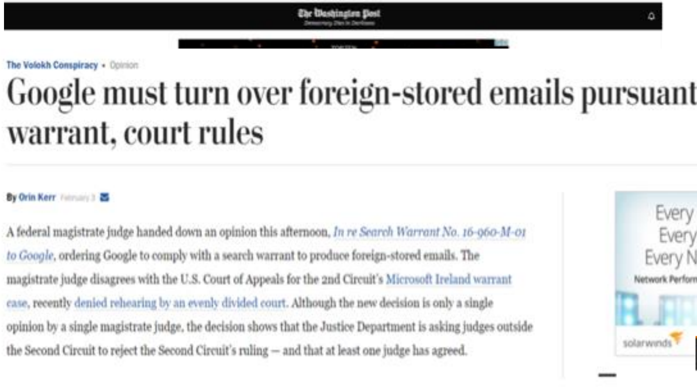
Figure 2. Who are the victims?

Source : 2019 Data Breach Investigations Report

verizon✓ business ready

https://enterprise.verizon.com/resources/reports/dbir/

Data residency means nothing today in Cloud solutions



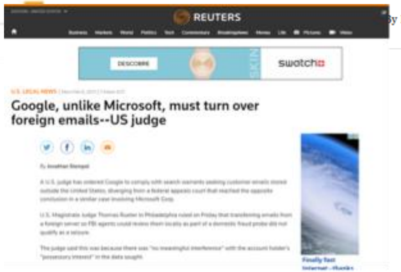
The Washington Post

The Volokh Conspiracy • Opinion

Google must turn over foreign-stored emails pursuant to warrant, court rules

By Orin Kerr February 3

A federal magistrate judge handed down an opinion this afternoon, *In re Search Warrant No. 16-960-M-01 to Google*, ordering Google to comply with a search warrant to produce foreign-stored emails. The magistrate judge disagrees with the U.S. Court of Appeals for the 2nd Circuit's Microsoft Ireland warrant case, recently denied rehearing by an evenly divided court. Although the new decision is only a single opinion by a single magistrate judge, the decision shows that the Justice Department is asking judges outside the Second Circuit to reject the Second Circuit's ruling – and that at least one judge has agreed.



REUTERS

U.S. LEGAL NEWS

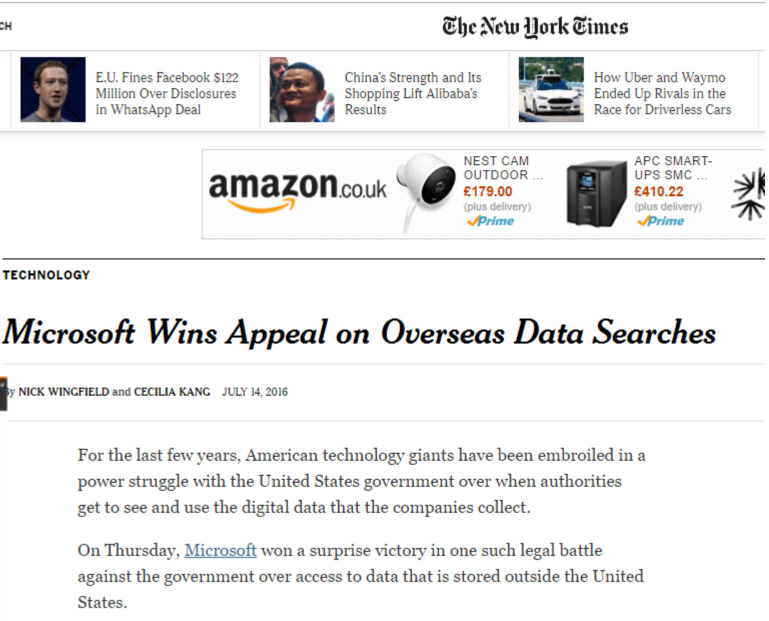
Google, unlike Microsoft, must turn over foreign emails--US judge

By Jonathan Stempel

A U.S. judge has ordered Google to comply with search warrants seeking customer emails stored outside the United States, diverging from a federal appeals court that reached the opposite conclusion in a similar case involving Microsoft Corp.

U.S. Magistrate Judge Thomas Rueter in Philadelphia ruled on Friday that transferring emails from a foreign server so FBI agents could review them locally as part of a domestic fraud probe did not qualify as a seizure.

The judge said this was because there was "no meaningful interference" with the account holder's "possessory interest" in the data sought.



SEARCH

The New York Times

E.U. Fines Facebook $122 Million Over Disclosures in WhatsApp Deal

China's Strength and Its Shopping Lift Alibaba's Results

How Uber and Waymo Ended Up Rivals in the Race for Driverless Cars

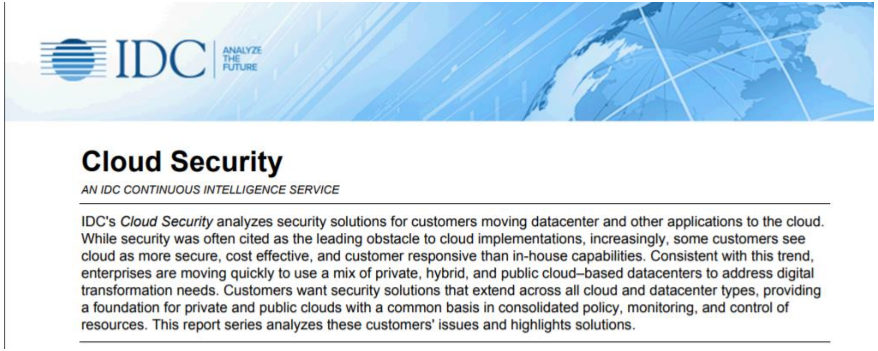
TECHNOLOGY

Microsoft Wins Appeal on Overseas Data Searches

By NICK WINGFIELD and CECILIA KANG JULY 14, 2016

For the last few years, American technology giants have been embroiled in a power struggle with the United States government over when authorities get to see and use the digital data that the companies collect.

On Thursday, Microsoft won a surprise victory in one such legal battle against the government over access to data that is stored outside the United States.



Cloud Security

AN IDC CONTINUOUS INTELLIGENCE SERVICE

IDC's *Cloud Security* analyzes security solutions for customers moving datacenter and other applications to the cloud. While security was often cited as the leading obstacle to cloud implementations, increasingly, some customers see cloud as more secure, cost effective, and customer responsive than in-house capabilities. Consistent with this trend, enterprises are moving quickly to use a mix of private, hybrid, and public cloud–based datacenters to address digital transformation needs. Customers want security solutions that extend across all cloud and datacenter types, providing a foundation for private and public clouds with a common basis in consolidated policy, monitoring, and control of resources. This report series analyzes these customers' issues and highlights solutions.

"While security was often cited as the leading obstacle to cloud implementations, increasingly, some customers see cloud as more secure, cost effective, and customer responsive than in-house capabilities. "

Source :
https://www.idc.com/getdoc.jsp?containerId=IDC_P31286

Legislation and regulation for cloud service

General Data Protection Regulation (GDPR)

May 25
2018

Compliance
Mandate

Increase Data
Subjects Rights

Increasing
Fines

99 Articles of Law

GDPR Principles

- Lawfulness, Fairness and Transparency of the processing
- Purpose Limitation
- Data minimization and proportionality
- Data quality and accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

GDPR quick summary

Consent has to be freely given, informed, unambiguous and can be revoked at any time.

Data Portability, the right to export and edit the data, with the right to change Service Provider

Data Processors are now directly accountable for compliance with data protection laws jointly with Data Controllers

Data Privacy Officers – aka DPOs are required, can be external to the company

Data Protection Impact Assessments (DPIAs) are required under certain circumstances

Data breaches need to be reported within 72 hours

Huge number of data control rights, like the right to be forgotten and the right to freeze data processing.

Privacy by default and by design is mandatory

Webex support for GDPR

- Cisco has published Privacy Data Sheets discussing how Cisco processes personal data in the delivery of our offers, including our WebEx Teams and Messenger:

  https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-webex-teams-privacy-data-sheet.pdf

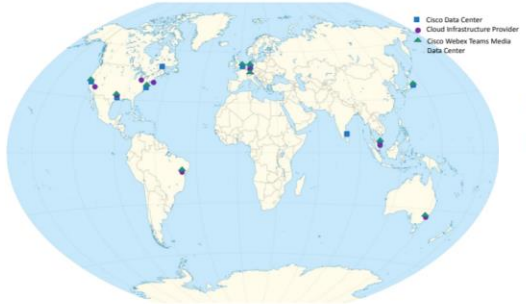
  https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-webex-messenger-privacy-data-sheet.pdf

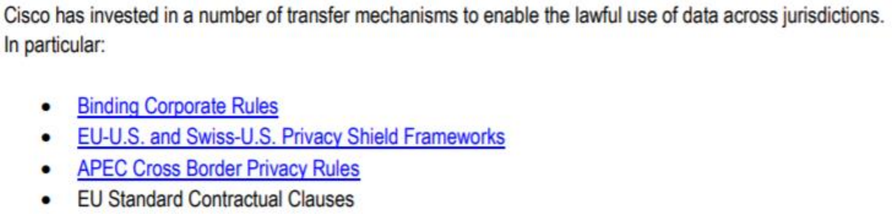
- These data sheets can help customers in meeting their GDPR and other privacy-related obligations when using Cisco's offers.

Cross-Border Transfers

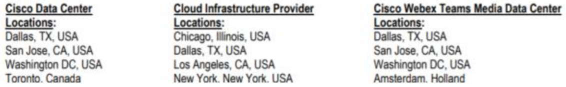
The documents identifies where the different datacenters that hosts the service are located, but also for each product where the processing and storage occurs.

Also talks about the transfer mechanisms supported for Webex


■ Cisco Data Center
● Cloud Infrastructure Provider
▲ Cisco Webex Teams Media Data Center


Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions. In particular:

- Binding Corporate Rules
- EU-U.S. and Swiss-U.S. Privacy Shield Frameworks
- APEC Cross Border Privacy Rules
- EU Standard Contractual Clauses



Cisco Data Center Locations:	Cloud Infrastructure Provider Locations:	Cisco Webex Teams Media Data Center Locations:
Dallas, TX, USA	Chicago, Illinois, USA	Dallas, TX, USA
San Jose, CA, USA	Dallas, TX, USA	San Jose, CA, USA
Washington DC, USA	Los Angeles, CA, USA	Washington DC, USA
Toronto. Canada	New York. New York. USA	Amsterdam. Holland

Third Party Service Providers and Information Security Incident Management

Third-party service providers provide the same level of data protection and information security that you can expect from Cisco.

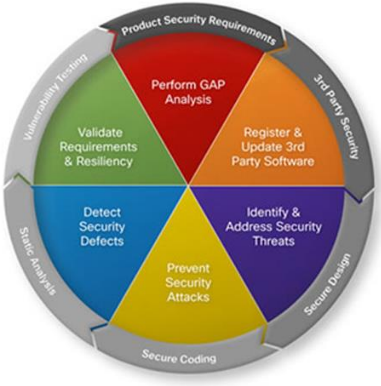
We do not rent or sell your information.

Current list of Cisco Webex Teams third-party service providers with access to personal data can be provided upon request.

We have a company wide process to notify customers and partners of security incidents by using PSIRT's, CSIRTS's and ASIG's.

Cisco Secure Development Lifecycle (CSDL)

The Cisco Secure Development Lifecycle (CSDL) is a repeatable and measurable process designed to increase resiliency and trustworthiness of Cisco products.



- Uses industry leading technology and practices
- Mature and applicable across multiple operating systems
- Adaptable to Agile, DevOps, and Waterfall development methods
- In Cisco Product Development Methodology (CPDM)
- Part of ISO9000 compliance requirements
- CSDL conforms with the guidelines of ISO 27034, the standard for “Information Technology – Security Techniques – Application Security”
    - CSDL provides specific tools and processes to accelerate Cisco's development methodology and culture toward developing secure, resilient and trustworthy products.

A Program of certifications for Webex Teams to offer cloud services that you can trust

Best practices

Data center compliance

- ISO 27001/ISO 27017/ISO 27018
- ISO 9001
- SOC 2 Type 2 and SOC 3
- Cloud Computing Compliance Controls Catalog (C5)
- In addition, eDiscovery, CASB integrations for DLP, retention settings, Legal Hold and many more security controls for compliance

Data privacy

- HIPAA: Data privacy and security provisions for safeguarding medical information
- GDPR: Processing by an individual, a company, or an organization of personal data relating to individuals in the E.U.

Cross-border controls

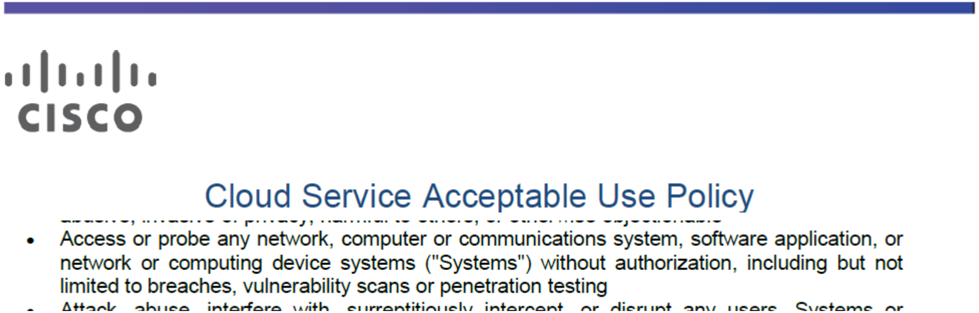
- E.U.-U.S. privacy shield
- Swiss-U.S. privacy shield
- APEC cross-border privacy rules

External Security Audits and PEN tests

- Cisco or any cloud vendor don’t allow for PEN tests against their cloud components. Clearly stated in the Cloud Service Acceptable Use Policy sign by the customer.

- To address this rule, Cisco provide **attestation reports** done by 3rd parties companies that market recognized, in fact that is one of the requirements for SOC 2 Type I, document can be request to CIC.

- Customer can do PEN tests against the hybrid components, but they are required to tell Cisco about it.



Cloud Service Acceptable Use Policy

abusive, invasive of privacy, harmful to others, or otherwise objectionable

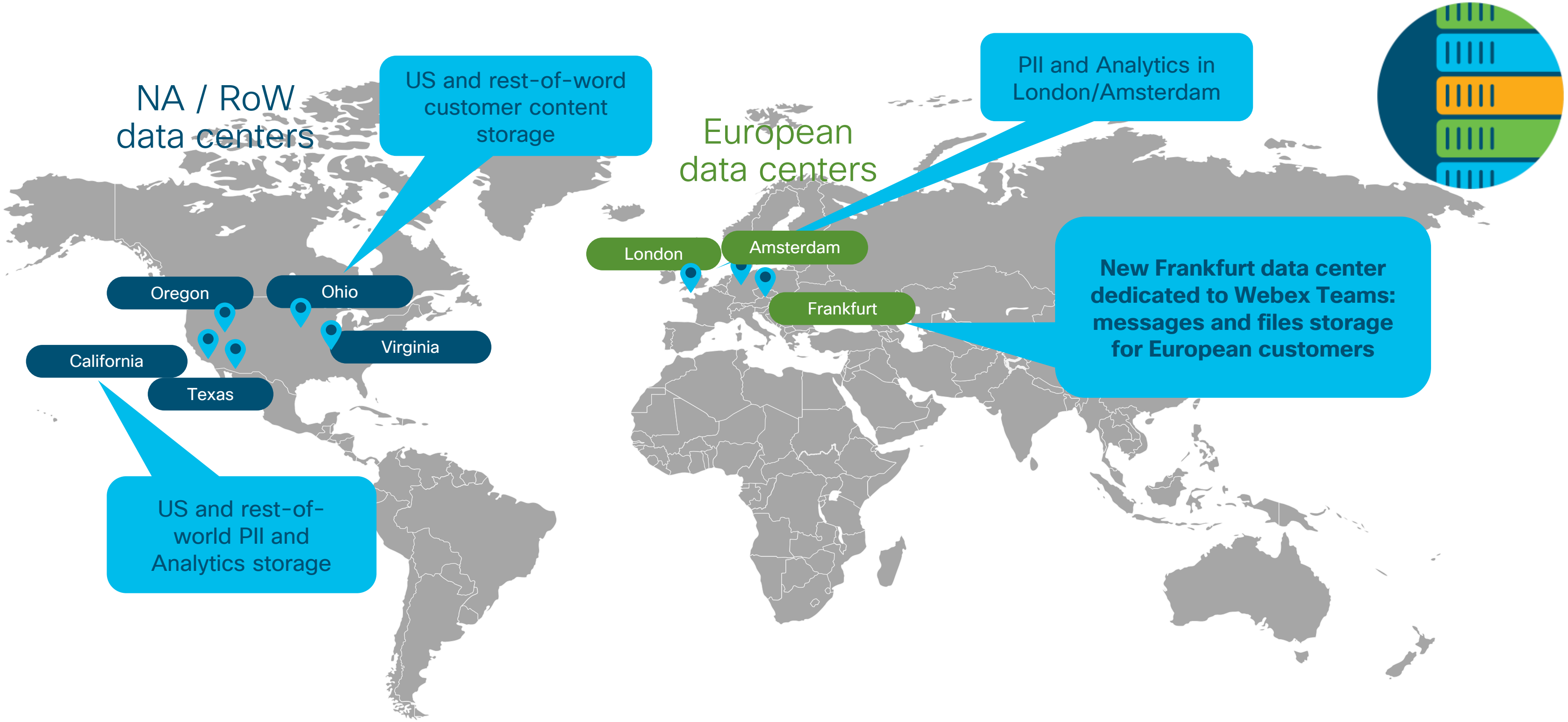
- Access or probe any network, computer or communications system, software application, or network or computing device systems ("Systems") without authorization, including but not limited to breaches, vulnerability scans or penetration testing
- Attack, abuse, interfere with, surreptitiously intercept, or disrupt any users, Systems or

Data Locality

Why Data Locality?

Data privacy	Open, global collaboration	Enterprise grade
Keep data local in regional data centers	Fast authentication and seamless collaboration	Scalable, resilient, responsive

New data center to keep your data closer



US and rest-of-word customer content storage

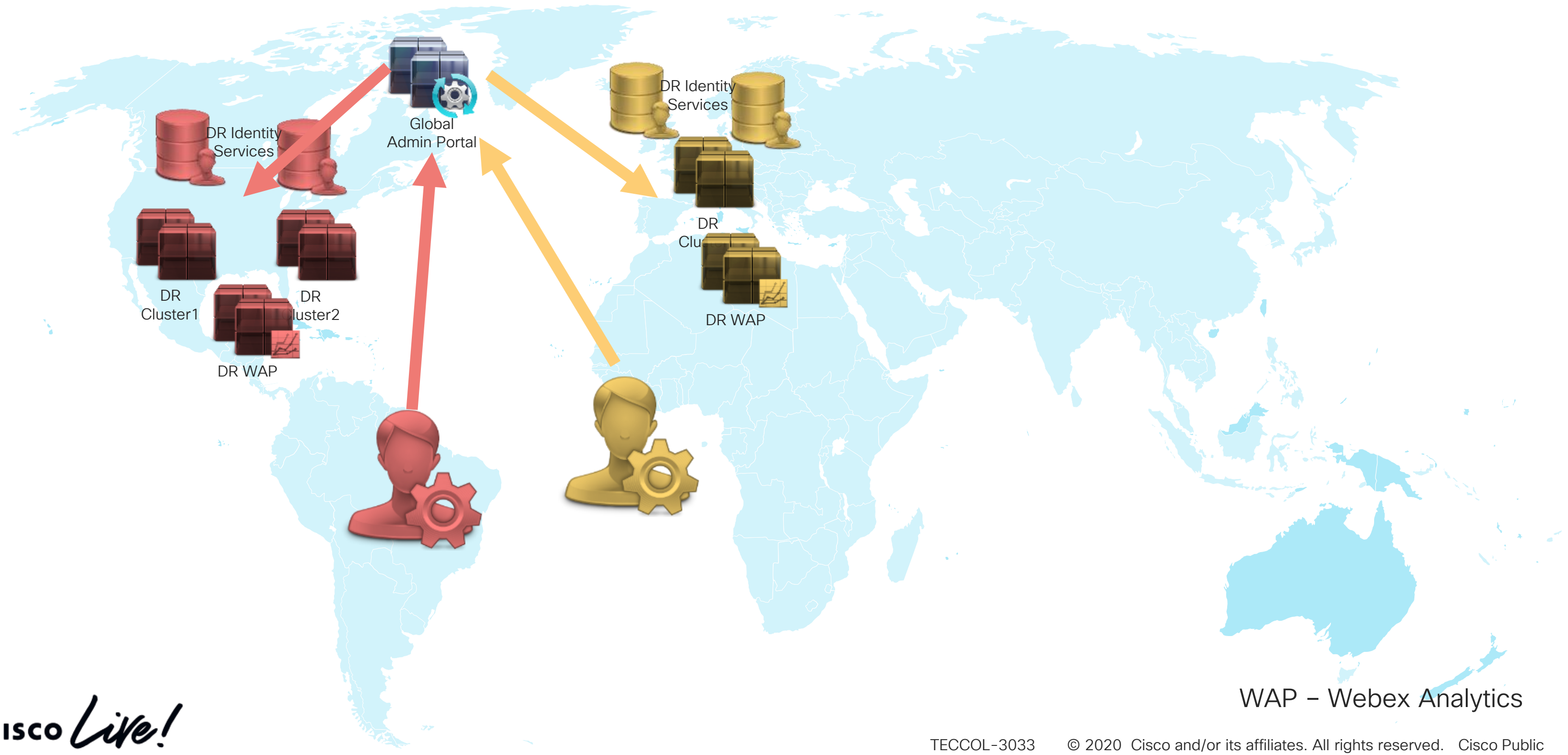
US and rest-of-world PII and Analytics storage

PII and Analytics in London/Amsterdam

New Frankfurt data center dedicated to Webex Teams: messages and files storage for European customers

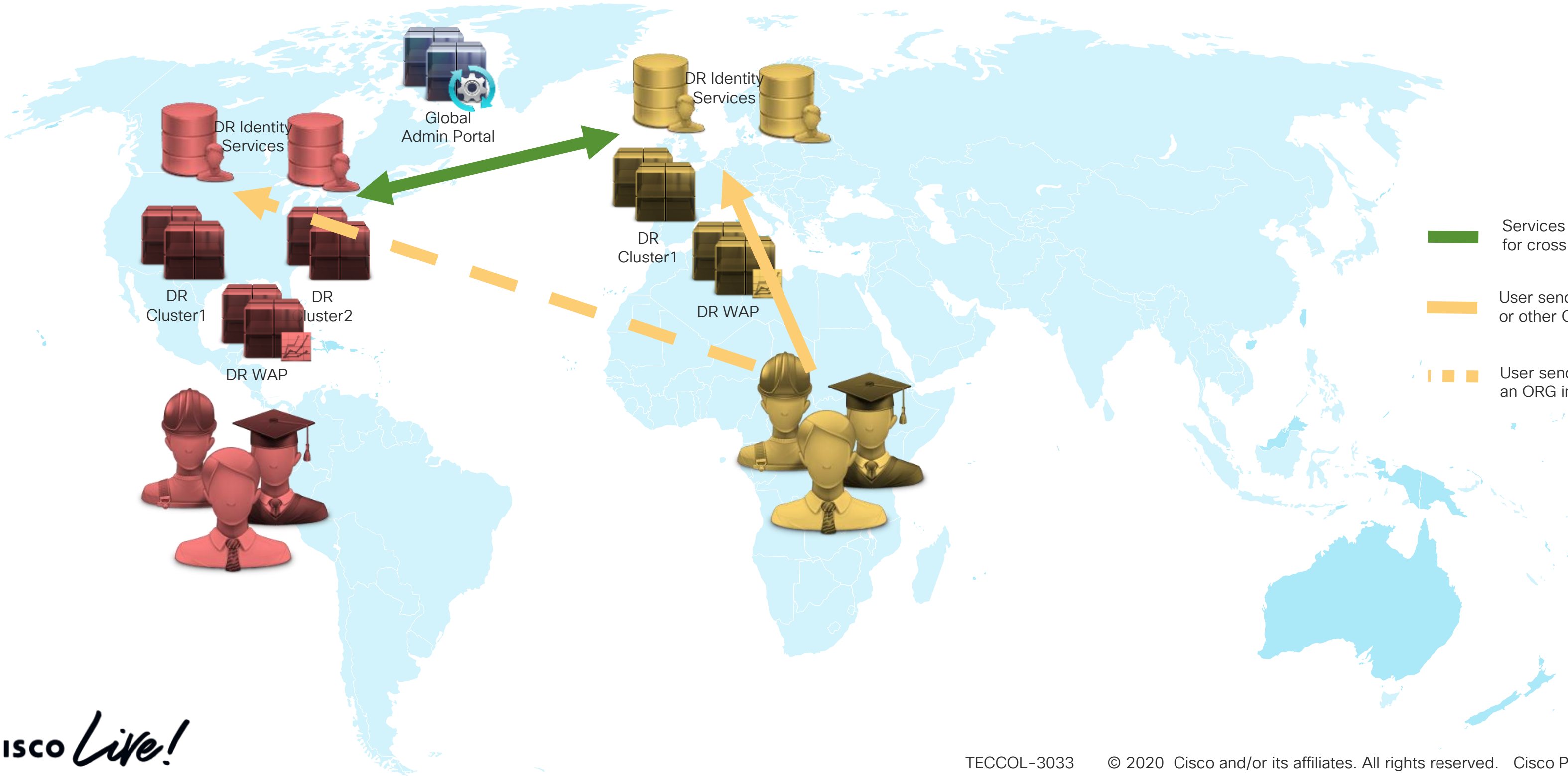
Architecture for the Webex Federation Services

Administration Services



WAP – Webex Analytics

Architecture for the Webex Federation Services
User Services



Global
Admin Portal

DR Identity
Services

DR
Cluster1

DR
luster2

DR WAP

DR Identity
Services

DR
Cluster1

DR WAP

🟩 Services Exchange breadcrumbs for cross-cluster message

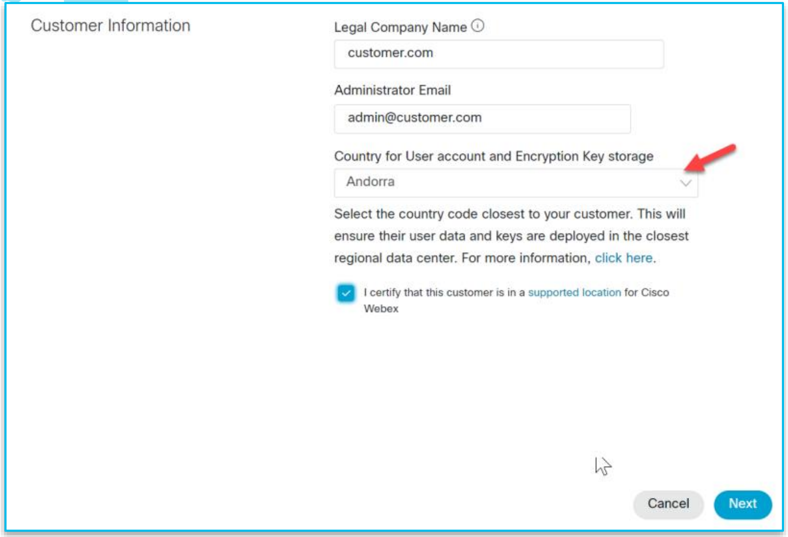
🟨 User sends message to his ORG or other ORG in the same Location

▪ ▪ ▪ User sends message to an Paulon an ORG in another location

Which ORG's will get to the European Datacenters ?

DR Identity Services
DR Clu
DR WAP

Any Webex ORG, that when will be created with the location of a country in EMEAR (Europe, Middle East, Africa and Russia) will be provision in the European Cluster



Customer Information

Legal Company Name ⓘ

customer.com

Administrator Email

admin@customer.com

Country for User account and Encryption Key storage

Andorra

Select the country code closest to your customer. This will ensure their user data and keys are deployed in the closest regional data center. For more information, click here.

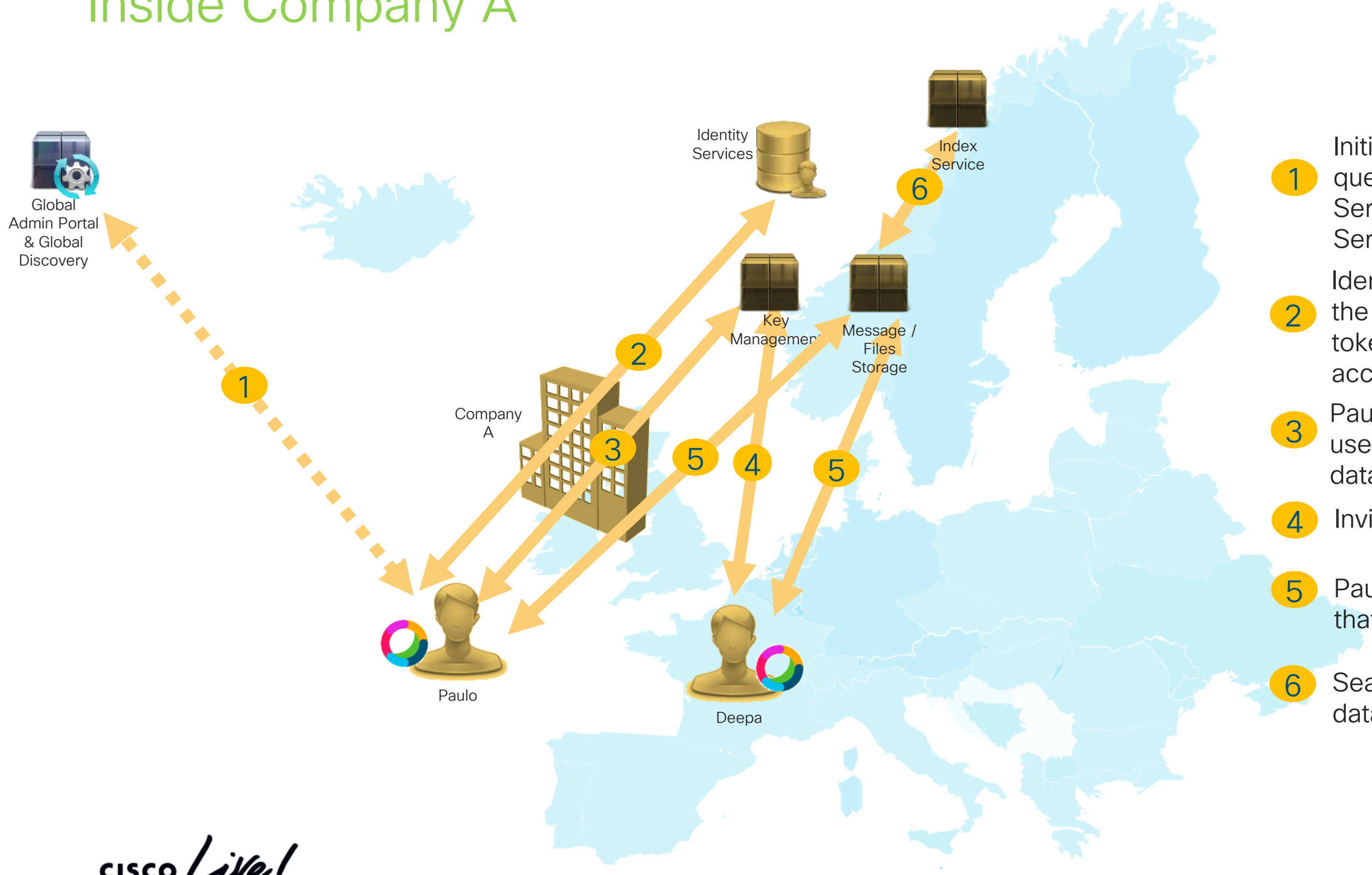
☑ I certify that this customer is in a supported location for Cisco Webex

Federation/Data locality Use cases details

- European User Messaging – Same Data Center
- European Media Processing for Cloud Devices Devices – Same Data Center
- European Whiteboarding – Same Data Center
- European Users Messaging – Across Data Centers
- 1-1 Conversations Rules
- Calendar Data – Across Data Centers
- E-Discovery Services – Across Data Centers
- Analytics

EMEAR User Messaging - Same Data Center

Inside Company A



1 Initial, after installing Webex Teams, questions to GDS (Global Discovery Service) to know where his Identity Services resides

2 Identity Services in EMEA Authenticate the Paulo, then provides an OAuth token for services Authorization access.

3 Paulo creates a space with Deepa and uses one Key issue from EMEA datacenter

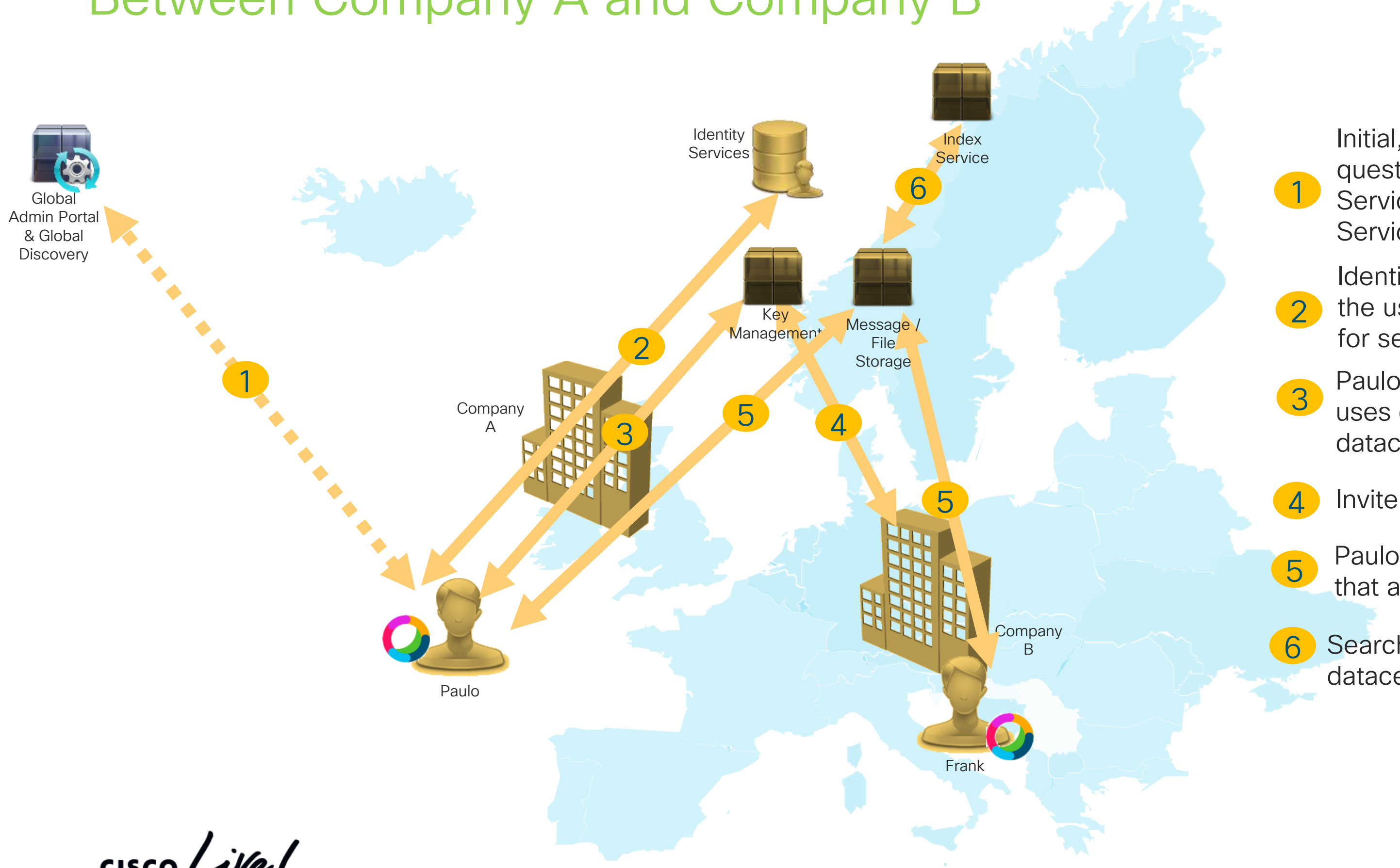
4 Invite and share key with Deepa

5 Paulo and Deepa exchange messages that are stored in EMEA datacenter

6 Search indexes created in EMEA datacenter

European User Messaging – Same Data Center

Between Company A and Company B



1 Initial, after installing Webex Teams, questions to GDS (Global Discovery Service) to know where his Identity Services resides

2 Identity Services in EMEA Authenticate the user, then provide an OAuth token for services Authorization access.

3 Paulo creates a space with Frank and uses one Key issue from EMEA datacenter

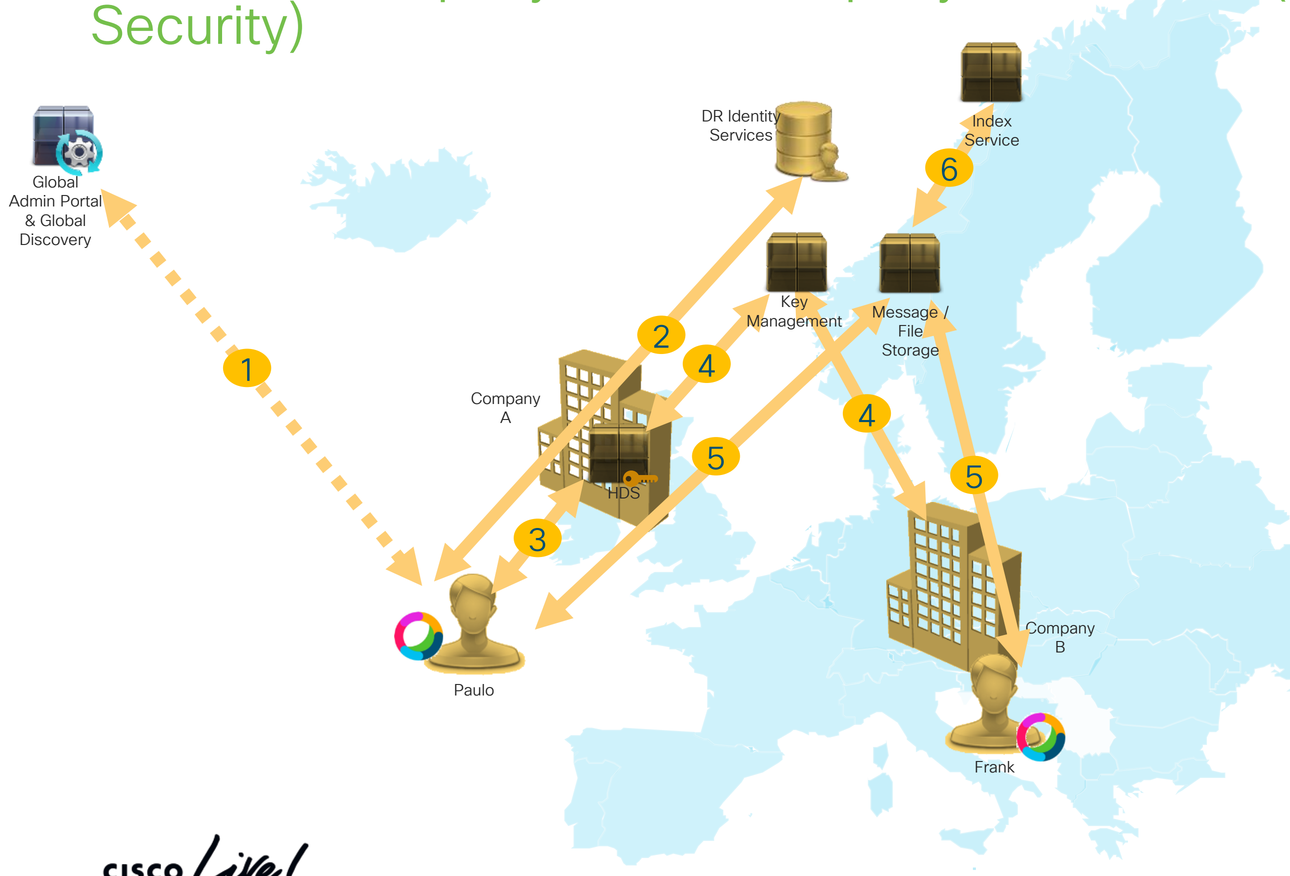
4 Invite and share key with Frank

5 Paulo and Frank exchange messages that are stored in EMEA datacenter

6 Search indexes created in EMEA datacenter

European User Messaging – Same Data Center

Between Company A and Company B with HDS (Hybrid Data Security)



1 Initial, after installing Webex Teams, questions to GDS (Global Discovery Service) to know where his Identity Services resides

2 Identity Services in EMEA Authenticate the user, then provide an OAuth token for services Authorization access.

3 Paulo creates a space with Frank and uses one Key from his company HDS

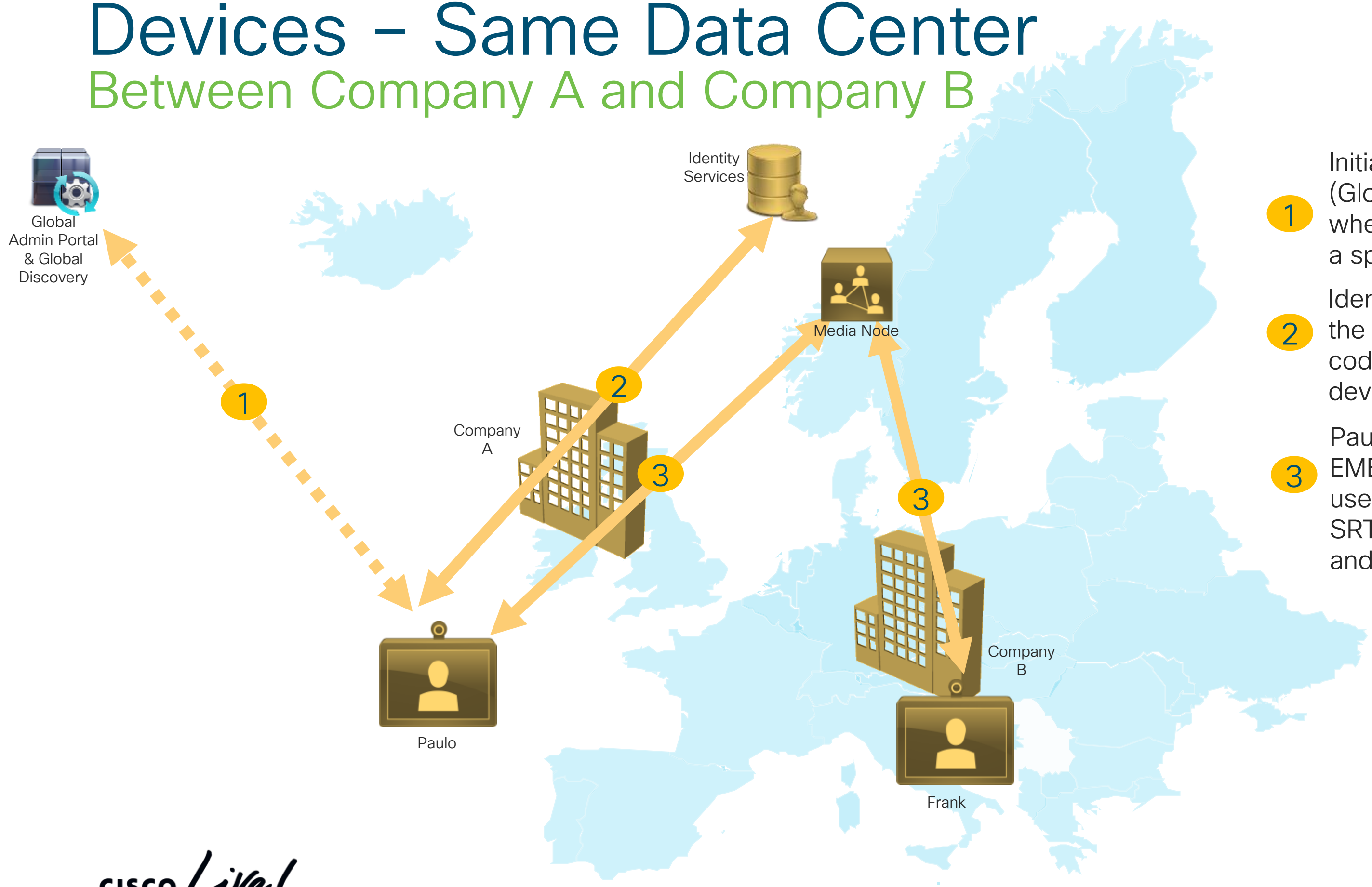
4 Invite Frank to a conversation and Company A HDS gives the key to Frank via EMEA Key Management system

5 Paulo and Frank exchange messages that are stored in EMEA datacenter

6 Search indexes created in EMEA datacenter

European Media Processing for Cloud Devices Devices – Same Data Center

Between Company A and Company B



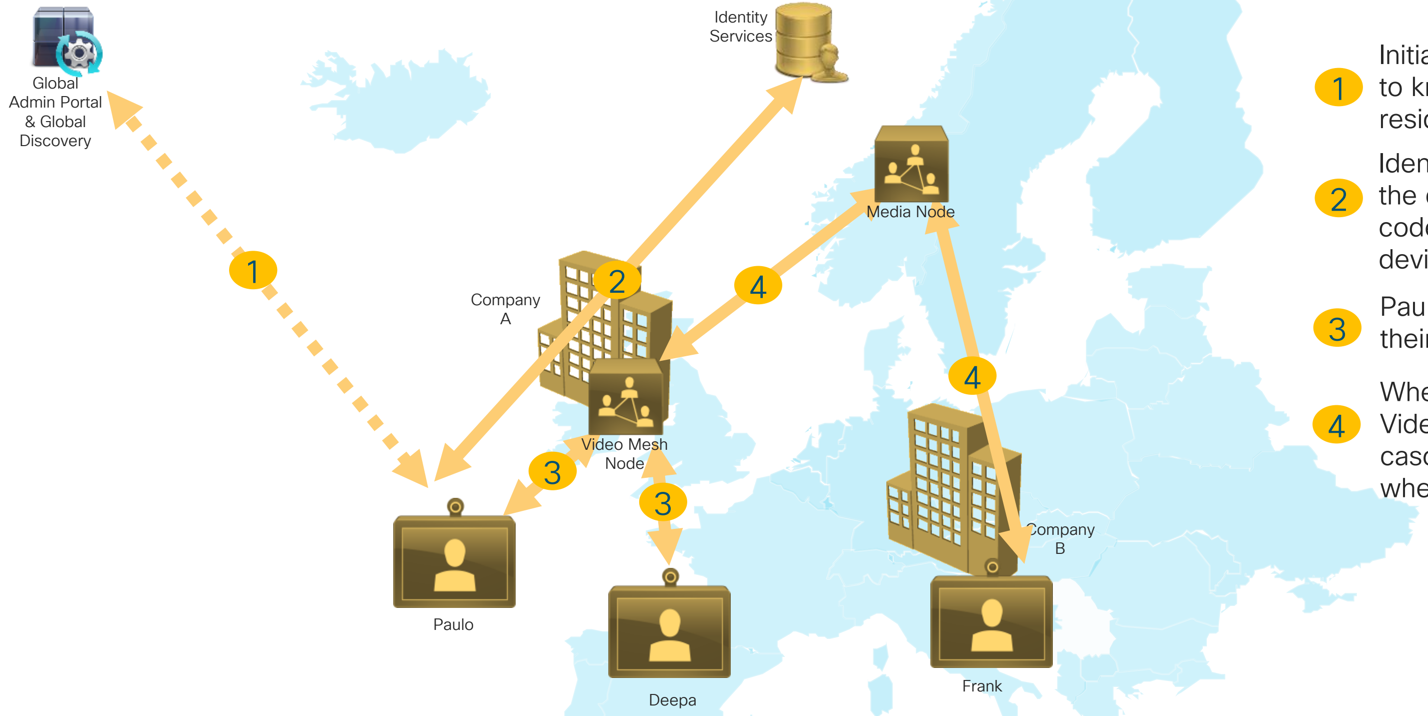
1 Initial video device questions to GDS (Global Discovery Service) to know where his Identity Services resides for a specific activation code.

2 Identity Services in EMEA authenticate the device based on the activation code , and register it in the EMEA device database

3 Paulo calls Frank using media nodes in EMEA datacenter, for signalization it uses WebRTC over TLS and for media SRTP with SDES between endpoint and Media nodes

European Media Processing for Cloud Devices – Same Data Center

Between Company A and Company B with VMN (Video Mesh Node)



1 Initial video device questions to GDS to know where his Identity Services resides for a specific activation code.

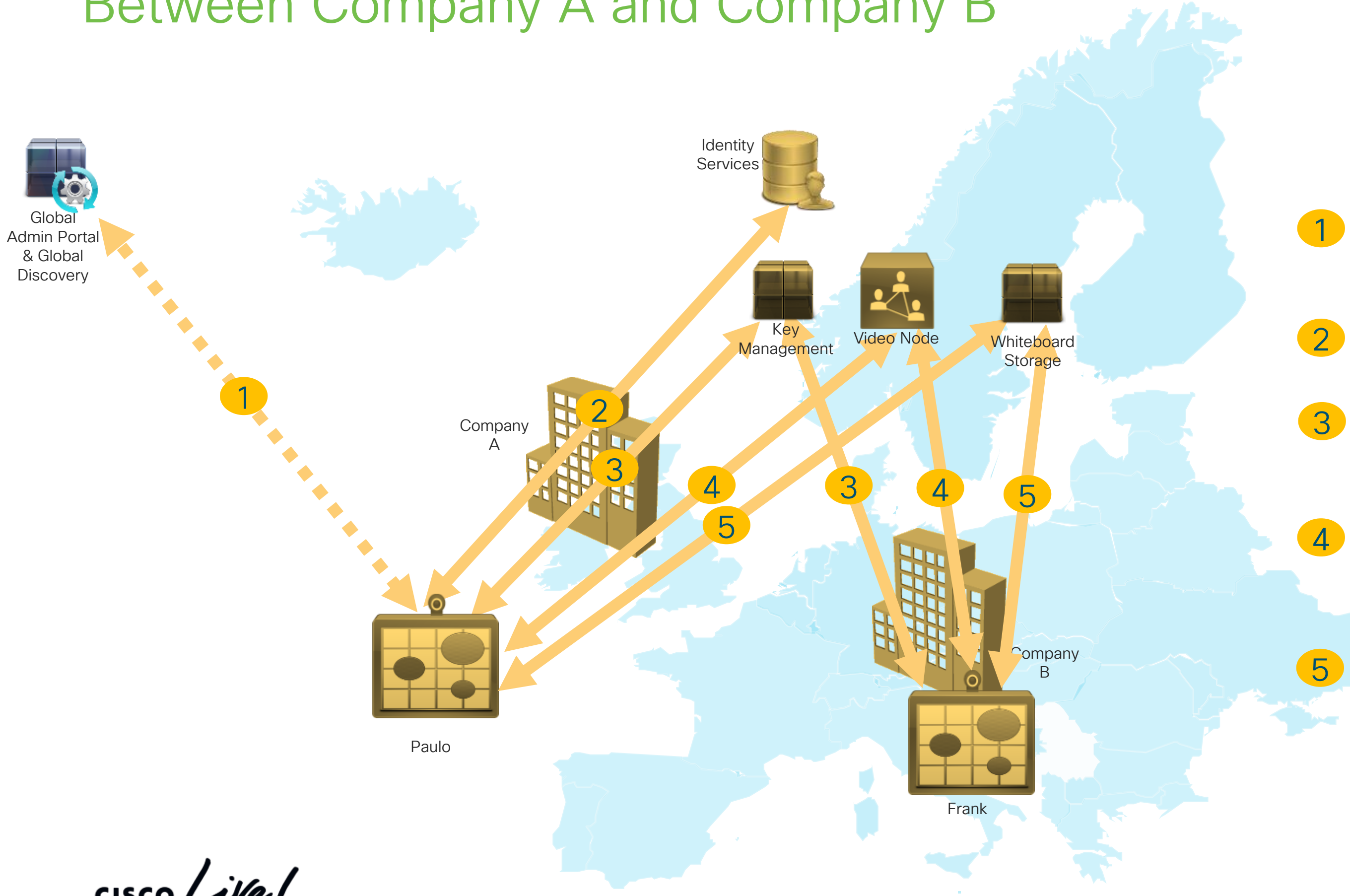
2 Identity Services in EMEA authenticate the device based on the activation code , and register it in the EMEA device database

3 Paulo and Deepa join a conference in their company Video Mesh Node

4 When Frank join the conference, the Video Mesh node of Company A will cascade to the EMEA Media Node, where Frank joined

European Whiteboarding – Same Data Center

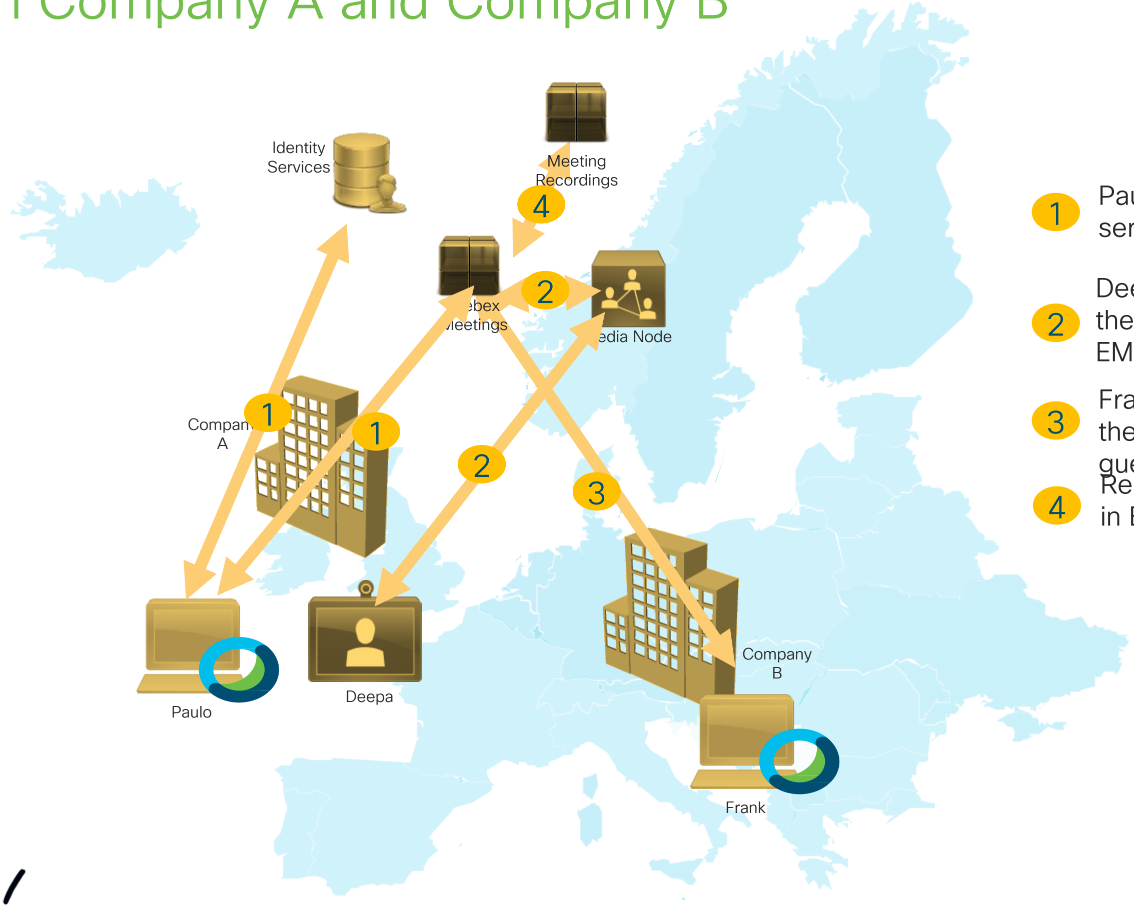
Between Company A and Company B



1. Initial video device questions to GDS to know where his Identity Services resides for a specific activation code
2. Identity Services in EMEA authenticate the device based on the activation code provide an OAuth token
3. Paulo starts an whiteboard with Frank and requires a key for encryption of the content
4. Paulo calls Frank using media nodes in EMEA datacenter, for signalization it uses WebRTC over TLS and for media SRTP with SDES between endpoint and Media nodes
5. Whiteboard strokes are stores encrypted in EMEA datacenter

European Webex Meetings - Same Data Center

Between Company A and Company B



1 Paulo authenticates in EMEA Identity services and starts an Webex Meeting

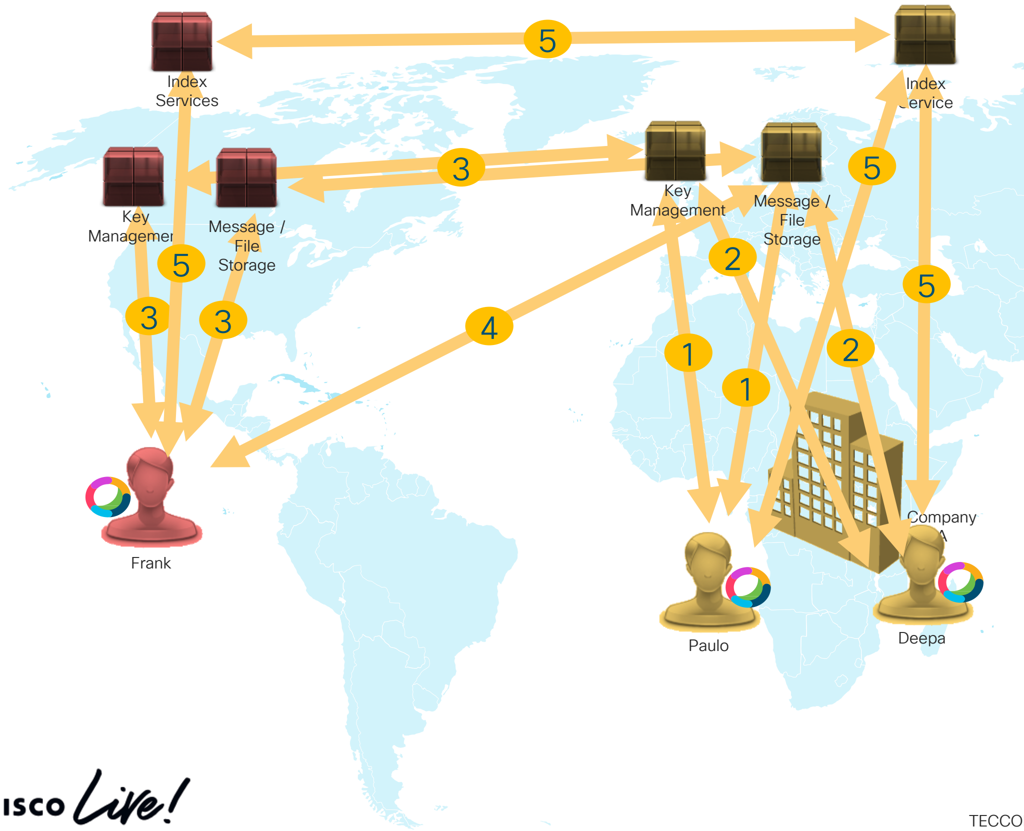
2 Deepa from the same company joins the meeting from a video device via EMEA Media Node

3 Frank from company B in EMEA join the meeting hosted in EMEA as a guest

4 Recording of the Meetings are hosted in EMEA datacenters

European Users Messaging – Across Data Centers

Between Company A in EMEAR and Americas User



1 Paulo creates a space with a keys given EMEAR datacenter and content and files will be store in EMEA

2 Keys and access to the space will be provided to Deepa

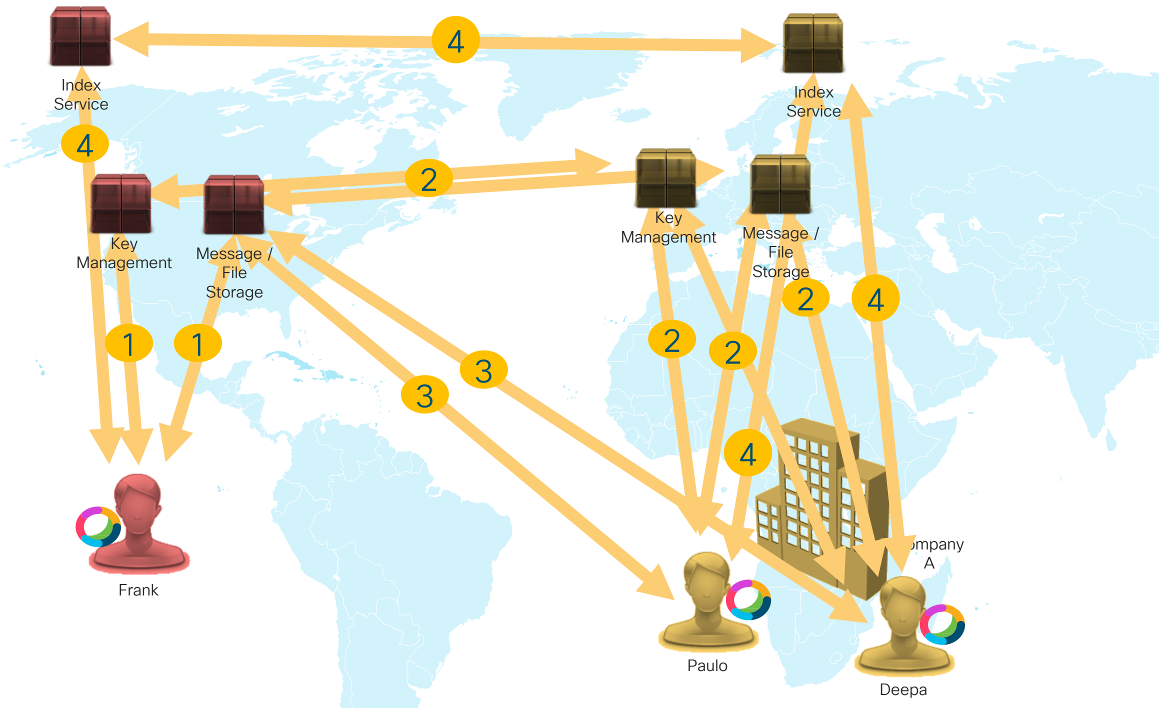
3 Frank is invited and receives the key via US datacenter and receives a remote reference breadcrumb, pointing to the message in EMEA cluster

4 Frank follows the breadcrumb to get messages and/or file from EMEA datacenter
Any content created by Frank will be hosted in EMEA

5 One-way hashed indexes for searches are store in both clusters, all users clients (Paulo, Deepa, and Frank) do the search in their clusters.

European Users Messaging – Across Data Centers

Between Americas User and Users from Company A in EMEAR



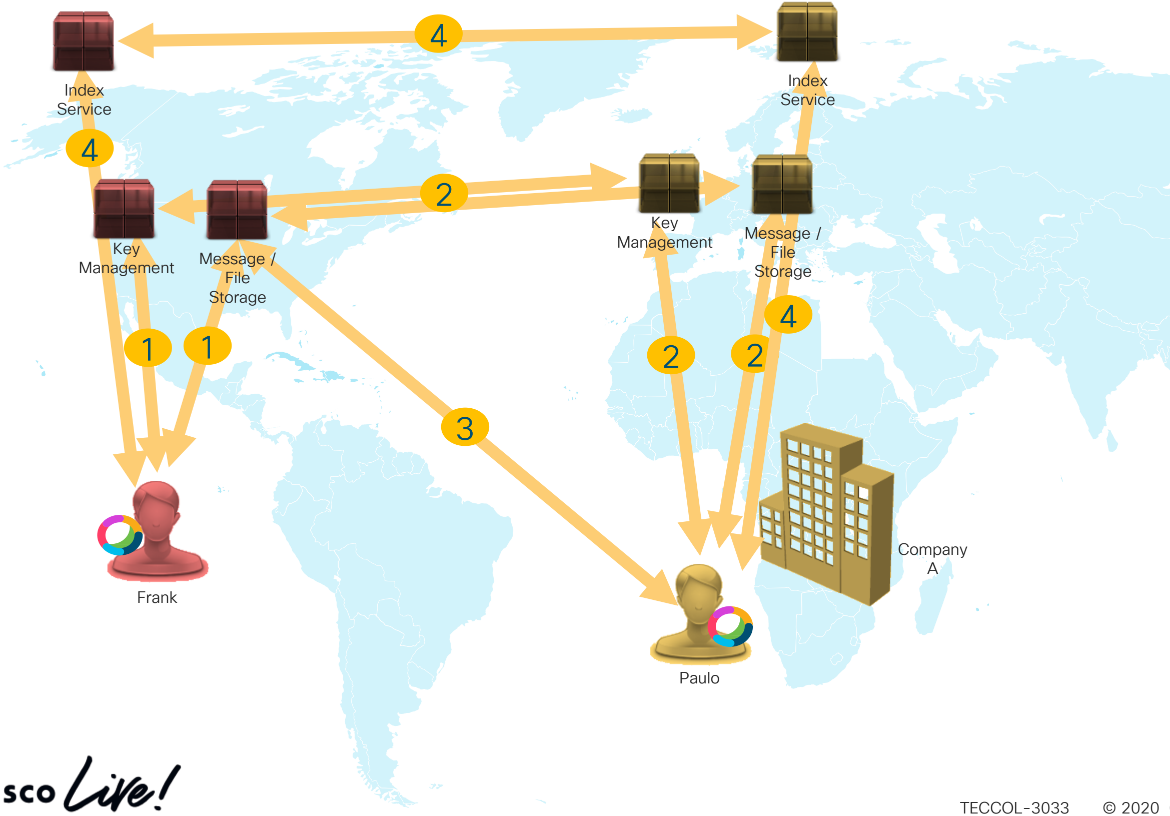
1 Frank for consumer ORG or US customer ORG creates a space with a keys given by US datacenter, content and files will be store in US

2 Paulo and II are invited and receives the key via EMEA datacenter and receives a remote reference breadcrumbs, pointing to the US cluster

3 Paulo and II follows the breadcrumb to get messages and files from US datacenter.
Any content created by Paulo and II will be hosted in US

4 One-way hashed indexes for searches are store in both clusters, all users clients do the search in their clusters.

1-1 Conversations Rules



1 Frank from consumer ORG or US customer ORG creates a 1:1 space with an EMEA user, or the other way around, a keys is given by US datacenter, content and files will be store in US

2 Paulo receives the key via EMEA datacenter and receives a remote reference breadcrumbs, pointing to the US cluster

3 Paulo follows the breadcrumb to get messages and files from US datacenter.

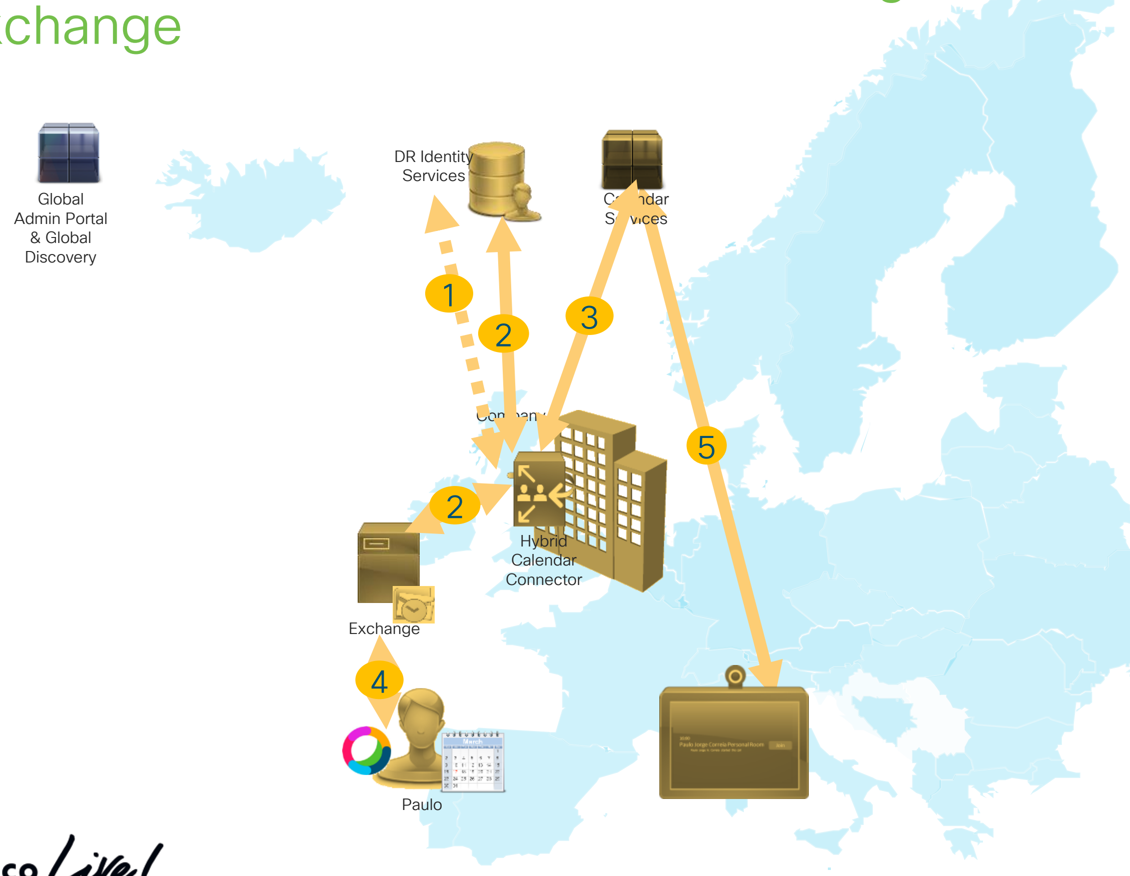
Any content created by Frank or I will be hosted in US

4 One-way hashed indexes for searches are store in both clusters, both users clients do the search in their clusters.

cisco Live!

Calendar Data – Same and Across Data Center

Calendar Services for a customer using On-Prem Microsoft Exchange



Global Admin Portal & Global Discovery
DR Identity Services
Calendar Services
1
2
3
5
Company
2
Hybrid Calendar Connector
Exchange
4
Paulo

1 Hybrid Calendar Connector is aware of the cluster it should connect to through the organization it is configured for

2 Calendar connector Authenticates to EMEA Identity Services and gets an OAuth token and Authenticate to Exchange using Delegation accounts

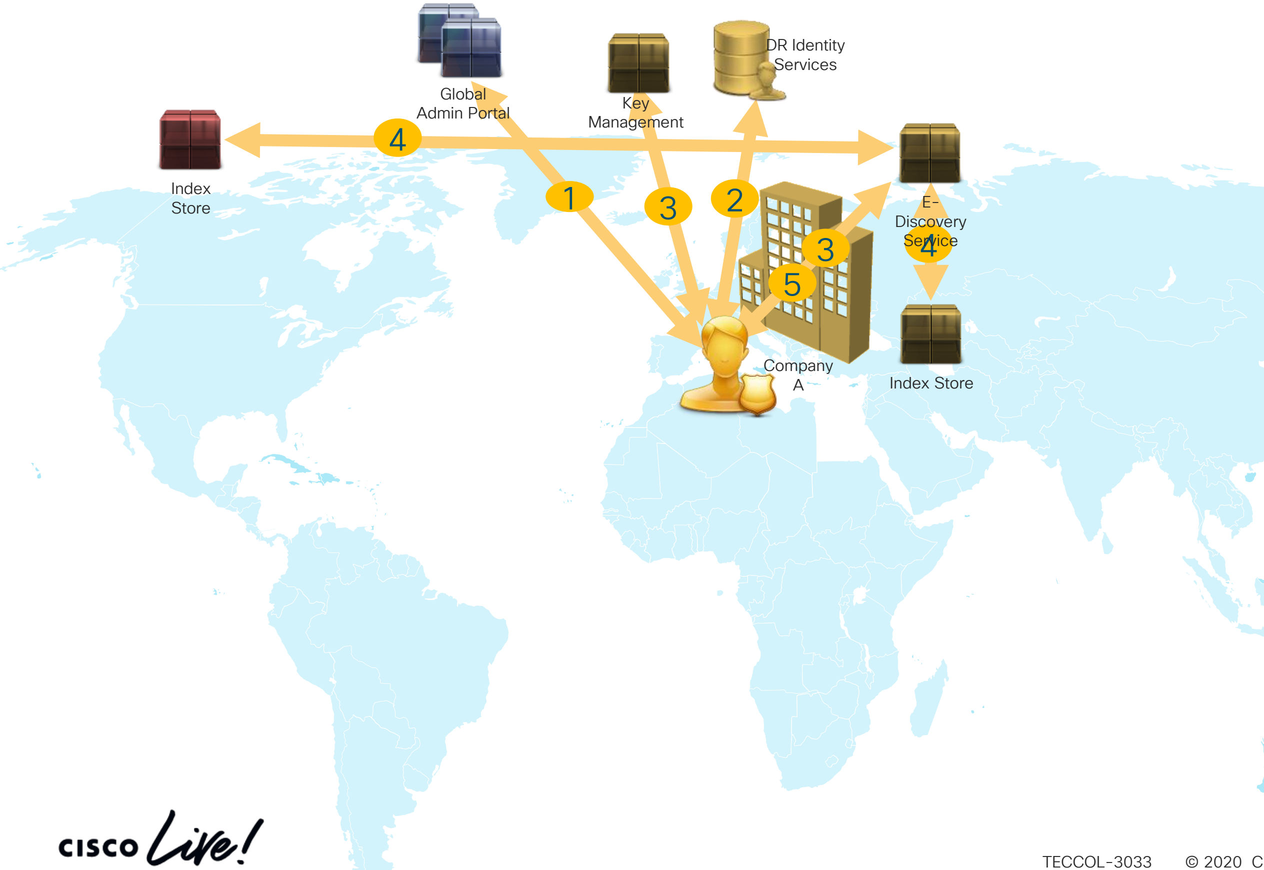
3 Calendar connector uses EMEA Calendar Services to manage users schedules

4 User Schedules meeting or is invited to a scheduled meeting. This meeting information is stored in users' local cluster. There is a copy of this meeting information for each user, so this works the same across Data Centers

5 At the time of the meeting, EMEA Calendar Services sends notifications for One Button to Push (OBTP) in the HW and SW endpoints

E-Discovery Services – Across Data Centers

E-discovery



1 Compliance Office connects to Global Webex Administrator Portal

2 Compliance Officer authenticates in EMEA Identity Services

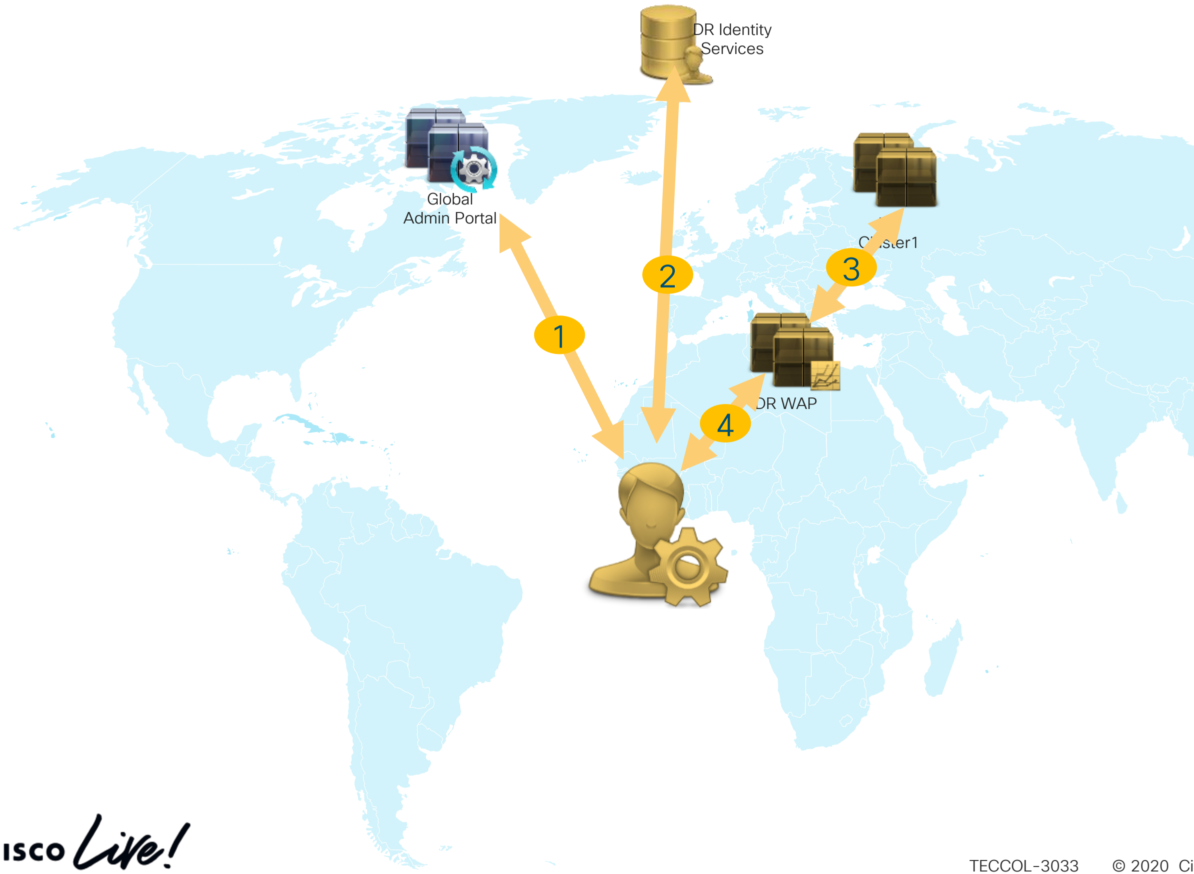
3 Compliance office get Key from EMEA KMS to formulate the search request

4 E-discovery Services queries all the Index services (EMEA and US) for content on the search request

5 Search result returned from each data center are stored locally (US and EMEA) using the EMEA Key for encryption. The client app used by the Compliance Office collates the search results from both data centers and decrypts using the key from EMEA KMS.

Analytics

Analytics Services



1 EMEA Administrator connect to Webex Global Admin Portal

2 Administrator Authenticates in EMEA Identity Services and gets an OAuth token to have access to the portal

3 Webex Teams and Device services store Analytics information in EMEA WAP

4 Administrator uses EMEA WAP to get the analytics and troubleshooting information needed *(Note: Meetings analytics/troubleshooting is global)*

The Webex data residency difference

Simplified administration	Single, global identity authorization and authentication with local PII storage. No guest accounts required.
Secure cross-company collaboration	Organizational visibility and control over content shared by users with external organizations.
More control, true encryption	Global key access with local key storage (federated and secure) and encryption of data in use, at rest and in transit.
Cross-cluster messaging: Separate, yet linked data storage	**Cross-border message data remain in their respective countries, linked by “breadcrumbs” – giving you visibility and control and enabling global eDiscovery.**
Inclusion of all media across Teams & Meetings	**Messages, files, whiteboards and localized media processing are all stored in the same place.**

When it comes to securing collaboration data, companies trust Cisco

Protect your most sensitive data in use, in rest, in transit

Enable secure cross-company collaboration

Meet regulatory compliance and data protection mandates

Cloud Collaboration Architecture

Security Challenge

The way Users want to work vs. Corporate IT

Open Collaboration

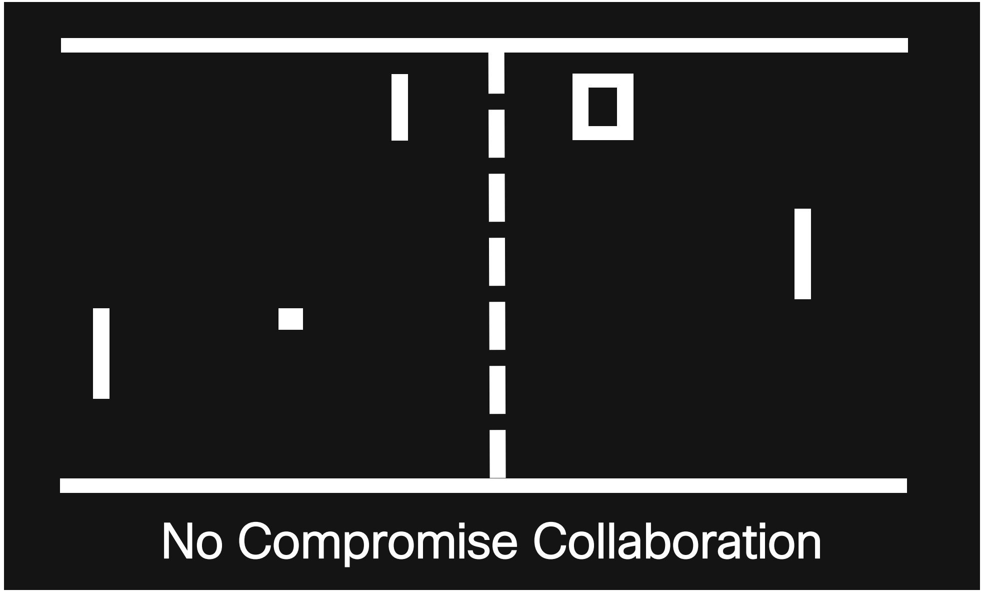
Anywhere Access

Fully Searchable

Cloud Managed

Data / App Integrated

✓



Secured

Compliant

Encrypted

Enterprise Integrated

Discoverable

✓

360-degree approach to security and compliance

NEW

Protect Against Malware

Prevent loss of information

Secure the apps and devices

Secure the content and data privacy

Comply with legal and regulatory

Secure the user identity and access

Empower the customer

cisco Live!

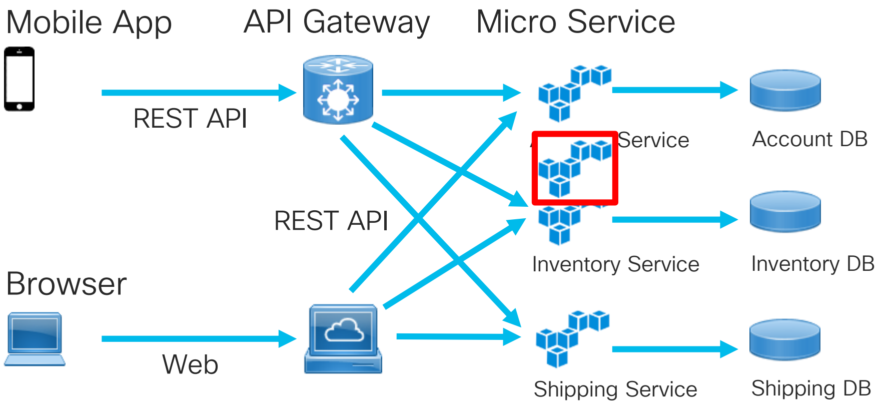
Micro-Services

What are Micro-Services?

Definition: Micro-services - also known as the micro-service architecture - is an architectural style that structures an application as a collection of loosely coupled services, which implement business capabilities. The micro-service architecture enables the continuous delivery/deployment of large, complex applications.

Let's take a look at this theory…

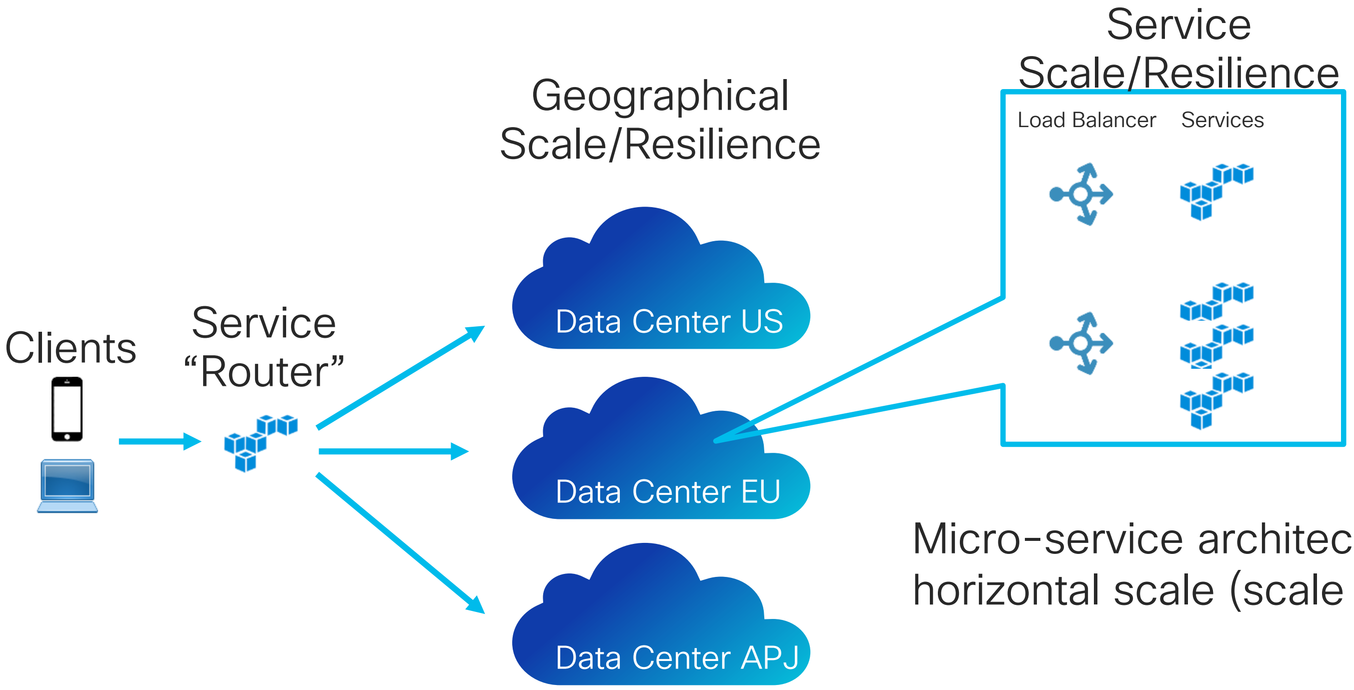
Generic business application example



- Each Micro-service is relatively small
- Each service can be developed independently of other services – easier to deploy new versions of service frequently
- Easier to scale development
- Improved fault isolation. Example memory leak in one service affects only that particular service
- Each service can be developed and deployed independently

What are Micro-Services?

"Infinite" scale for a global application



Micro-service architecture allows for horizontal scale (scale out)

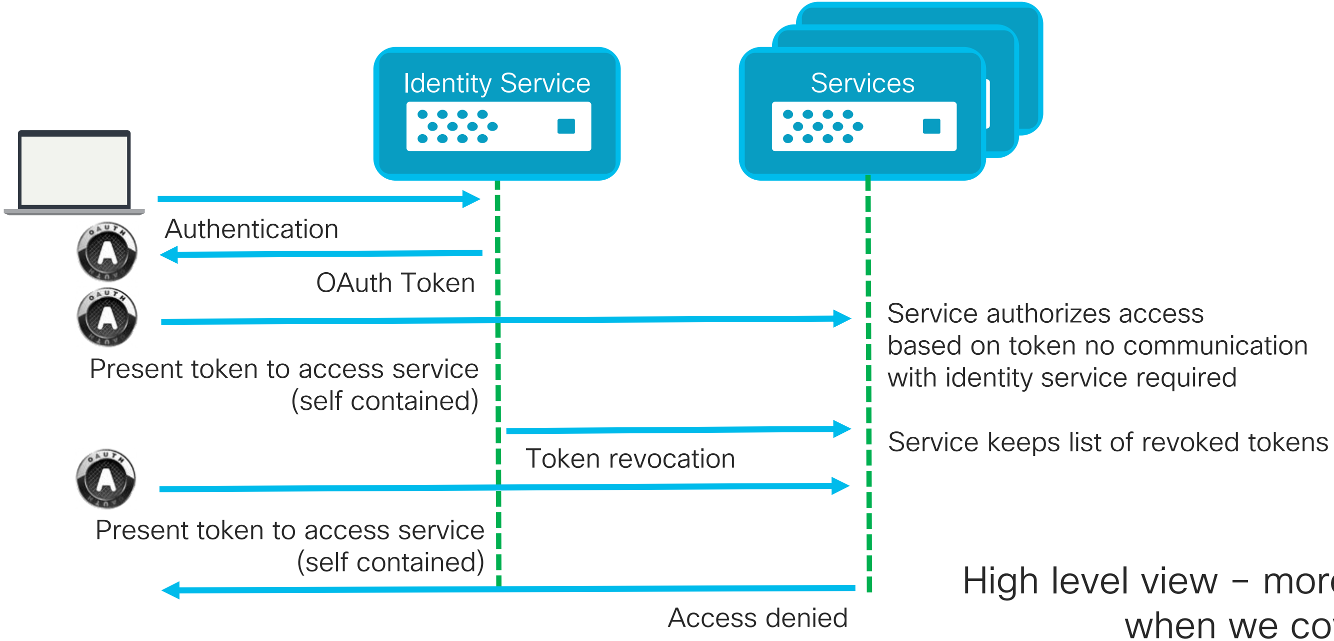
What are Micro-Services?

Architectural requirements

- Requires inter-service communication mechanism
- Implementing uses cases that span multiple services requires careful coordination between teams
- Deployment complexity
- Authorization cross services (see next slide)

What are Micro-Services?

Authorization of service access Cisco Webex Teams



Identity Service
Services
Authentication
OAuth Token
Present token to access service (self contained)
Token revocation
Present token to access service (self contained)
Access denied

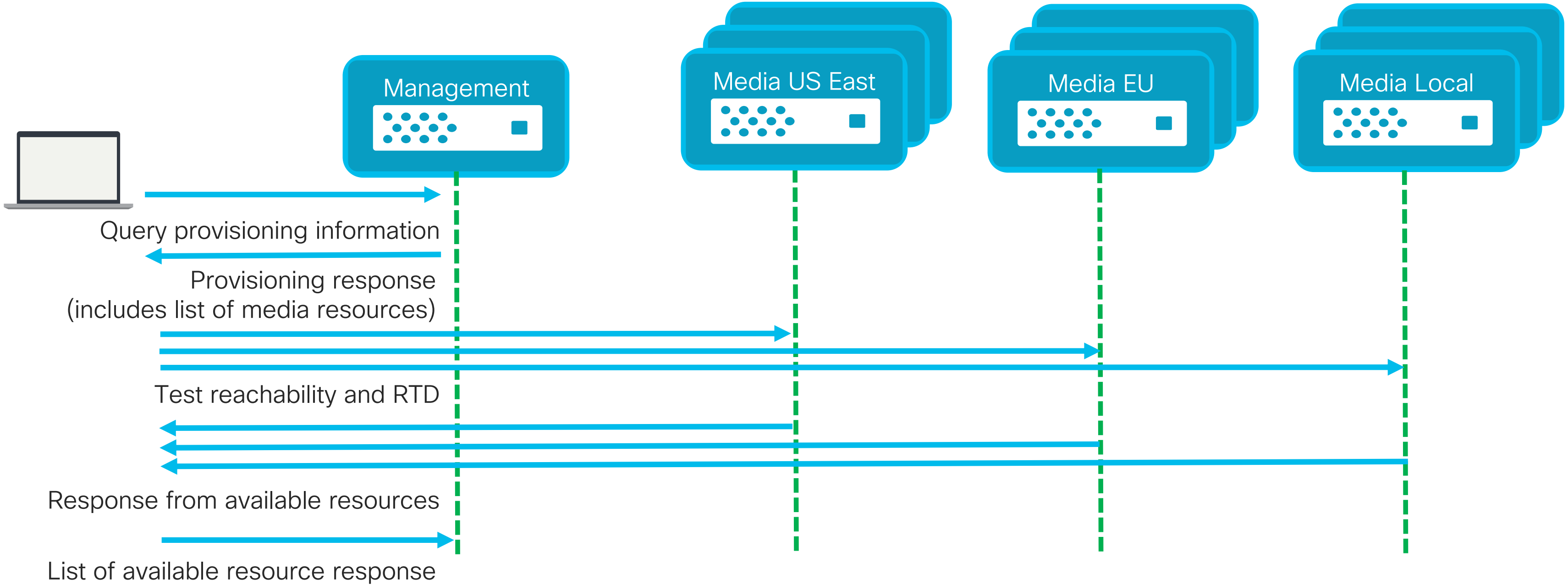
Service authorizes access based on token no communication with identity service required

Service keeps list of revoked tokens

High level view – more on OAuth later in the day when we cover Cisco Webex Pro Pack

Cisco Webex Teams Micro-Services

Selection example for Media Services

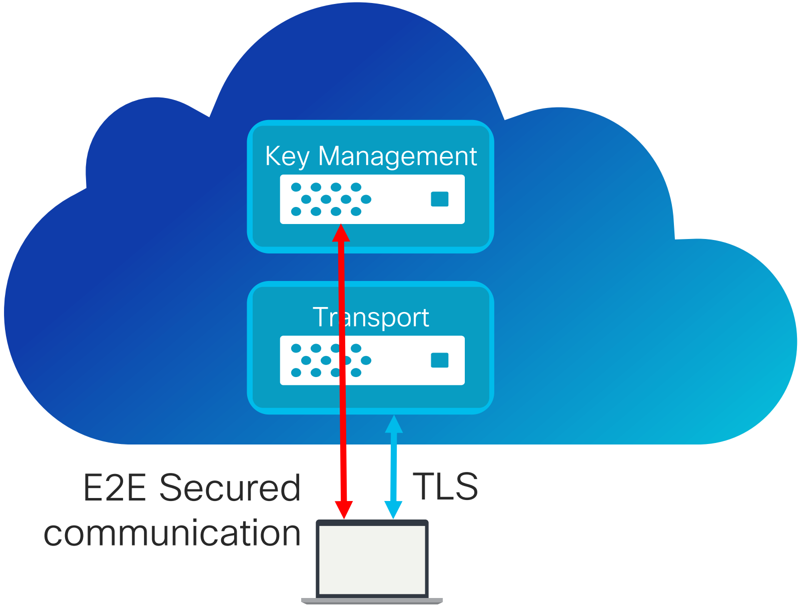

Management
Media US East
Media EU
Media Local
Query provisioning information
Provisioning response
(includes list of media resources)
Test reachability and RTD
Response from available resources
List of available resource response

Abstract representation

Cisco Webex Meetings and Teams Architecture

Cisco Webex Architecture

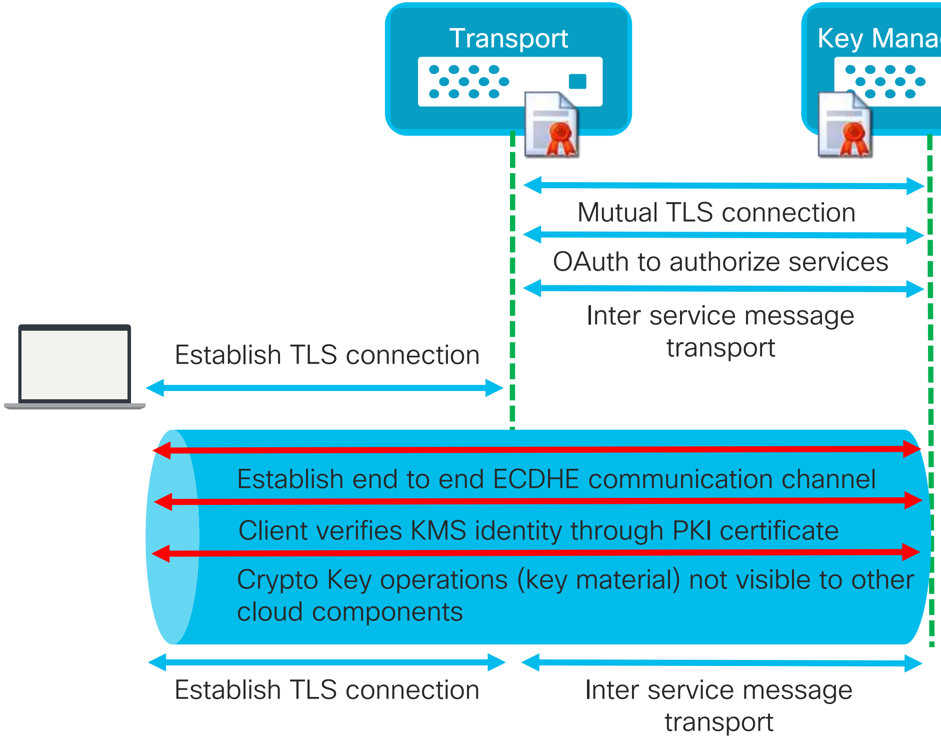
End to End Secure Communication



- Content (messages, files, space titles, etc.) is encrypted using symmetric AES256 in GCM mode
- Client to Key Management communication is secured by Elliptic Curve Diffie-Hellman Ephemeral ECDHE key exchange with a per session EC key
- Client to server communication is secured with TLS ECDHE (i.e. RSA AES 256 GCM SHA384)
- Security architecture limits exposure of key material

Cisco Webex Architecture

End to End Secure Communication

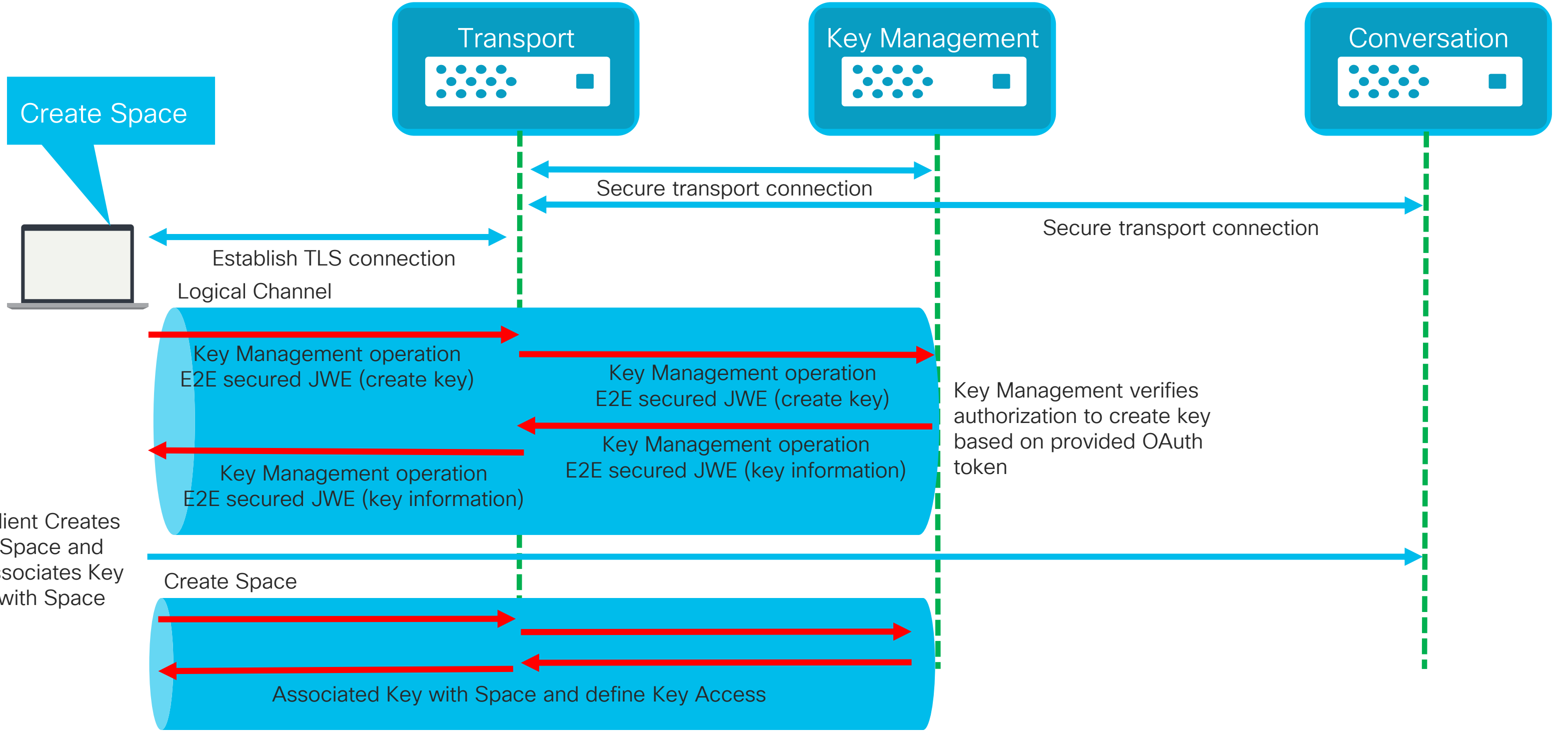


Transport
Key Management
Mutual TLS connection
OAuth to authorize services
Inter service message transport
Establish TLS connection
Establish end to end ECDHE communication channel
Client verifies KMS identity through PKI certificate
Crypto Key operations (key material) not visible to other cloud components
Establish TLS connection
Inter service message transport

- Secure TLS REST interfaces
- Interaction between services based on certificate based MTLS
- Service components authorization by OAuth Tokens
- Secure client connection to service over TLS
- End to End Client to Key Management channel negotiated ECDHE
- Identity of Key Management Service verified by PKI certificate
- Client to Key Management crypto key operations E2E secured over transport layer JSON Web Encryption (JWE, RFC 7516)

Cisco Webex Architecture

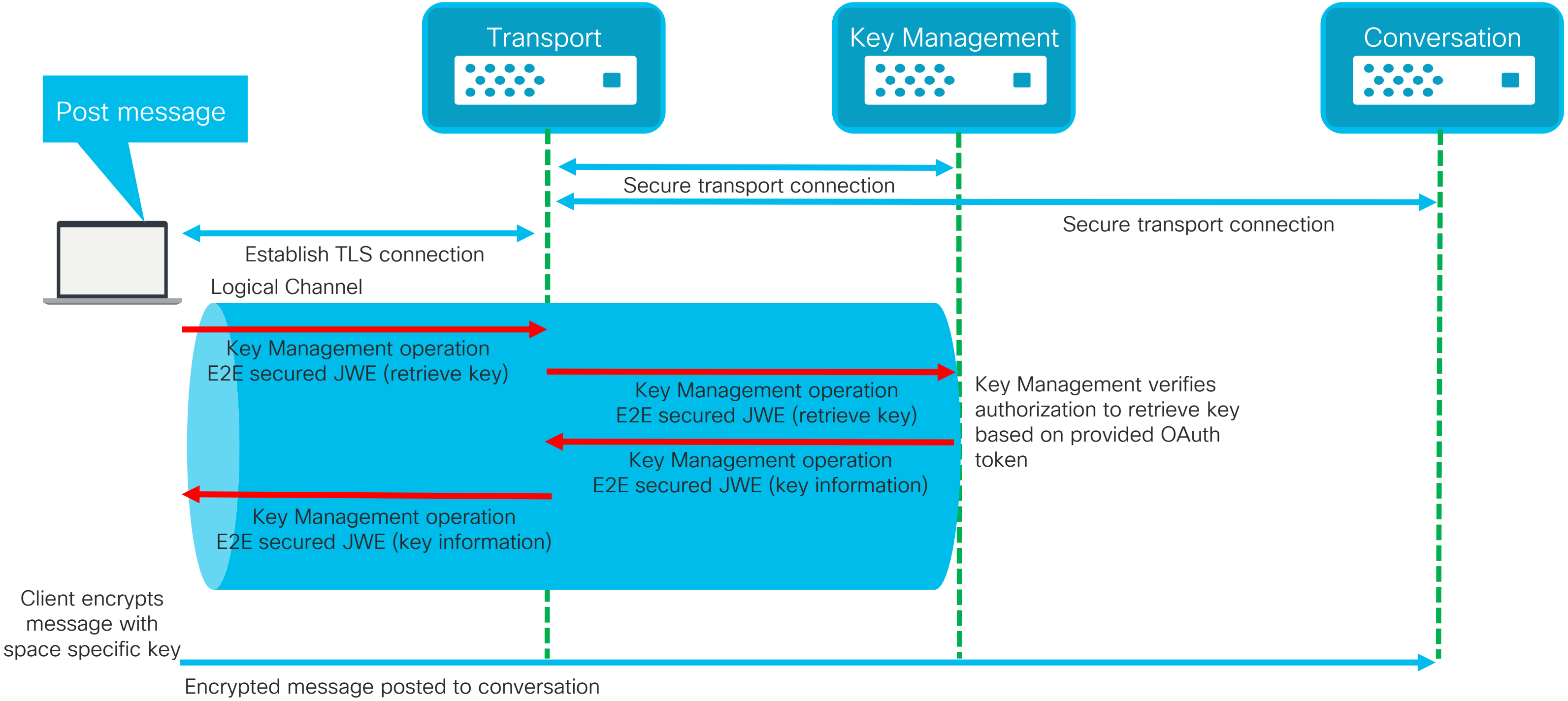
End to End Secure Communication – Space Creation



Transport
Key Management
Conversation
Create Space
Secure transport connection
Secure transport connection
Establish TLS connection
Logical Channel
Key Management operation
E2E secured JWE (create key)
Key Management operation
E2E secured JWE (create key)
Key Management verifies authorization to create key based on provided OAuth token
Key Management operation
E2E secured JWE (key information)
Key Management operation
E2E secured JWE (key information)
Client Creates Space and associates Key with Space
Create Space
Associated Key with Space and define Key Access

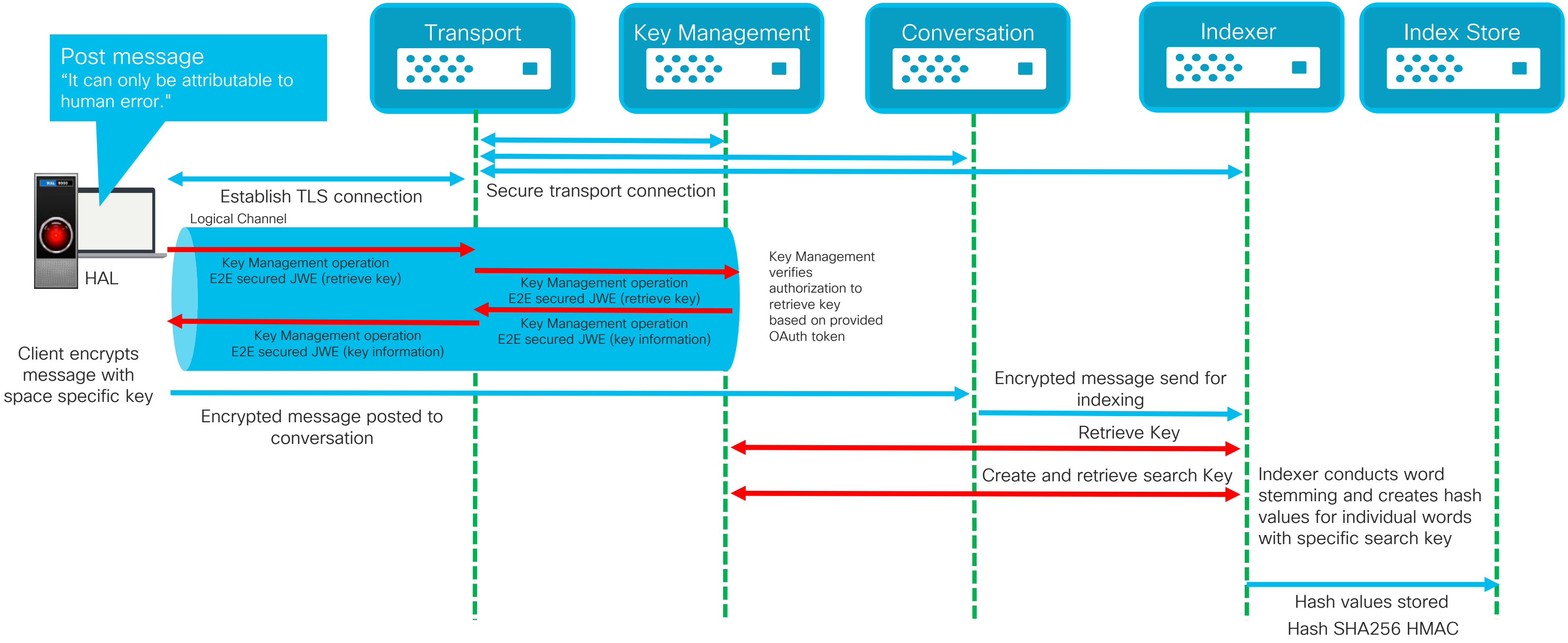
Cisco Webex Architecture

End to End Secure Communication – Post Message



Cisco Webex Architecture

End to End Secure Communication – How to search?



Post message
"It can only be attributable to human error."

Establish TLS connection

Secure transport connection

Logical Channel

Key Management operation
E2E secured JWE (retrieve key)

Key Management operation
E2E secured JWE (retrieve key)

Key Management operation
E2E secured JWE (key information)

Key Management operation
E2E secured JWE (key information)

Key Management verifies authorization to retrieve key based on provided OAuth token

Client encrypts message with space specific key

Encrypted message posted to conversation

Encrypted message send for indexing

Retrieve Key

Create and retrieve search Key

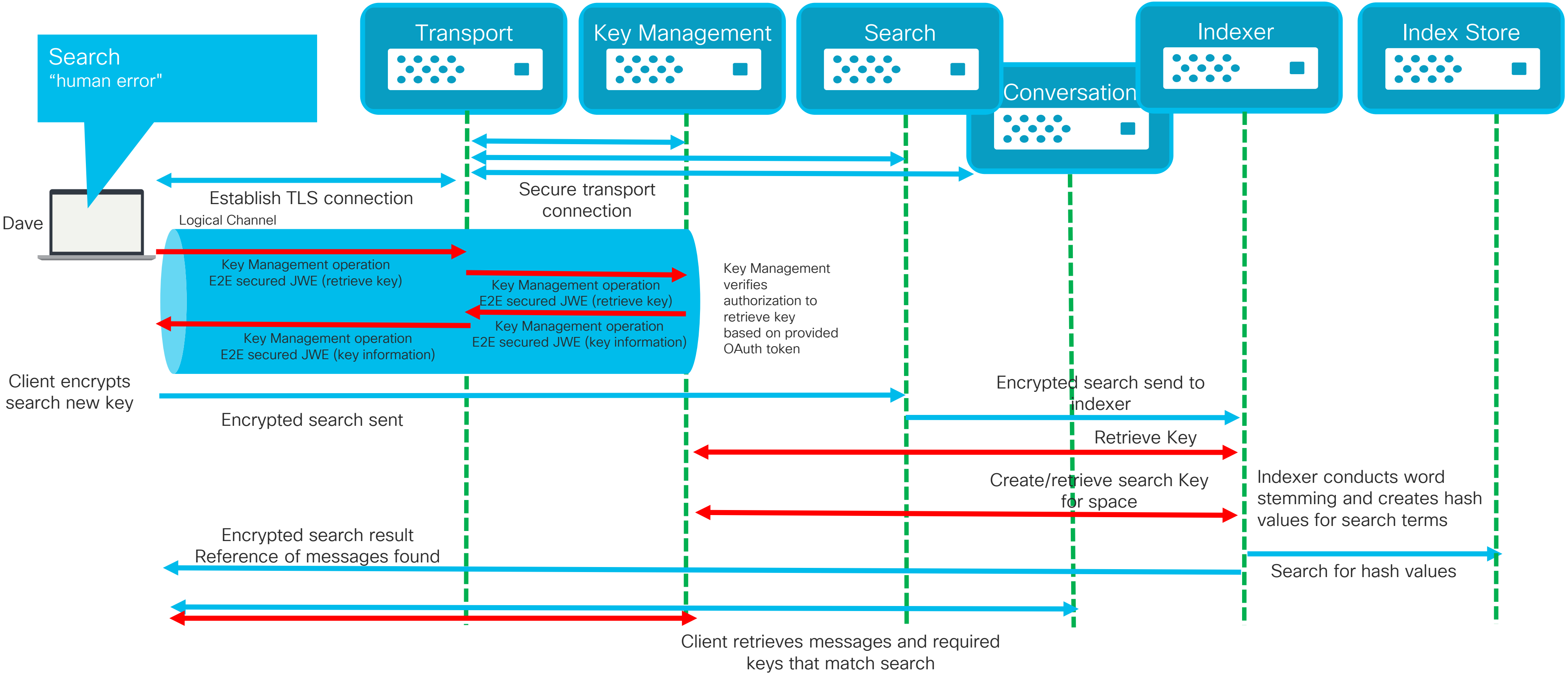
Indexer conducts word stemming and creates hash values for individual words with specific search key

Hash values stored

Hash SHA256 HMAC

Cisco Webex Architecture

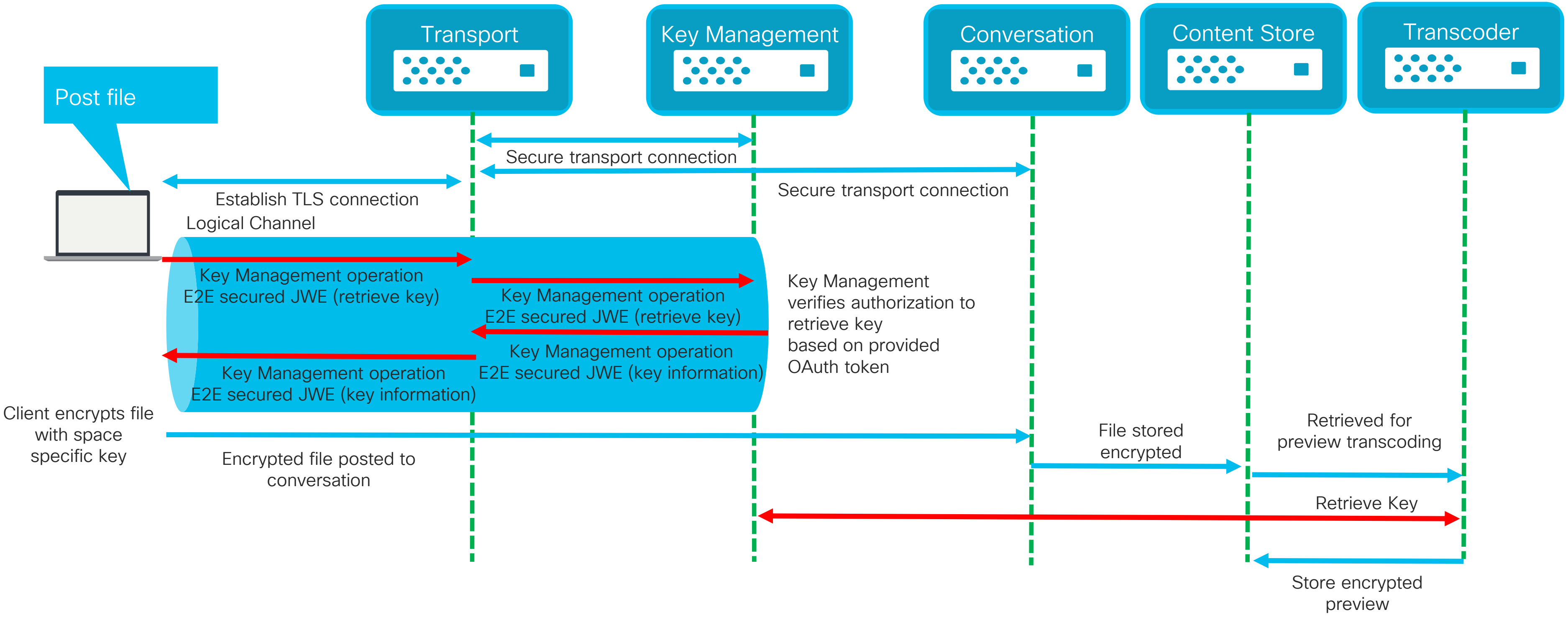
End to End Secure Communication – How to search?



Search
"human error"
Transport
Key Management
Search
Conversation
Indexer
Index Store
Dave
Establish TLS connection
Secure transport connection
Logical Channel
Key Management operation
E2E secured JWE (retrieve key)
Key Management operation
E2E secured JWE (retrieve key)
Key Management operation
E2E secured JWE (key information)
Key Management operation
E2E secured JWE (key information)
Key Management verifies authorization to retrieve key based on provided OAuth token
Client encrypts search new key
Encrypted search sent
Encrypted search send to indexer
Retrieve Key
Create/retrieve search Key for space
Indexer conducts word stemming and creates hash values for search terms
Encrypted search result
Reference of messages found
Search for hash values
Client retrieves messages and required keys that match search

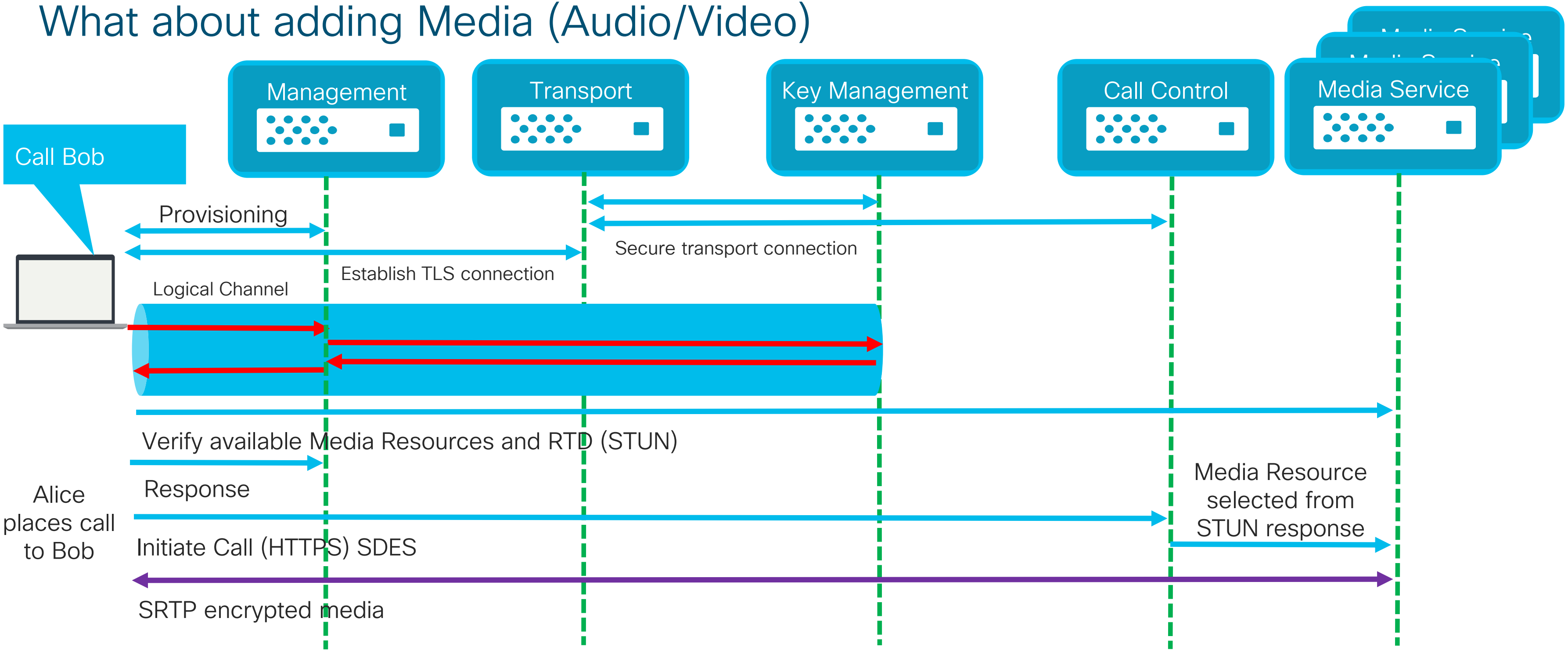
Cisco Webex Architecture

End to End Secure Communication – Post Content



Cisco Webex Architecture

What about adding Media (Audio/Video)



Media not encrypted end to end.
E2E media encryption requires switching only, media transcoding not possible. Endpoints establish connection to Key Management to retrieve additional information.

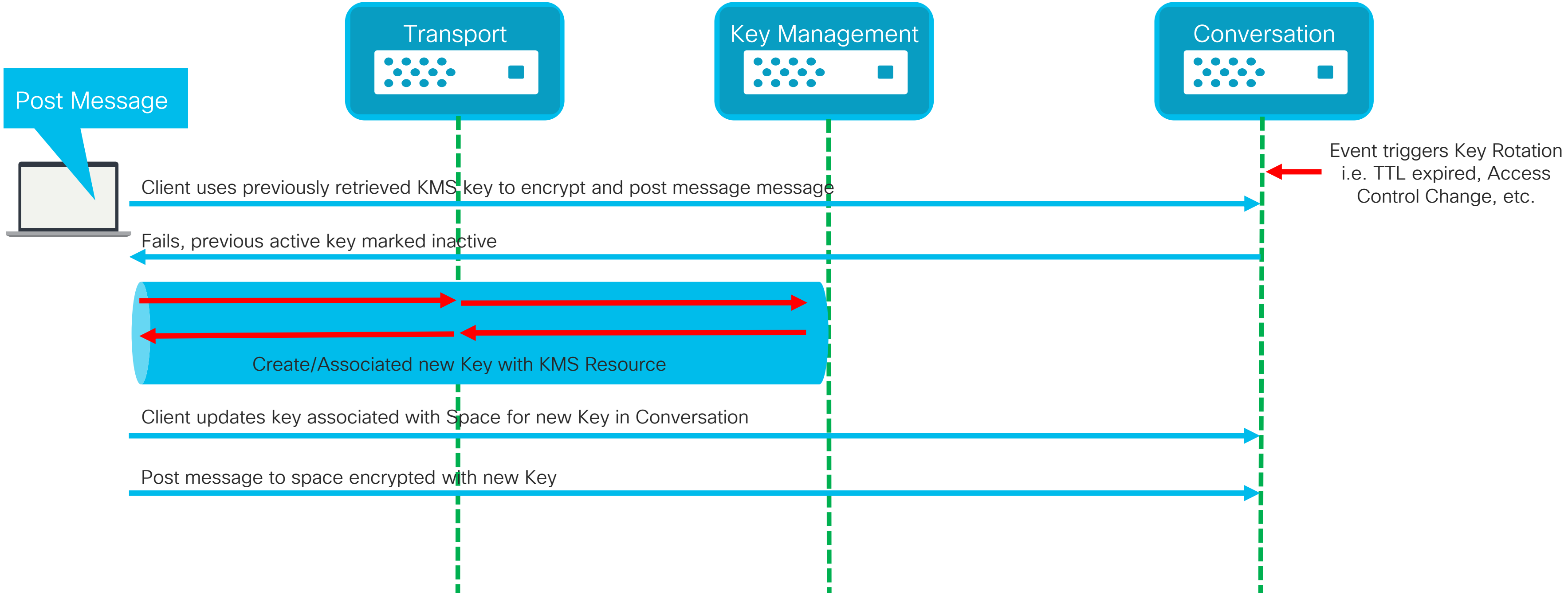
A look into the future...

Further enhancing Security

Introducing Key Rotation

Space Conversation Example – Active Rotation

Future


Transport
Key Management
Conversation
Post Message
Event triggers Key Rotation i.e. TTL expired, Access Control Change, etc.
Client uses previously retrieved KMS key to encrypt and post message message
Fails, previous active key marked inactive
Create/Associated new Key with KMS Resource
Client updates key associated with Space for new Key in Conversation
Post message to space encrypted with new Key

Logical Channel

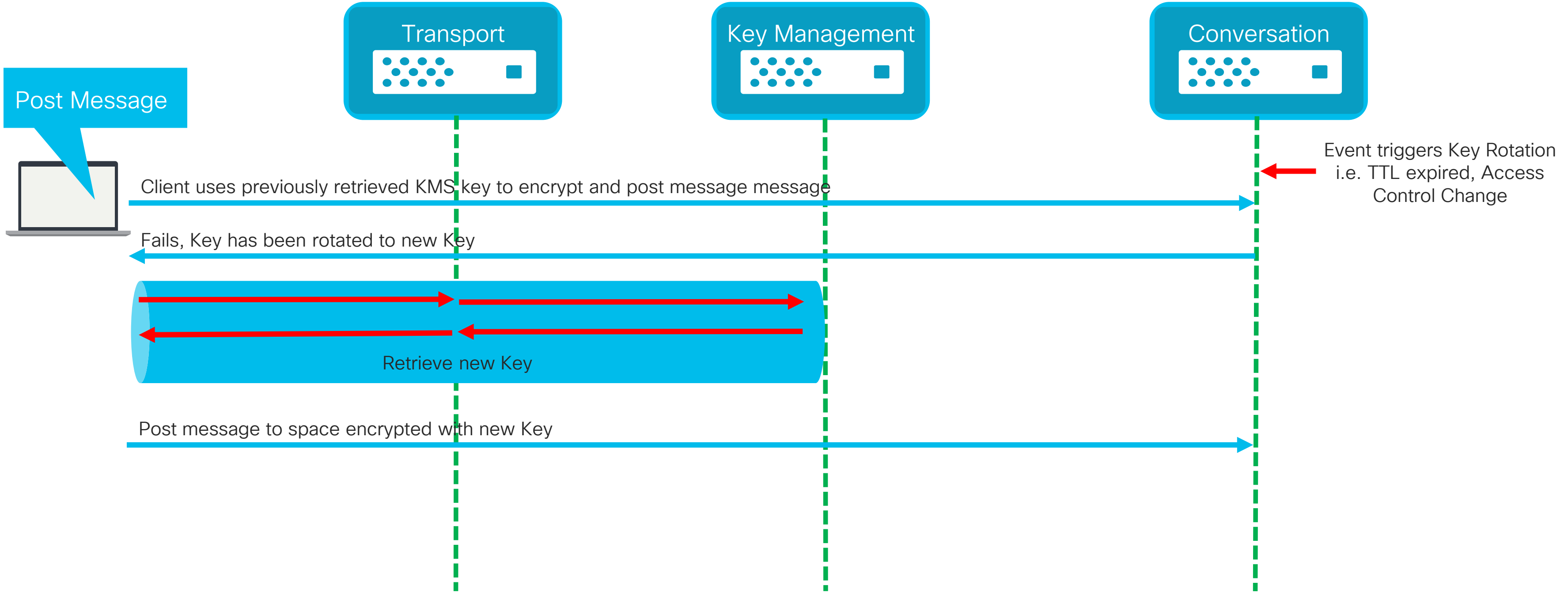
Subject to change

Further enhancing Security

Introducing Key Rotation

Space Conversation Example – Passive Rotation

Future


Transport
Key Management
Conversation
Post Message
Event triggers Key Rotation
i.e. TTL expired, Access
Control Change
Client uses previously retrieved KMS key to encrypt and post message message
Fails, Key has been rotated to new Key
Retrieve new Key
Post message to space encrypted with new Key

Logical Channel

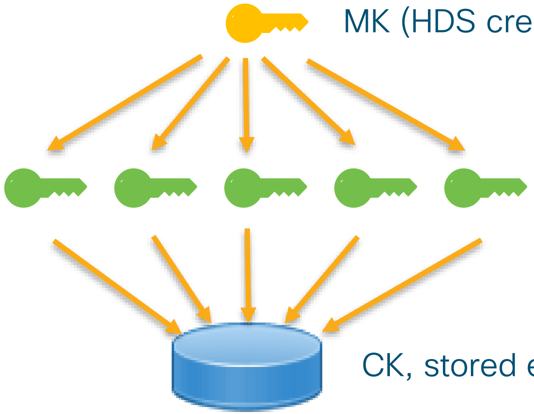
Subject to change

Future

Further enhancing Security

Introducing KMS Key Hierarchy

Current Architecture KMS/HDS

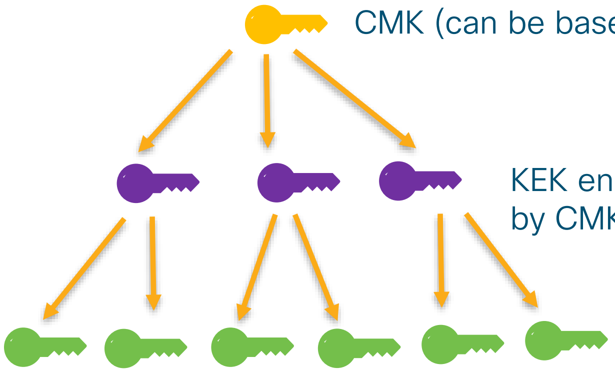


MK (HDS created as part of ISO)

CK, encrypted by MK

CK, stored encrypted in DB

Future Architecture KMS/HDS



CMK (can be based on HSM)

KEK encrypted by CMK

CK encrypted with KEK

- New architecture allows for Customer Master Key to be provided by Hardware Security Module (HSM) for cloud and HDS. Additional Level of Security as CMK never “leaves” the HSM
- Cisco Cloud KMS to have organization specific Customer Master Key

  Customer revokes HSM CMK all KEK/CK are rendered inaccessible
- In the case compromise CMK and/or KEK can be rotated, this will trigger re-encryption of all downstream keys

Subject to change

MK – Master Key
CK – Content Key
KEK – Key Encryption Key
CMK – Customer Master Key

Further enhancing Security

Introducing KMS Key Hierarchy

Future

Feature iterations planned

- Master Key for Cisco CloudKMS protected by AWS CloudHSM
- Per Organization Master Key for Cisco CloudKMS protected by AWS CloudHSM
- One Premise HSM support for Hybrid Data Security (Gemalto Safenet)

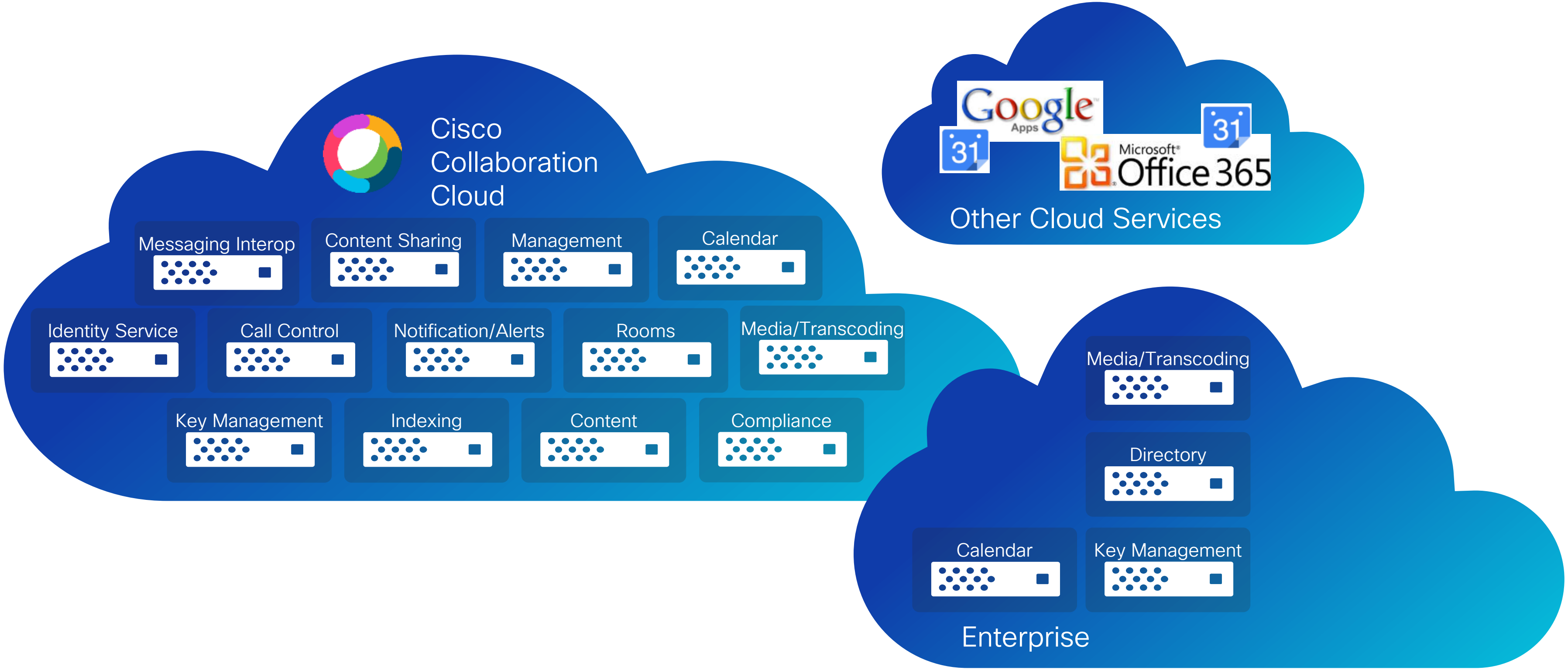
Exact dates? Stay tuned we are working diligently on this for you …

Subject to change

Cisco Webex Hybrid Services

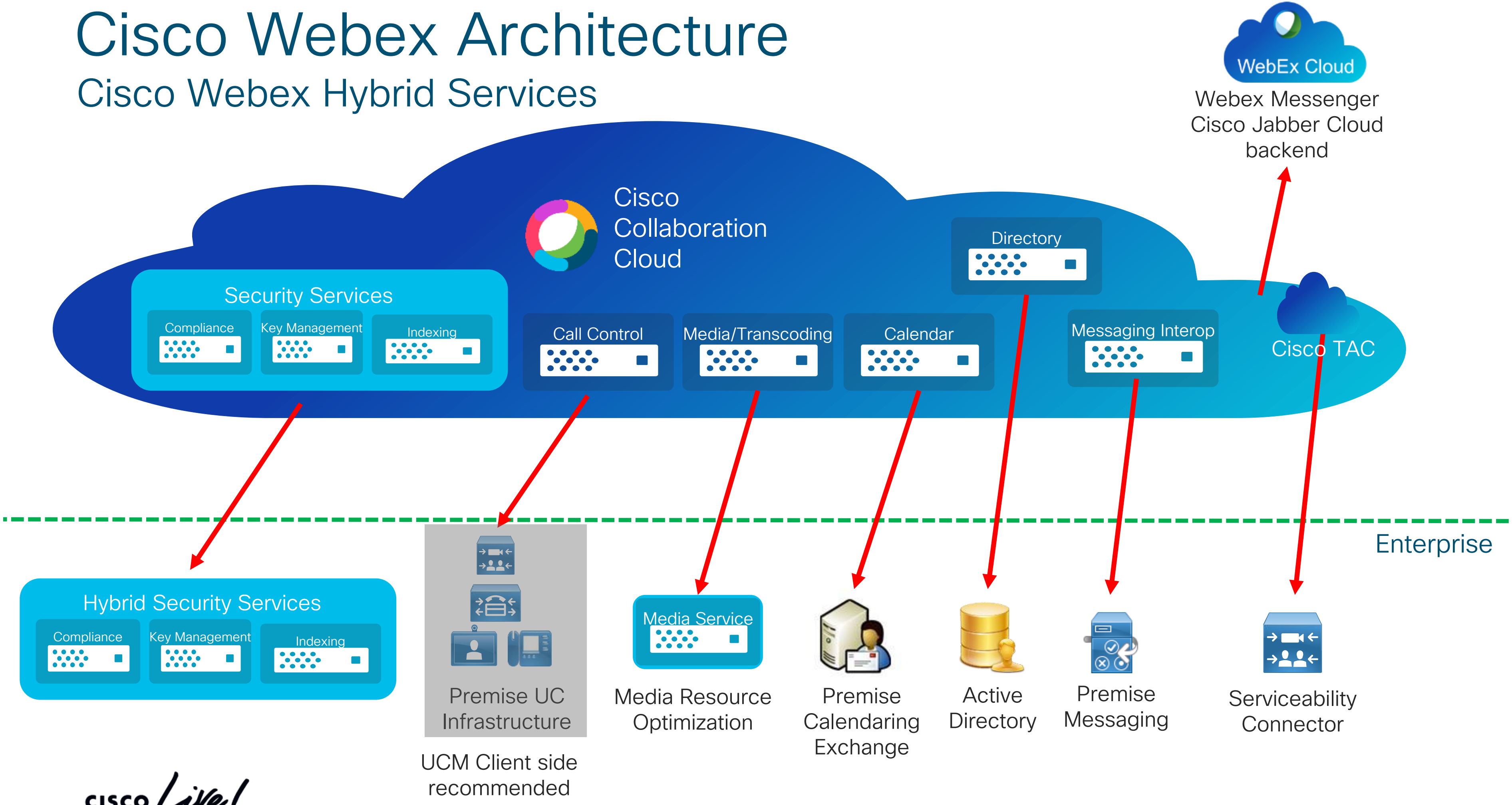
Cisco Webex Architecture

Combining Cloud with the Enterprise Hybrid Services



Cisco Webex Architecture

Cisco Webex Hybrid Services



Cisco Webex Architecture

Cisco Webex Hybrid Service – Platform

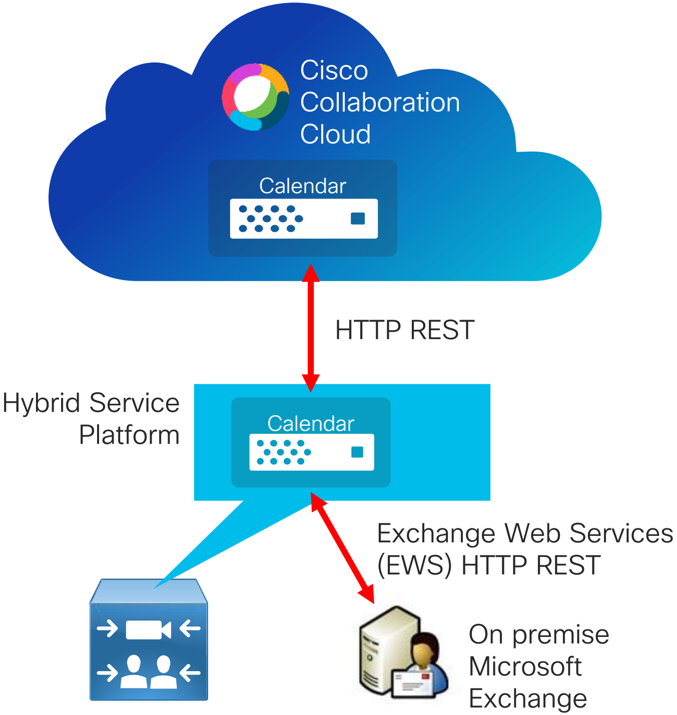
Cisco Expressway foundation for many Hybrid Services

- Latest version of Cisco Expressway recommended. Support for n-1 releases
- Provides platform for Cisco Cloud Connectors which enable individual hybrid services
- Connectors managed by Cisco Cloud Platform, no upgrades on Cisco Expressway software required for deployment of new version
- Connector **only** establish outbound connections towards Cloud Service. No inbound ports required on firewall
- Connector platform supports use of outbound HTTP proxy
- Hybrid Services architecture emphasis on protecting and utilizing existing investments
- Utilize existing Cisco Expressway clustering capabilities for redundancy and scale
- Decouples software dependencies between cloud service and other on premise components
  (some services require a minimum version for other on premise components, please check documentation for latest information)

Cisco Webex Architecture

Cisco Webex Hybrid Service – Calendar

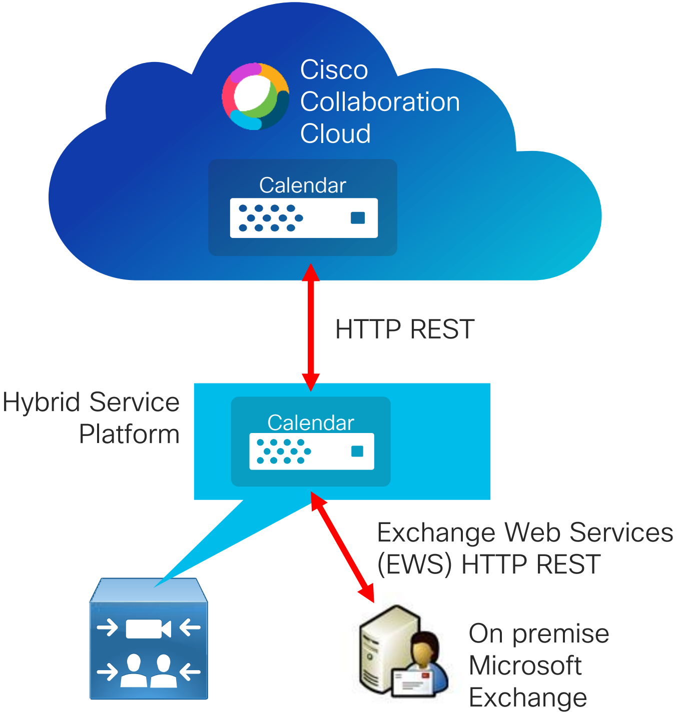
See hidden Slides for Reference on how to configure Expressway Hybrid Services


Cisco Collaboration Cloud
Calendar
HTTP REST
Hybrid Service Platform
Calendar
Exchange Web Services (EWS) HTTP REST
On premise Microsoft Exchange

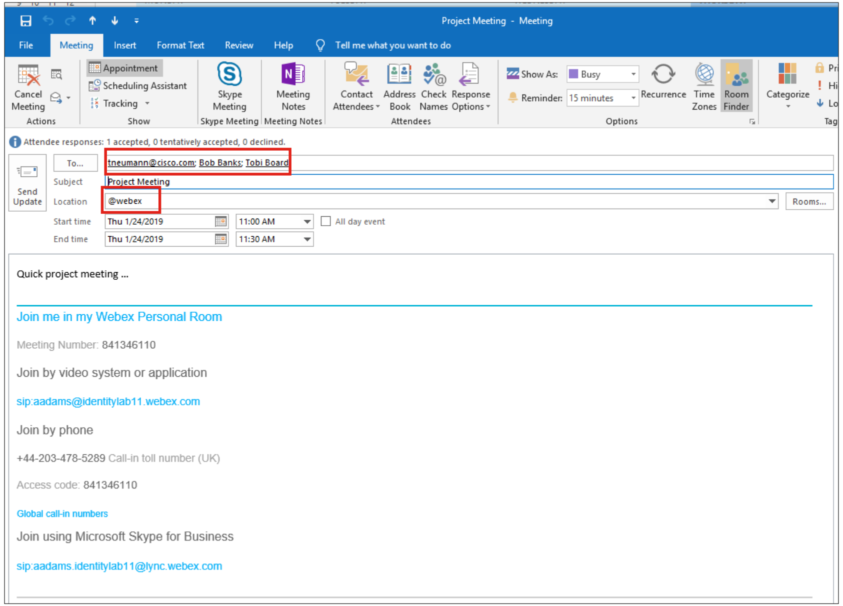
Cisco Webex Architecture

Cisco Webex Hybrid Service – Calendar

See hidden Slides for Reference on how to configure Expressway Hybrid Services



Easy scheduling of meetings with no plugins – create meeting and/or Cisco Webex Teams Space



Attendee responses: 1 accepted, 0 tentatively accepted, 0 declined.

To... tneumann@cisco.com; Bob Banks; Tobi Board

Subject: Project Meeting

Location: @webex

Start time: Thu 1/24/2019 11:00 AM □ All day event

End time: Thu 1/24/2019 11:30 AM

Show As: Busy

Reminder: 15 minutes

Quick project meeting ...

Join me in my Webex Personal Room

Meeting Number: 841346110

Join by video system or application

sip:aadams@identitylab11.webex.com

Join by phone

+44-203-478-5289 Call-in toll number (UK)

Access code: 841346110

Global call-in numbers

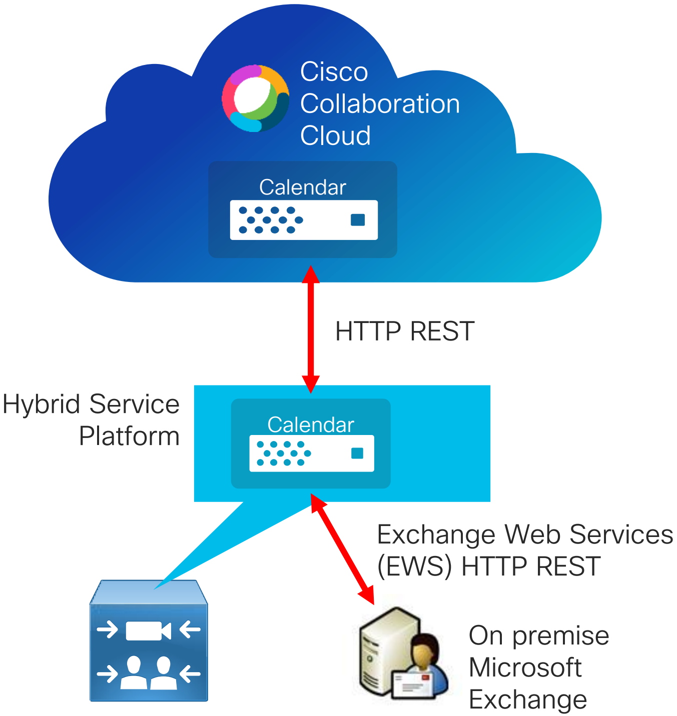
Join using Microsoft Skype for Business

sip:aadams.identitylab11@lync.webex.com

Cisco Webex Architecture

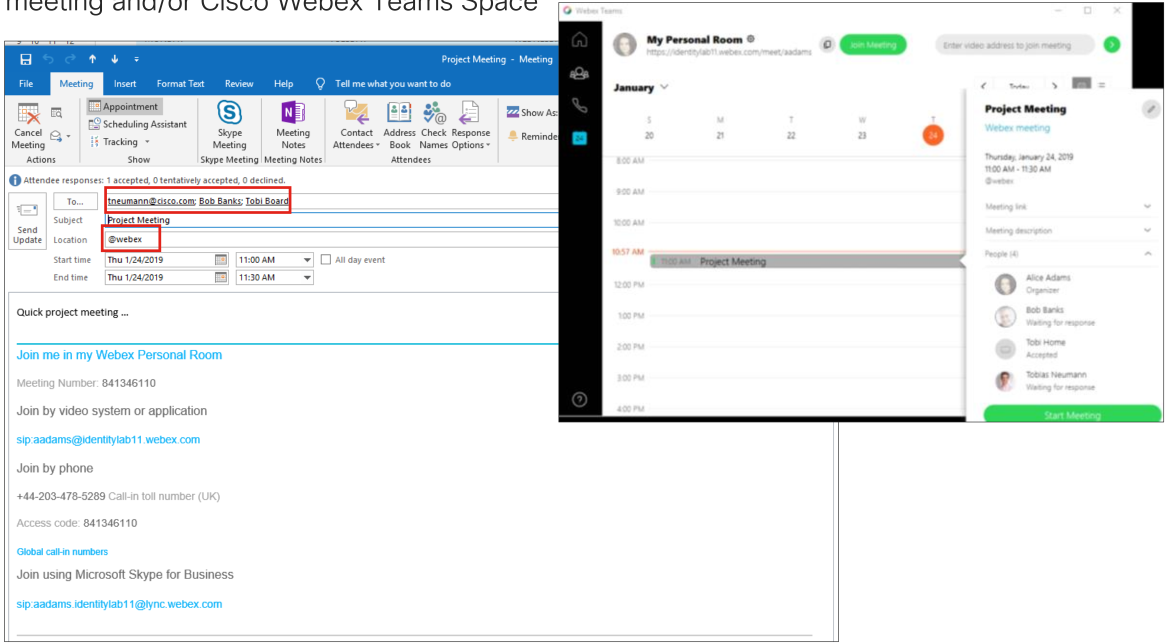
Cisco Webex Hybrid Service – Calendar

See hidden Slides for Reference on how to configure Expressway Hybrid Services


Cisco Collaboration Cloud
Calendar
HTTP REST
Hybrid Service Platform
Calendar
Exchange Web Services (EWS) HTTP REST
On premise Microsoft Exchange

Easy scheduling of meetings with no plugins – create meeting and/or Cisco Webex Teams Space

Meeting list available in Cisco Webex Teams Single Button to Join



Attendee responses: 1 accepted, 0 tentatively accepted, 0 declined.

To... tneumann@cisco.com; Bob Banks; Tobi Board

Subject: Project Meeting

Location: @webex

Start time: Thu 1/24/2019 11:00 AM ☐ All day event

End time: Thu 1/24/2019 11:30 AM

Quick project meeting ...

Join me in my Webex Personal Room

Meeting Number: 841346110

Join by video system or application

sip:aadams@identitylab11.webex.com

Join by phone

+44-203-478-5289 Call-in toll number (UK)

Access code: 841346110

Global call-in numbers

Join using Microsoft Skype for Business

sip:aadams.identitylab11@lync.webex.com

Project Meeting

Webex meeting

Thursday, January 24, 2019
11:00 AM - 11:30 AM
@webex

Meeting link

Meeting description

People (4)

Alice Adams – Organizer

Bob Banks – Waiting for response

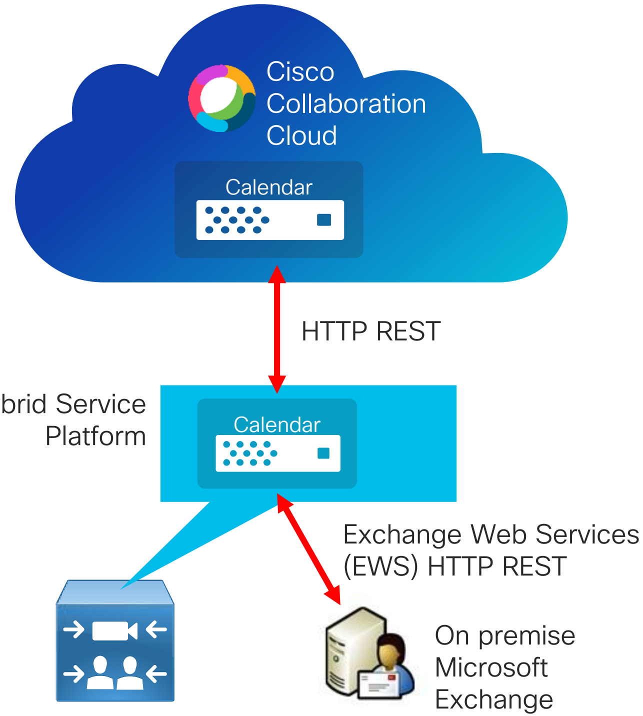
Tobi Home – Accepted

Tobias Neumann – Waiting for response

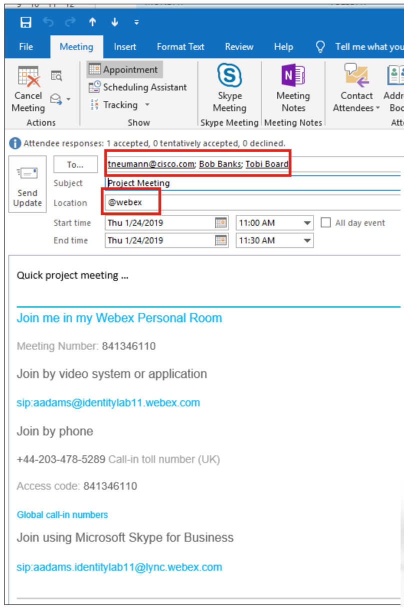
Cisco Webex Architecture

Cisco Webex Hybrid Service – Calendar

See hidden Slides for Reference on how to configure Expressway Hybrid Services


Cisco Collaboration Cloud
Calendar
HTTP REST
Hybrid Service Platform
Calendar
Exchange Web Services (EWS) HTTP REST
On premise Microsoft Exchange

Easy scheduling of meetings with no plugins – create meeting and/or Cisco Webex Teams Space



Attendee responses: 1 accepted, 0 tentatively accepted, 0 declined.

To... tneumann@cisco.com; Bob Banks; Tobi Board

Subject: Project Meeting

Location: @webex

Start time: Thu 1/24/2019 11:00 AM □ All day event

End time: Thu 1/24/2019 11:30 AM

Quick project meeting ...

Join me in my Webex Personal Room

Meeting Number: 841346110

Join by video system or application

sip:aadams@identitylab11.webex.com

Join by phone

+44-203-478-5289 Call-in toll number (UK)

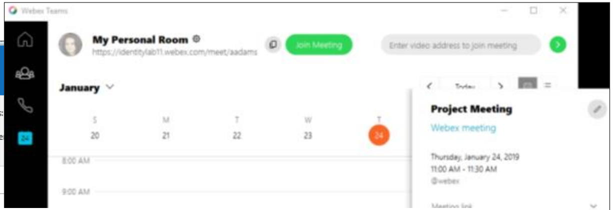
Access code: 841346110

Global call-in numbers

Join using Microsoft Skype for Business

sip:aadams.identitylab11@lync.webex.com

Meeting list available in Cisco Webex Teams Single Button to Join



Project Meeting

Webex meeting

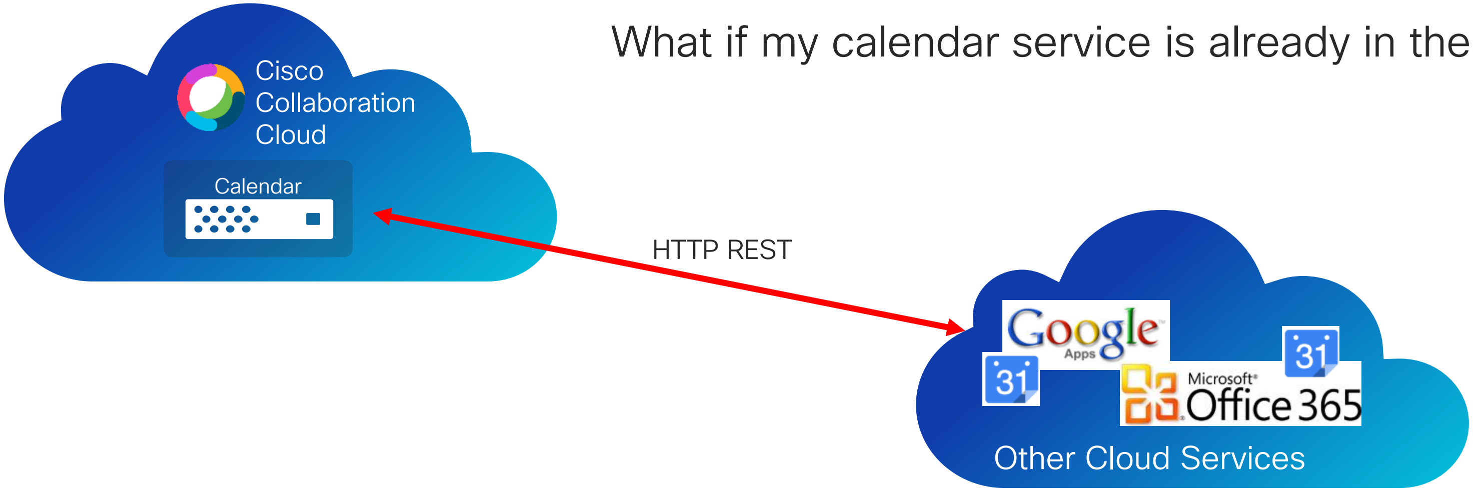
Thursday, January 24, 2019
11:00 AM - 11:30 AM
@webex

One Button the Push experience on cloud registered Collaboration Systems

Cisco Webex Architecture

Cisco Webex Hybrid Service – Calendar Cloud

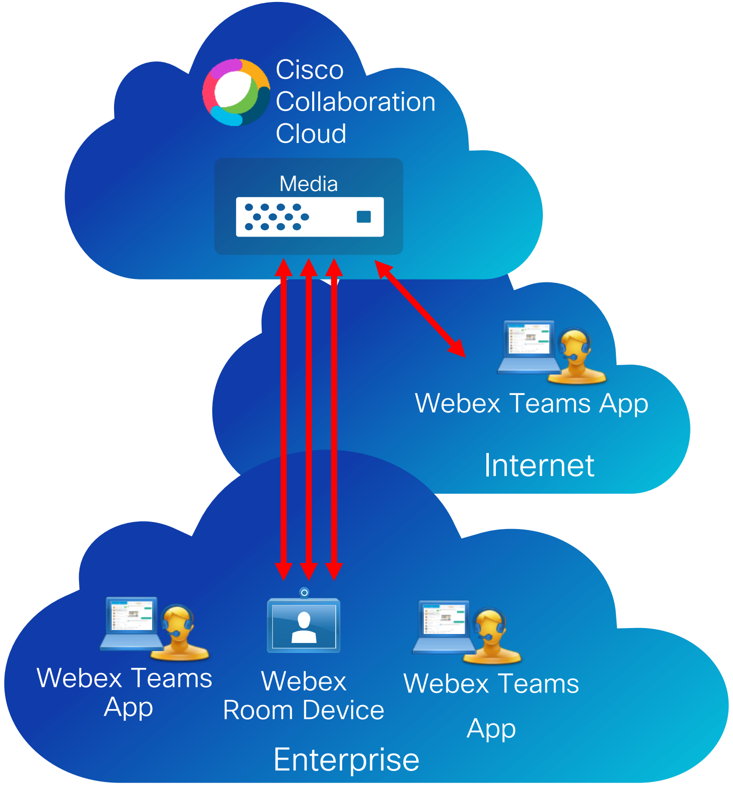
What if my calendar service is already in the cloud?



Cloud Calendar connector available for Google Calendar and Microsoft O365 Exchange Online

Cisco Webex Architecture

Cisco Webex Edge Video Mesh



Problem Statement

1:1 meetings and multi party meetings use media resource in the cloud

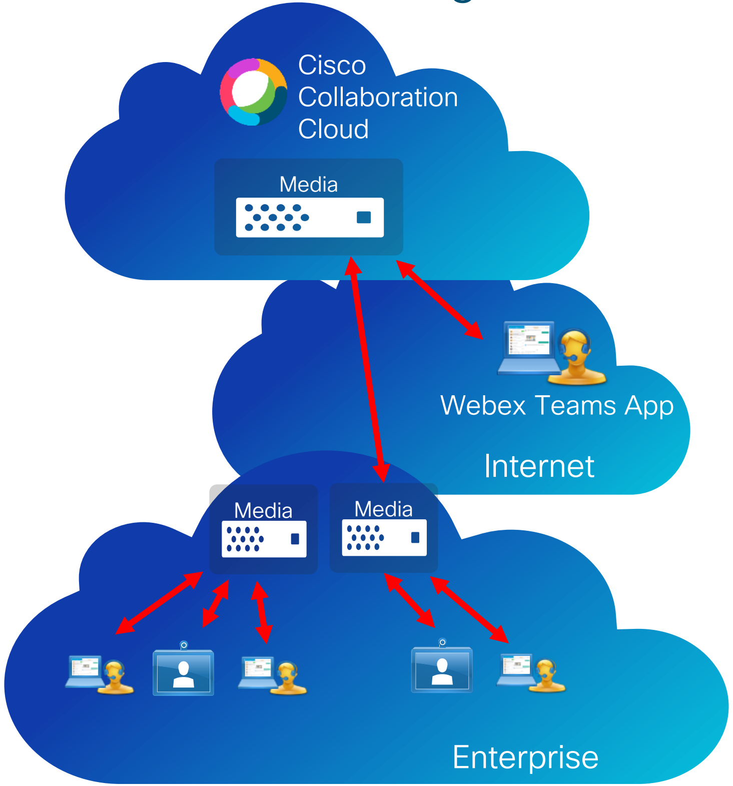
Media and signaling go from and to the cloud

Increased bandwidth requirement for Internet traffic with adoption of Cisco Webex Meetings and Teams

Possible impact on meeting experience by high delay between endpoint end media resources

Cisco Webex Architecture

Cisco Webex Edge Video Mesh

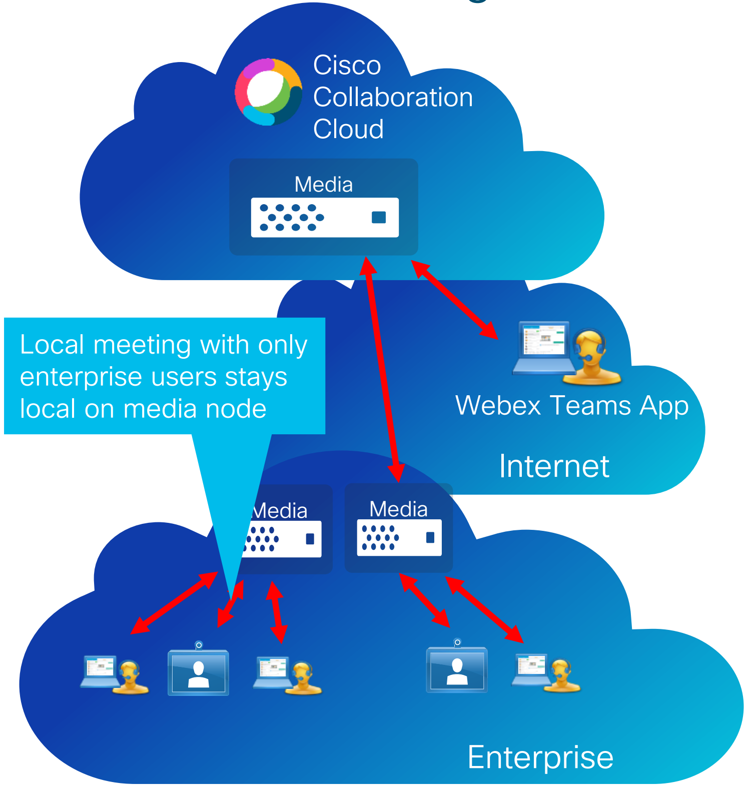


Advantages for Cisco Webex Edge Video Mesh

- Same media resources deployed in Cisco Cloud available in customer enterprise environment
- Available for free for customers with paid Cisco Webex Teams subscription
- Provided as VMware OVA template
- Customers can deploy media nodes across multiple locations, optimizing media quality and bandwidth utilization
- Automatic overflow to cloud
- Automatic upgrades of media nodes
- Cisco Webex Control Hub single pane management

Cisco Webex Architecture

Cisco Webex Edge Video Mesh



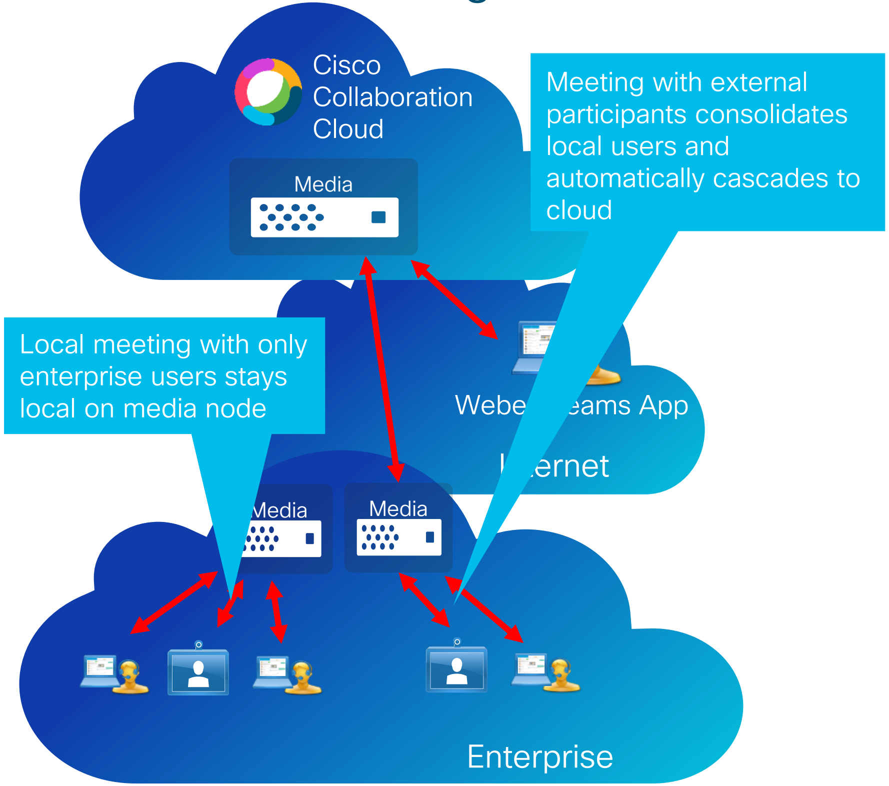
Local meeting with only enterprise users stays local on media node

Advantages for Cisco Webex Edge Video Mesh

- Same media resources deployed in Cisco Cloud available in customer enterprise environment
- Available for free for customers with paid Cisco Webex Teams subscription
- Provided as VMware OVA template
- Customers can deploy media nodes across multiple locations, optimizing media quality and bandwidth utilization
- Automatic overflow to cloud
- Automatic upgrades of media nodes
- Cisco Webex Control Hub single pane management

Cisco Webex Architecture

Cisco Webex Edge Video Mesh



Meeting with external participants consolidates local users and automatically cascades to cloud

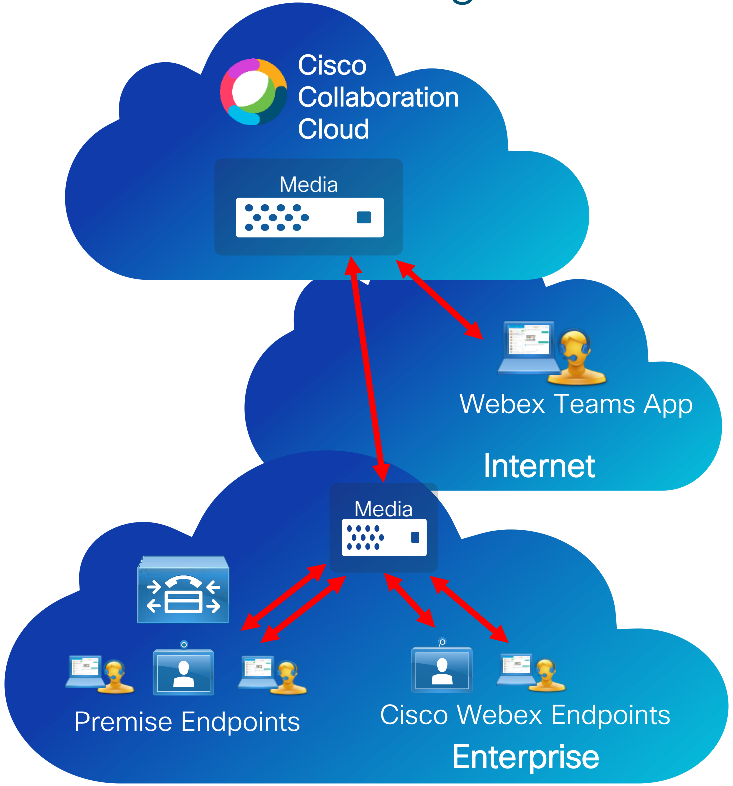
Local meeting with only enterprise users stays local on media node

Advantages for Cisco Webex Edge Video Mesh

- Same media resources deployed in Cisco Cloud available in customer enterprise environment
- Available for free for customers with paid Cisco Webex Teams subscription
- Provided as VMware OVA template
- Customers can deploy media nodes across multiple locations, optimizing media quality and bandwidth utilization
- Automatic overflow to cloud
- Automatic upgrades of media nodes
- Cisco Webex Control Hub single pane management

Cisco Webex Architecture

Cisco Webex Edge Video Mesh



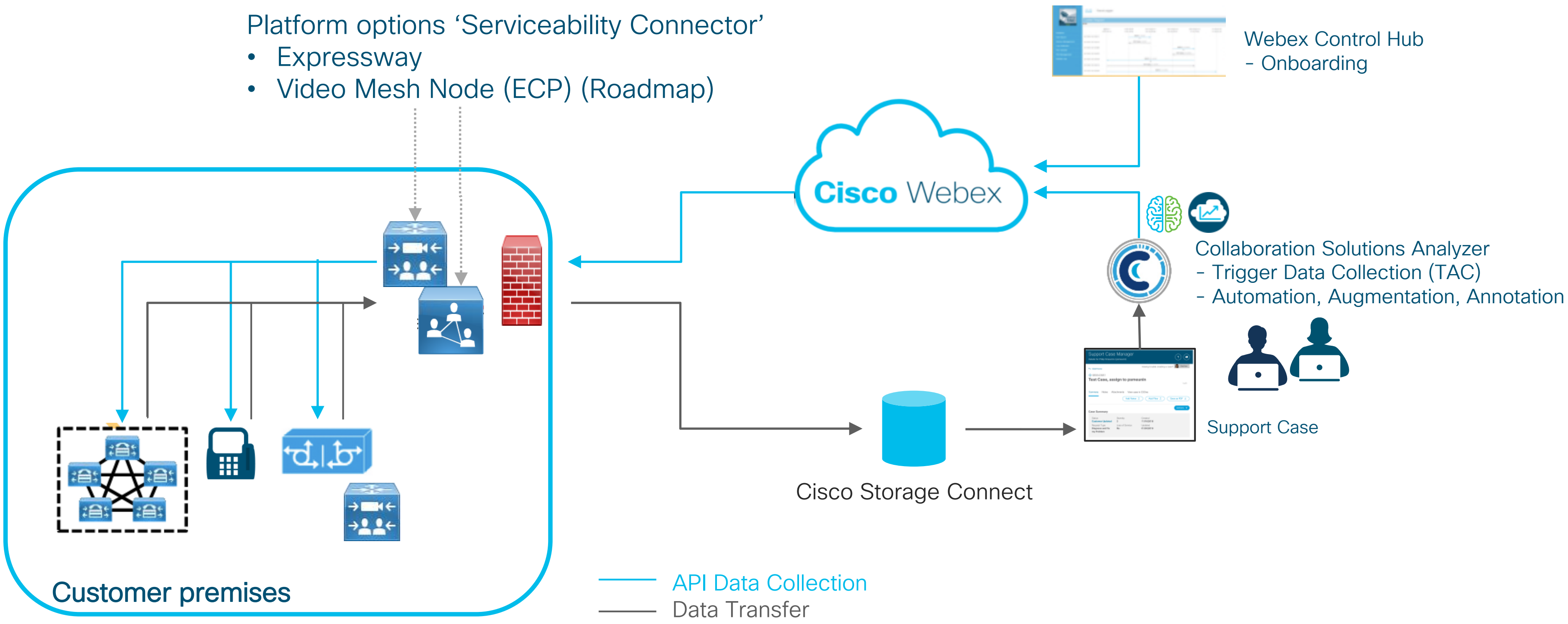
Cisco Webex Edge Video Mesh Integration with existing premise resources

- Premise endpoints can utilize Webex Edge Video Mesh resources
- Provides quality and bandwidth optimization for existing infrastructure
- Available for @meet.ciscoSpark.com and @<customer>.webex.com (CMR)
- Requires Cisco CMR 3.5

Cisco Webex Architecture

Cisco Serviceability Connector

Please check BRKCOL-2135 for further details



Platform options 'Serviceability Connector'

- Expressway
- Video Mesh Node (ECP) (Roadmap)

Cisco Webex
Webex Control Hub
- Onboarding
Collaboration Solutions Analyzer
- Trigger Data Collection (TAC)
- Automation, Augmentation, Annotation
Support Case
Cisco Storage Connect
Customer premises

API Data Collection

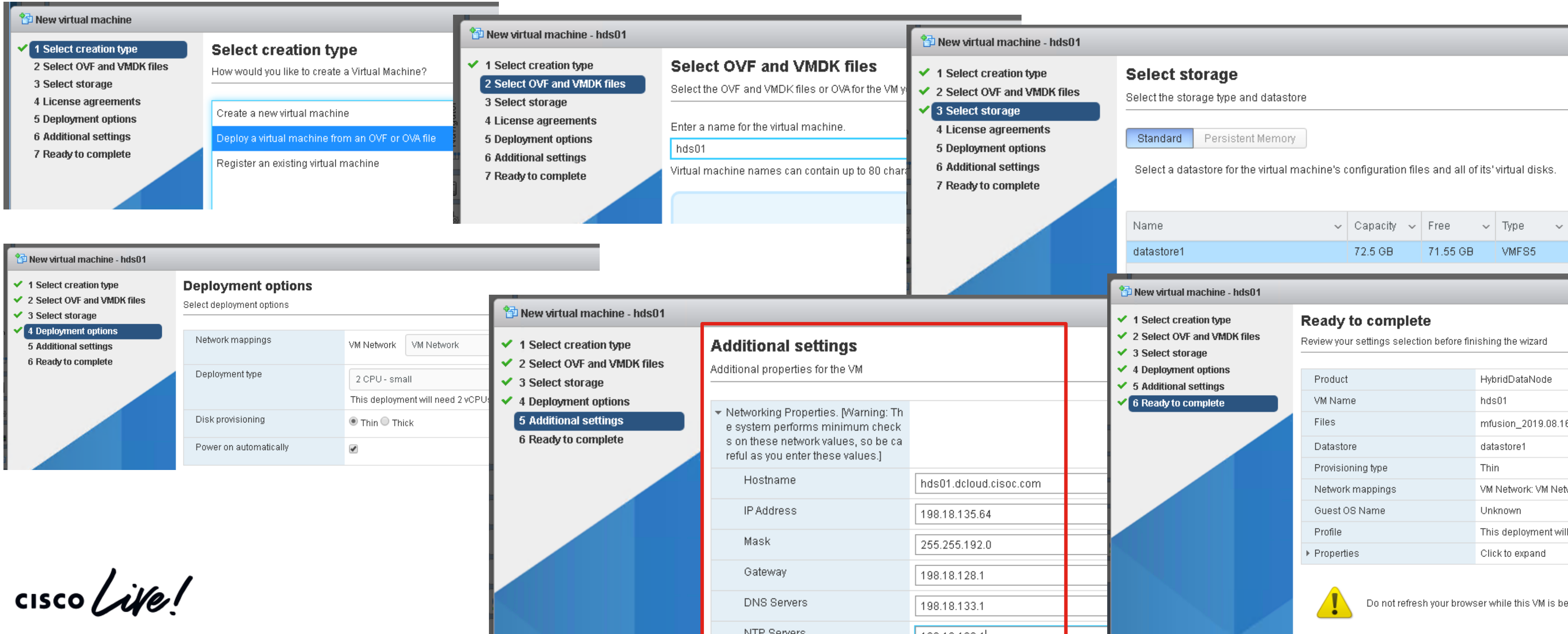
Data Transfer

Cisco Webex Architecture

Cisco Hybrid Services Platform News (Video Mesh & Hybrid Data Security)

New OVA deployment wizard

Cisco Hybrid Services supported for VMware ESXi 6.0 or higher



New virtual machine

- ✓ 1 Select creation type
- 2 Select OVF and VMDK files
- 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select creation type

How would you like to create a Virtual Machine?

- Create a new virtual machine
- Deploy a virtual machine from an OVF or OVA file
- Register an existing virtual machine

New virtual machine - hds01

- ✓ 1 Select creation type
- 2 Select OVF and VMDK files
- 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM y

Enter a name for the virtual machine.

hds01

Virtual machine names can contain up to 80 chara

New virtual machine - hds01

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select storage

Select the storage type and datastore

Standard | Persistent Memory

Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type
datastore1	72.5 GB	71.55 GB	VMFS5

New virtual machine - hds01

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- 5 Additional settings
- 6 Ready to complete

Deployment options

Select deployment options

Network mappings	VM Network: VM Network
Deployment type	2 CPU - small This deployment will need 2 vCPUs
Disk provisioning	● Thin ○ Thick
Power on automatically	☑

New virtual machine - hds01

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- 5 Additional settings
- 6 Ready to complete

Additional settings

Additional properties for the VM

Networking Properties. [Warning: The system performs minimum checks on these network values, so be careful as you enter these values.]

Hostname	hds01.dcloud.cisoc.com
IP Address	198.18.135.64
Mask	255.255.192.0
Gateway	198.18.128.1
DNS Servers	198.18.133.1
NTP Servers	

New virtual machine - hds01

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Additional settings
- ✓ 6 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

Product	HybridDataNode
VM Name	hds01
Files	mfusion_2019.08.1
Datastore	datastore1
Provisioning type	Thin
Network mappings	VM Network: VM Net
Guest OS Name	Unknown
Profile	This deployment will
Properties	Click to expand

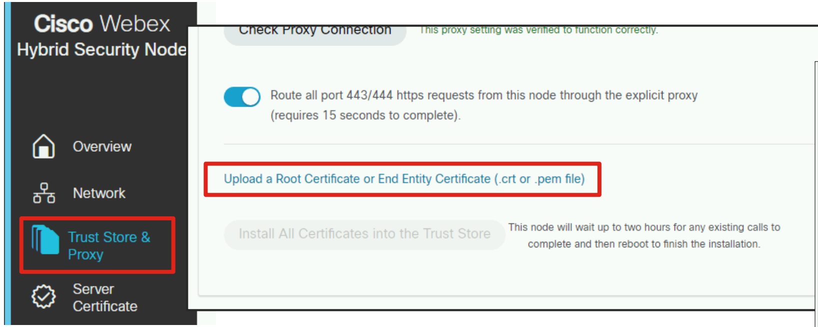
Do not refresh your browser while this VM is be

Cisco Webex Architecture

Cisco Hybrid Services Platform News (Video Mesh & Hybrid Data Security)

Install Enterprise Root CA Certificate(s)

- Navigate to https://<fqdn or IP address of hybrid VM>/setup
- Acknowledge self signed certificate warning



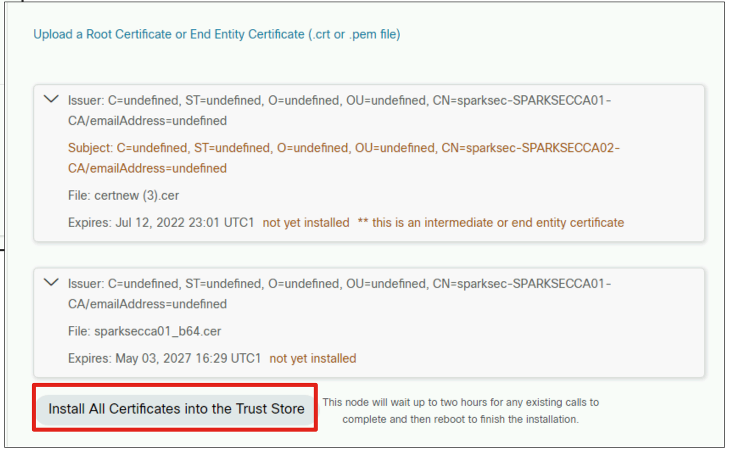
Cisco Webex Hybrid Security Node

This proxy setting was verified to function correctly.

Route all port 443/444 https requests from this node through the explicit proxy (requires 15 seconds to complete).

Upload a Root Certificate or End Entity Certificate (.crt or .pem file)

This node will wait up to two hours for any existing calls to complete and then reboot to finish the installation.



Upload a Root Certificate or End Entity Certificate (.crt or .pem file)

Issuer: C=undefined, ST=undefined, O=undefined, OU=undefined, CN=sparksec-SPARKSECCA01-CA/emailAddress=undefined

Subject: C=undefined, ST=undefined, O=undefined, OU=undefined, CN=sparksec-SPARKSECCA02-CA/emailAddress=undefined

File: certnew (3).cer

Expires: Jul 12, 2022 23:01 UTC1 not yet installed ** this is an intermediate or end entity certificate

Issuer: C=undefined, ST=undefined, O=undefined, OU=undefined, CN=sparksec-SPARKSECCA01-CA/emailAddress=undefined

File: sparksecca01_b64.cer

Expires: May 03, 2027 16:29 UTC1 not yet installed

This node will wait up to two hours for any existing calls to complete and then reboot to finish the installation.

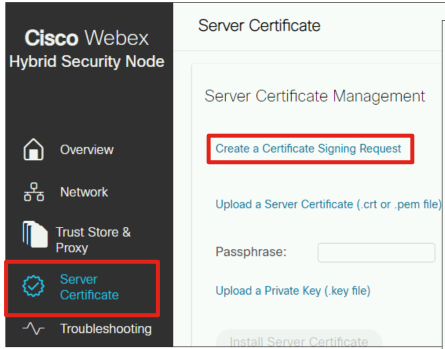
Example shows root and subordinate/intermediate Certificate Authority

Cisco Webex Architecture

Cisco Hybrid Services Platform News (Video Mesh & Hybrid Data Security)

Install Enterprise CA Server Certificate

- Navigate to https://<fqdn or IP address of hybrid VM>/setup
- Acknowledge self signed certificate warning



Server Certificate

Server Certificate Management

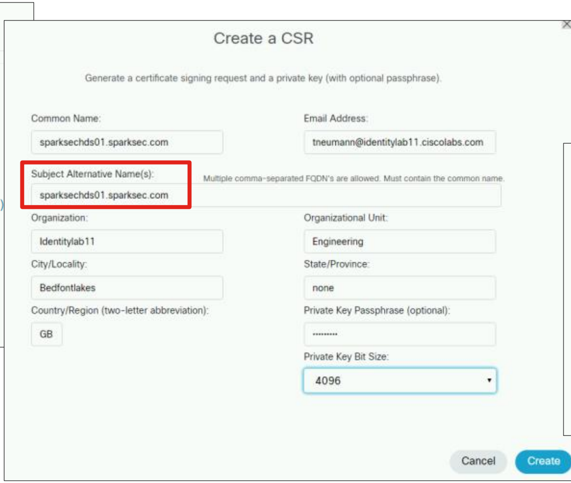
Create a Certificate Signing Request

Upload a Server Certificate (.crt or .pem file)

Passphrase:

Upload a Private Key (.key file)

Install Server Certificate



Create a CSR

Generate a certificate signing request and a private key (with optional passphrase).

Common Name: sparksechds01.sparksec.com

Email Address: tneumann@identitylab11.ciscolabs.com

Subject Alternative Name(s): sparksechds01.sparksec.com — Multiple comma-separated FQDN's are allowed. Must contain the common name.

Organization: Identitylab11

Organizational Unit: Engineering

City/Locality: Bedfontlakes

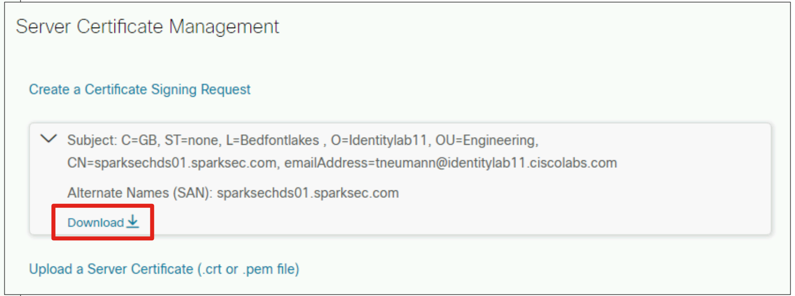
State/Province: none

Country/Region (two-letter abbreviation): GB

Private Key Passphrase (optional): ••••••••

Private Key Bit Size: 4096

Make sure SAN is set correctly, Google and Firefox will not accept certificates not containing the CN as SAN!



Server Certificate Management

Create a Certificate Signing Request

Subject: C=GB, ST=none, L=Bedfontlakes , O=Identitylab11, OU=Engineering, CN=sparksechds01.sparksec.com, emailAddress=tneumann@identitylab11.ciscolabs.com

Alternate Names (SAN): sparksechds01.sparksec.com

Download

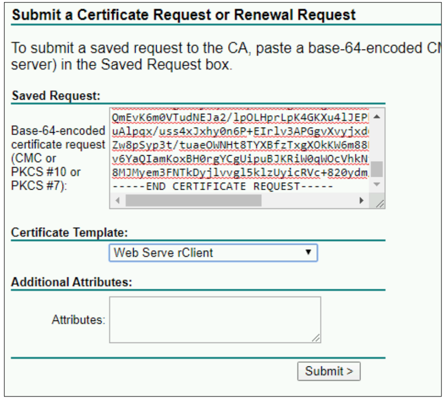
Upload a Server Certificate (.crt or .pem file)

- Download CSR and issue certificate from Enterprise CA

Cisco Webex Architecture

Cisco Hybrid Services Platform News (Video Mesh & Hybrid Data Security)

Install Enterprise CA Server Certificate



Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CI
server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
QmEvK6m0VTudNEJa2/lpOLHprLpK4GKXu4lJEP
uAlpqx/uss4xJxhy0n6P+EIrlv3APGgvXvyjxd
Zw8pSyp3t/tuaeOWNHt8TYXBfzTxgXOkKW6m88
v6YaQIamKoxBH0rgYCgUipuBJKRiW0qWOcVhkN
8MJMyem3FNTkDyjlvvgl5klzUyicRVc+820ydm
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

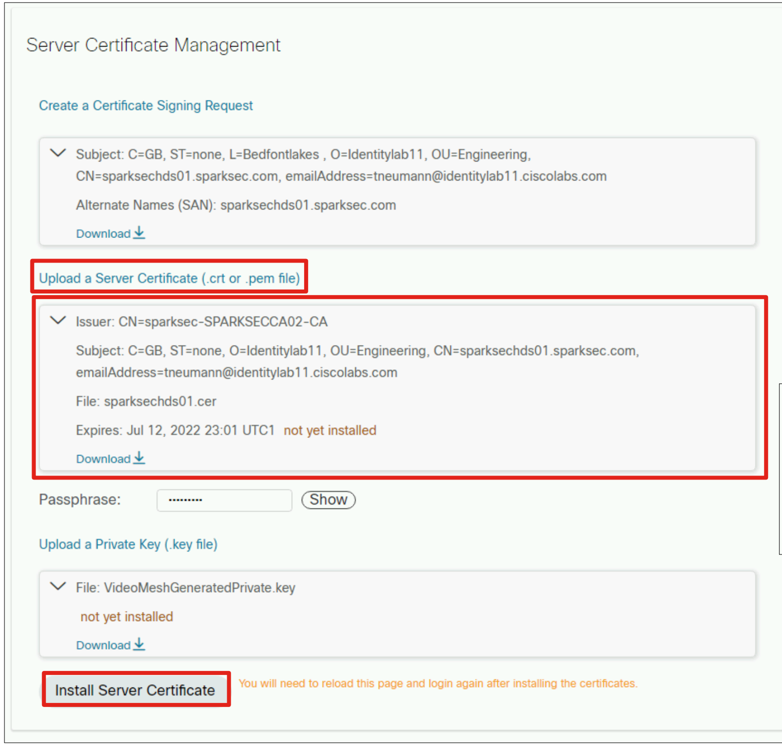
Web Serve rClient ▾

Additional Attributes:

Attributes:

Submit >

Example MS Enterprise CA



Server Certificate Management

Create a Certificate Signing Request

Subject: C=GB, ST=none, L=Bedfontlakes , O=Identitylab11, OU=Engineering, CN=sparksechds01.sparksec.com, emailAddress=tneumann@identitylab11.ciscolabs.com

Alternate Names (SAN): sparksechds01.sparksec.com

Download

Upload a Server Certificate (.crt or .pem file)

Issuer: CN=sparksec-SPARKSECCA02-CA

Subject: C=GB, ST=none, O=Identitylab11, OU=Engineering, CN=sparksechds01.sparksec.com, emailAddress=tneumann@identitylab11.ciscolabs.com

File: sparksechds01.cer

Expires: Jul 12, 2022 23:01 UTC1 not yet installed

Download

Passphrase: ········· Show

Upload a Private Key (.key file)

File: VideoMeshGeneratedPrivate.key

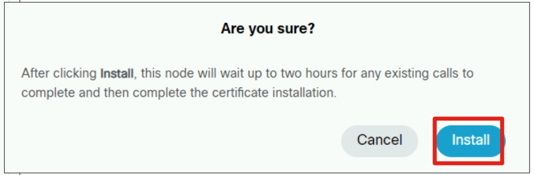
not yet installed

Download

Install Server Certificate

You will need to reload this page and login again after installing the certificates.

- Upload CA Server Certificate
- Install Server Certificate
- Acknowledge Warning Dialog



Are you sure?

After clicking **Install**, this node will wait up to two hours for any existing calls to complete and then complete the certificate installation.

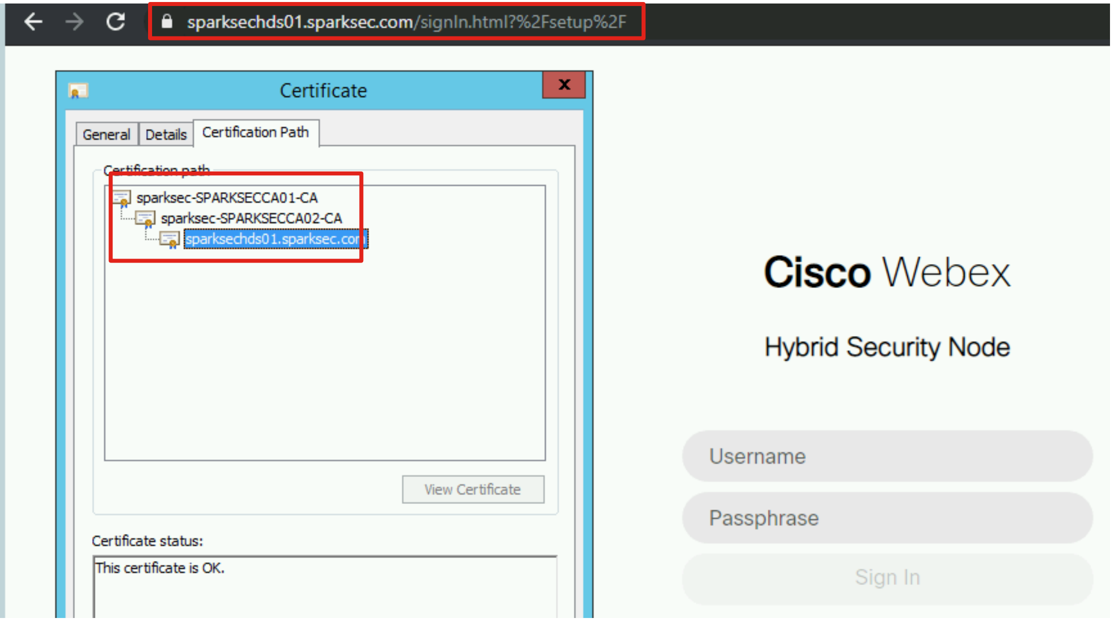
Cancel Install

Cisco Webex Architecture

Cisco Hybrid Services Platform News (Video Mesh & Hybrid Data Security)

BREAKING NEWS

Install Enterprise CA Server Certificate



sparksechds01.sparksec.com/signIn.html?%2Fsetup%2F

Certificate

General | Details | Certification Path

Certification path

- sparksec-SPARKSECCA01-CA
  - sparksec-SPARKSECCA02-CA
    - sparksechds01.sparksec.com

Certificate status:

This certificate is OK.

Cisco Webex

Hybrid Security Node

- Reload browser
- Cisco Hybrid Service using Enterprise CA server certificate

Identity

Which Protocols do we see in Identity Management

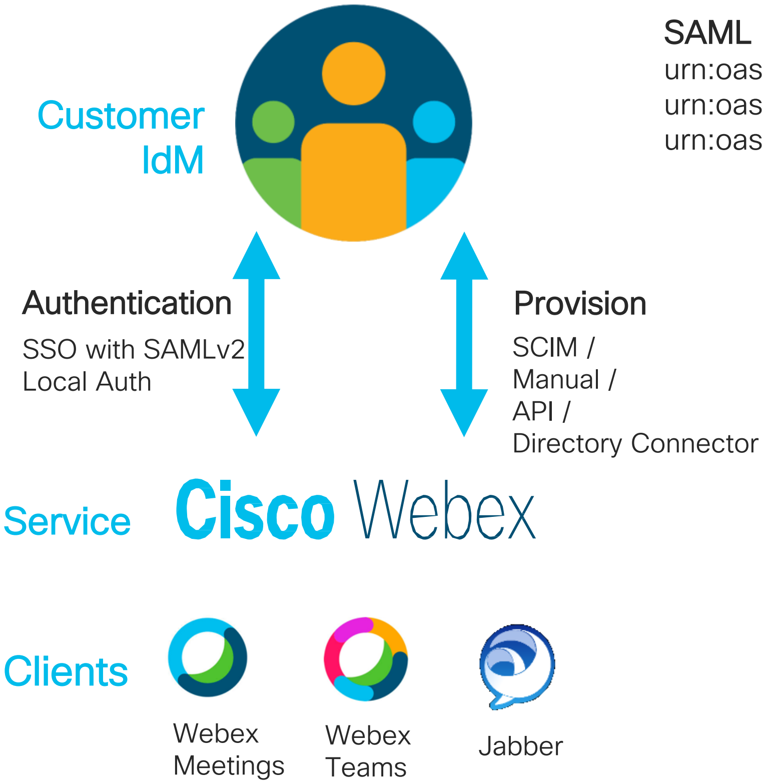
SAML Security Assertion Markup Language defined under OASIS Security Services Technical Committee (SSTC) Standards.

OAuth is a Authorisation Framework defined by IETF under RFC 6749

SCIM System for Cross-domain Identity Management, 2.0 was release under IETF as RFC 7643 and 7644

Cisco Collaboration Applications

Cisco Webex with Control Hub



Customer IdM

Authentication

SSO with SAMLv2
Local Auth

Provision

SCIM /
Manual /
API /
Directory Connector

Service Cisco Webex

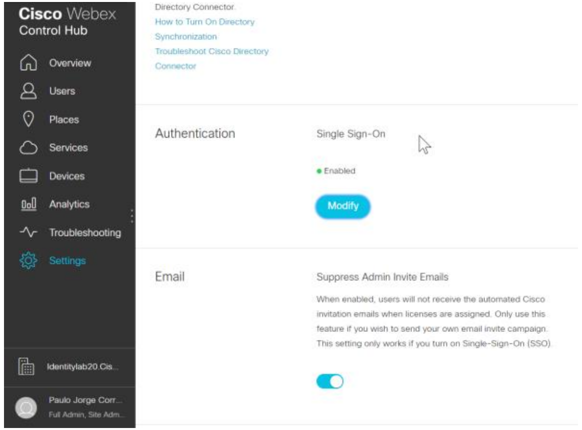
Clients

SAML NameID-formats Supported :

urn:oasis:names:tc:SAML:2.0:nameid-format:transient
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Provision URL

https://admin.webex.com/



Directory Connector.
How to Turn On Directory Synchronization
Troubleshoot Cisco Directory Connector

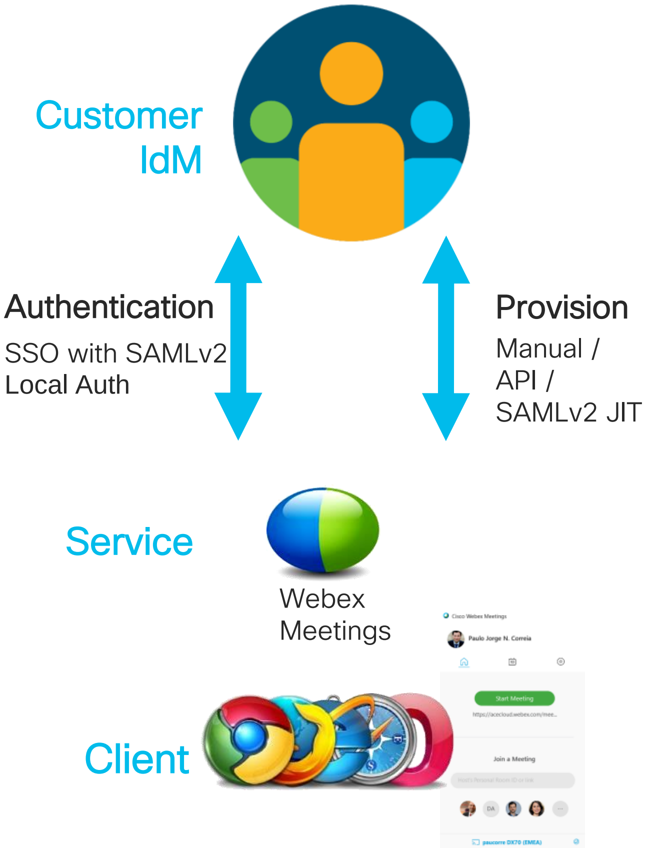
Authentication: Single Sign-On
● Enabled
Modify

Email: Suppress Admin Invite Emails

When enabled, users will not receive the automated Cisco invitation emails when licenses are assigned. Only use this feature if you wish to send your own email invite campaign. This setting only works if you turn on Single-Sign-On (SSO).

Cisco Collaboration Applications

Cisco Webex Meetings with Site Admin



Authentication

SSO with SAMLv2
Local Auth

Provision

Manual /
API /
SAMLv2 JIT

Cisco Webex Meetings

Paulo Jorge N. Correia

Start Meeting

https://acecloud.webex.com/mee...

Join a Meeting

Host's Personal Room ID or link

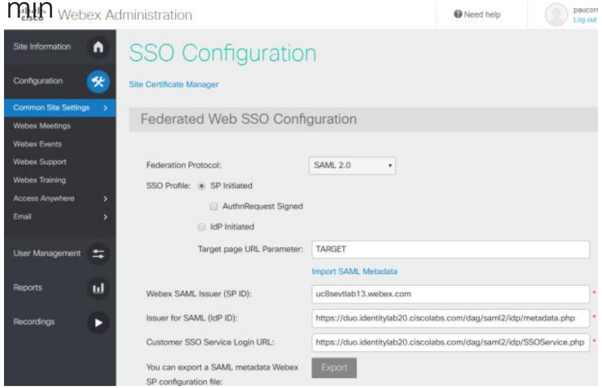
paucorre DX70 (EMEA)

SAML NameID-formats Supported :

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
…………
………….

Provision URL

https://{CustomerName}.webex.com/admin



SSO Configuration

Site Certificate Manager

Federated Web SSO Configuration

Federation Protocol: SAML 2.0

SSO Profile: ● SP Initiated

□ AuthnRequest Signed

○ IdP Initiated

Target page URL Parameter: TARGET

Import SAML Metadata

Webex SAML Issuer (SP ID): uc8sevtlab13.webex.com *

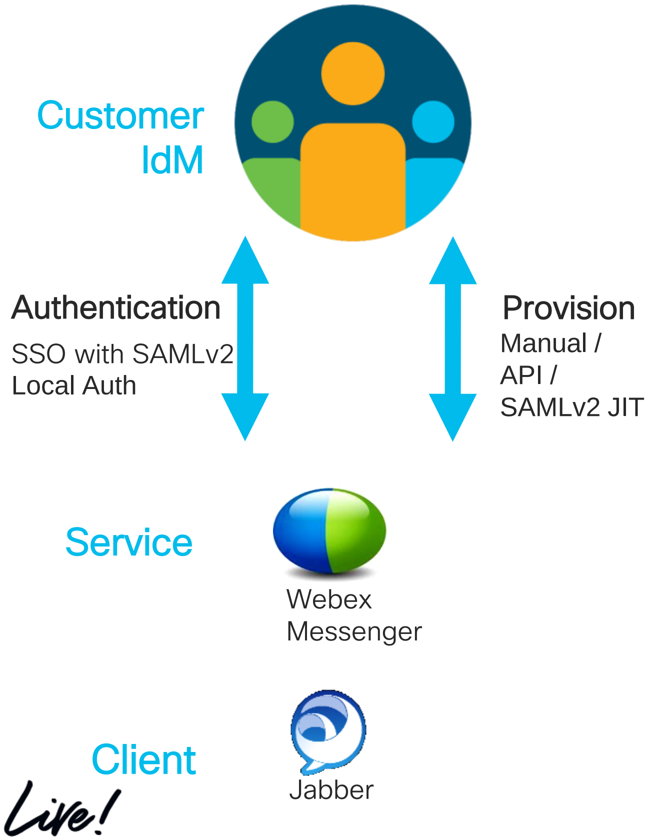
Issuer for SAML (IdP ID): https://duo.identitylab20.ciscolabs.com/dag/saml2/idp/metadata.php *

Customer SSO Service Login URL: https://duo.identitylab20.ciscolabs.com/dag/saml2/idp/SSOService.php *

You can export a SAML metadata Webex SP configuration file: Export

Cisco Collaboration Applications

Cisco Webex Messenger

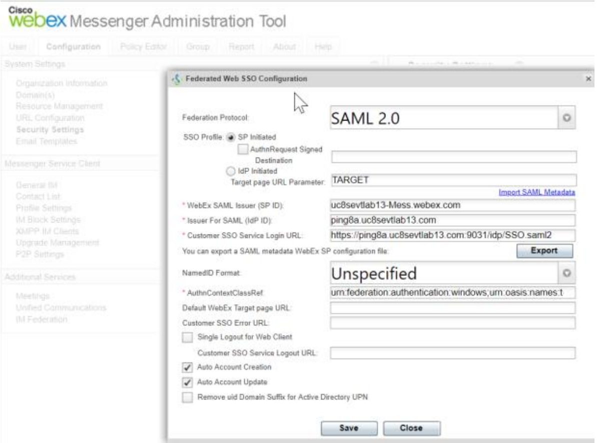


SAML NameID-formats Supported :

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
……………..
……………..

Provision URL

https://x02wapi.webexconnect.com/wbxconnect/acs/widgetserver/mashkit/apps/standalone.html?app=WBX.base.orgadmin&TrackID=111&hbxref=&goid=ConnectAdmin



Federation Protocol: SAML 2.0

SSO Profile: ● SP Initiated
□ AuthnRequest Signed
Destination:
○ IdP Initiated
Target page URL Parameter: TARGET

Import SAML Metadata

* WebEx SAML Issuer (SP ID): uc8sevtlab13-Mess.webex.com
* Issuer For SAML (IdP ID): ping8a.uc8sevtlab13.com
* Customer SSO Service Login URL: https://ping8a.uc8sevtlab13.com:9031/idp/SSO.saml2

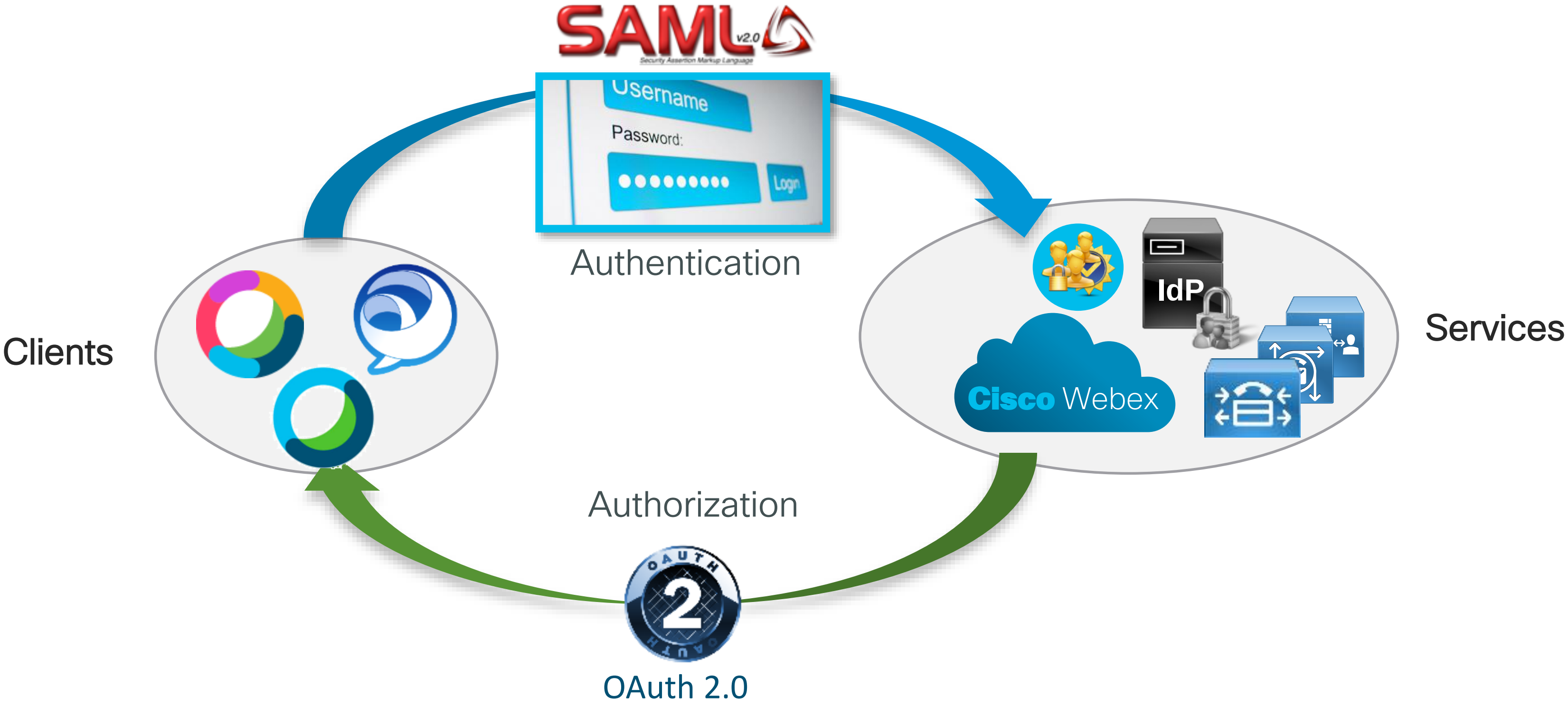
You can export a SAML metadata WebEx SP configuration file: Export

NamedID Format: Unspecified
* AuthnContextClassRef: urn:federation:authentication:windows;urn:oasis:names:t
Default WebEx Target page URL:
Customer SSO Error URL:

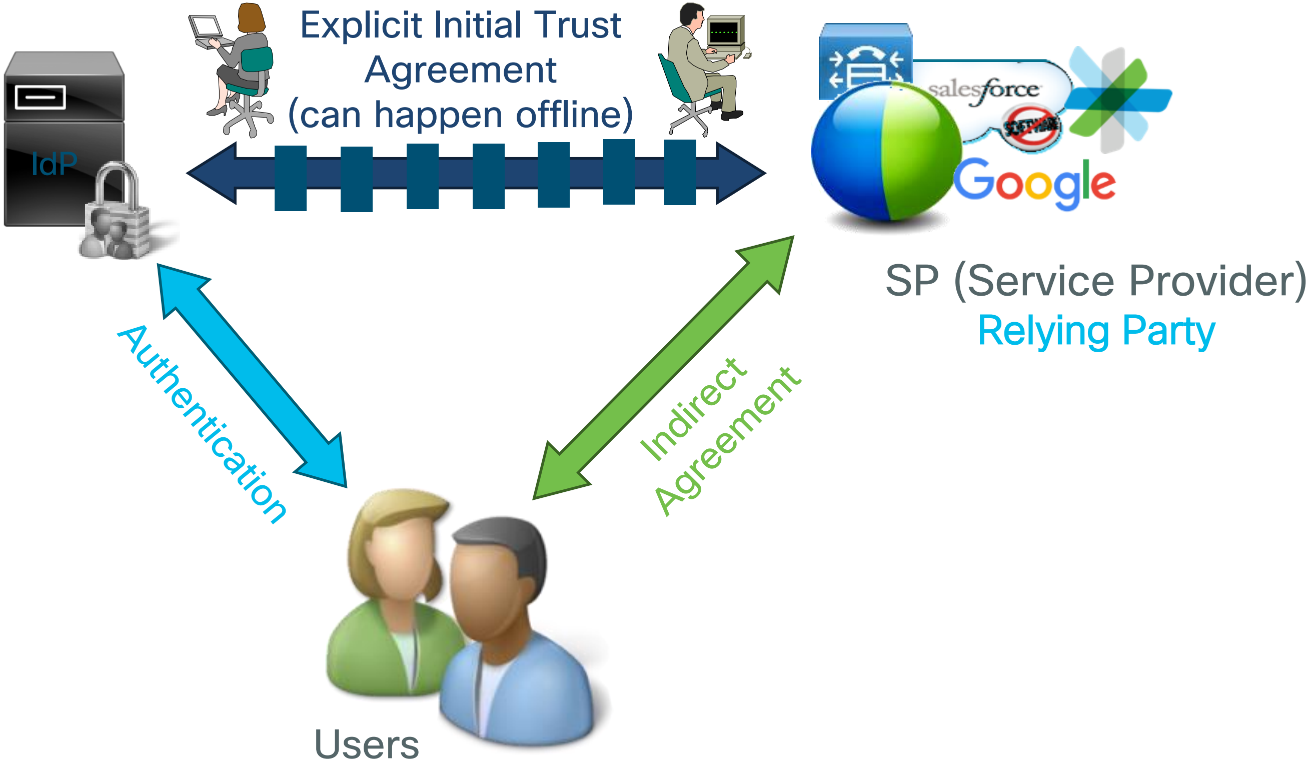
□ Single Logout for Web Client
Customer SSO Service Logout URL:
☑ Auto Account Creation
☑ Auto Account Update
□ Remove uid Domain Suffix for Active Directory UPN

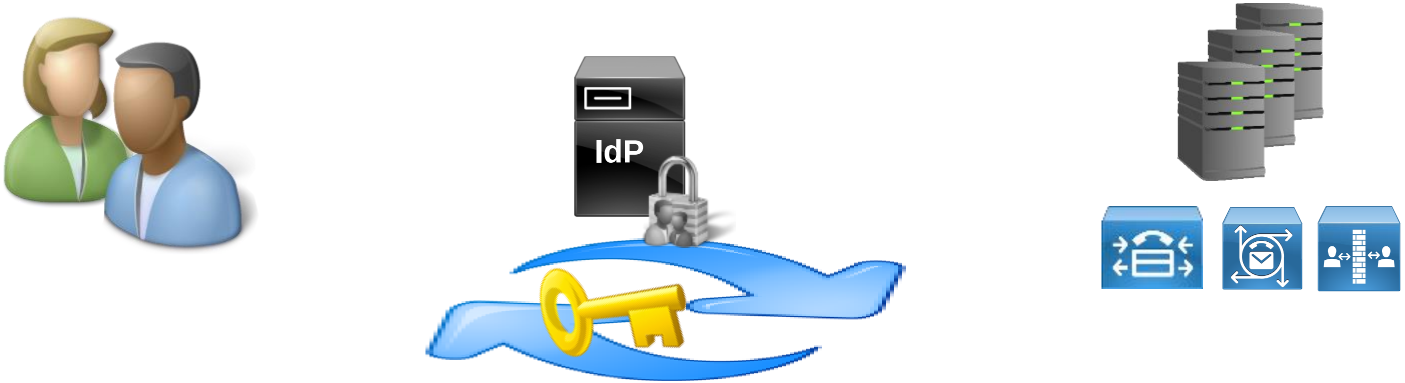
Authentication and Authorization

(SAML and OAuth)



Identity Framework





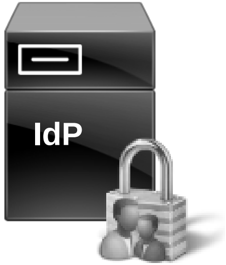
Single Sign-On

A session/user authentication process that enables a user to provide credentials only once in order to access multiple applications.
The process authenticates the user for all the applications they have been given rights to without further prompts when they switch applications during the session.

Role of an Identity Provider (IdP)

Validate who you are

- Review personally identifying information that proves you are who you say you are: identity proofing *(e.g., driver's license, passport, biometric data)*
- Assign attributes (name, role, email address) in the identity management system



Transact authentication requests

- Verify that the person seeking access to a resource is the one previously identified and approved, by utilizing some form of authentication *(e.g., username and password)*

Which IdP Does Cisco Supports ?

Cisco supports any IdP vendor that is compliant with the **SAMLv2** Oasis Standard.

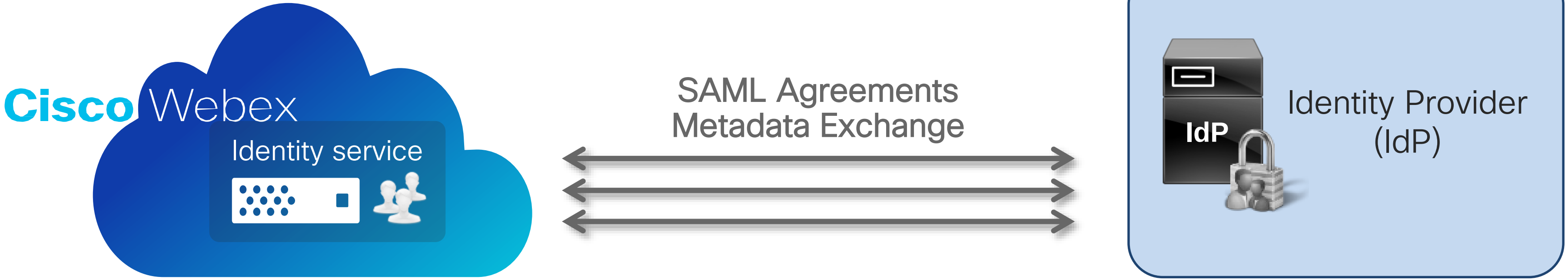
Internally in our development test cycles, we test our products against selected authentication methods of the follow IdP’s :

- Microsoft Active Directory Federation Services (ADFS) 2.0
- Open Access Manager (OpenAM) 11.0
- PingFederate 6.10.0.4

okta
Ping Identity
ORACLE
IDENTITY MANAGEMENT
ca technologies
FORGEROCK

f5
salesforce
NetIQ
Shibboleth
Microsoft

SAML SSO Configuration for Webex in Control Hub
Steps to Enable Single Sign-on

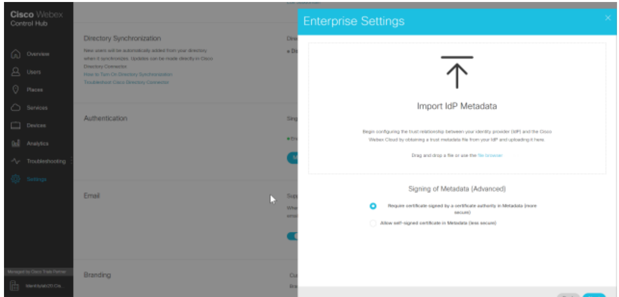


1
- Download SP Metadata

2
- Configure IdP
- Upload SP Metadata
- Download IdP Metadata

3
- Integrate With 3rd Party Identity Provider
- Choose Signed or not Signed Metadata
- Upload IdP Metadata
- Test SSO Connection

Collaboration Admin Identity Admin



Cisco Webex Control Hub

Overview
Users
Places
Services
Devices
Analytics
Troubleshooting
Settings

Managed by Cisco Trials Partner
identitylab20 Cis...

Directory Synchronization

New users will be automatically added from your directory when it synchronizes. Updates can be made directly in Cisco Directory Connector.

How to Turn On Directory Synchronization
Troubleshoot Cisco Directory Connector

Authentication

Email

Branding

Enterprise Settings

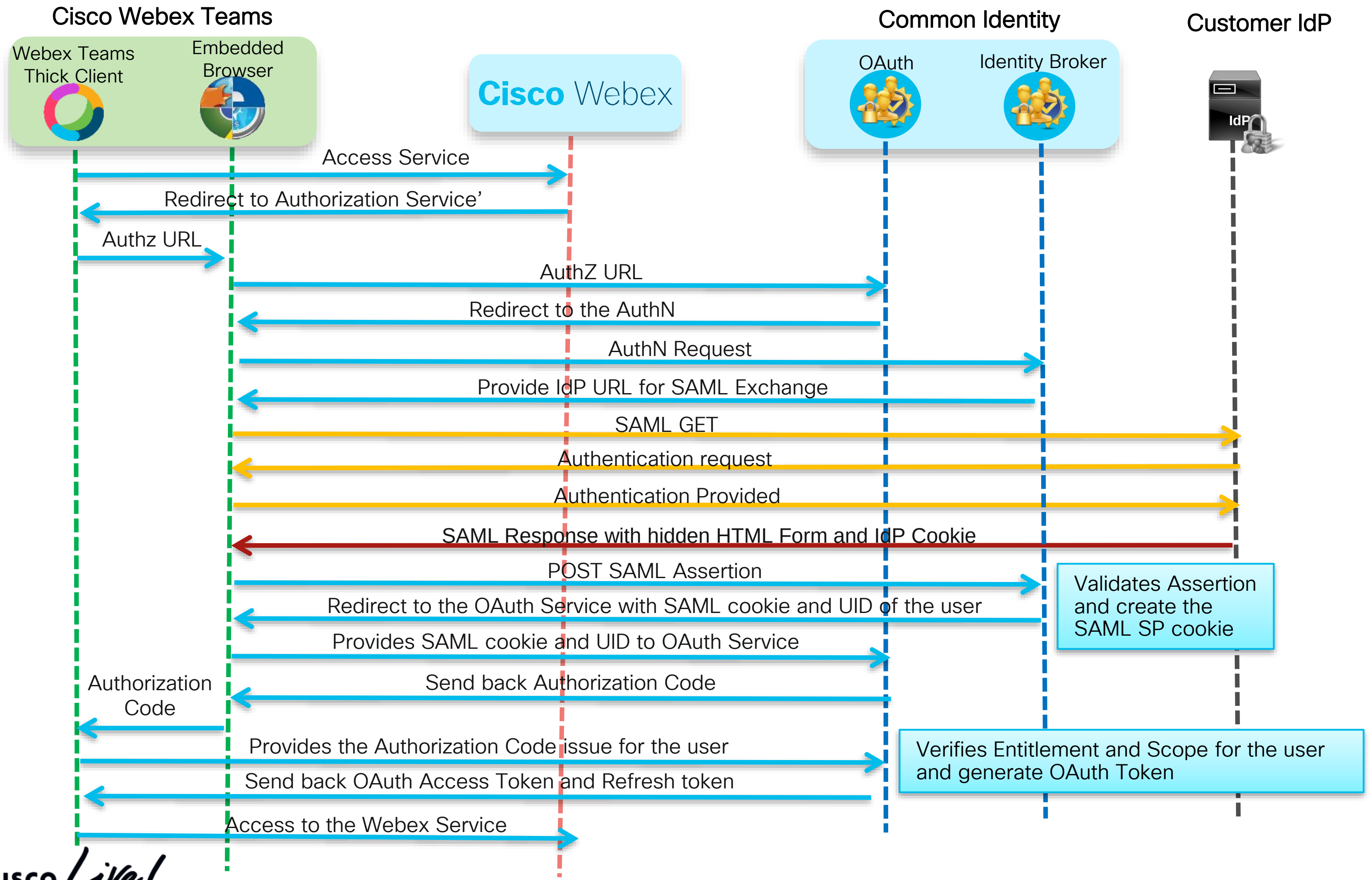
Import IdP Metadata

Begin configuring the trust relationship between your identity provider (IdP) and the Cisco Webex Cloud by obtaining a trust metadata file from your IdP and uploading it here.

Drag and drop a file or use the file browser

Signing of Metadata (Advanced)

● Require certificate signed by a certificate authority in Metadata (more secure)
○ Allow self-signed certificate in Metadata (less secure)



Cisco Webex Teams

Webex Teams Thick Client

Embedded Browser

Cisco Webex

Common Identity

OAuth

Identity Broker

Customer IdP

IdP

Access Service

Redirect to Authorization Service’

Authz URL

AuthZ URL

Redirect to the AuthN

AuthN Request

Provide IdP URL for SAML Exchange

SAML GET

Authentication request

Authentication Provided

SAML Response with hidden HTML Form and IdP Cookie

POST SAML Assertion

Validates Assertion and create the SAML SP cookie

Redirect to the OAuth Service with SAML cookie and UID of the user

Provides SAML cookie and UID to OAuth Service

Send back Authorization Code

Authorization Code

Provides the Authorization Code issue for the user

Verifies Entitlement and Scope for the user and generate OAuth Token

Send back OAuth Access Token and Refresh token

Access to the Webex Service

SAML Assertion from IdP to Webex in CH

```
<saml2p:Response
Destination="https://idbroker.webex.com/idb/Consumer/metaAlias/ea7c1420-
711d-4916-95f8-22de53230d1e/sp"
                ID="_157561492b8068bb78f4cb242ad4f006"
InResponseTo="s2e747a3b284812b71ccd8ac1dce98d00cbfa7555b"
                IssueInstant="2017-01-30T17:13:22.572Z"
                Version="2.0"
                xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                >
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
                 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                 >https://shib9a.cisco.net/idp/shibboleth</saml2:Issuer>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </saml2p:Status>
     <saml2:Assertion ID="_574a68c9ba24935315c606a48902e50f"
                    IssueInstant="2017-01-30T17:13:22.572Z"
                    Version="2.0"
                    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                    xmlns:xs="http://www.w3.org/2001/XMLSchema"
                    >
        <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://shib9a.cisco.net/idp/shibboleth</saml2:Issuer>
```

Same Relay state as the SAML request from the Webex

Successful SAML Assertion

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
            <ds:Reference URI="#_574a68c9ba24935315c606a48902e50f">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces PrefixList="xs"
                                                xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
                                                />
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                <ds:DigestValue>f4B90sjgqWCRJaUycRL7XS2ncdw=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>L0n0SdlaXFyL4Eg6.......</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>
                <ds:X509Certificate>MIIDKzCCAhOgAwIBAgIUNXw.........<ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
```

IdP Signature and Certificate for Webex to validate

SAML Assertion from IdP to Webex in CH

```
<saml2:Subject>
          <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
                      NameQualifier="https://shib9a.cisco.net/idp/shibboleth"
                      SPNameQualifier="https://idbroker.webex.com/ea7c1420-711d-4916-95f8-
22de53230d1e">_306e0e97b606cc3199a28e72c95aa206
           </saml2:NameID>
          <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
             <saml2:SubjectConfirmationData Address="172.16.36.50"
InResponseTo="s2e747a3b284812b71ccd8ac1dce98d00cbfa7555b“ NotOnOrAfter="2017-01-30T17:18:22.572Z"
Recipient="https://idbroker.webex.com/idb/Consumer/metaAlias/ea7c1420-711d-4916-95f8-22de53230d1e/sp"/>
          </saml2:SubjectConfirmation>
      </saml2:Subject>
      <saml2:Conditions NotBefore="2017-01-30T17:13:22.572Z"
                      NotOnOrAfter="2017-01-30T17:18:22.572Z">
          <saml2:AudienceRestriction>
             <saml2:Audience>https://idbroker.webex.com/ea7c1420-711d-4916-95f8-22de53230d1e</saml2:Audience>
          </saml2:AudienceRestriction>
      </saml2:Conditions>
```

NameID format, Webex supported **transient, unspecified and email**

IdP confirmation to the request

Time window when this SAML assertion is accepted

Entity ID that this assertion should apply to

NameID-formats support by Webex in CH

UNSPECIFIED

```
<saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified“
NameQualifier="https://shib9a.cisco.net/idp/shibboleth"
SPNameQualifier="https://idbroker.webex.com/ea7c1420-
711d-4916-95f8-22de53230d1e">
        _306e0e97b606cc3199a28e72c95aa206
</saml2:NameID>
<saml2:AttributeStatement>
        <saml2:Attribute Name="uid“
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified">
                <saml2:AttributeValue
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:type="xs:string">
                paucorre@identitylab20.ciscolabs.com
                </saml2:AttributeValue>
        </saml2:Attribute>
</saml2:AttributeStatement>
```

NameID format **unspecified** require SPNameQualifier and the extra attribute (uid) statement

NameID format **email** require SPNameQualifier but doesn’t require any extra attribute

EMAIL

```
<saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress“
SPNameQualifier="https://idbroker.webex.com/ea7c1420-711d-
4916-95f8-22de53230d1e">
        paucorre@identitylab20.ciscolabs.com
</saml:NameID>
```

TRANSIENT

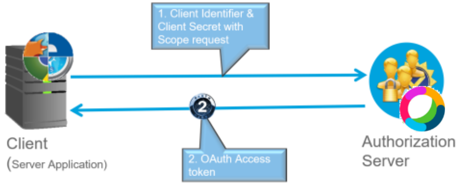
```
<saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:transient" NameQualifier="ping8a.uc8sevtlab13.com“
SPNameQualifier="https://idbroker.webex.com/8538f9ff-4f12-
440a-9880-3488bc3eb146">
        RbtO77X6eKfPUF5OhPrAKTCE88e
</saml:NameID>
<saml:AttributeStatement>
        <saml:Attribute Name="uid“
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml:AttributeValue xsi:type="xs:string“
xmlns:xs=http://www.w3.org/2001/XMLSchema
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
                paucorre@uc8sevtlab13.com
                </saml:AttributeValue>
        </saml:Attribute>
</saml:AttributeStatement>
```

NameID format **transient** require SPNameQualifier and the extra attribute (uid) statement

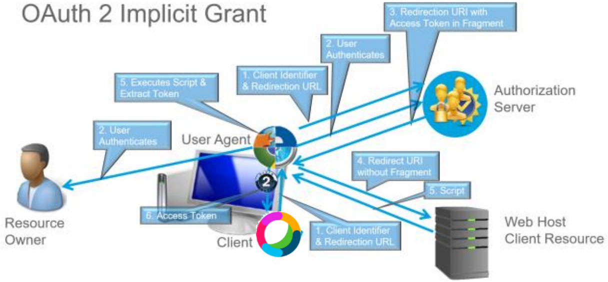
OAuth 2.0 Authorization Grants Flows supported in Control Hub

- There are different methods to get the OAuth tokens defined in the RFC
- Cloud products support three different OAuth grant flows
    - Authorization Code
    - Implicit
    - Client Credentials

OAuth 2 Client Credentials Grant

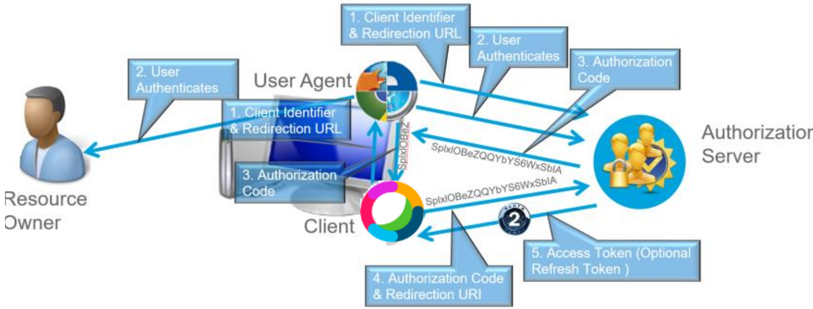


OAuth 2 Implicit Grant



3. Redirection URI with Access Token in Fragment
2. User Authenticates
1. Client Identifier & Redirection URL
5. Executes Script & Extract Token
Authorization Server
2. User Authenticates
User Agent
2
4. Redirect URI without Fragment
5. Script
6. Access Token
Resource Owner
Client
1. Client Identifier & Redirection URL
Web Host Client Resource

OAuth 2 Authentication Code Grant

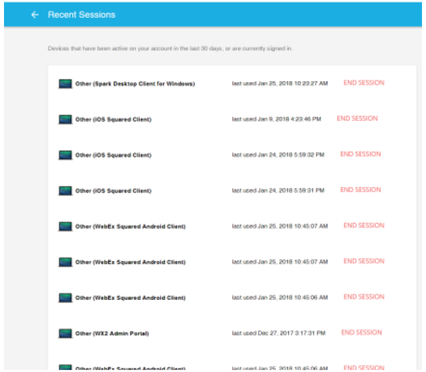


OAuth Token types and duration for Control Hub

Tokens types	Description
Webex Self Contained Access Token	Self Contained Access tokens are using JWT format and are Encrypted (JWE) and signed (JWS), by default have a duration of 12 hours.
Webex Refresh Token	Refresh tokens are using JWT format signed (JWS), by default have a duration of 60 days, but if the user provide it to get another access token they will be automatic extend to 60 days again, so in normal operations the user will never be logout.
Webex Self Contained Access Token	Provided by develop.webex.com to be use for API's and with a duration of 12 hours, can't be refresh.
Webex Anonymous Token	Will be use for guest access to Webex meetings, without the capability of generating content, have a duration of 49 hours and can't be refresh.
Webex Unverified Token	Will be use for guest access to Webex meetings with the capabilities of generating content (Whiteboard, conversations, etc), have a duration of 12 hours.

OAuth Token Revocation in Control Hub

1. Users can revoke tokens from any devices that he uses by login to https://idbroker.webex.com/idb/profile#/tokens

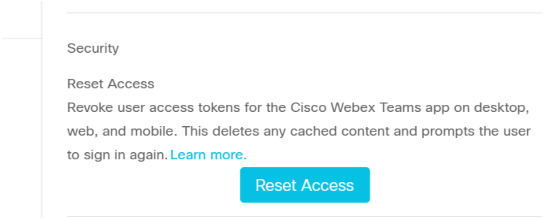


← Recent Sessions

Devices that have been active on your account in the last 30 days, or are currently signed in.

Other (Spark Desktop Client for Windows)	last used Jan 25, 2018 10:23:27 AM	END SESSION
Other (iOS Squared Client)	last used Jan 9, 2018 4:23:46 PM	END SESSION
Other (iOS Squared Client)	last used Jan 24, 2018 5:59:32 PM	END SESSION
Other (iOS Squared Client)	last used Jan 24, 2018 5:59:31 PM	END SESSION
Other (WebEx Squared Android Client)	last used Jan 25, 2018 10:45:07 AM	END SESSION
Other (WebEx Squared Android Client)	last used Jan 25, 2018 10:45:07 AM	END SESSION
Other (WebEx Squared Android Client)	last used Jan 25, 2018 10:45:06 AM	END SESSION
Other (WX2 Admin Portal)	last used Dec 27, 2017 3:17:31 PM	END SESSION
Other (WebEx Squared Android Client)	last used Jan 25, 2018 10:45:06 AM	END SESSION

2. Administrator Revocation via Control Hub with Pro Pack



Security

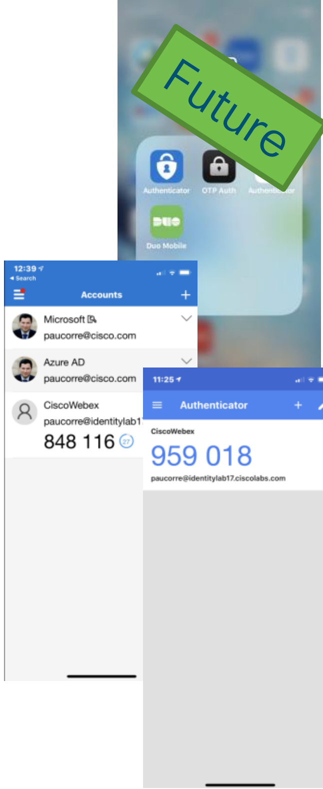
Reset Access

Revoke user access tokens for the Cisco Webex Teams app on desktop, web, and mobile. This deletes any cached content and prompts the user to sign in again. Learn more.

Having simple MFA without IdP

Webex Identity service provides a option where you can use MFA without the need for an IdP, you will only need one of the OTP software products available in the market.

We recommend Duo Mobile and/or Google Authenticator, but it work with most of the clients available in the mobile stores.



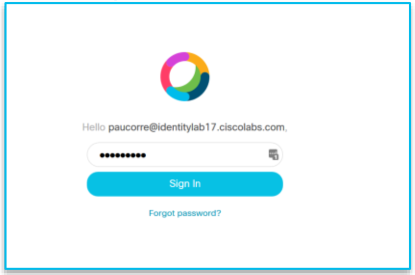
Microsoft
paucorre@cisco.com

Azure AD
paucorre@cisco.com

CiscoWebex
paucorre@identitylab1
848 116

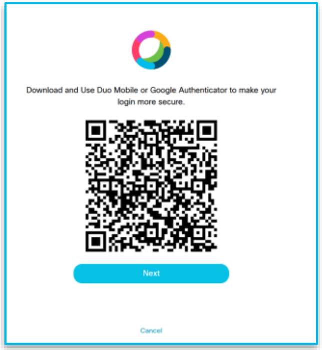
CiscoWebex
959 018
paucorre@identitylab17.ciscolabs.com

Step 1



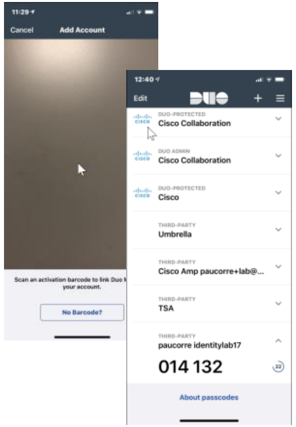
Hello paucorre@identitylab17.ciscolabs.com,

Step 2



Download and Use Duo Mobile or Google Authenticator to make your login more secure.

Step 3



Scan an activation barcode to link Duo M your account.

DUO-PROTECTED
Cisco Collaboration

DUO ADMIN
Cisco Collaboration

DUO-PROTECTED
Cisco

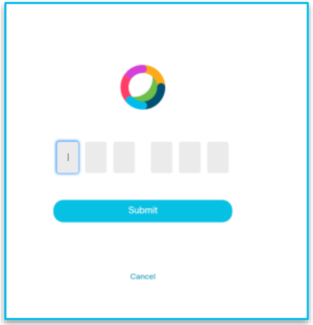
THIRD-PARTY
Umbrella

THIRD-PARTY
Cisco Amp paucorre+lab@...

THIRD-PARTY
TSA

THIRD-PARTY
paucorre identitylab17
014 132

Step 4

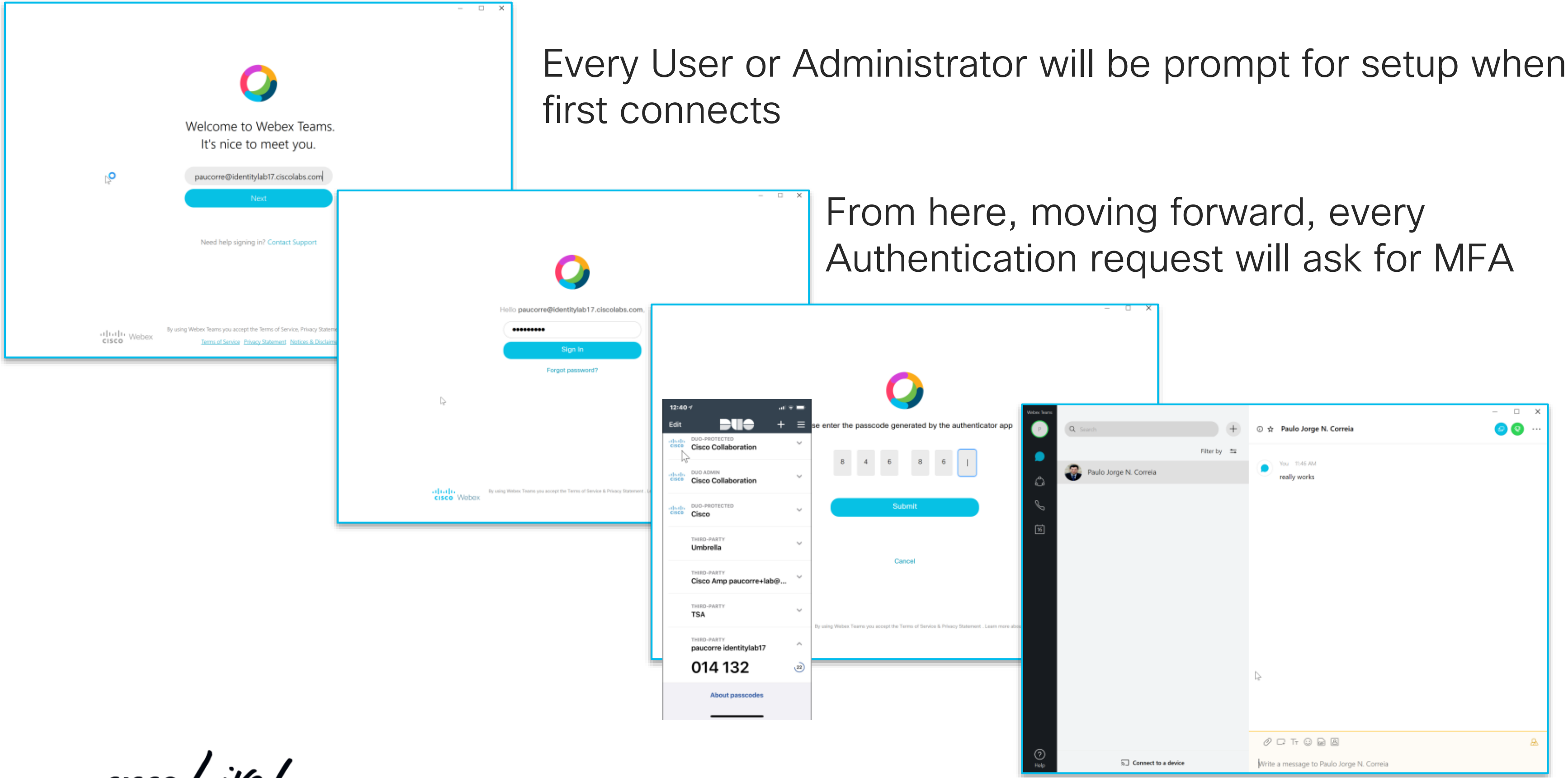


Clients and administration experience

Future

Every User or Administrator will be prompt for setup when he first connects

From here, moving forward, every Authentication request will ask for MFA



Welcome to Webex Teams.
It's nice to meet you.

paucorre@identitylab17.ciscolabs.com

Next

Need help signing in? Contact Support

By using Webex Teams you accept the Terms of Service, Privacy Statement

Terms of Service Privacy Statement Notices & Disclaimers

Hello paucorre@identitylab17.ciscolabs.com

••••••••••

Sign In

Forgot password?

By using Webex Teams you accept the Terms of Service & Privacy Statement

...se enter the passcode generated by the authenticator app

8 4 6 8 6 |

Submit

Cancel

By using Webex Teams you accept the Terms of Service & Privacy Statement . Learn more abo...

12:40

Edit DUO

DUO-PROTECTED
Cisco Collaboration

DUO ADMIN
Cisco Collaboration

DUO-PROTECTED
Cisco

THIRD-PARTY
Umbrella

THIRD-PARTY
Cisco Amp paucorre+lab@...

THIRD-PARTY
TSA

THIRD-PARTY
paucorre identitylab17
014 132

About passcodes

Webex Teams

Search

Filter by

Paulo Jorge N. Correia

Paulo Jorge N. Correia

You 11:46 AM
really works

Connect to a device

Write a message to Paulo Jorge N. Correia

Help

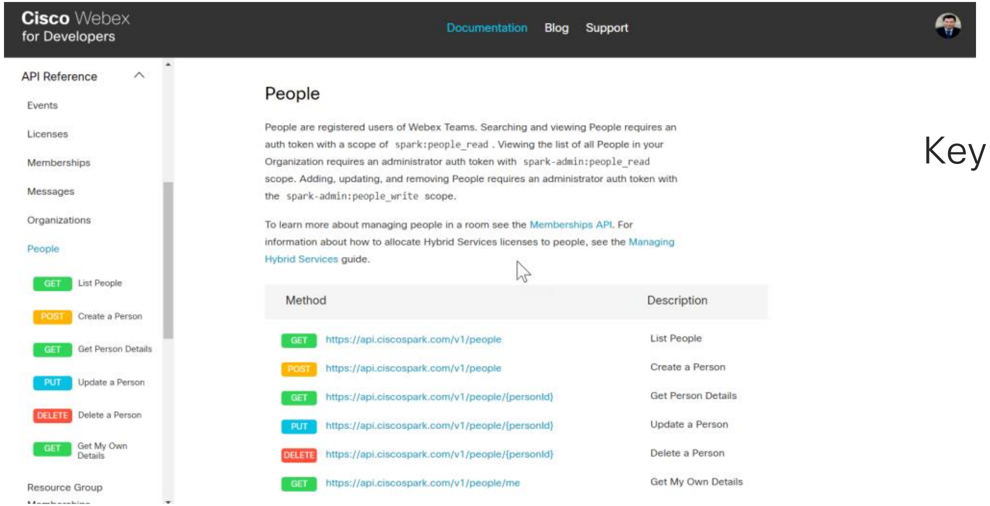
Webex User Account Management Options

Options	Description
Manual or CSV updates through Org Admin	Admin can use Webex Control Hub to manage user accounts
User Invite	User can invite another user to use Webex Teams
Directory Connector	Automatic method for creating, updating and deactivating user accounts and groups. Account information will be synchronized from Customer Active Directory
SCIM protocol	Automatic method for creating, updating and deactivating user accounts from IdP's that are SCIM enabled.
People API	Create, Delete, Update and List users by using API's
Account Linking	Customer with Webex meetings under Site admin, and provision user in Webex Control Hub

Which provision mechanisms can be used with each other ?

	Manual and/or CSV	Account Linking	People API's	SCIM	Directory Connector
Manual and/or CSV	✅	✅	✅	✅	❌
Account Linking	✅	✅	✅	✓	✓
People API's	✅	✅	✅	✅	❌
SCIM	✅	✓	✅	✅	❌
Directory Connector	❌	✓	❌	❌	✅

Manage People API



People

People are registered users of Webex Teams. Searching and viewing People requires an auth token with a scope of `spark:people_read` . Viewing the list of all People in your Organization requires an administrator auth token with `spark-admin:people_read` scope. Adding, updating, and removing People requires an administrator auth token with the `spark-admin:people_write` scope.

To learn more about managing people in a room see the Memberships API. For information about how to allocate Hybrid Services licenses to people, see the Managing Hybrid Services guide.

Method	Description
GET https://api.ciscospark.com/v1/people	List People
POST https://api.ciscospark.com/v1/people	Create a Person
GET https://api.ciscospark.com/v1/people/{personId}	Get Person Details
PUT https://api.ciscospark.com/v1/people/{personId}	Update a Person
DELETE https://api.ciscospark.com/v1/people/{personId}	Delete a Person
GET https://api.ciscospark.com/v1/people/me	Get My Own Details

https://develop.webex.com/resource-people.html

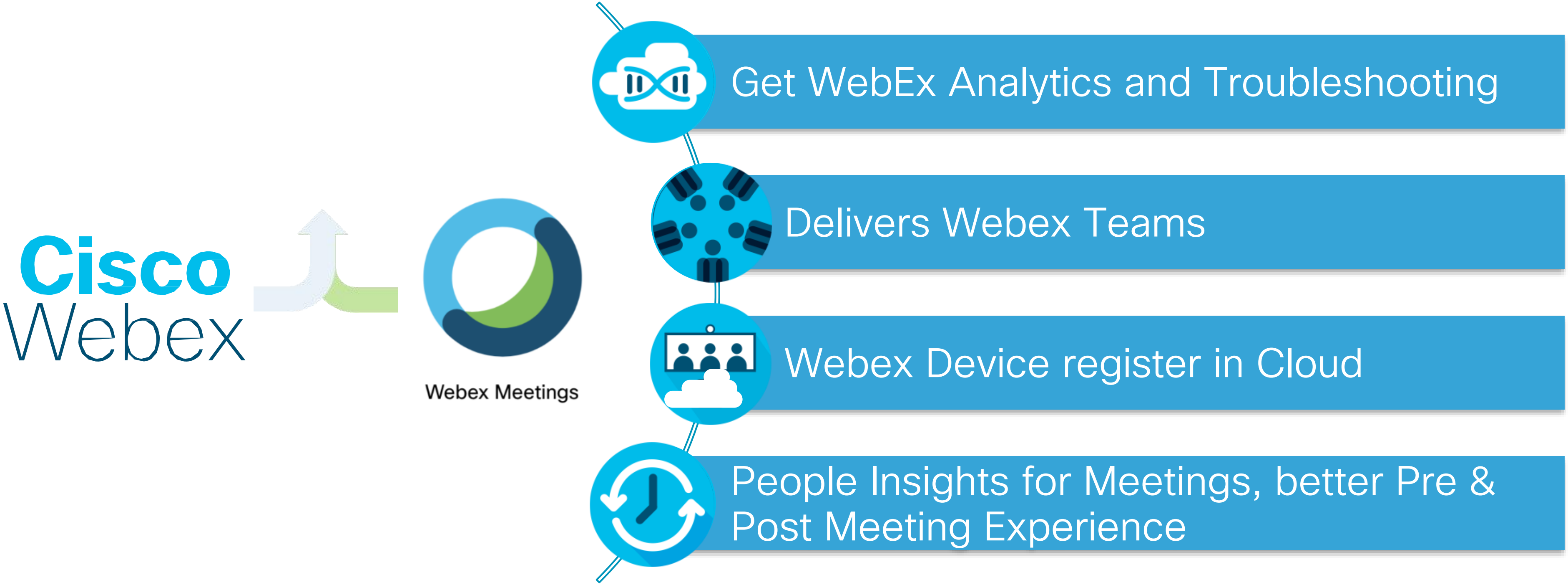
Benefit:

- Manage users and licensing via an API to control exactly who has access to specific services and provide better security

Key Capabilities

- Create a person dynamically with the right license and entitlement to the right services
- Delete a person to ensure there access is revoked to meet compliance rules
- Update a person in case their phone, address or profile has changed because of a promotion
- List people so you can be in the know about the people in your organization
- Get Me details so you can make sure your details are up to date

Benefits of Linking



Get WebEx Analytics and Troubleshooting

Delivers Webex Teams

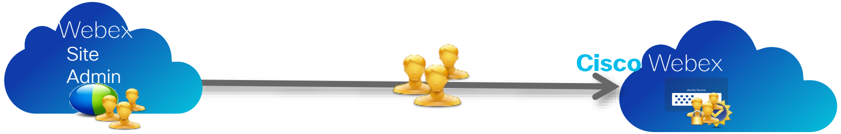
Webex Device register in Cloud

People Insights for Meetings, better Pre & Post Meeting Experience

https://help.webex.com/en-us/341eud/Link-Cisco-Webex-Sites-to-Control-Hub

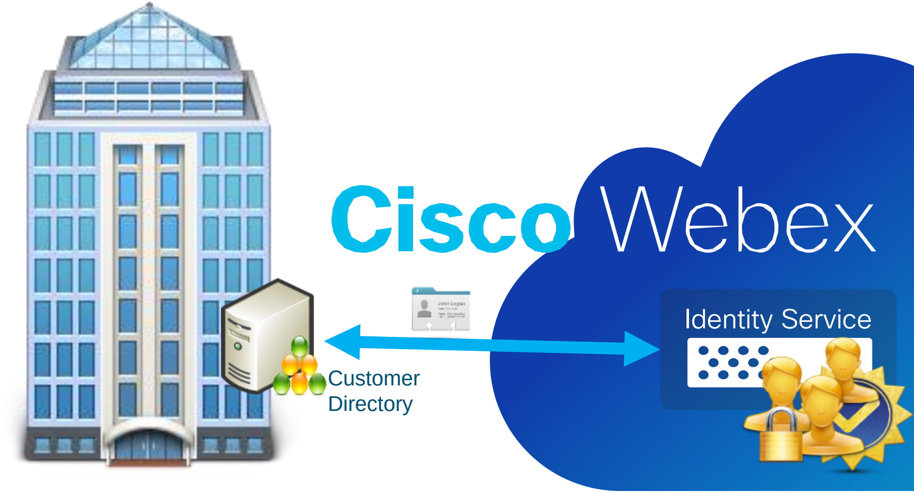
Automatic Linking of Sites/Users to Cisco Webex Control Hub

- All sites and users will be automatically linked with Cisco Webex Control Hub in the new phase.
- The new phase will only apply to Webex Meeting sites with subscription.
- The new phase will not be applicable for sites hosted in EU Datacenters, or FedRAMP.
- In previous interactions of Site Linking 2000 sites were already done, apart from the ones done manually.
- Automatic user synchronization done twice a day.

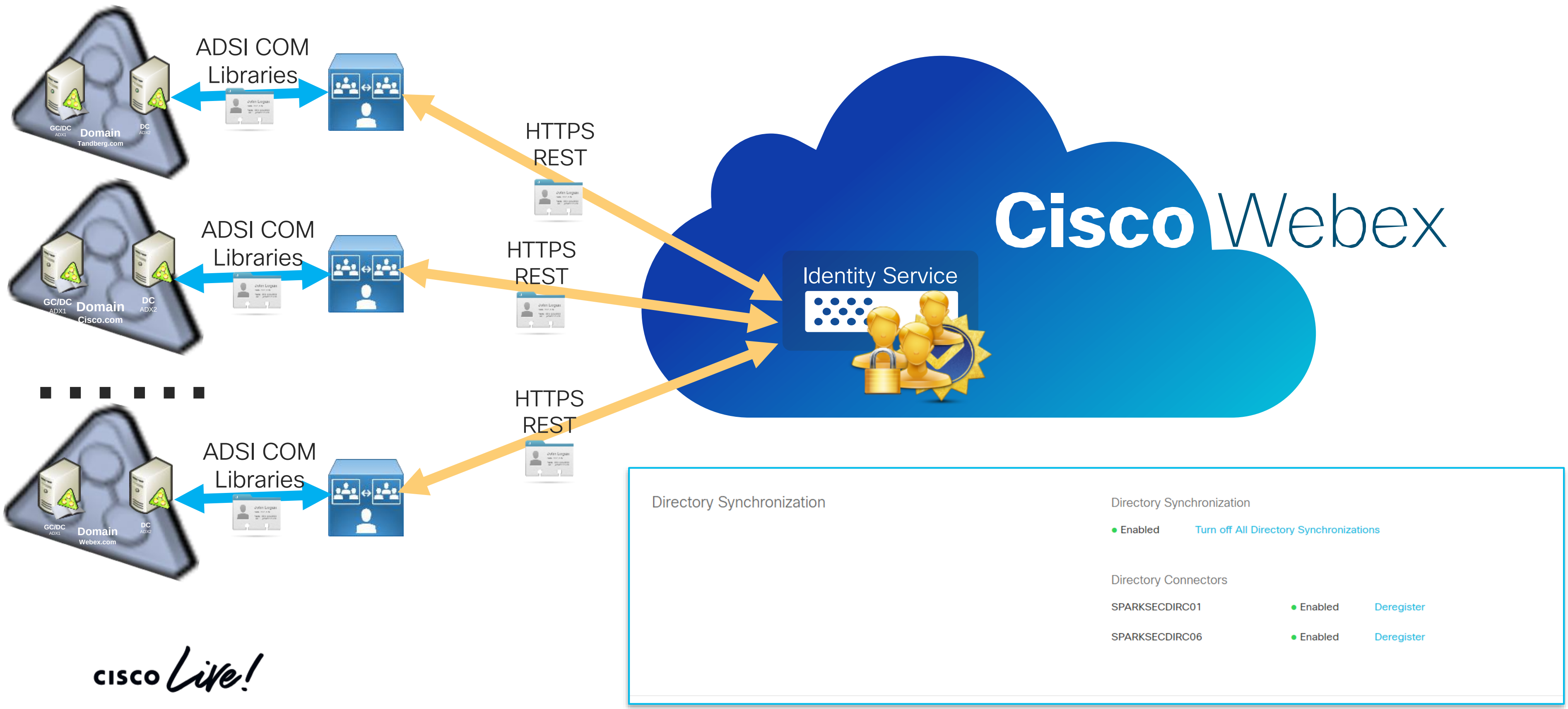


Directory Connector

- Full synchronization and incremental synchronization
- Scheduled synchronization
- Multiple Domains/Forests supported
- LDAP filters
- Dry Run
- User Attribute Mapping and modifications
- Using Service Account or User Account
- Avatar Sync
- Troubleshooting
- Auto-upgrade
- High Availability (HA)



Directory Connector



Directory Synchronization

Directory Synchronization

● Enabled Turn off All Directory Synchronizations

Directory Connectors

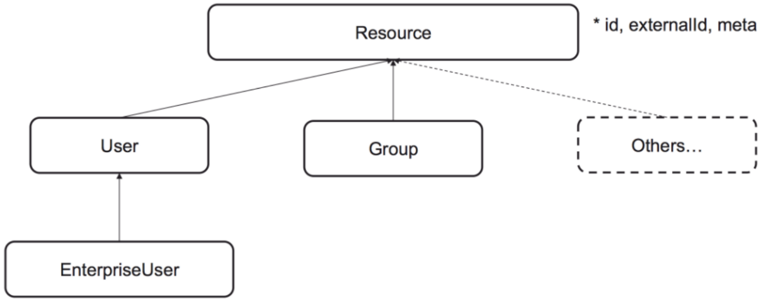
SPARKSECDIRC01	● Enabled	Deregister
SPARKSECDIRC06	● Enabled	Deregister

What is SCIM ?

The System for Cross-domain Identity Management (SCIM) specification is designed to make managing user identities in cloud-based applications and services easier.

Its intent is to reduce the cost and complexity of user management operations by providing a common user schema and extension model, as well as binding documents to provide patterns for exchanging this schema using standard protocols. In essence: make it fast, cheap, and easy to move users in to, out of, and around the cloud.

Normally we will see a Model like :

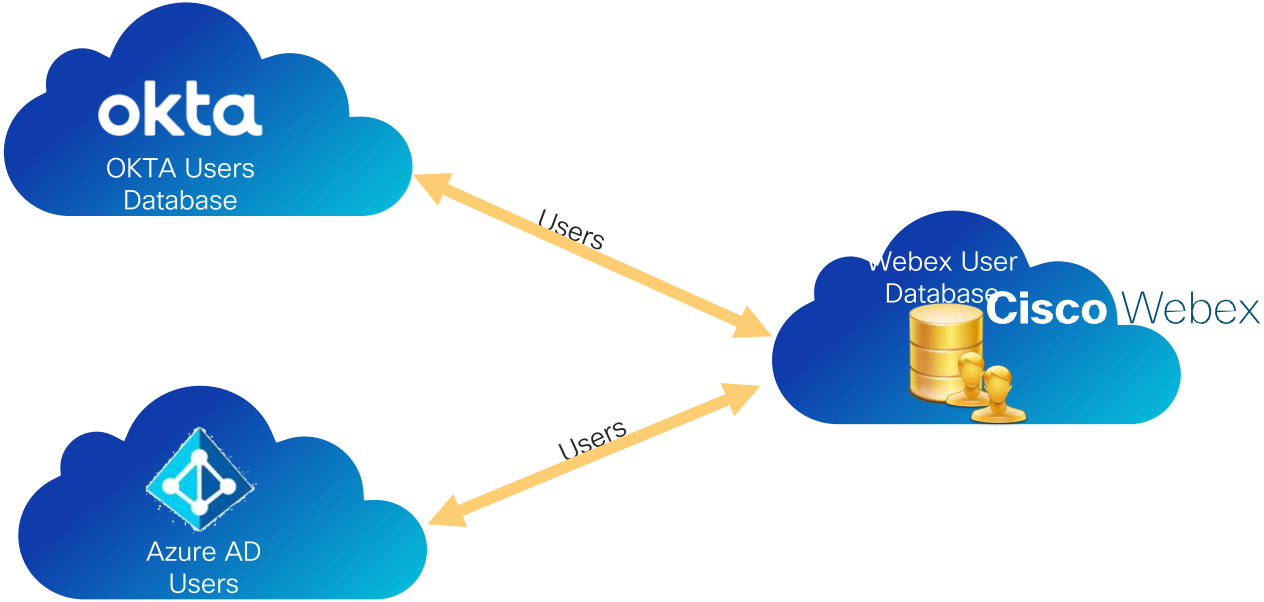


http://www.simplecloud.info/

Example of an user object pass by the IdM to Cisco Webex

```
{
  "schemas":["urn:scim:schemas:core:1.0"],
  “externalId”:”a54028dd-f9ab-4c02-9526-
a27bc158b04d”,
  "userName": “paucorre@cisco.com",
  "name":{
    "givenName":“Paulo Jorge",
    "familyName":“Correia"
  },
  "displayName": “Paulo Jorge Correia",
  "preferredLanguage":"en_US",
  "locale":"en_US",
  "timezone":"America/Denver",
  "phoneNumbers":[
   {
     "value": "+351253123456",
     "type": "work"
   },
   {
     "value": "+351911234567",
     "type": "mobile"
   }
  ],
  "addresses": [
    {
      "type": "work",
      "streetAddress": “Av. 31 Janeiro, 603",
      "locality": “Braga",
      "region": “Minho",
      "postalCode": “4710-452",
      "country": “PT"
    }
  ],
  “emails":[
   {
     “email": “paucorre@cisco.com”,
     "type": “work“
     “primary”: true
   },
   {
     “email": “paulo.jncc@gmail.com",
     "type": “home"
   }
  ],
  "title": “Technical Solutions Architect",
  "organization": “Cisco Systems",
  "department": “EMEAR",
  "photos": [{
    "type": "photo",
    "value": "http://test.com/test.jpg"
  },
  {
    "type": "thumbnail",
    "value": "http://test.com/test.jpg"
  }],
  "ims": [{
    "type": "xmpp",
    "value": “paucorre@xmpp.com",
    "primary": true
  },
  {
    "type": "gtalk",
    "value": “paucorre@gtalk.com"
  }],
  “active": True,
  "sipAddresses": [
    {
      "type": "cloud-calling",
      "value": "sips:paucorre@cisco.com"
    },
    {
      "type": "personal-room",
      "primary": true,
      "value": "sip:paucorre@acecloud.webex.com"
    }
  ],
}
```

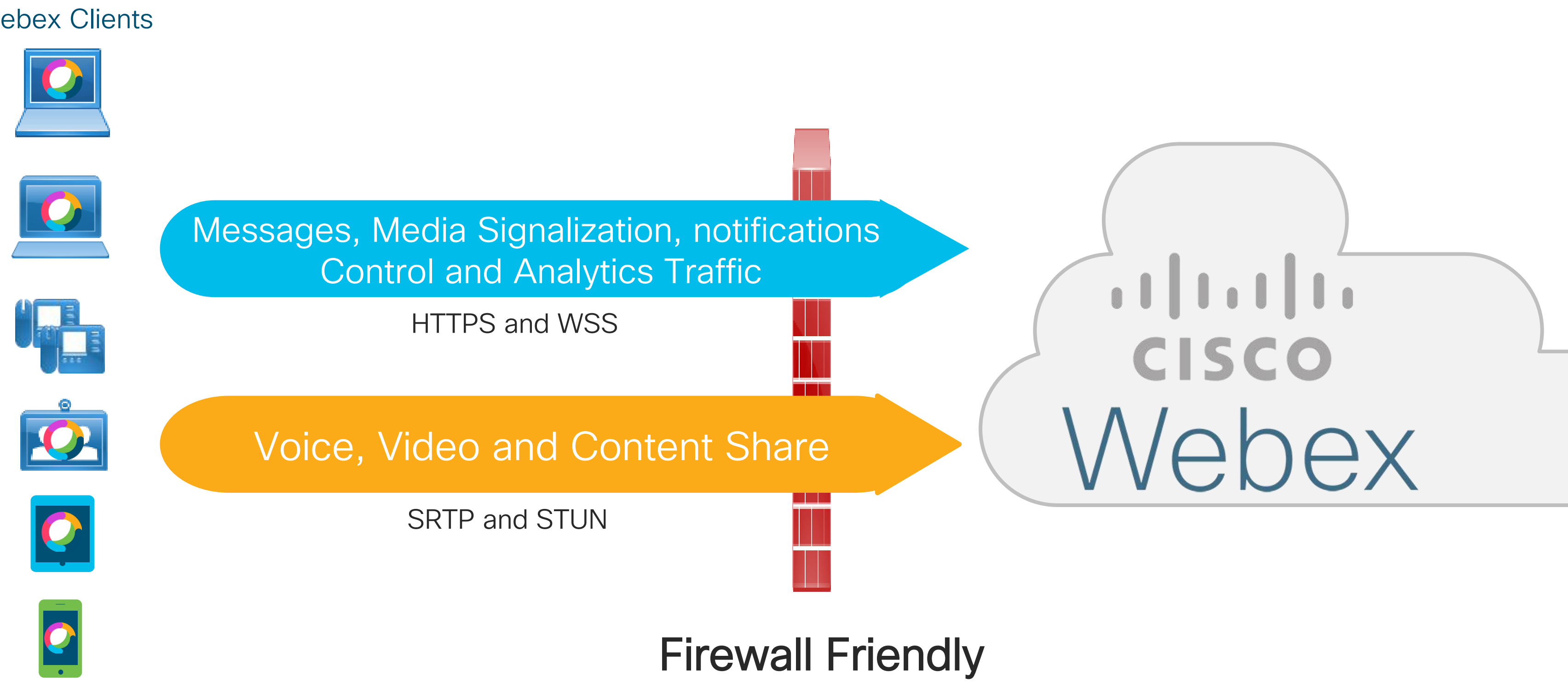
SCIM integrations



Webex Service connection to the Cloud

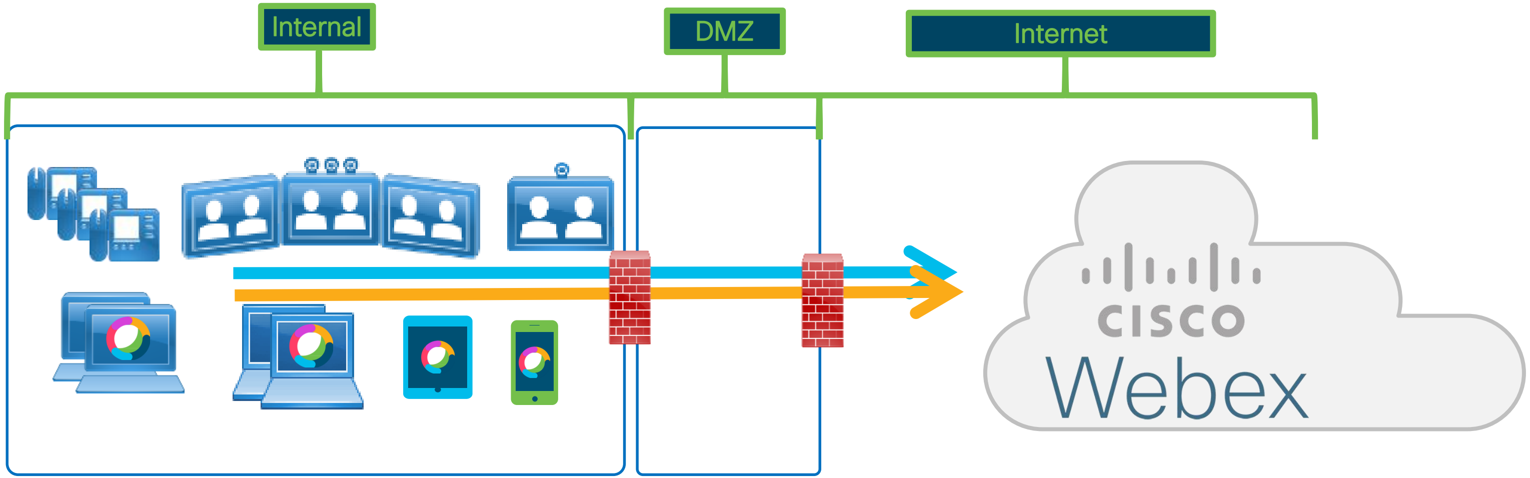
Media types for Cisco Webex Teams Service

Type of traffic


Webex Clients
Messages, Media Signalization, notifications
Control and Analytics Traffic
HTTPS and WSS
Voice, Video and Content Share
SRTP and STUN
Firewall Friendly
cisco
Webex

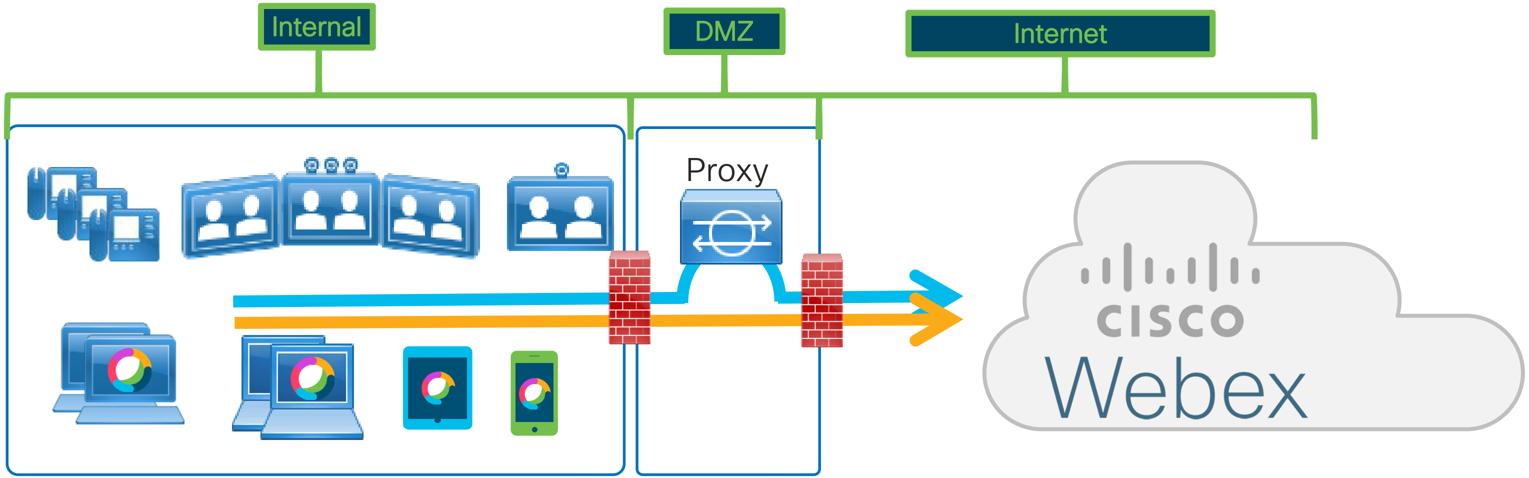
Traffic Flow

Scenario 1- Security relax customer, policies only enforce in the FW



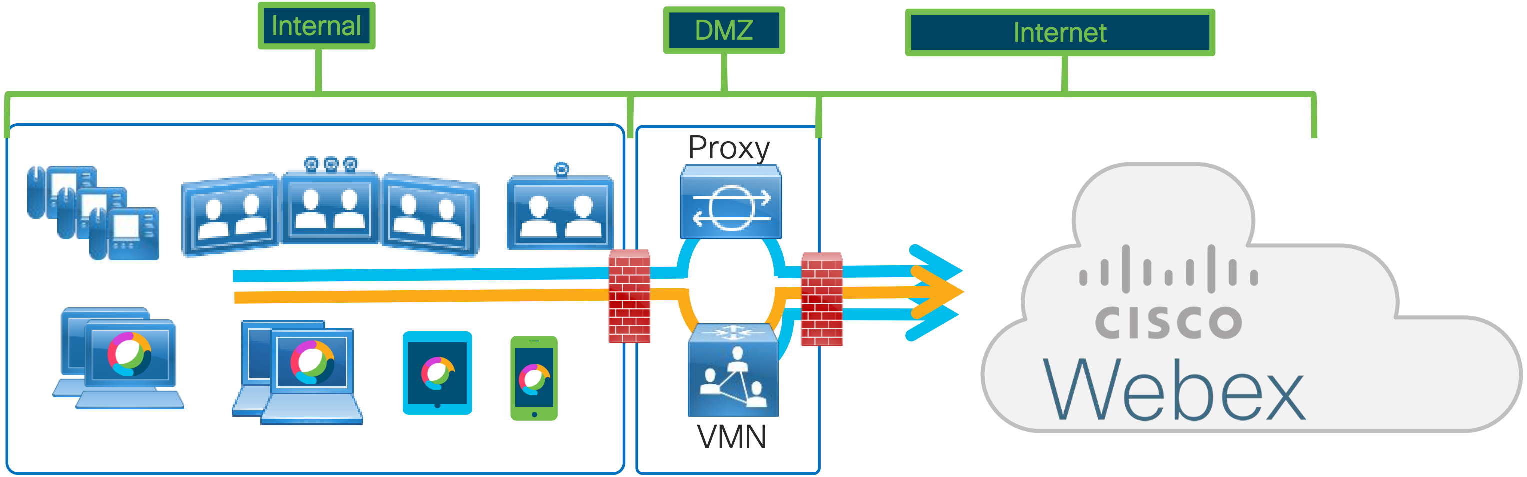
Traffic Flow

Scenario 2- Security aware customer, policies enforce in the FW and Proxy



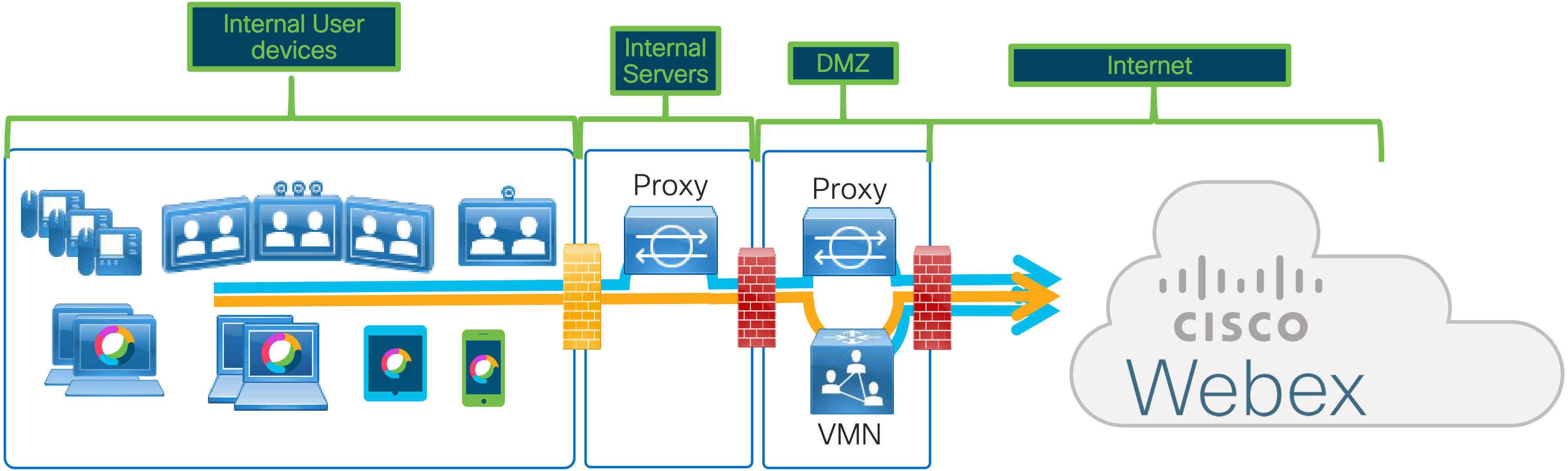
Traffic Flow

Scenario 3 - Security focus customer, policies enforce in the FW and Proxy and no direct connection to internet



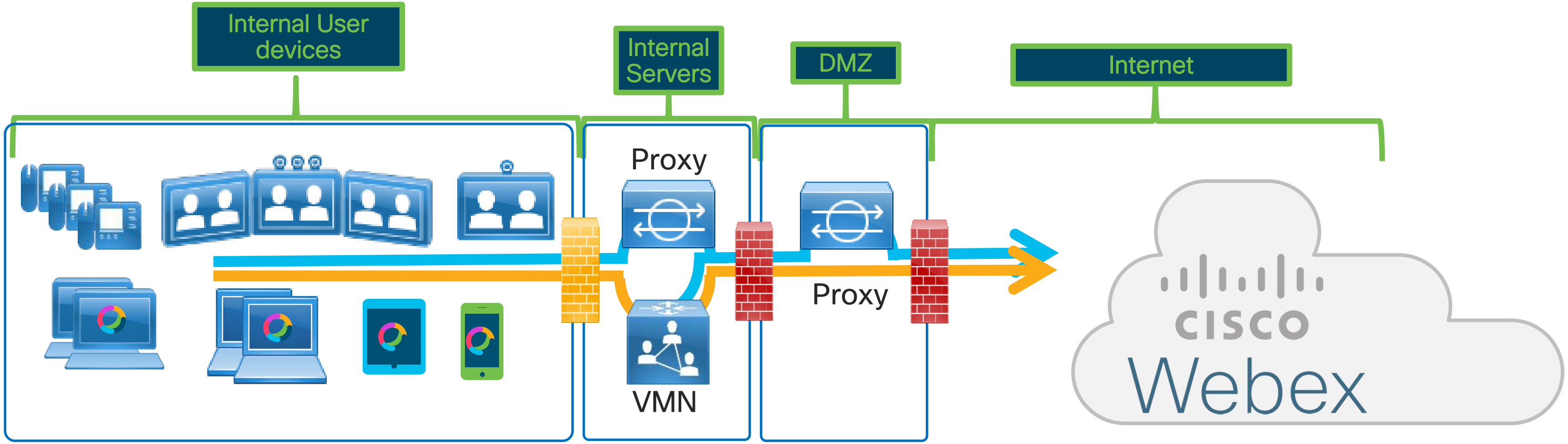
Traffic Flow

Scenario 4.1 – Extreme Security Customer, policies enforce in the FW and Proxy and no direct connection to internet but communication to DMZ are screened



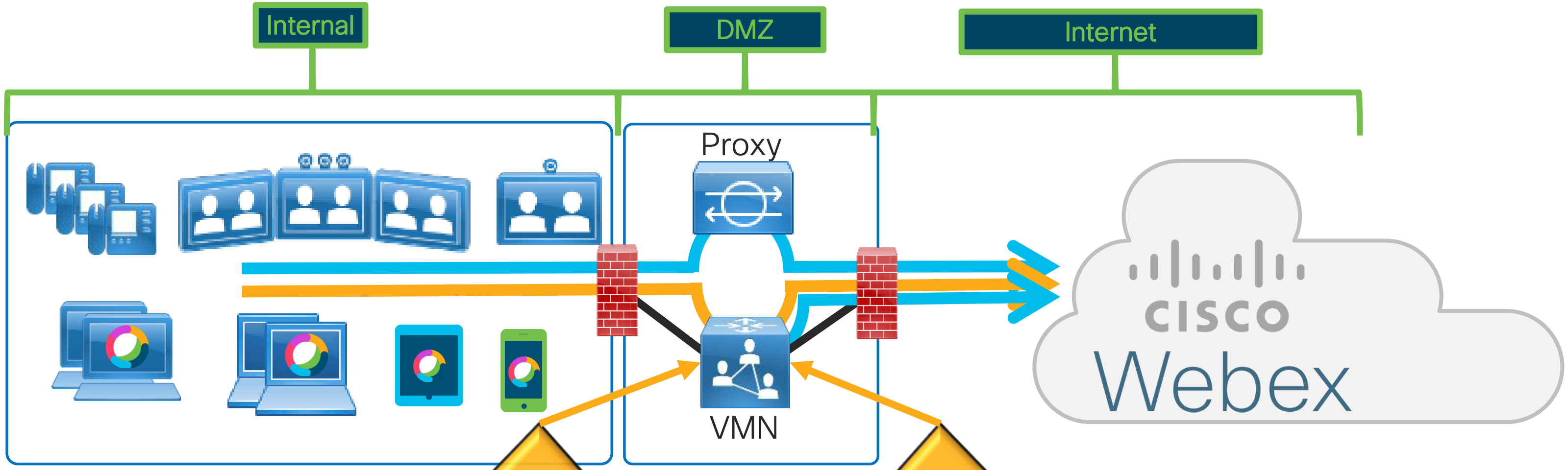
Traffic Flow

Scenario 4.2 – Extreme Security Customer, policies enforce in the FW and Proxy and no direct connection to internet but communication to DMZ are screened



Traffic Flow

Scenario 5 – Similar to Scenario 3 but leveraging Dual NIC VMN



Internal Interface:

Management Web Interface
Management CLI Interface
VMN Cluster Cascading
VMN Registration in Control Hub will use this IP

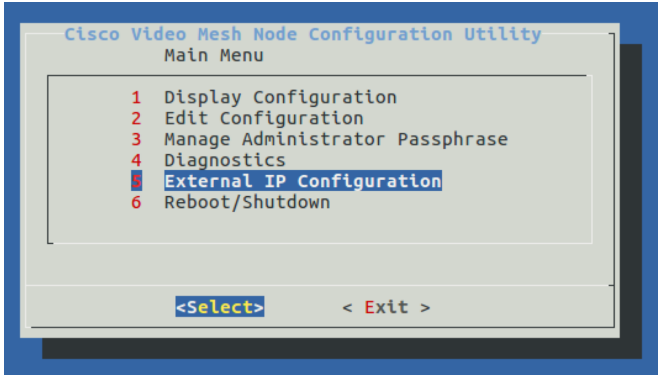
External Interface:

Connectivity to Cisco Collaboration Cloud
Cascading to Cloud Video Mesh Nodes

Video Mesh Node Dual NIC

Configuration

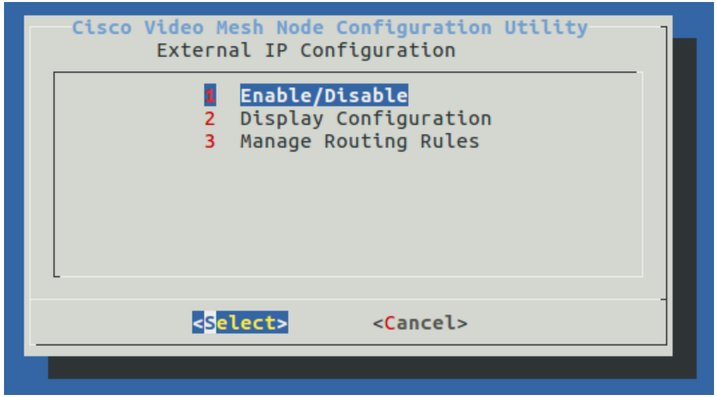
- External IP configuration needs to be enabled explicitly when required.
- External IP can be enabled before or after registration.
- Maintenance Mode is required if registered to production environment.
- Menu Options
  - **Enable/Disable** – Configure external IP or switch back to Single interface mode
  - **Display Configuration** – Display the external IP configuration
  - **Manage Routing Rules** – View, Add and Delete the routing rules.



```
Cisco Video Mesh Node Configuration Utility
                 Main Menu

         1  Display Configuration
         2  Edit Configuration
         3  Manage Administrator Passphrase
         4  Diagnostics
         5  External IP Configuration
         6  Reboot/Shutdown

          <Select>          < Exit >
```



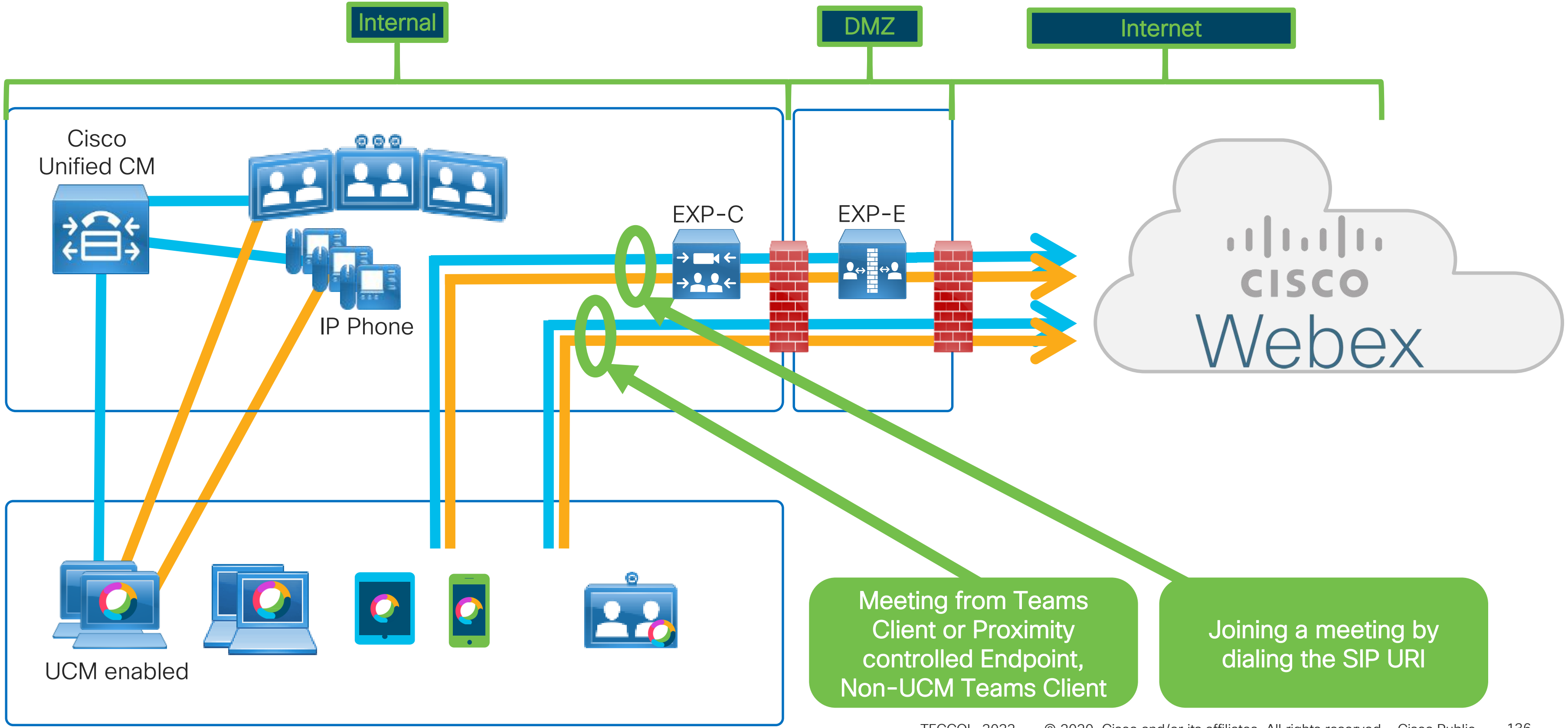
```
Cisco Video Mesh Node Configuration Utility
          External IP Configuration

         1  Enable/Disable
         2  Display Configuration
         3  Manage Routing Rules

          <Select>          <Cancel>
```

Traffic Flow

Webex Teams UCM Calling – Signaling and Media

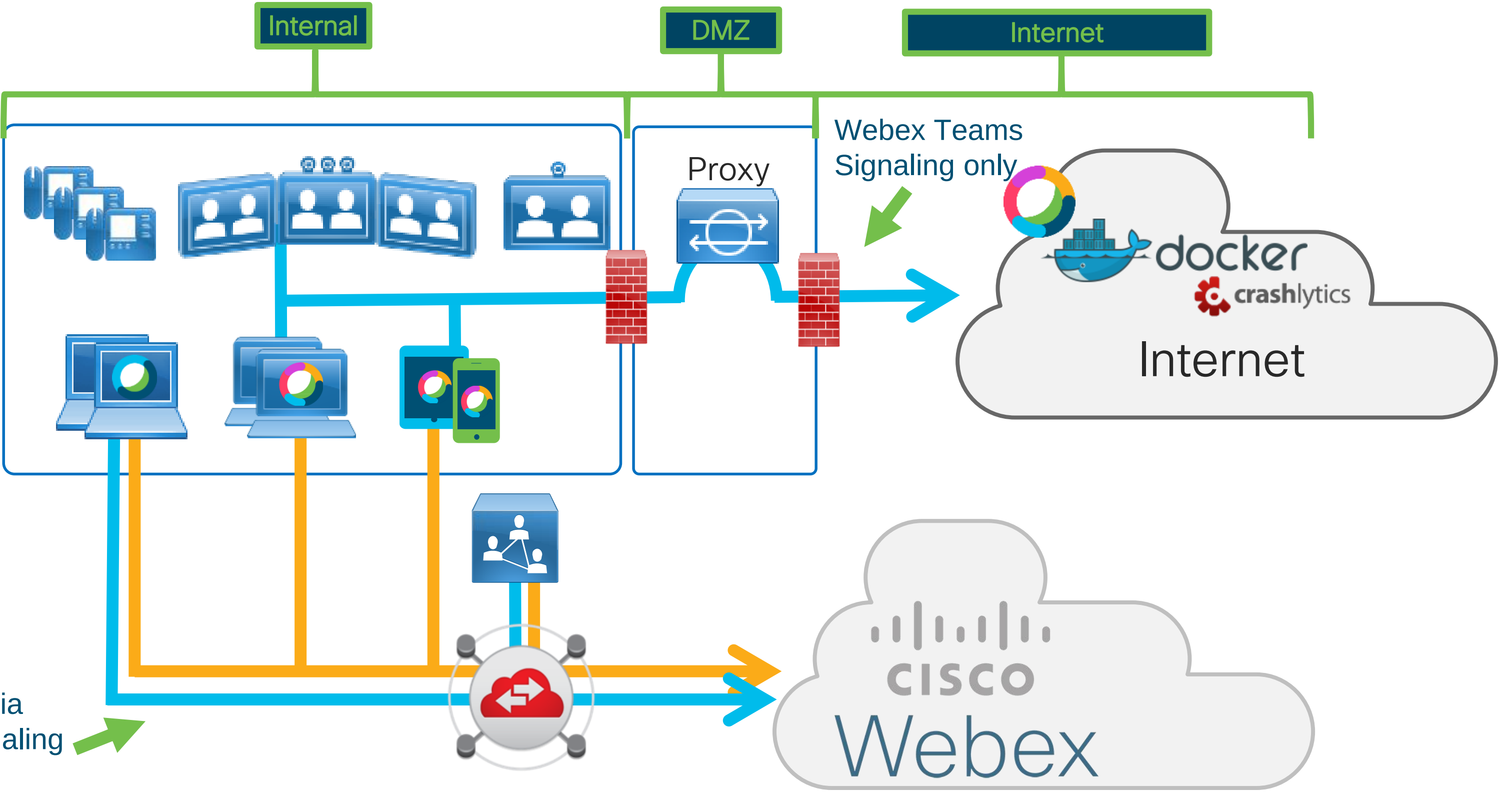


Meeting from Teams Client or Proximity controlled Endpoint, Non-UCM Teams Client

Joining a meeting by dialing the SIP URI

Traffic Flow

Webex Edge Connect

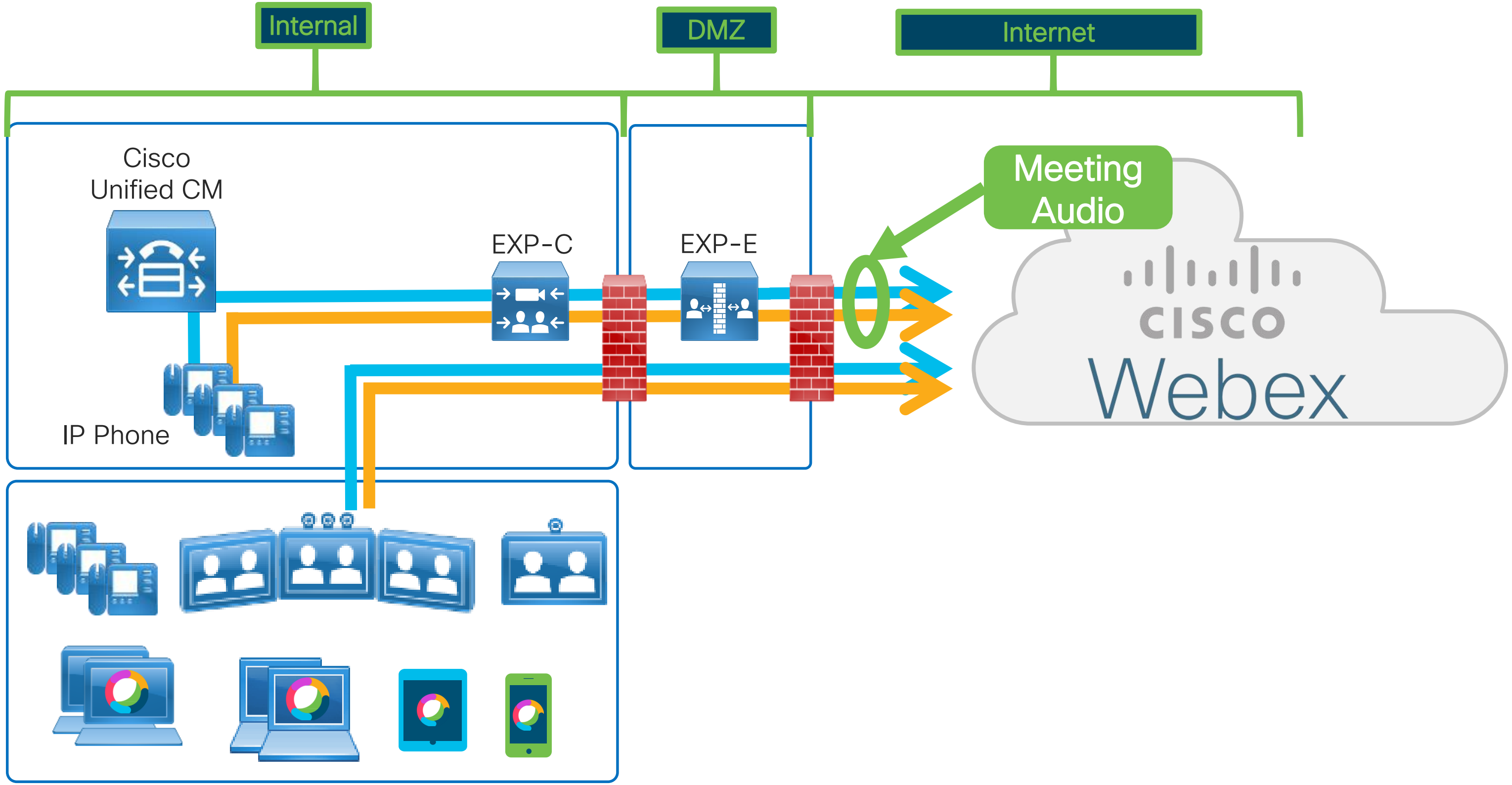


Webex Teams
Signaling only

Webex Teams Media
Webex Meetings Media
Webex Meetings Signaling

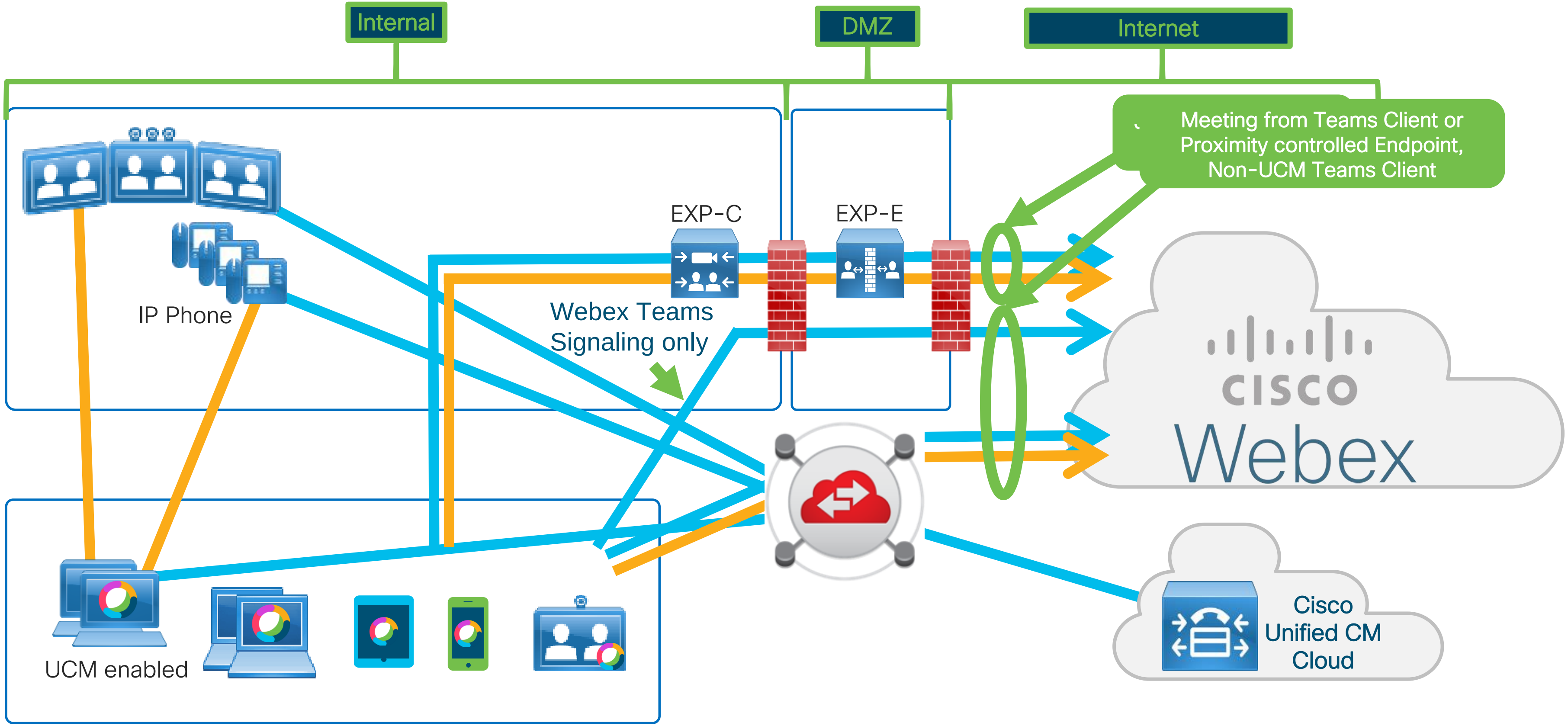
Traffic Flow

Webex Edge Audio



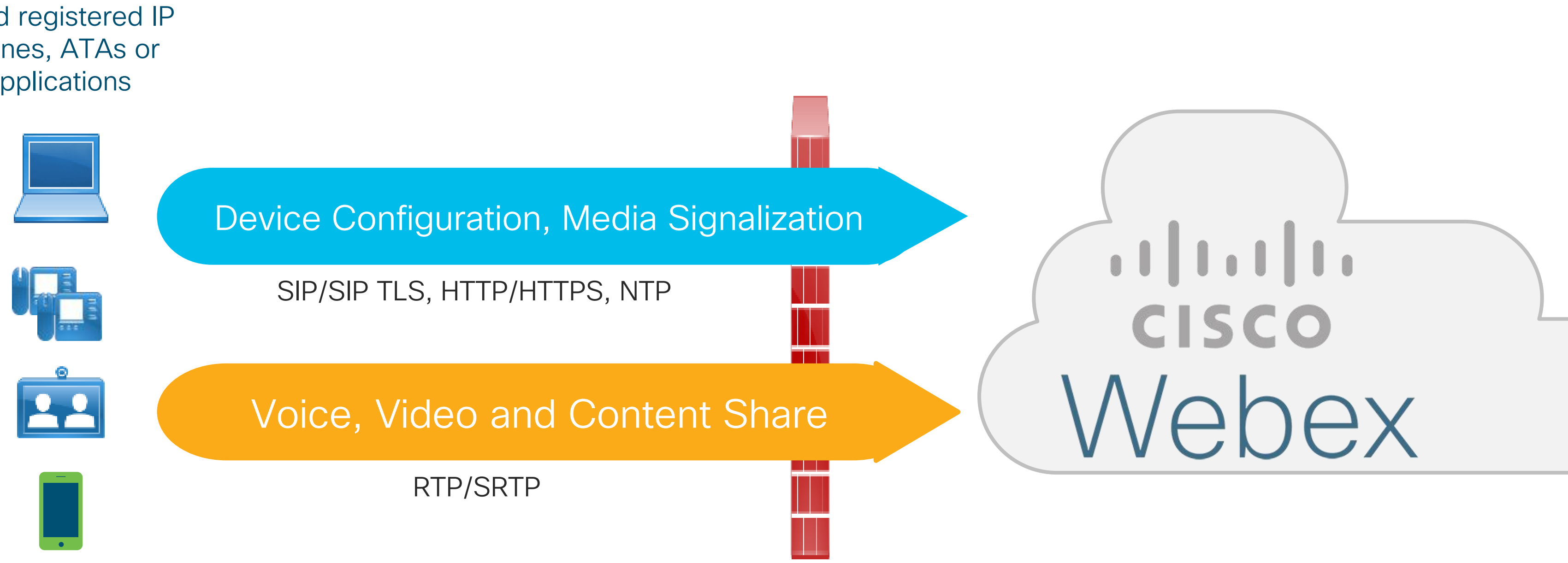
Traffic Flow

Webex Teams UCM Cloud Calling – Signaling and Media


Internal
DMZ
Internet
Meeting from Teams Client or Proximity controlled Endpoint, Non-UCM Teams Client
EXP-C
EXP-E
IP Phone
Webex Teams Signaling only
cisco
Webex
Cisco Unified CM Cloud
UCM enabled

Media types for Cisco Webex Calling Service

Type of traffic

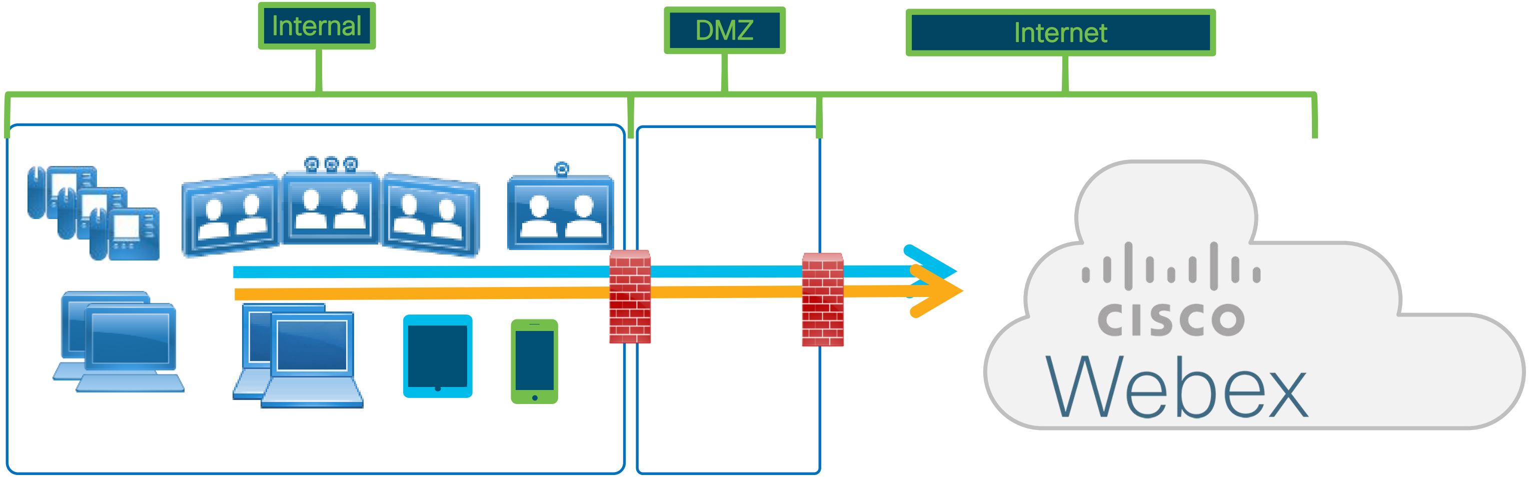


Cloud registered IP Phones, ATAs or Applications
Device Configuration, Media Signalization
SIP/SIP TLS, HTTP/HTTPS, NTP
Voice, Video and Content Share
RTP/SRTP
cisco
Webex

Firewall Friendly

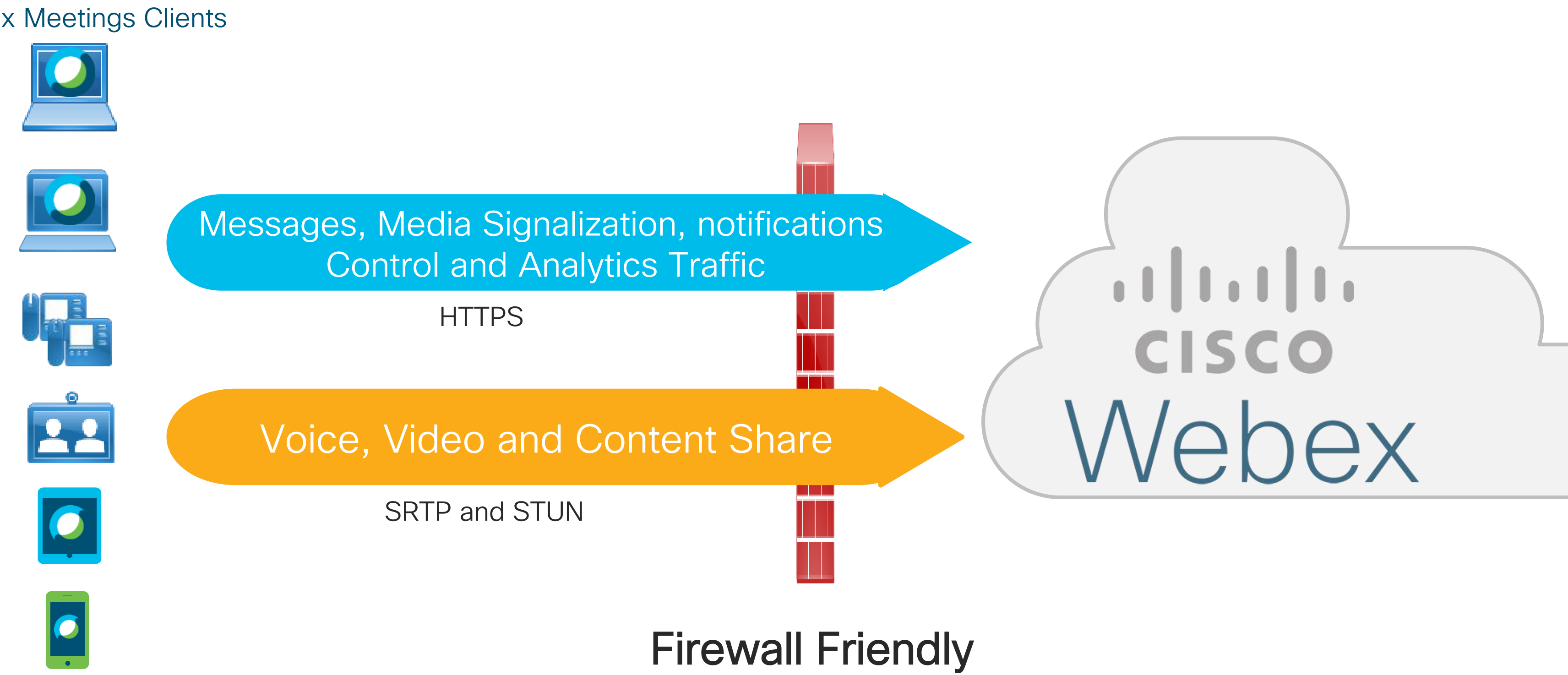
Traffic Flow

Webex Teams Calling – Signaling and Media



Media types for Cisco Webex Meeting Service

Type of Traffic

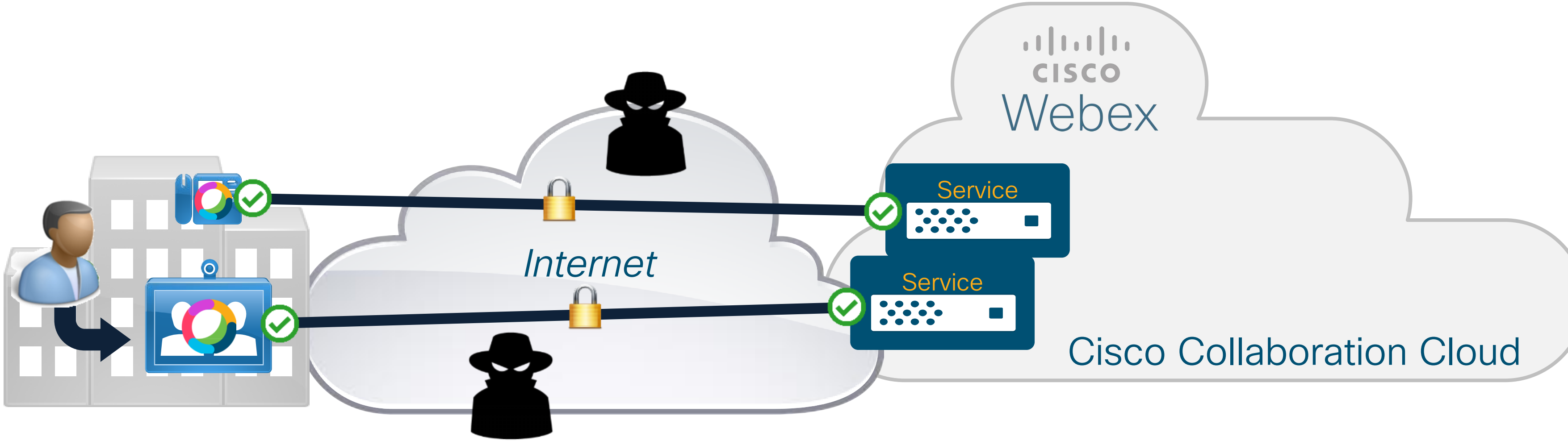

Webex Meetings Clients
Messages, Media Signalization, notifications Control and Analytics Traffic
HTTPS
Voice, Video and Content Share
SRTP and STUN
cisco
Webex

Firewall Friendly

Onboarding

Cloud Onboarding for Hardware Endpoints

Objectives



- Easy activation/onboarding experience:

  Device input interface constraints

- Secure

  Protection from eavesdropping, man-in-the-middle, brute force attacks

Cloud Onboarding for Hardware Endpoints

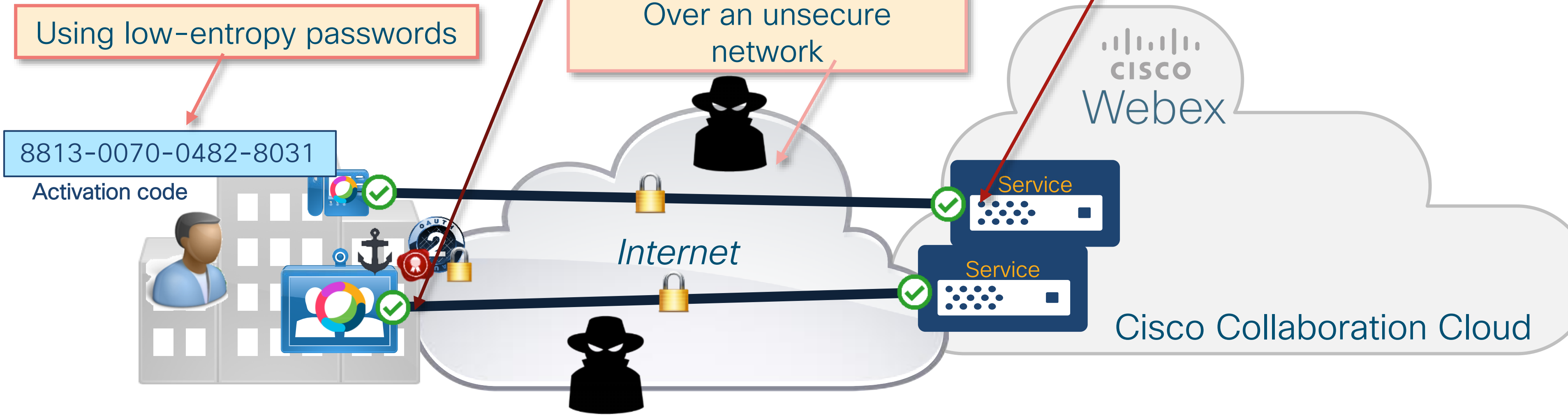
Algorithm Requirements

Securely download OAuth tokens and trust anchors

Mutually authenticate client and cloud infrastructure

Using low-entropy passwords

Over an unsecure network



➔ Diffie-Hellman Password-Authenticated Key Exchange

Cloud Onboarding for Hardware Endpoints

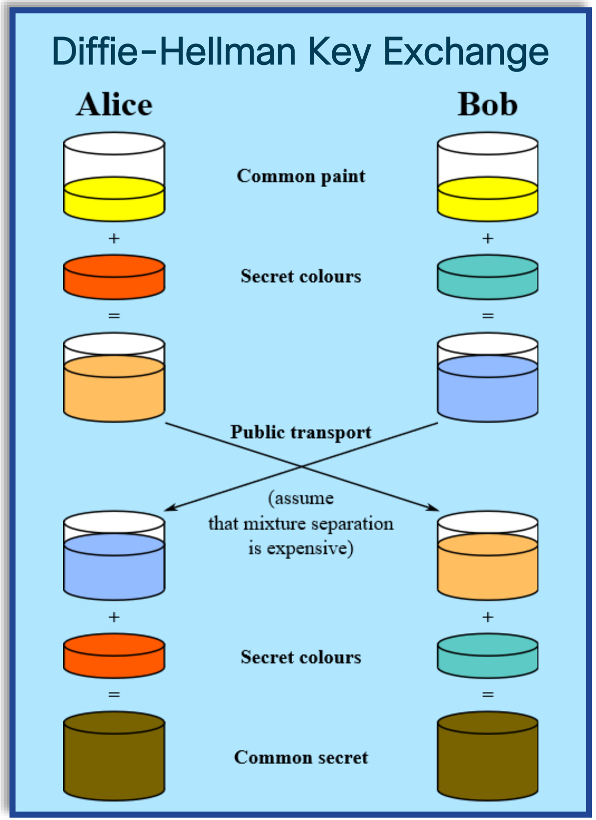
Diffie-Hellman Password-Authenticated Key Exchange

Diffie-Hellman (DH) key exchange:

- Securely exchange cryptographic keys over unsecure transport
- Based on computational complexity of mathematic functions (discrete logarithm, elliptic curve)
- Unauthenticated—susceptible to man-in-the-middle attacks

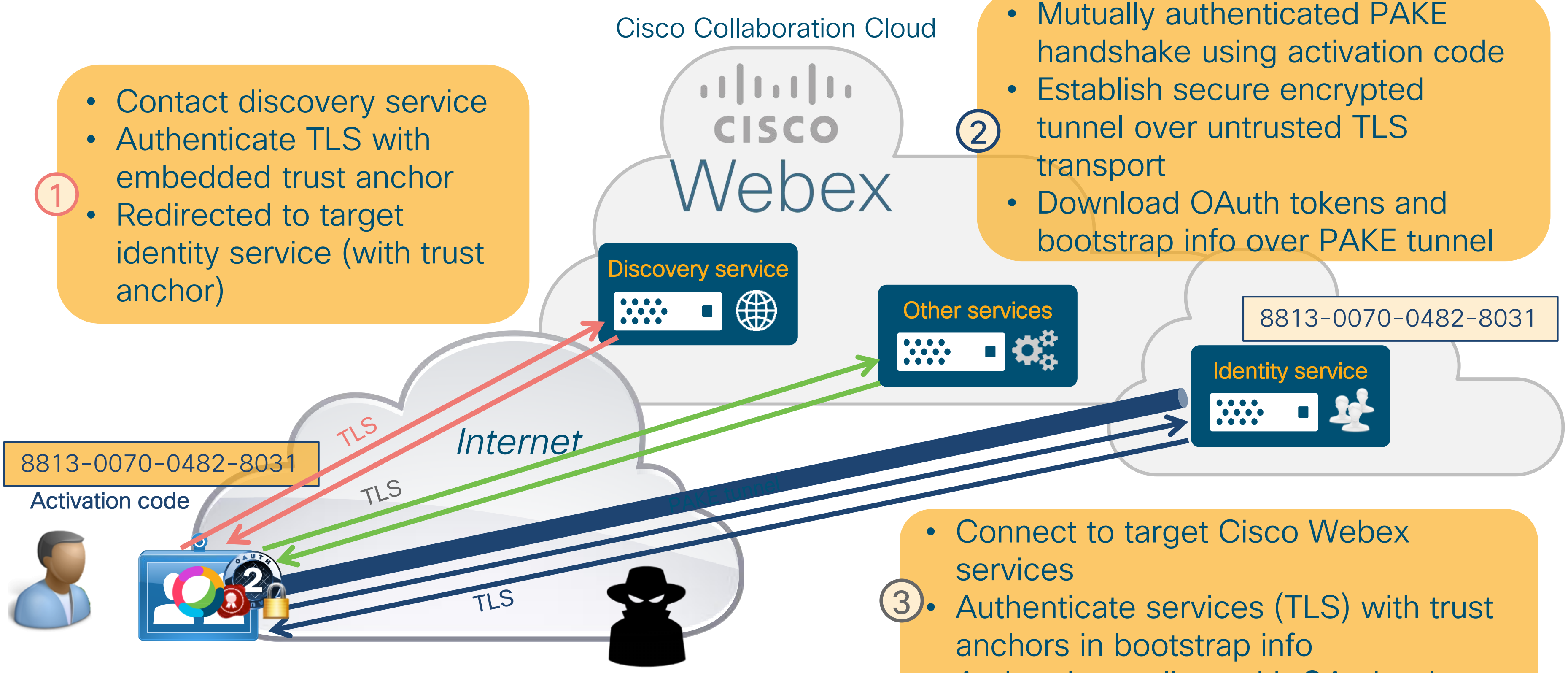
Password-Authenticated key exchange (PAKE):

- Variant of DH that leverages shared knowledge of a password to derive the cryptographic keys
- Authenticated—prevents man-in-the-middle attacks
- Achieves strong security with weak passwords (e.g., 16-digit activation code)



Cloud Onboarding for Hardware Endpoints

Simplified Flow



1

- Contact discovery service
- Authenticate TLS with embedded trust anchor
- Redirected to target identity service (with trust anchor)

2

- Mutually authenticated PAKE handshake using activation code
- Establish secure encrypted tunnel over untrusted TLS transport
- Download OAuth tokens and bootstrap info over PAKE tunnel

3

- Connect to target Cisco Webex services
- Authenticate services (TLS) with trust anchors in bootstrap info
- Authenticate client with OAuth token

Cloud Onboarding of Hardware Endpoints

Strength of Security

- Brute Force Attack on Activation Code bootstrap:
  - Comfortably **within FIPS** recommendations *(FIPS 140-2, FIPS 140-3 2007 Draft)*
    - Less than one in 100,000,000 that a random attempt will succeed
    - For multiple attempts, less than one in 10,000,000 that a random attempt will succeed
  - This is due to combination of length (10^{16} combinations), short expiration time, and projected simultaneous bootstrapping devices

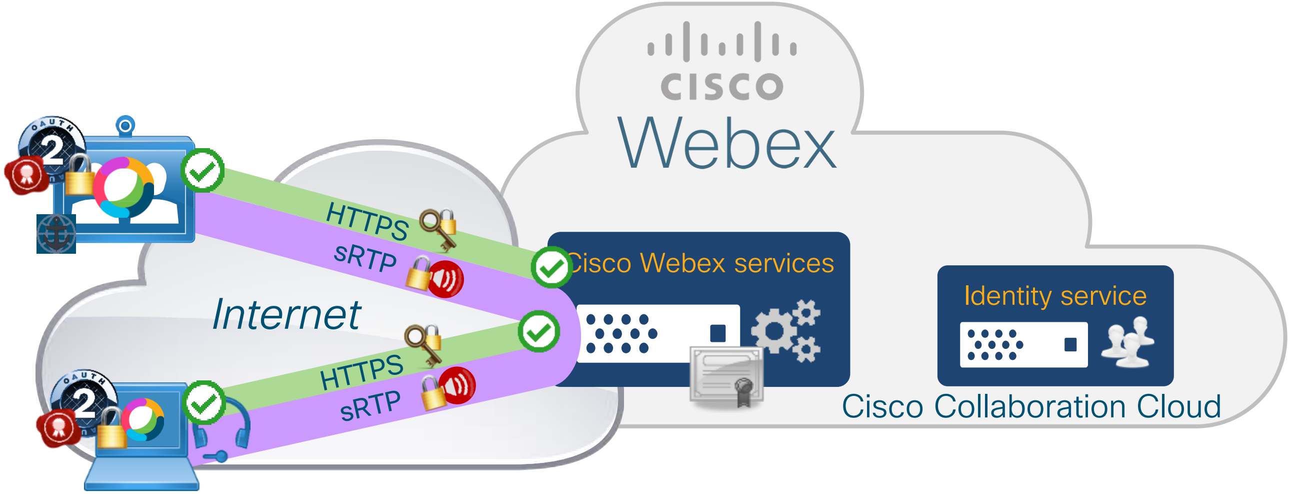
- Man in the Middle Attack on 3072-bit Diffie-Hellman PAKE handshake:
  - Extensive TLS Logjam attack (2015) literature available on strength of Discrete Log Diffie-Hellman:

    "It is plausibly within NSA's resources to have performed number field sieve precomputations for at least a small number of 1024-bit Diffie-Hellman groups"

    *"Precomputation for a 2048-bit group is around 109 times harder than for a 1024-bit group, so **2048-bit Diffie-Hellman will remain secure** barring a major algorithmic improvement"*

    https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf

Security Considerations

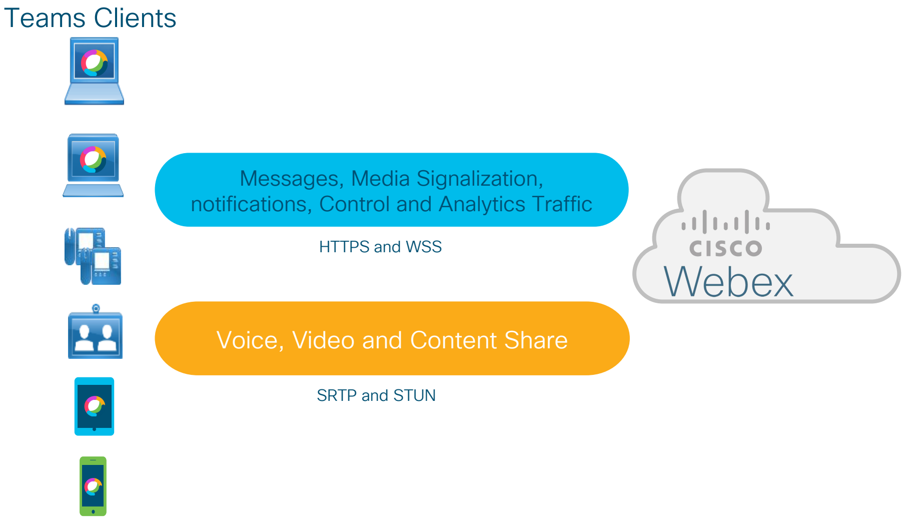


- Cisco Webex endpoints and clients validate certificate chain of cloud services
- Cisco Webex cloud services authenticate client connections with OAuth tokens
  - No need for MIC in hardware endpoints (thanks to onboarding process)
- Media encrypted – encryption keys exchanged in SDP over HTTPS (SDES)

Proxy support

Proxy support – what does it mean?

- When we talk about proxy support we only talking HTTPS and WSS traffic.
- **Media over proxies it isn't recommended**, proxy **were not design** to handle media, their performance is really bad and doesn't scale.


Teams Clients
Messages, Media Signalization, notifications, Control and Analytics Traffic
HTTPS and WSS
Voice, Video and Content Share
SRTP and STUN
cisco
Webex

Cisco Webex Clients – Proxy configuration

Config Type	Webex Meetings Mobile	Webex Meeting Desktop	Webex Room Devices	Webex Board	Webex Teams Windows	Webex Teams Mac	Webex Teams iOS	Webex Teams Android
Manual Config	✓	✓	✓	✓	✓	✓	✓	✓
GPO	✓	WIN	✗	✗	✓	✗	✗	✗
PAC	✓	✓	✓	✓	✓	✓	✓	✓
WPAD	iOS	✓	✓	✓	✓	✓	✓	✗

Cisco Webex Clients – Proxy Authentication

Config Type	Webex Meetings Mobile	Webex Meeting Desktop	Webex Room Devices	Webex Board	Webex Teams Windows	Webex Teams Mac	Webex Teams iOS	Webex Teams Android
No Auth	✓	✓	✓	✓	✓	✓	✓	✓
Basic	✓	✓	✓	✓	✓	✓	✓	✓
Digest	✓	✓	✓	✓	✗	✗	✓	✓
NTLM	✓	✓	✗	✗	✓	✓	✓	✓
Negotiate	✗	WIN	✗	✗	✓	✗	✗	✗

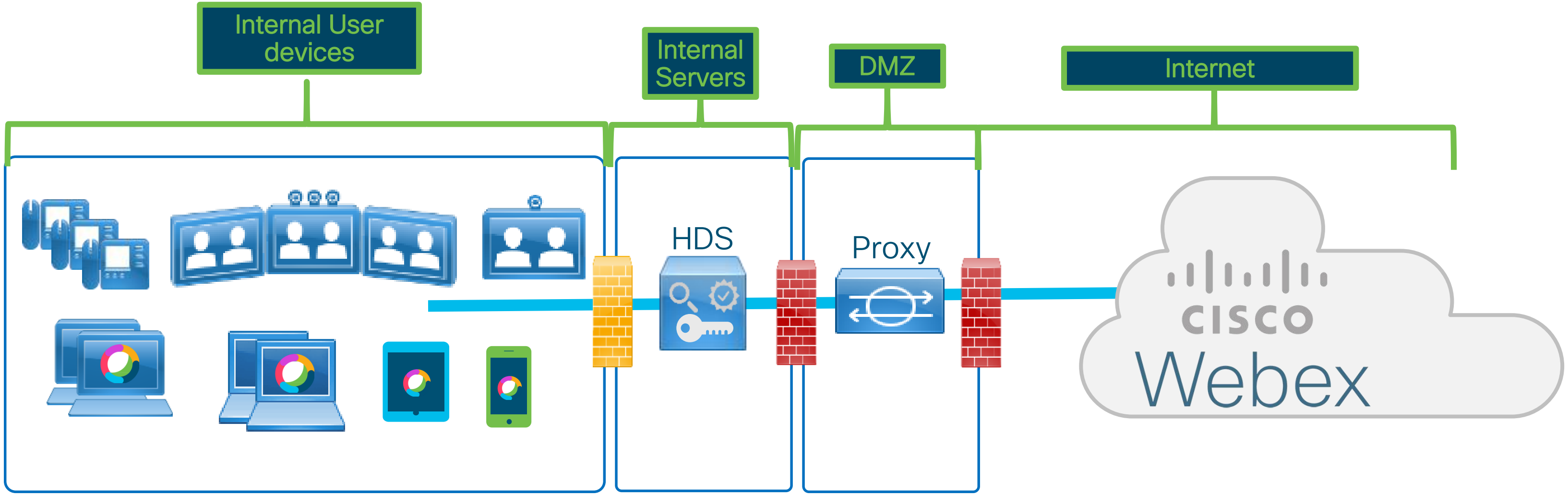
Cisco Webex Clients – Other Security Features

Config Type	Webex Meetings Mobile	Webex Meeting Desktop	Webex Room Devices	Webex Board	Webex Teams Windows	Webex Teams Mac	Webex Teams iOS	Webex Teams Android
802.1x	✓	✓	✓	✓	✓	✓	✓	✓
TLS Intercept	✗	✗	✗	✗	✓	✓	✓	✓
CDP	✗	✗	✓	✓	✗	✗	✗	✗
Media over HTTPS	✓	✓	✗	✗	✓	✓	✓	✓

Cisco Webex Calling – Proxy Support

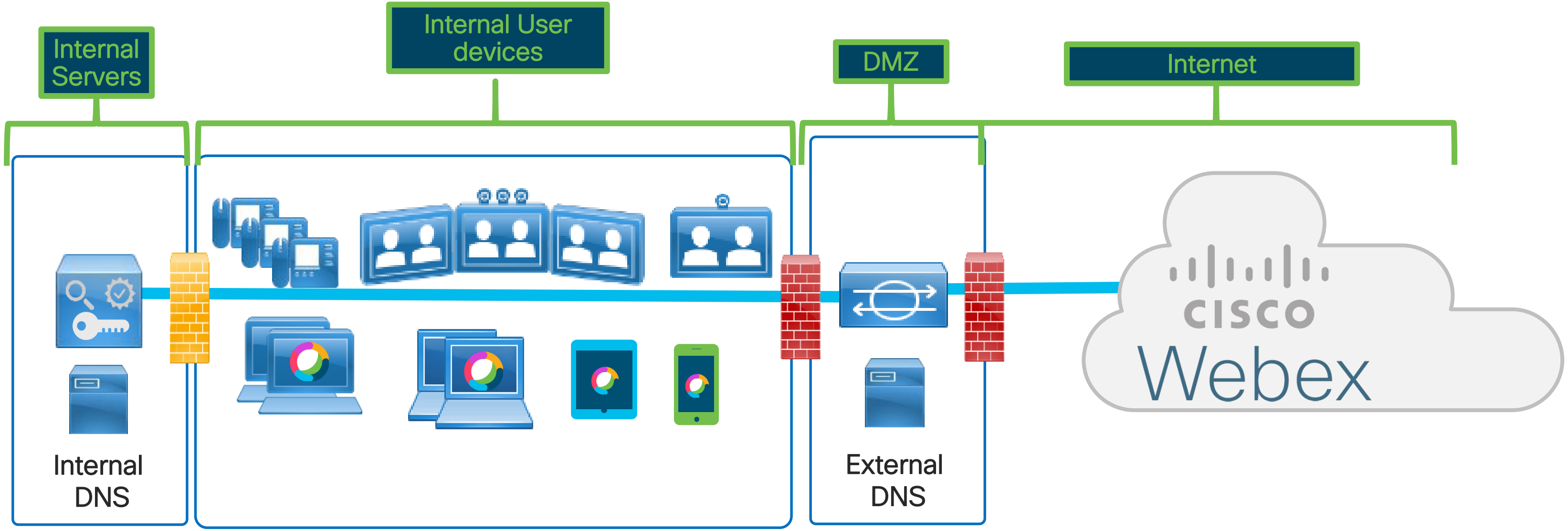
At this point it is recommended to allow all Webex Calling traffic to bypass a proxy.

Hybrid Data Security – Proxy Support



Authentication supported: Basic, Digest, NTLM

Hybrid Data Security - Internal Only DNS



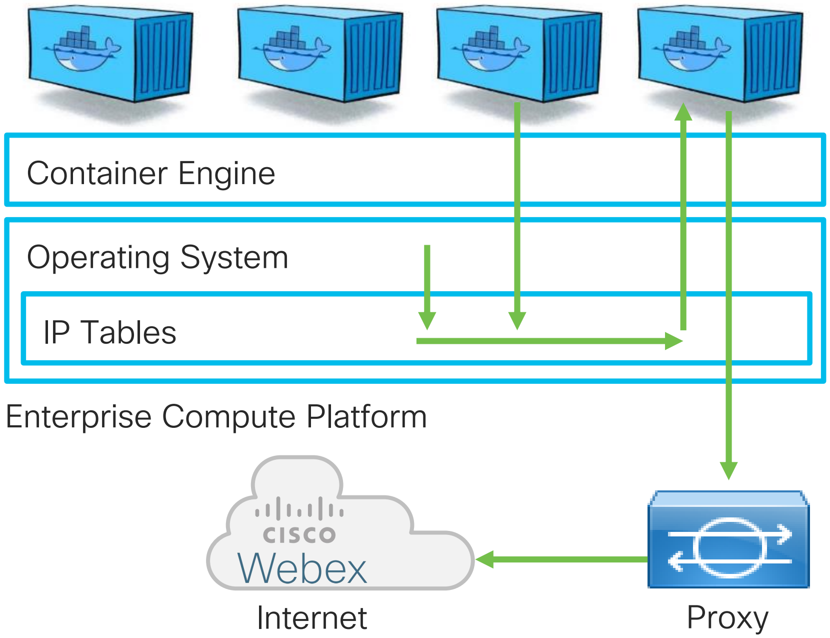
Internal DNS servers do not resolve external DNS names

External HTTP traffic is send to proxy, which queries an external DNS server to resolve URIs.

Hybrid Data Security - Internal Only DNS

BREAKING NEWS

Architecture of Hybrid Services (Video Mesh & HDS)



Proxy Container

Proxy support for Hybrid Services is implemented by utilizing IP Tables to intercept all HTTP requests (80 and 443).

All HTTP traffic is redirected via Proxy Container which is configured by administrator to direct traffic to the enterprise proxy

Hybrid Data Security - Internal Only DNS

Architecture of Hybrid Services with internal only DNS

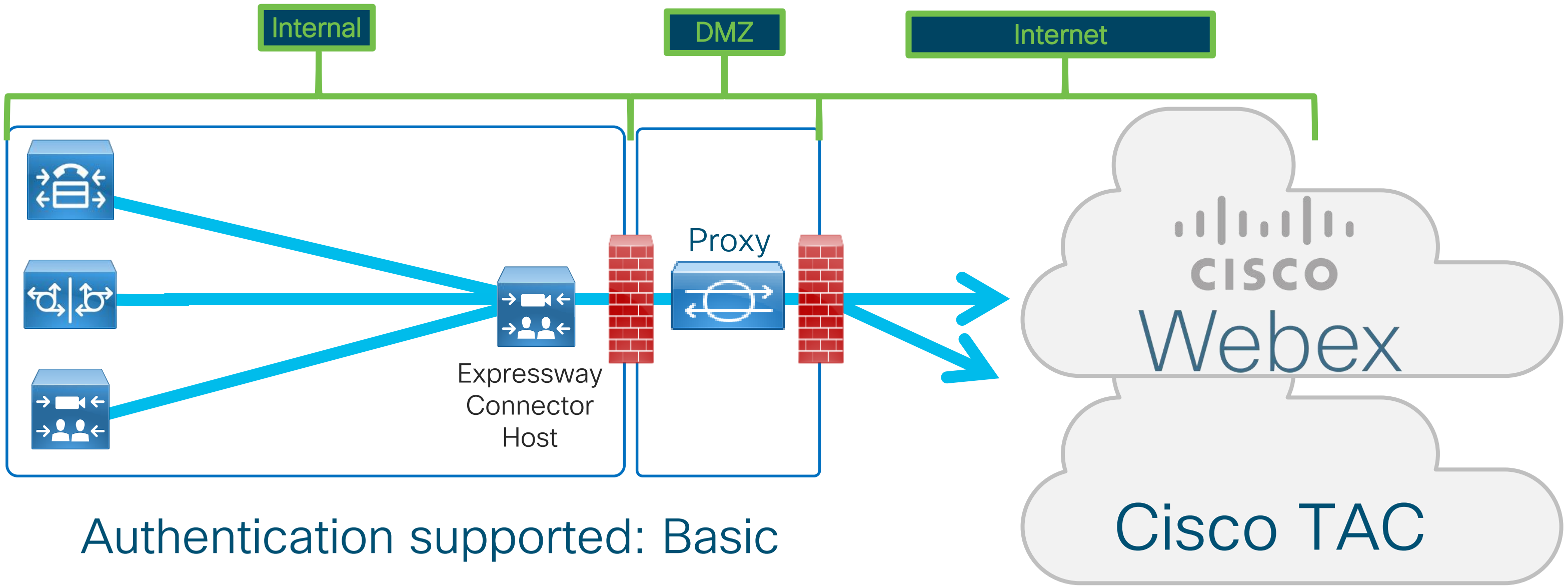
- Application/Container components are not aware traffic is being routed via proxy
- Certain action will fail as DNS resolution is not available

  Example: preregistration test of hybrid components tries DNS lookup and checks http connectivity. Fails in internal only DNS environment.

- New feature implemented into Hybrid Services platform allows HDS to be deployed in internal only DNS Proxy environments
- Currently only supported for Hybrid Data Security (HDS), support for Video Mesh being evaluated

  Ping tneumann@cisco.com on Cisco Webex Teams or Email in case you require support for Video Mesh

Cisco Webex Serviceability Connector Proxy Support



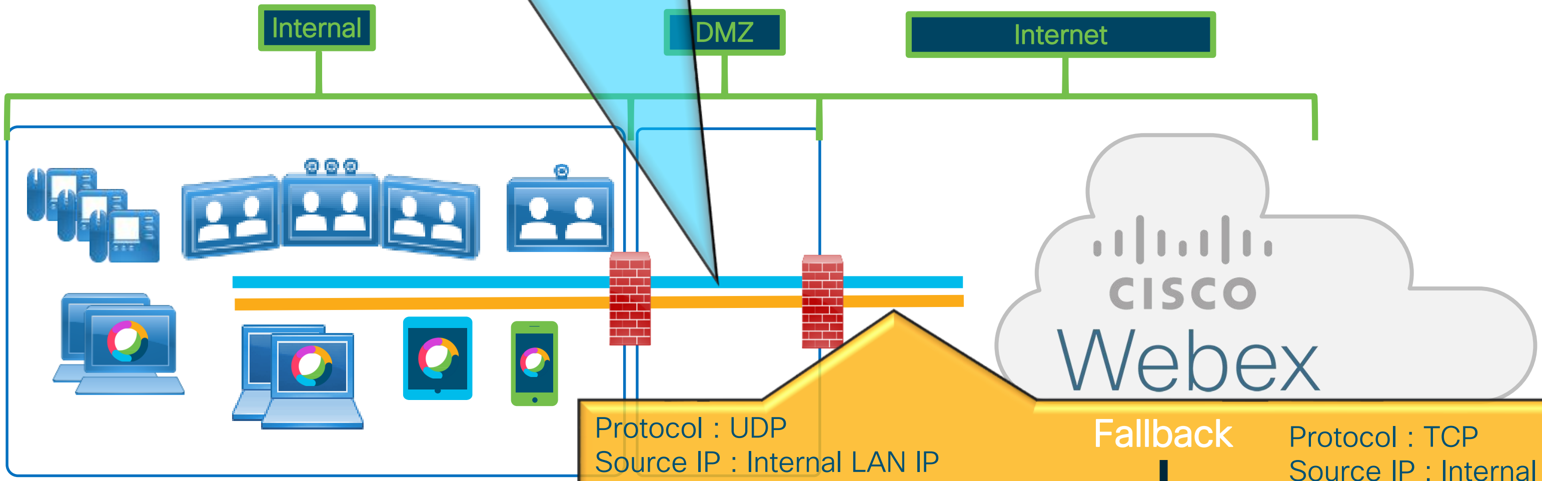
Authentication supported: Basic

Firewall support

Protocols and Ports used by Webex Teams

Assuming the simplest scenario with direct connection to the internet :

Protocol : TCP
Source IP : Internal LAN IP address Range
Source Port : Ephemeral
Destination IP : Any IP
Destination Port : **443**



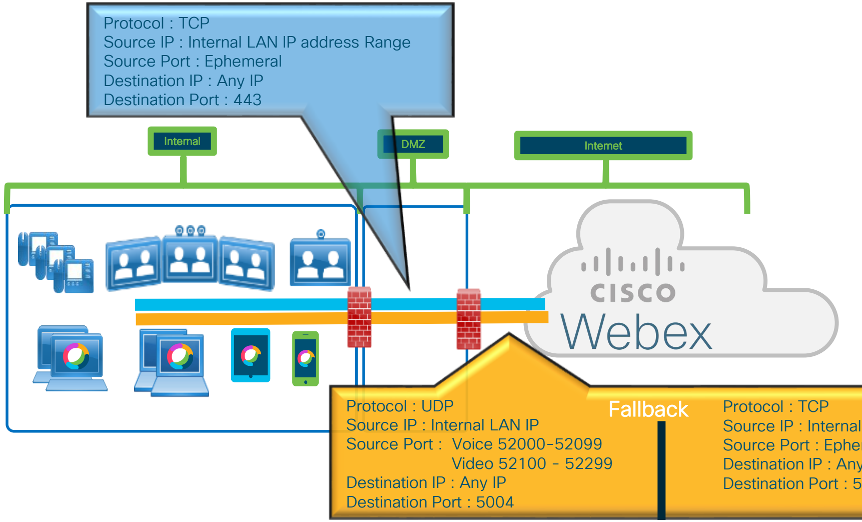
Protocol : UDP
Source IP : Internal LAN IP
Source Port : Voice **52000-52099**
Video **52100-52299**
Destination IP : Any IP
Destination Port : **5004**

Fallback

Protocol : TCP
Source IP : Internal LAN IP
Source Port : Ephemeral
Destination IP : Any IP
Destination Port : **5004**

Protocols and Ports used by Webex Teams

- From a Media perspective Webex Teams clients always try to use UDP but will fallback to TCP if UDP is close. TCP might impact media quality and it can’t guarantee quality for Real Time Media.
- As **last case scenario** for the software clients (Win, MAC, iOS and Android) we can use HTTP proxies for media, **but it isn’t recommended**. Cisco can’t help much if there will be quality issues with media.
- Webex Teams for Windows run as user application and every time that there is an upgrade a new version is installed which makes impossible to block ports, because of that today we use Ephemeral ports



Protocol : TCP
Source IP : Internal LAN IP address Range
Source Port : Ephemeral
Destination IP : Any IP
Destination Port : 443

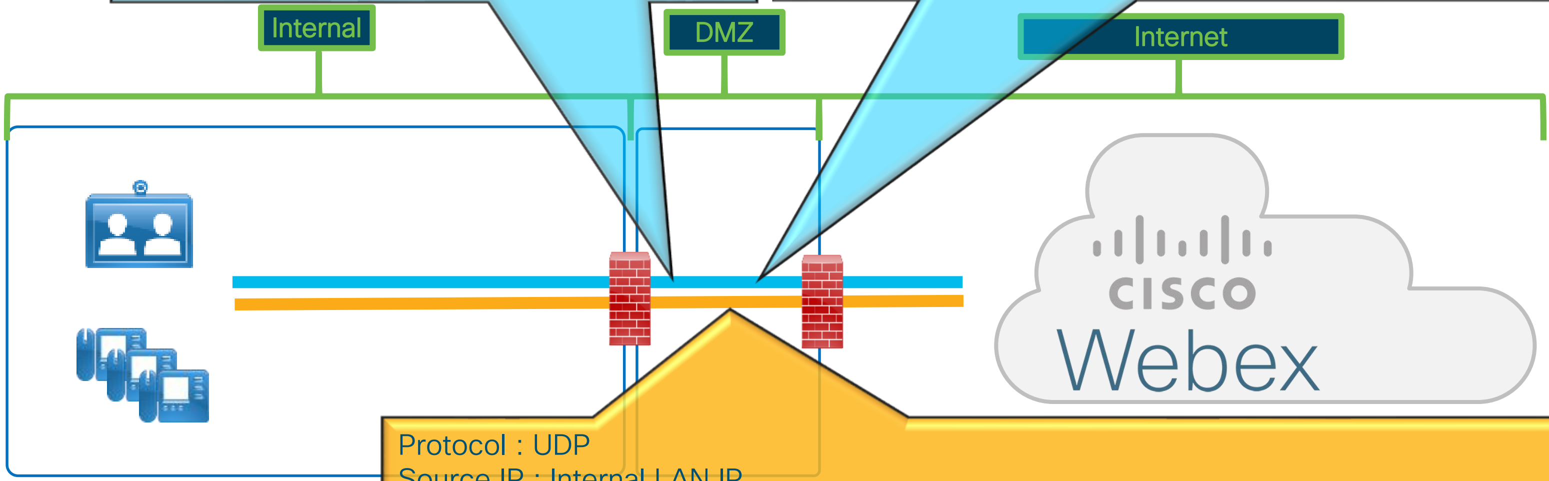
Protocol : UDP
Source IP : Internal LAN IP
Source Port : Voice 52000-52099
Video 52100 - 52299
Destination IP : Any IP
Destination Port : 5004

Fallback

Protocol : TCP
Source IP : Internal
Source Port : Ephe
Destination IP : Any
Destination Port : 5

Protocols and Ports used by Webex Calling

IP Phones, ATAs etc. (EMEA Example)



Usage: **Device Config**
Protocol : TCP
Source IP : Internal LAN IP address Range
Source Port : **Ephemeral**
Destination IP : 85.119.56.198, 85.119.57.198
Destination Port : **80, 443**

Usage: **Call Signaling**
Protocol : TCP
Source IP : Internal LAN IP address Range
Source Port : **5060-5080**
Destination IP : **85.119.56.128/26, 85.119.57.128/26, 185.115.196.0/25, 185.115.197.0/25**
Destination Port : **8934**

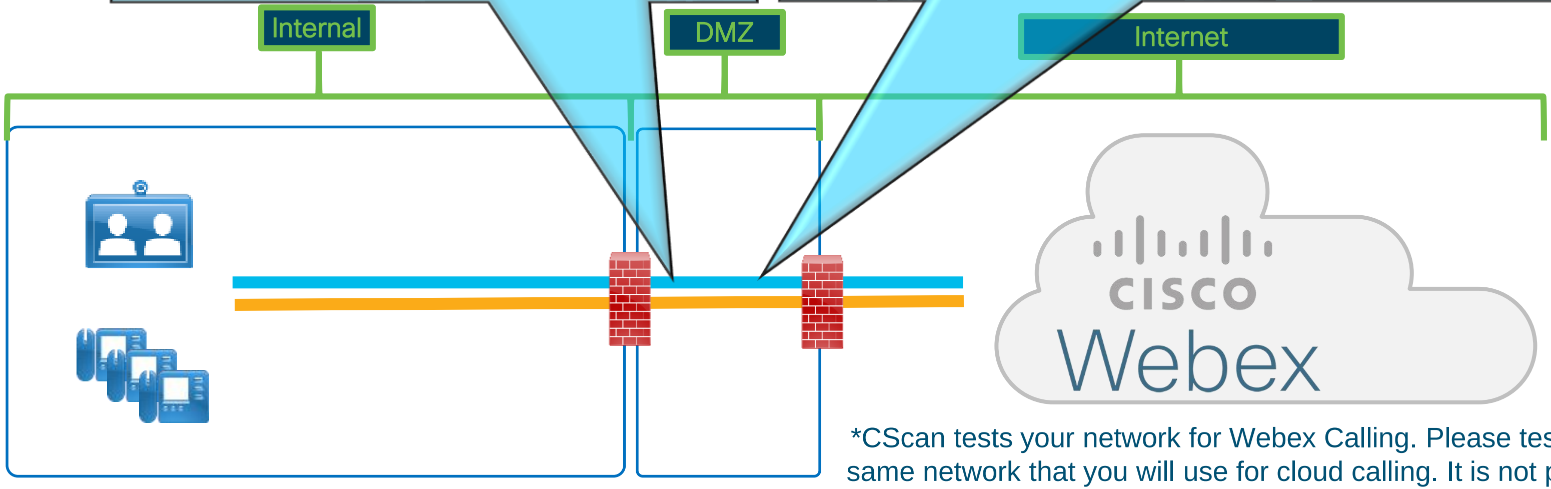
Protocol : UDP
Source IP : Internal LAN IP
Source Port : **19560-19660**
Destination IP : **85.119.56.128/26, 85.119.57.128/26, 185.115.196.0/25, 185.115.197.0/25**
Destination Port : **19560-65535**

Protocols and Ports used by Webex Calling

IP Phones, ATAs etc. (EMEA Example) – Additional Services

Usage: **NTP**
Protocol : TCP
Source IP : Internal LAN IP address Range
Source Port : **51494**
Destination IP : 85.119.56.218, 85.119.57.218
Destination Port : **123**

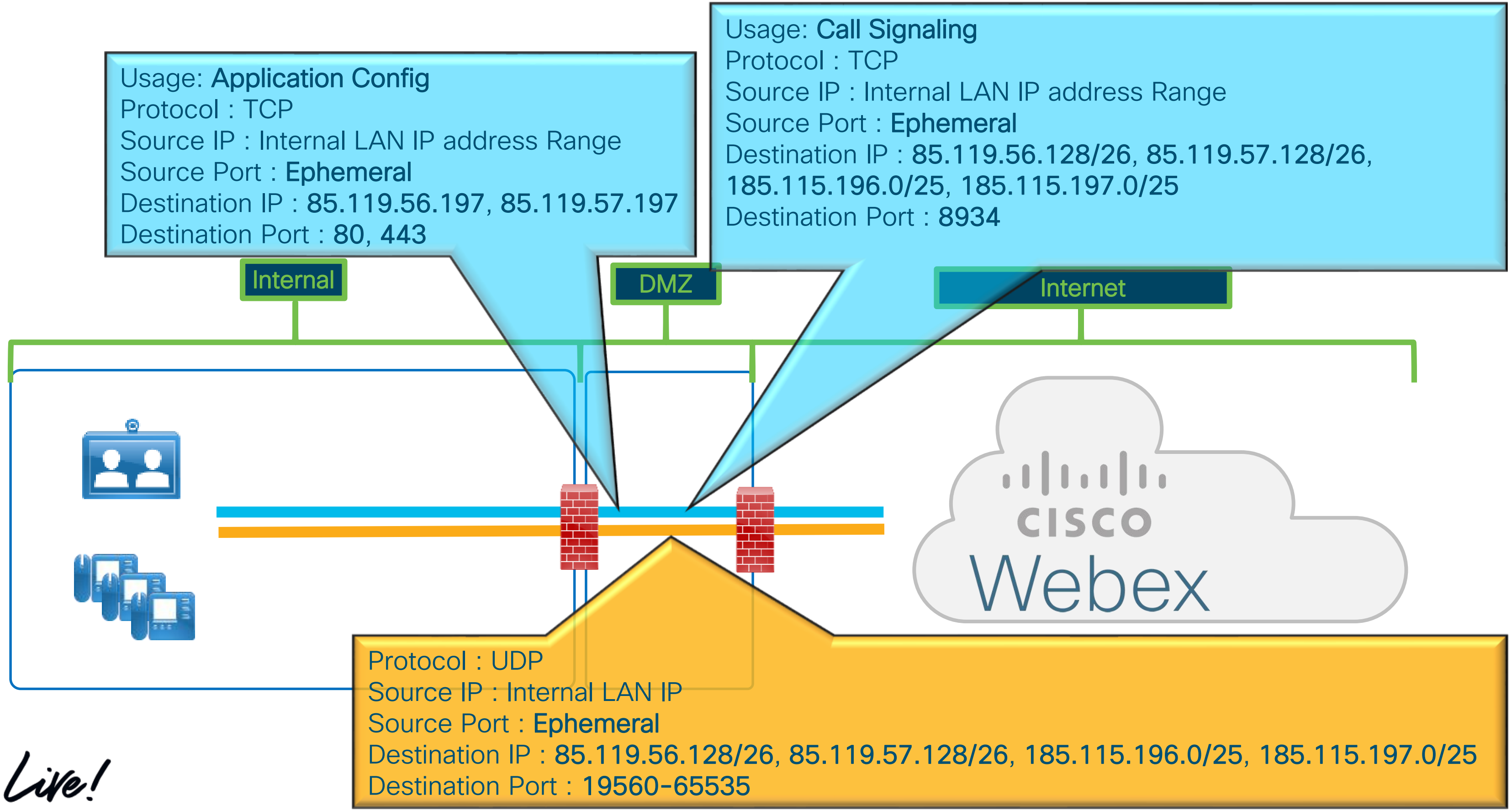
Usage: **CScan Tool***
Protocol : TCP
Source IP : **Ephemeral**
Source Port : **5060-5080**
Destination IP : **185.115.196.129**
Destination Port : **80, 443, 8934**



*CScan tests your network for Webex Calling. Please test from the same network that you will use for cloud calling. It is not possible to test every requirement from a web-based tool, please refer to the port requirements documentation for more details.
https://cscan.webex.com/

Protocols and Ports used by Webex Calling

Applications (EMEA Example)



Usage: **Application Config**
Protocol : TCP
Source IP : Internal LAN IP address Range
Source Port : **Ephemeral**
Destination IP : **85.119.56.197, 85.119.57.197**
Destination Port : **80, 443**

Usage: **Call Signaling**
Protocol : TCP
Source IP : Internal LAN IP address Range
Source Port : **Ephemeral**
Destination IP : **85.119.56.128/26, 85.119.57.128/26, 185.115.196.0/25, 185.115.197.0/25**
Destination Port : **8934**

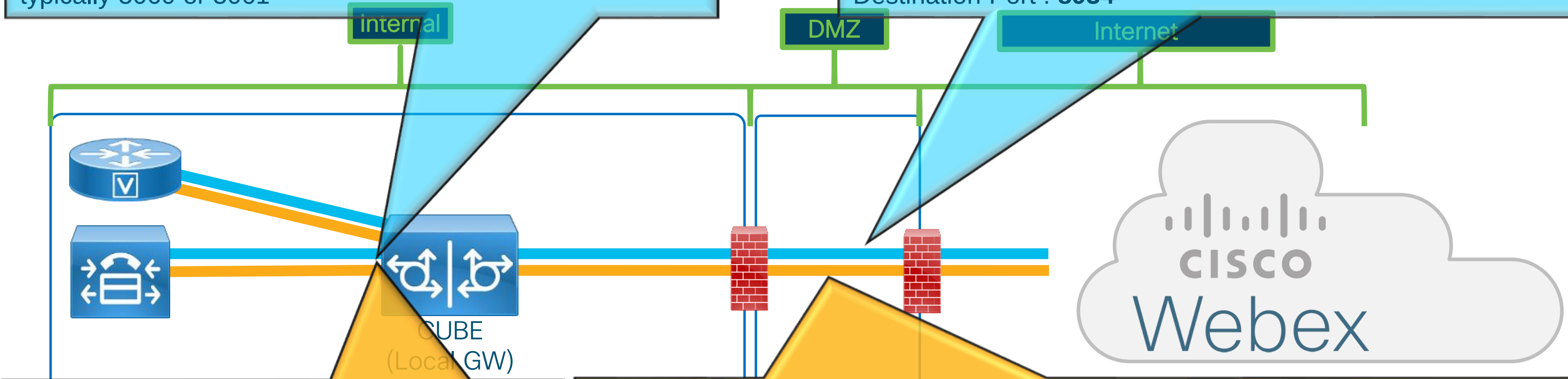
Protocol : UDP
Source IP : Internal LAN IP
Source Port : **Ephemeral**
Destination IP : **85.119.56.128/26, 85.119.57.128/26, 185.115.196.0/25, 185.115.197.0/25**
Destination Port : **19560-65535**

Protocols and Ports used by Webex Calling

VAR Local Gateway (EMEA Example)

Usage: **Call Signaling**
Protocol : TCP
Source IP : Local GW Internal NIC
Source Port : **8000-65535**
Destination IP : Your GW IP
Destination Port : Depends on PSTN option, eg. Unified CM typically 5060 or 5061

Usage: **Call Signaling**
Protocol : TCP
Source IP : Local GW External NIC
Source Port : **8000-65535**
Destination IP : **85.119.56.128/26**, **85.119.57.128/26**, **185.115.196.0/25**, **185.115.197.0/25**
Destination Port : **8934**



Protocol : UDP
Source IP : Local GW Internal NIC
Source Port : **8000-48000***
Destination IP : **Your GW IP**
Destination Port : **19560-65535**

Protocol : UDP
Source IP : Local GW External NIC
Source Port : **8000-48000*** (*configurable using **rtp-port range** command)
Destination IP : **85.119.56.128/26**, **85.119.57.128/26**, **185.115.196.0/25**, **185.115.197.0/25**
Destination Port : **19560-65535**

Port References for Webex Calling in Regions

Service Provider:

https://help.webex.com/en-us/b2exve/Port-Reference-Information-for-Cisco-Webex-Calling#id_119636

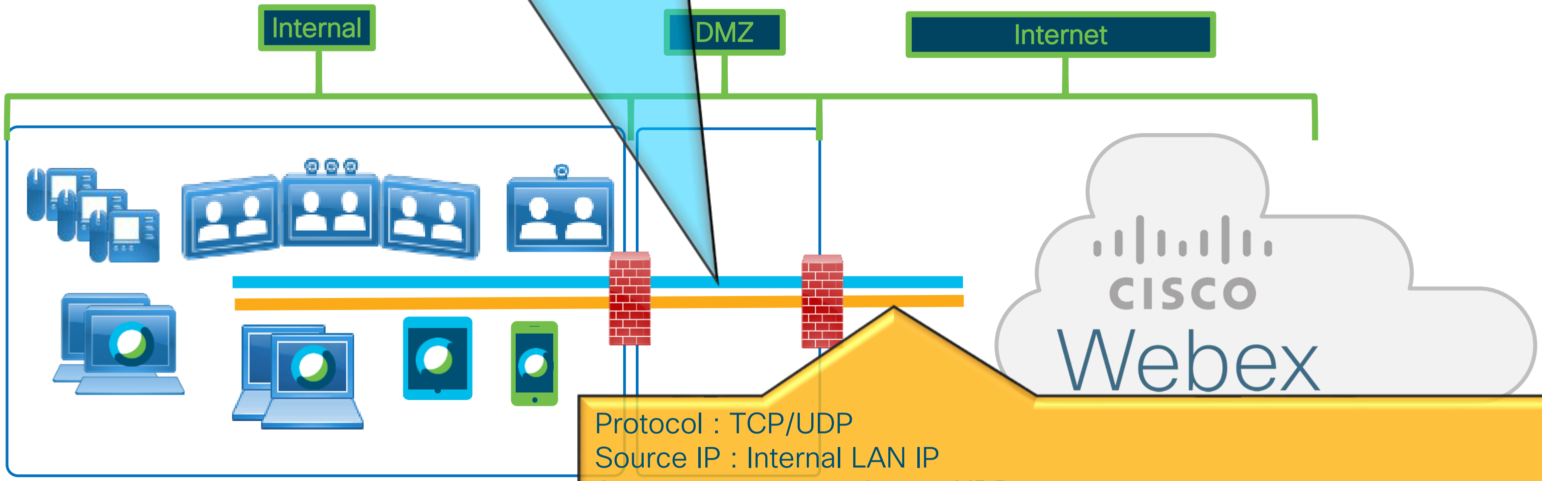
Value Added Reseller:

https://help.webex.com/en-us/b2exve/Port-Reference-Information-for-Cisco-Webex-Calling#id_119637

Protocols and Ports used by Webex Meetings

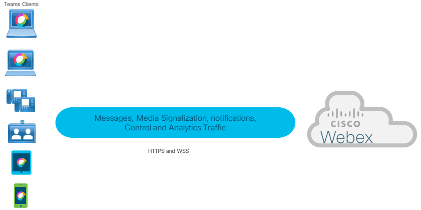
Assuming the simplest scenario with direct connection to the internet :

Protocol : TCP
Source IP : Internal LAN IP address Range
Source Port : **443**
Destination IP : Any IP
Destination Port : **443**

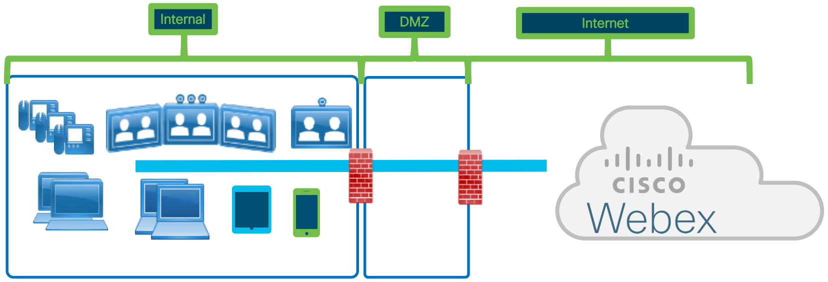


Protocol : TCP/UDP
Source IP : Internal LAN IP
Source Port : Voice/Video **UDP 48000-65535**
Sharing/Whiteboard/Media fallback **TCP 443**
Destination IP : Any IP
Destination Port : **TCP 443 / UDP 9000**

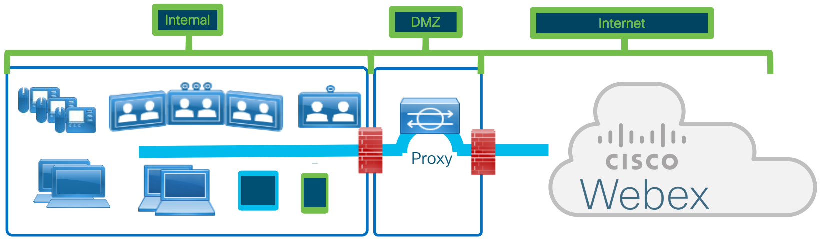
Message, Signalization, Notification and Control


Teams Clients
Messages, Media Signalization, notifications, Control and Analytics Traffic
HTTPS and WSS
cisco Webex

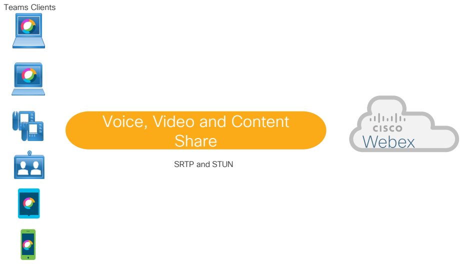
- Media goes directly to the internet using HTTPS WSS protocol.



- Signalization goes through Proxy (rules already in place in the firewall).

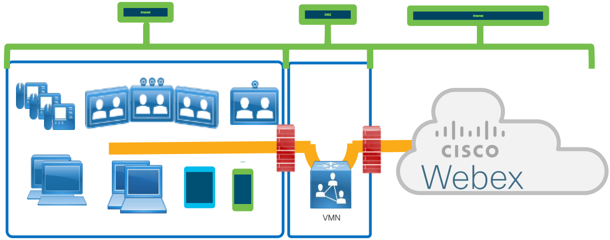


Media for Voice, Video and Content Sharing in Webex Teams



- **Option 1** – Access to the Webex Service through Video Mesh Node.
- **Option 2** – Direct access to the Webex Service using firewalls with STUN support.
- **Option 3** – Direct access to the Webex Service using UDP protocol for media using specific destination IP addresses.
- **Option 4** – Direct access to the Webex Service using UDP protocol for media.
- **Option 5** – Direct access to the Webex Service using TCP protocol for media.
- **Option 6** – Access to the Webex Service using Proxy.

Firewall rules for Media



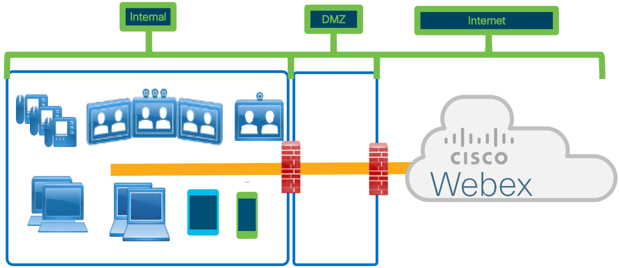
Option 1 – Access to the Webex Service through Video Mesh Node.

All clients inside the customer network would connect to the Video Mesh Node, if there will be participants outside the customer network then VMN would cascade the media flow to the cloud.

Unique sources, very well defines, if necessary, in special DMZ's to protect to connect to the Webex services in the Cloud.

Will open UDP connection to a destination port 5004, few additional ports needed, will be cover in the next section.

Firewall rules for Media



Option 2 – Using firewalls with STUN support

Defined in RFC3489.

Uses UDP from any Webex Teams client inside the customer network using source ports Voice 52000-52099

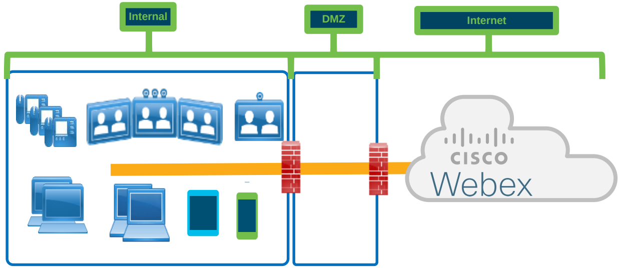
Video 52100-52299

Where the destination might be any IP address in the internet with destination port 5004

STUN allow to open up pinholes only if the system is webRTC compliant, and there is an external recipient expecting the traffic (prevents enterprise from being source of DDoS).

From a security perspective this is the recommended model but require Firewalls that use STUN for WebRTC traffic like Cisco ASA.

Firewall rules for Media



Option 3 – Direct access to the Webex Service using UDP protocol for media using specific destination IP addresses.

We require that the administrator configure the firewall to access inside initiated UDP flow with return to the same 5-Tuple (Source IP address/port number, destination IP address/port number and the protocol in use) with a 30s timeout on the creation of the pinhole, Bidirectional media is sent over this flow.

Uses UDP from any Webex client inside the customer network using source ports

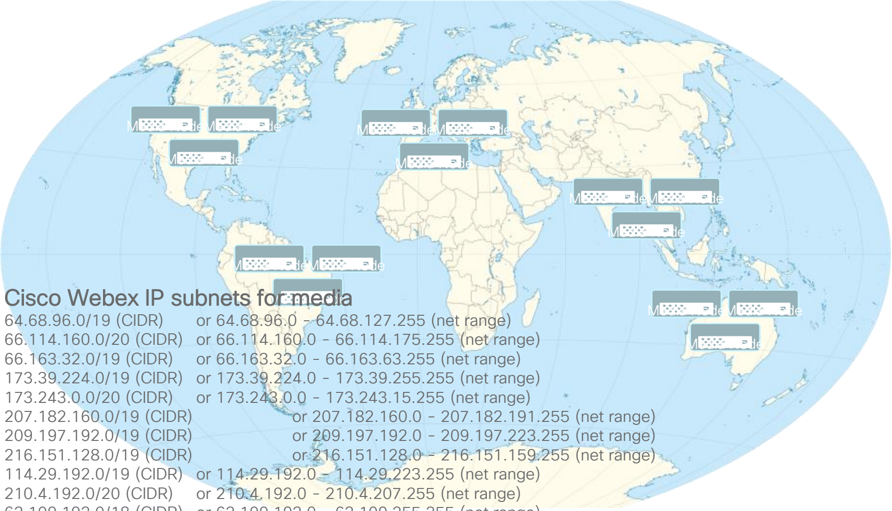
Voice 52000-52099

Video 52100-52299

Where the destination might be two /19 prefixed in the internet with destination port 5004

Firewall pinholes for Cisco IP Media Prefixes

US West	US East	Sydney	Frankfurt	Singapore
GA	GA	GA	GA	GA



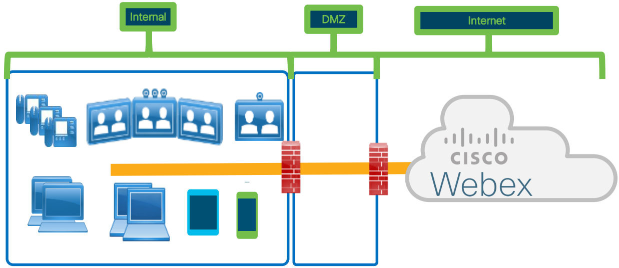
Cisco Webex IP subnets for media

64.68.96.0/19 (CIDR) or 64.68.96.0 - 64.68.127.255 (net range)
66.114.160.0/20 (CIDR) or 66.114.160.0 - 66.114.175.255 (net range)
66.163.32.0/19 (CIDR) or 66.163.32.0 - 66.163.63.255 (net range)
173.39.224.0/19 (CIDR) or 173.39.224.0 - 173.39.255.255 (net range)
173.243.0.0/20 (CIDR) or 173.243.0.0 - 173.243.15.255 (net range)
207.182.160.0/19 (CIDR) or 207.182.160.0 - 207.182.191.255 (net range)
209.197.192.0/19 (CIDR) or 209.197.192.0 - 209.197.223.255 (net range)
216.151.128.0/19 (CIDR) or 216.151.128.0 - 216.151.159.255 (net range)
114.29.192.0/19 (CIDR) or 114.29.192.0 - 114.29.223.255 (net range)
210.4.192.0/20 (CIDR) or 210.4.192.0 - 210.4.207.255 (net range)
62.109.192.0/18 (CIDR) or 62.109.192.0 - 62.109.255.255 (net range)
69.26.160.0/19 (CIDR) or 69.26.160.0 - 69.26.191.255 (net range)

Network Requirements
https://collaborationhelp.cisco.com/article/en-us/WBX000028782

Configuration recommendation
Add all ranges to your firewalls, so there is automatic failover with minimal disruption
Webex Meetings is by region
Webex Teams – not specified by region.

Firewall rules for Media



Option 4 – Direct access to the Webex Service using UDP protocol for media.

We require that the administrator configure the firewall to access inside initiated UDP flow with return to the same 5-Tuple (Source IP address/port number, destination IP address/port number and the protocol in use) with a 30s timeout on the creation of the pinhole, Bidirectional media is sent over this flow.

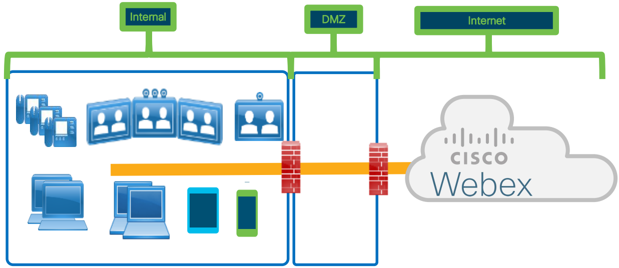
Uses UDP from any Webex client inside the customer network using source ports

Voice 52000-52099

Video 52100-52299

Where the destination might be any IP address in the internet with destination port 5004

Firewall rules for Media



Option 5 – Direct access to the Webex Service using TCP protocol for media.

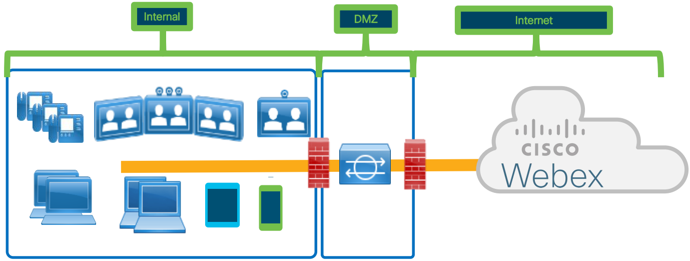
If clients can't reach the Webex Services using UDP port 5004, they will fallback to TCP.

Any Webex Teams client inside the customer network will use TCP with source ephemeral ports.

Where the destination might be any IP address in the internet with destination port 5004.

Using TCP protocol **might impact** the quality of the media, we always recommend that the customer use UDP for real time media.

Firewall rules for Media



Option 6 – Access to the Webex Service using Proxy.

If Webex Teams Software clients can't reach the Webex Services by any other mechanisms, they will use as last resource the HTTP proxies define in the system.

Proxy were not designed for real time media so even if they will work in PoC they will never be able to handle all the traffic that the Webex deployment can generate.

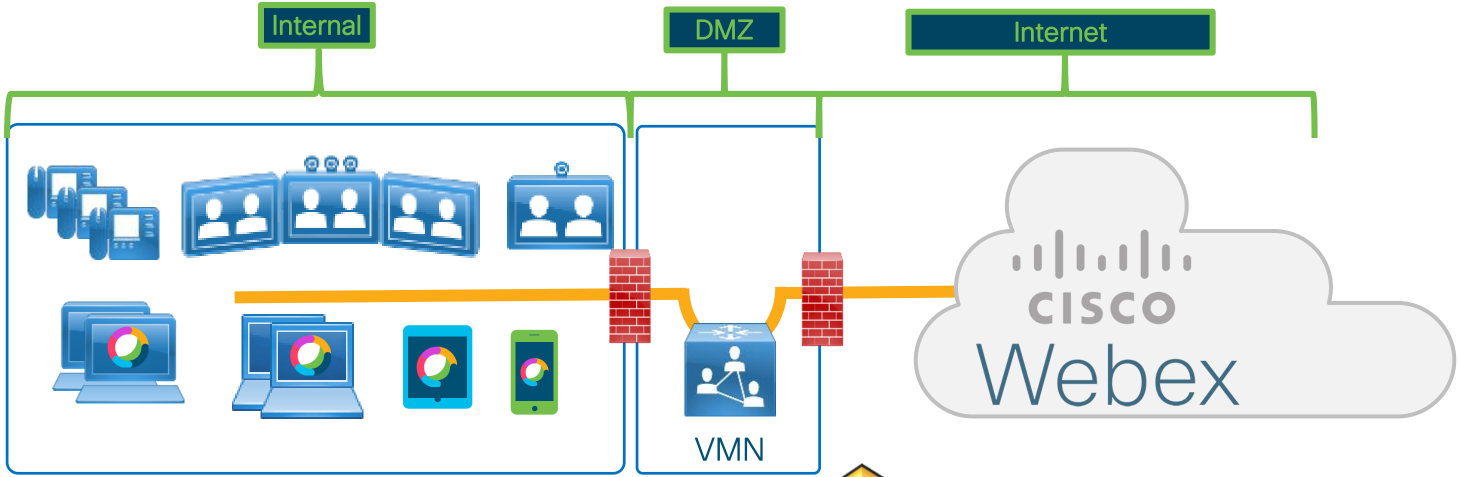
It is guarantee that at some point in time the experience will be really bad.

If direct access to the internet isn't an option for a specific customer, VMN is the solution, a "specialized proxy" for media.

Hybrid Services connection considerations

Video Mesh Node

Quality of Service disabled (default)

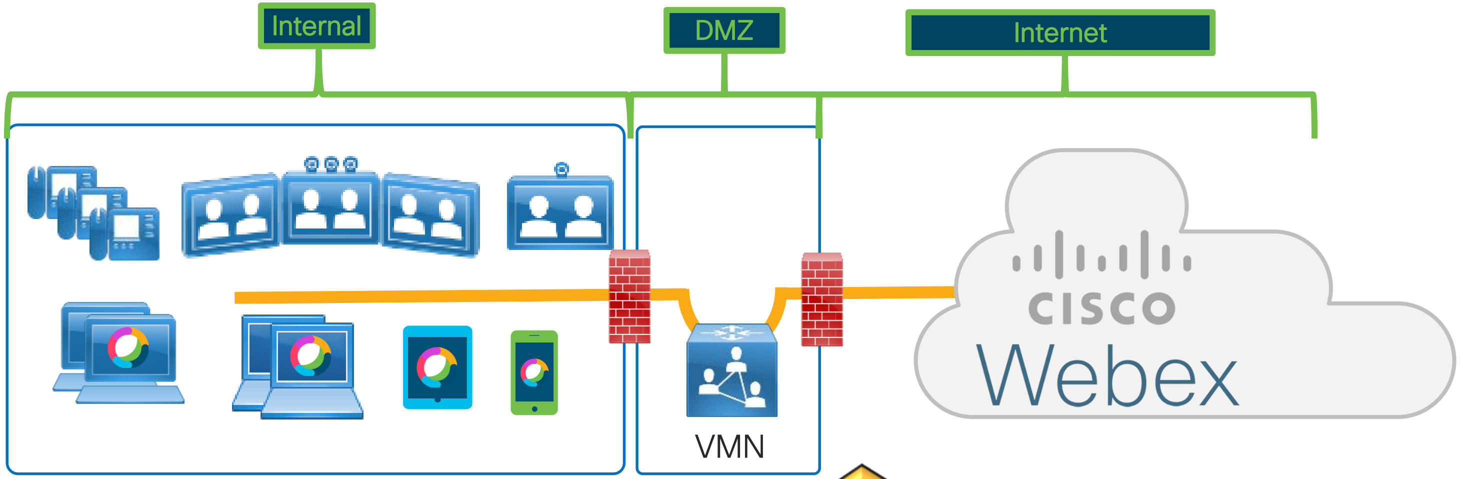


Client/Endpoint to VMN
Source IP : Internal LAN IP
Source Port : Voice **52000-52099**
Video **52100-52299**
Destination IP : VMN
Destination Port : **5004**

VMN to Cloud
Source IP : VMN
Source Port : Voice and Video
34000 to 34999
Destination IP : Any IP
Destination Port : **5004**

Video Mesh Node

Quality of Service enabled



Client/Endpoint to VMN

Source IP : Internal LAN IP

Source Port : Voice **52000-52099**
Video **52100-52299**

Destination IP : VMN

Destination Port : **5004**

VMN to Cloud

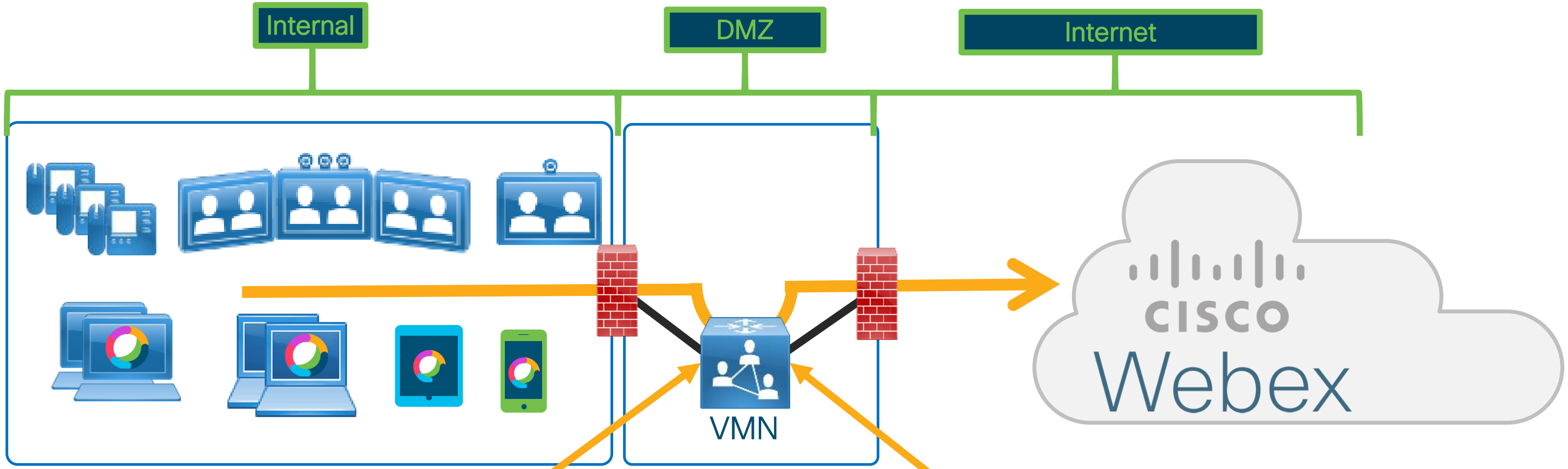
Source IP : VMN

Source Port : Voice **52500-62999**
Video **63000-65500**

Destination IP : Any IP

Destination Port : **5004**

Video Mesh Node – Dual NIC



Port ranges unchanged, but FW rules bound to Internal Interface IP

Port ranges unchanged, but FW rules bound to External Interface IP

Video Mesh Node

Media Considerations – No QoS enabled

Source IP Address	Destination IP Address	Source UDP Ports	Destinations UDP Ports	Media Type
Clients/Endpoints	Video Mesh Node	52000-52299	5004	STUN
Clients/Endpoints	Video Mesh Node	52000-52099	5004	Audio
Clients/Endpoints	Video Mesh Node	52100-52299	5004	Video
Video Mesh Node	Collaboration Cloud	34000-34999	5004	Audio
Video Mesh Node	Collaboration Cloud	34000-34999	5004	Video
Video Mesh Node	Video Mesh Node	34000-34999	5004	Audio
Video Mesh Node	Video Mesh Node	34000-34999	5004	Video

Video Mesh Node

Media Considerations – QoS enabled

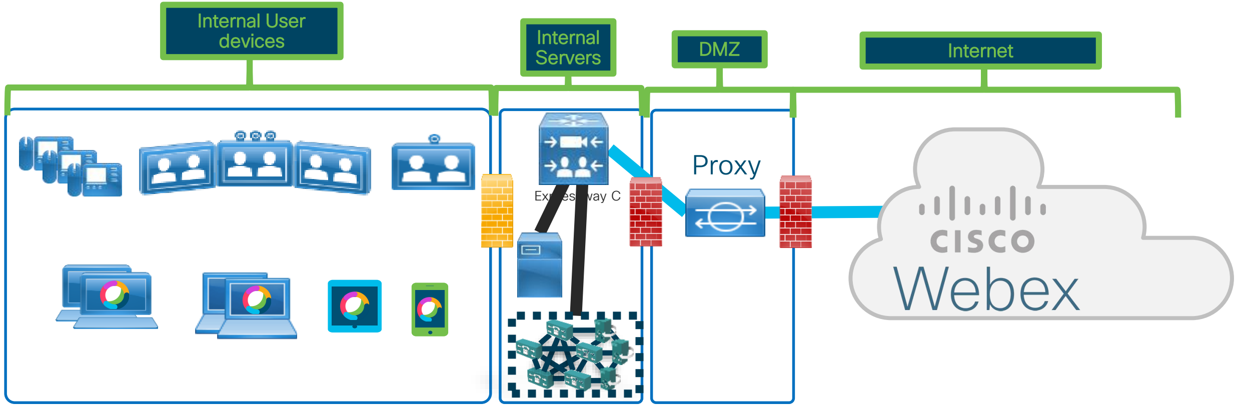
Source IP Address	Destination IP Address	Source UDP Ports	Destinations UDP Ports	Media Type
Clients/Endpoints	Video Mesh Node	52000-52299	5004	STUN
Clients/Endpoints	Video Mesh Node	52000-52099	5004	Audio
Clients/Endpoints	Video Mesh Node	52100-52299	5004	Video
Video Mesh Node	Collaboration Cloud	52500-62999	5004	Audio
Video Mesh Node	Collaboration Cloud	63000-65500	5004	Video
Video Mesh Node	Video Mesh Node	52500-62999	5004	Audio
Video Mesh Node	Video Mesh Node	63000-65500	5004	Video

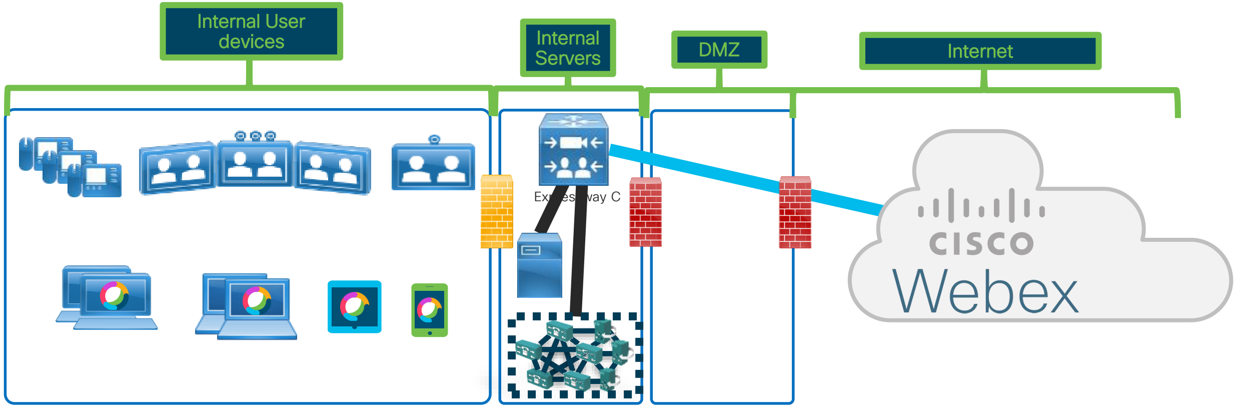
Video Mesh Node

Management Considerations

Source	Destination	Transport Protocol	Destinations Ports	Destination IP
Computer Management	Video Mesh Node	TCP	443	Any
Video Mesh Node	Collaboration Cloud	UDP -> NTP UDP -> DNS TCP -> HTTPS	123 53 444	Any
Video Mesh Node	Video Mesh Node	TCP -> HTTPS	5000,5001	Any
Video Mesh Node	Collaboration Cloud	TCP -> HTTPS	443	*.wbx2.com *.idbroker.webex.com

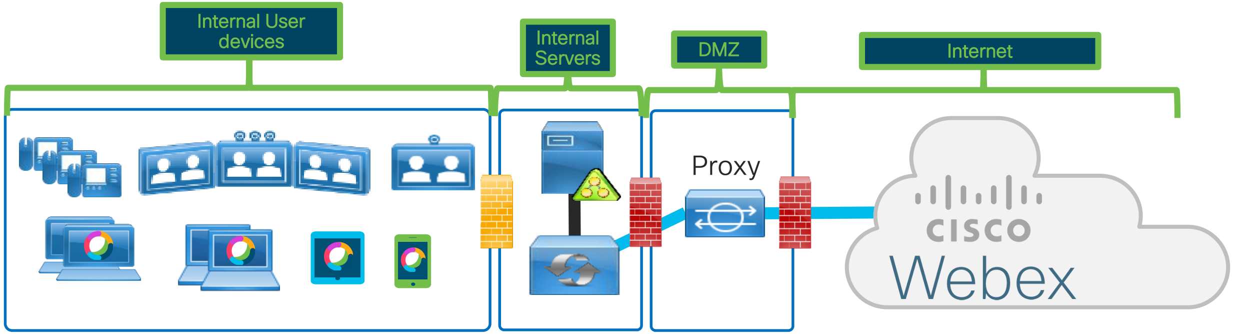
Expressway Connectors

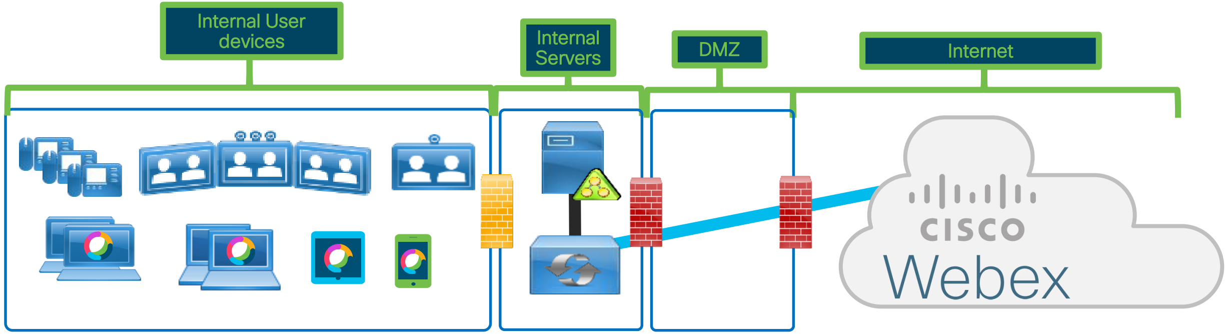




- If customer has proxies, we support only No Auth and Basic Authentication.
- If there isn't any proxy, we will use HTTPS to send traffic to the Webex cloud.

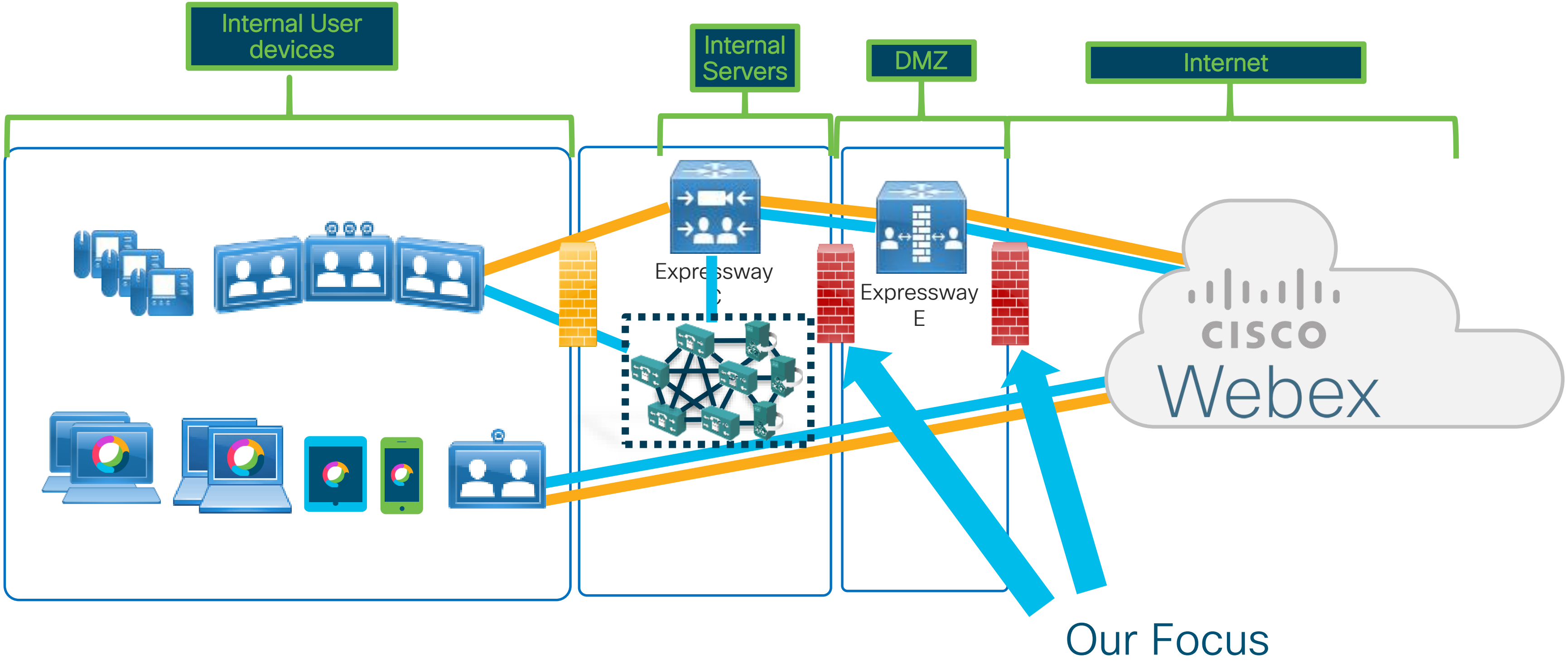
Directory Connector





- If Windows OS is configured for proxies, we will use it and send all traffic there
- If there isn't any proxies configured in the systems, we will use HTTPS to send traffic to the Webex cloud.

Hybrid Media Call/CMR Dial-in/VMN Cascading



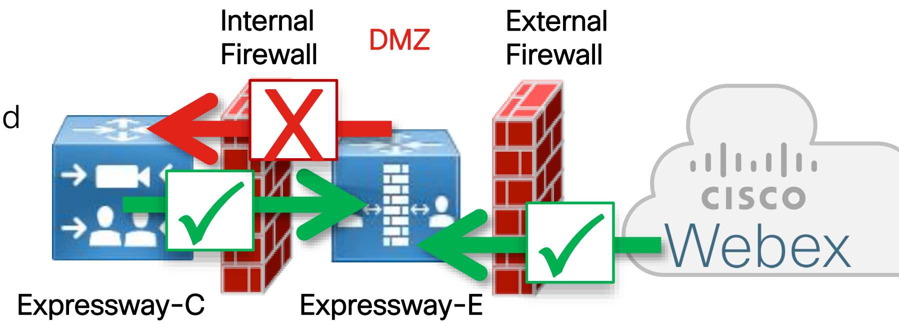
Hybrid Media Call/CMR Dial-in/VMN Cascading

Firewall Port Details

No inbound ports required to be opened on the internal firewall

Internal firewall needs to allow the following outbound connections from Expressway-C to Expressway-E

- SIP: TCP 7001
- Traversal Media: UDP 36000 to 36011
- HTTPS (tunneled over SSH between Expressway-C and Expressway-E): TCP 2222

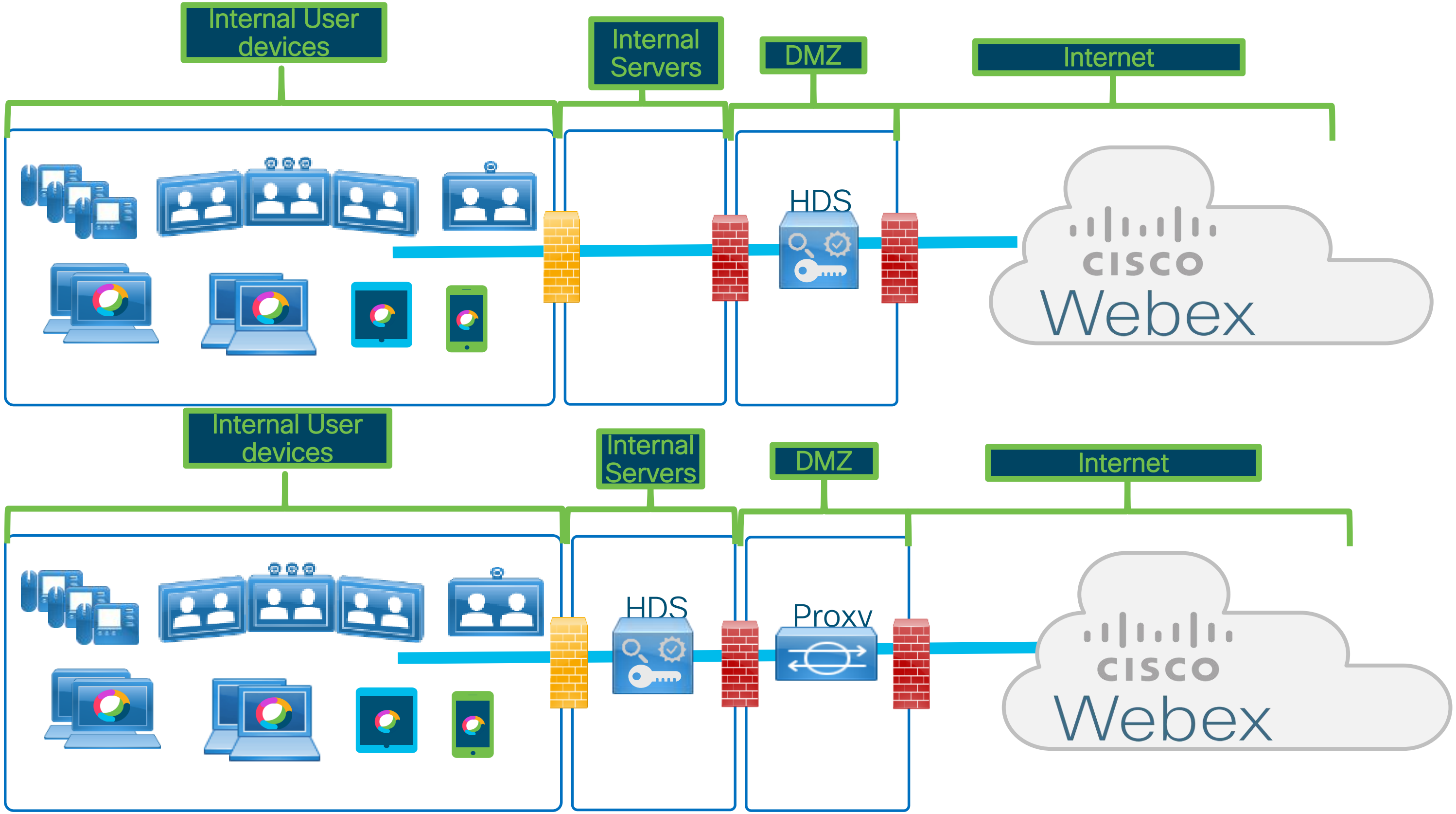


External firewall needs to allow the following inbound connections to Expressway

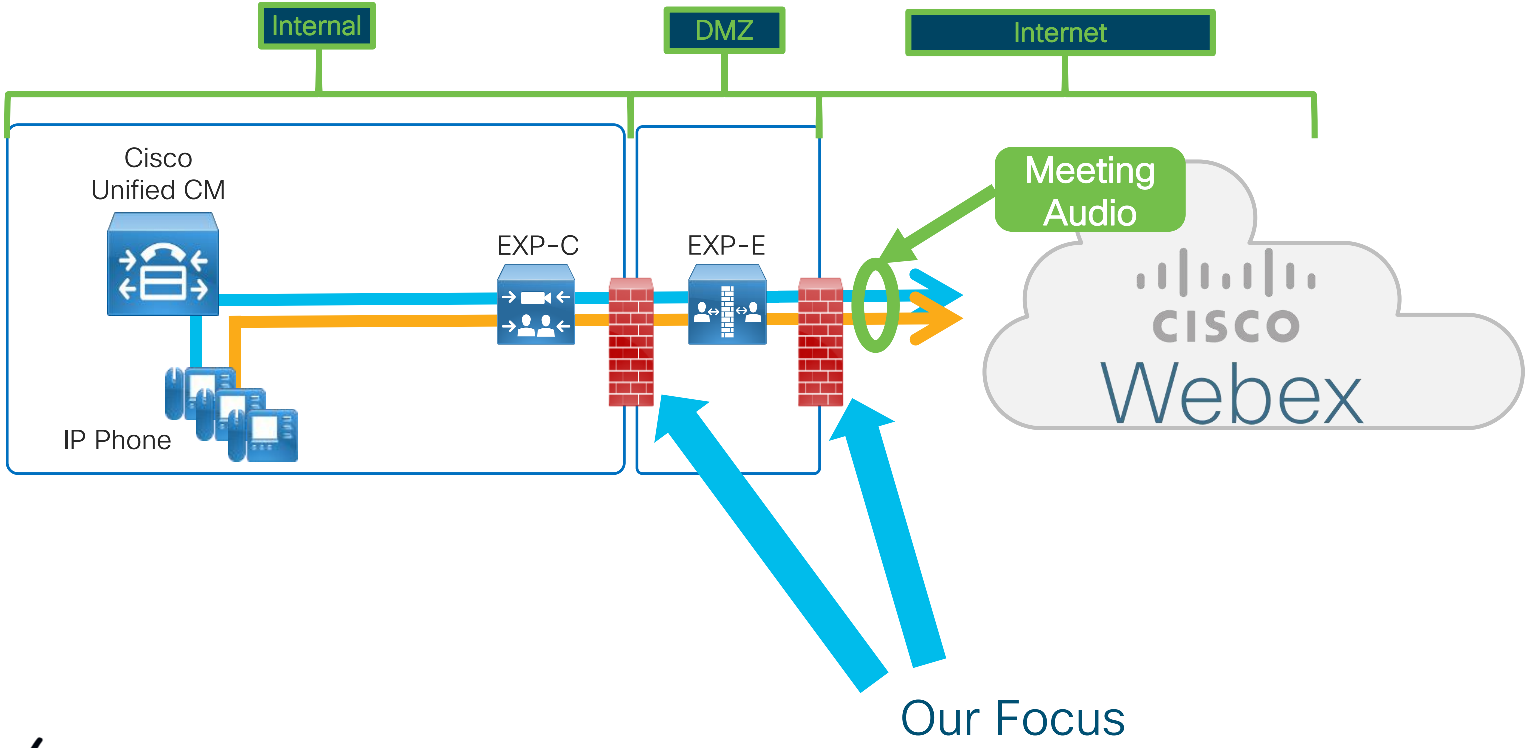
- SIP: TCP 5061 (Call signaling)
- Media: UDP 36002 to 59999 (Voice and video)

We can calculate the port range we really use by multiple the number of simultaneous calls that we are going to have by 12. This way, for example we know if we expect 100 calls maximum the ports need to be open in the External FW will be 36002-37202 (1200 UDP ports)

Hybrid Data Security



Webex Edge Audio



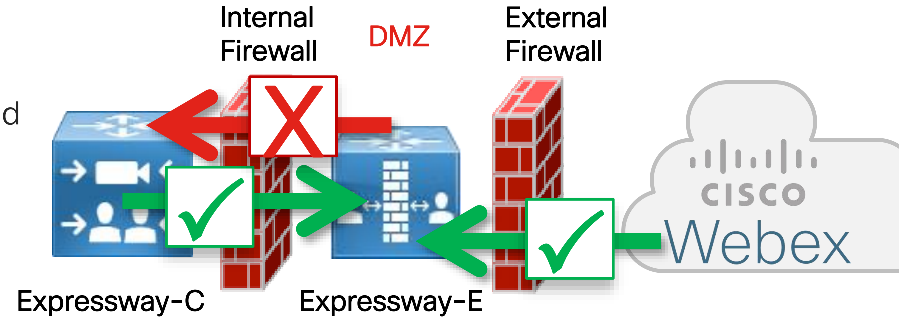
Cisco Expressway for Webex Edge Audio

Firewall Port Details

Configuration different to existing Expressway Traversal for B2B Video!!!

Internal firewall needs to allow the following outbound connections from Expressway-C to Expressway-E

- SIP: TCP 7003
- Traversal Media: UDP 36000 to 36011
- HTTPS (tunneled over SSH between Expressway-C and Expressway-E): TCP 2222

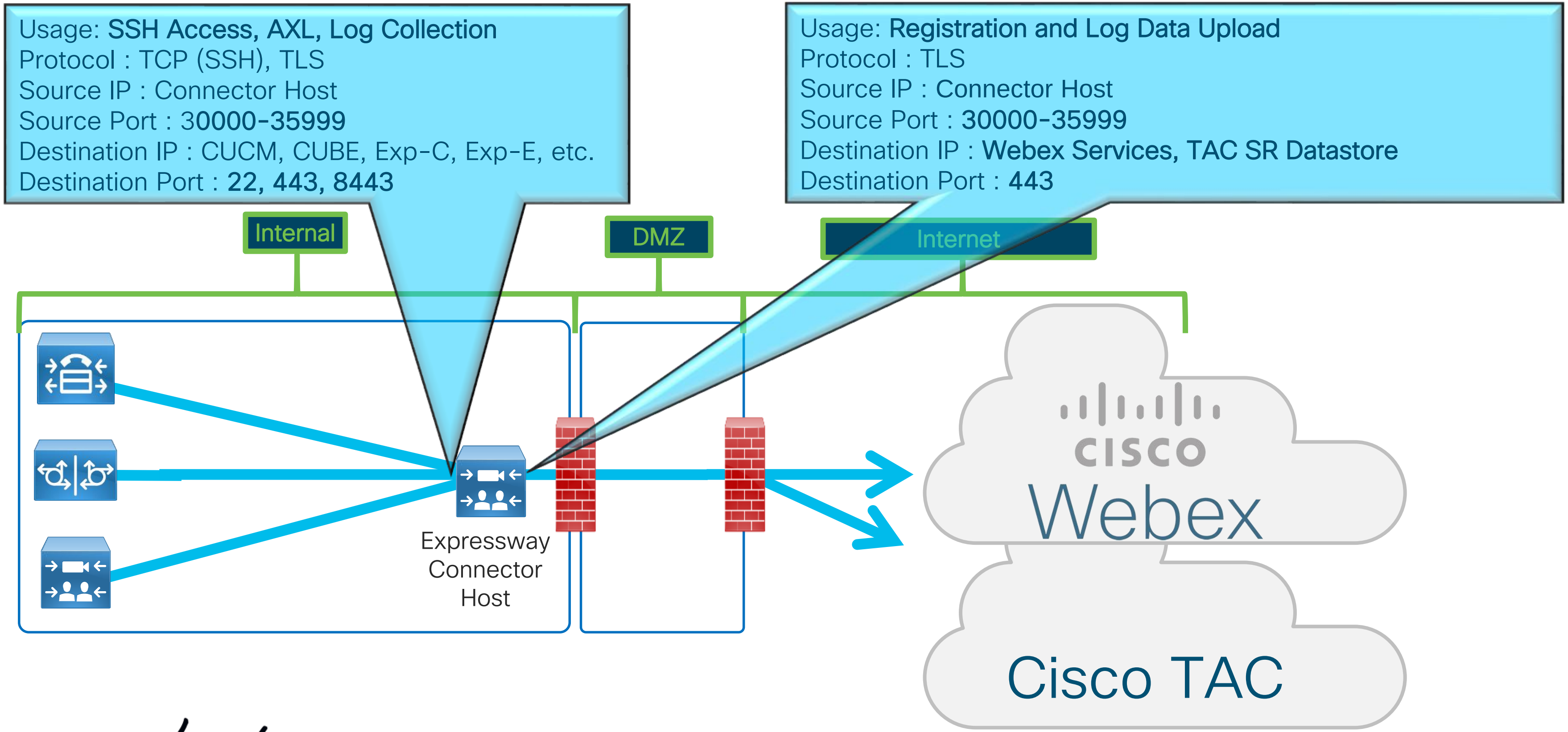


External firewall needs to allow the following inbound connections to Expressway

- SIP: TCP 5061,5062 Inbound (Call signaling/Mutual TLS)
- SIP: 5061, 5065 Outbound (Call Signaling/DNS SRV Records configured Control Hub for LUA Script)
- Media: UDP 36000 to 59999 (Voice and video)

Note: Create a new Neighbor Zone to CUCM, a new Traversal Zone and a new DNS Zone (before x8.11) or Webex Zone (after x8.11). This will ensure that e.g. incoming traffic to CUCM can be handled differently. (Allow PSTN Access for Webex/Prevent PSTN Access for incoming B2B calls.

Cisco Webex Serviceability Connector



Usage: **SSH Access, AXL, Log Collection**
Protocol : TCP (SSH), TLS
Source IP : Connector Host
Source Port : **30000-35999**
Destination IP : CUCM, CUBE, Exp-C, Exp-E, etc.
Destination Port : **22, 443, 8443**

Usage: **Registration and Log Data Upload**
Protocol : TLS
Source IP : Connector Host
Source Port : **30000-35999**
Destination IP : **Webex Services, TAC SR Datastore**
Destination Port : **443**

Enterprise Class security features for Cloud

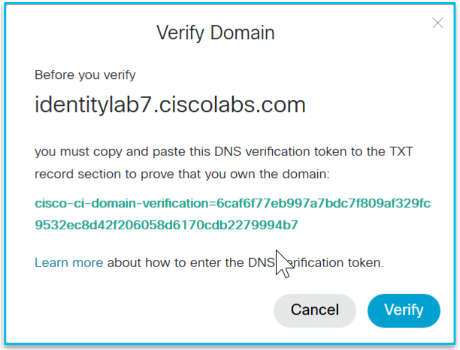
Content Ownership

Claiming users and Domain Verification

Now we can claim users from the Consumer Org or for other customer ORG's.

That is only possible if the DNS domain of the user is verify.

The DNS domain can be verify in multiple ORG's



Verify Domain

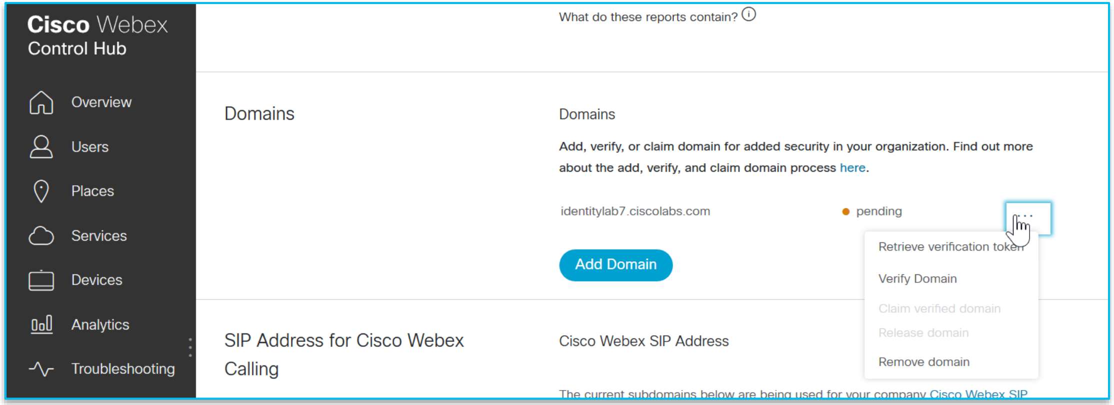
Before you verify

identitylab7.ciscolabs.com

you must copy and paste this DNS verification token to the TXT record section to prove that you own the domain:

cisco-ci-domain-verification=6caf6f77eb997a7bdc7f809af329fc9532ec8d42f206058d6170cdb2279994b7

Learn more about how to enter the DNS verification token.



What do these reports contain?

Domains

Domains

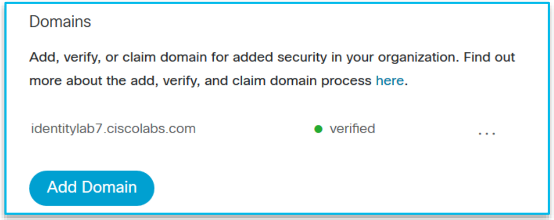
Add, verify, or claim domain for added security in your organization. Find out more about the add, verify, and claim domain process here.

identitylab7.ciscolabs.com ● pending

SIP Address for Cisco Webex Calling

Cisco Webex SIP Address

The current subdomains below are being used for your company Cisco Webex SIP



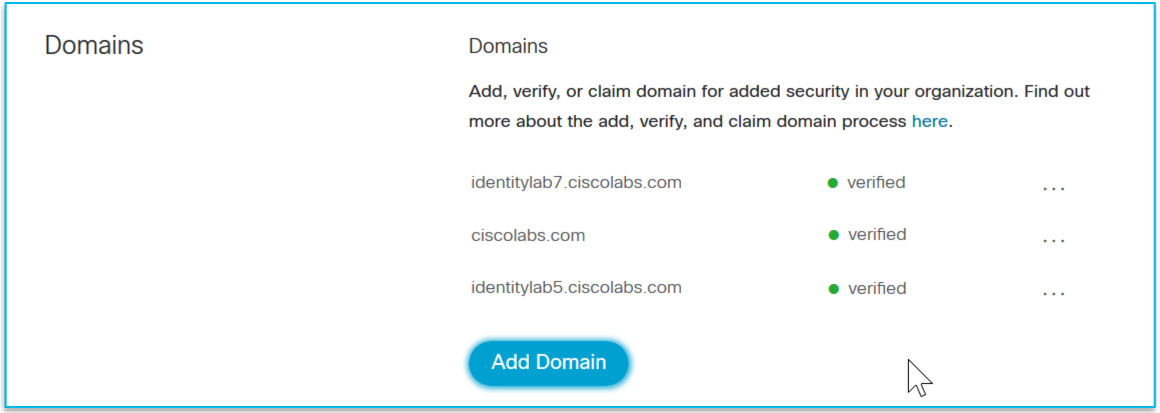
Domains

Add, verify, or claim domain for added security in your organization. Find out more about the add, verify, and claim domain process here.

identitylab7.ciscolabs.com ● verified ...

Verification Domains and Sub-Domains

- You can verify Top level domains.
- You only need to do DNS validation for the top level domain
- Sub-domains need to be specify but don't need DNS validation.



Domains

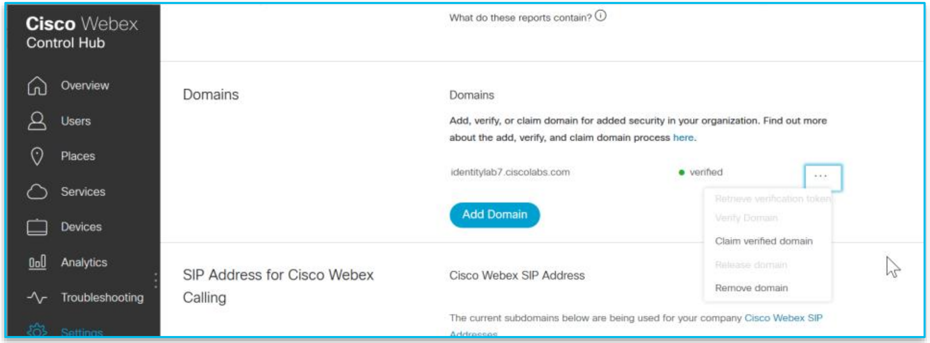
Domains

Add, verify, or claim domain for added security in your organization. Find out more about the add, verify, and claim domain process here.

identitylab7.ciscolabs.com	● verified	...
ciscolabs.com	● verified	...
identitylab5.ciscolabs.com	● verified	...

Claim the Domain

- Can only be done after Verification of domain
- Any User created after Domain Claim will immediately appear in the User list of that ORG, no matter if the user is self boarded, is boarded by another ORG, and is Side boarded.
- It is recommended that auto License template is configured before enabling this.



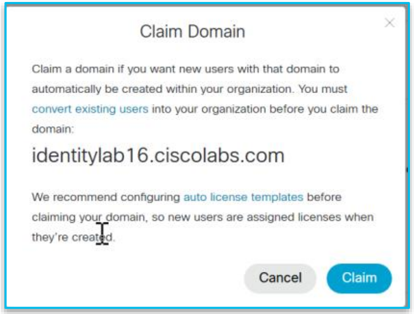
Domains

Add, verify, or claim domain for added security in your organization. Find out more about the add, verify, and claim domain process here.

identitylab7.ciscolabs.com ● verified

Cisco Webex SIP Address

The current subdomains below are being used for your company Cisco Webex SIP Addresses



Claim a domain if you want new users with that domain to automatically be created within your organization. You must convert existing users into your organization before you claim the domain:

identitylab16.ciscolabs.com

We recommend configuring auto license templates before claiming your domain, so new users are assigned licenses when they're created.

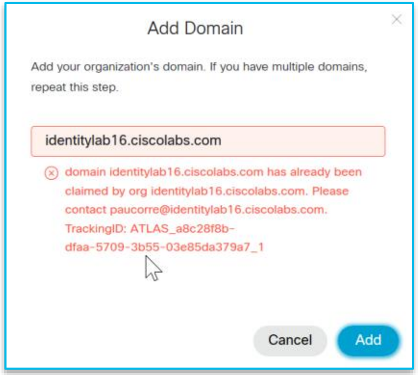
Claiming the Domain

- Users **created before** the Domain Claim will need to be **manual claim**, before or after the Domain Claim process

- **Same** User Claiming **rules** applies as domains that are only verify.

- A specific **DNS domain can only be claim** in a single ORG

- There is no limit on the number of domains you can claim for your organization. However, if you have **more than 20 claimed domains** in a Cisco Webex organization, you **may encounter issues** with converting users.

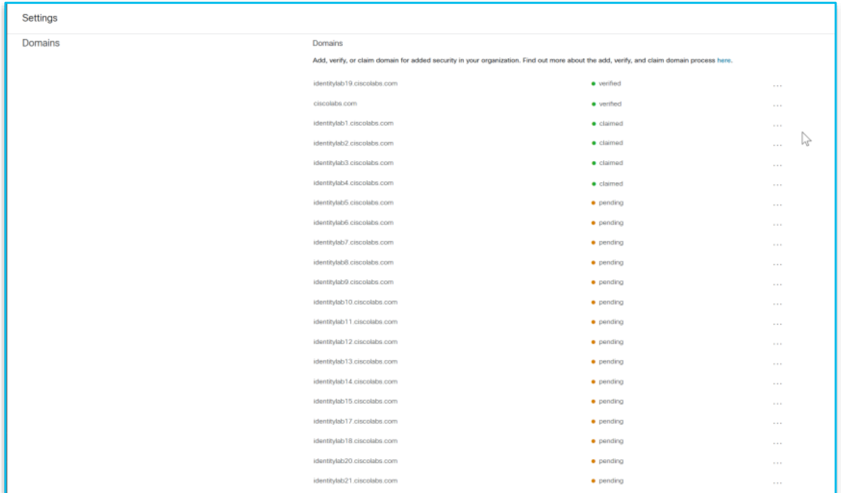


Add Domain

Add your organization's domain. If you have multiple domains, repeat this step.

identitylab16.ciscolabs.com

domain identitylab16.ciscolabs.com has already been claimed by org identitylab16.ciscolabs.com. Please contact paucorre@identitylab16.ciscolabs.com. TrackingID: ATLAS_a8c28f8b-dfaa-5709-3b55-03e85da379a7_1



Settings

Domains

Domains

Add, verify, or claim domain for added security in your organization. Find out more about the add, verify, and claim domain process here.

identitylab19.ciscolabs.com	● verified	...
ciscolabs.com	● verified	...
identitylab1.ciscolabs.com	● claimed	...
identitylab2.ciscolabs.com	● claimed	...
identitylab3.ciscolabs.com	● claimed	...
identitylab4.ciscolabs.com	● claimed	...
identitylab5.ciscolabs.com	● pending	...
identitylab6.ciscolabs.com	● pending	...
identitylab7.ciscolabs.com	● pending	...
identitylab8.ciscolabs.com	● pending	...
identitylab9.ciscolabs.com	● pending	...
identitylab10.ciscolabs.com	● pending	...
identitylab11.ciscolabs.com	● pending	...
identitylab12.ciscolabs.com	● pending	...
identitylab13.ciscolabs.com	● pending	...
identitylab14.ciscolabs.com	● pending	...
identitylab15.ciscolabs.com	● pending	...
identitylab17.ciscolabs.com	● pending	...
identitylab18.ciscolabs.com	● pending	...
identitylab20.ciscolabs.com	● pending	...
identitylab21.ciscolabs.com	● pending	...

What does Content Ownership get you?

	Owning Organization	Participating Organization
CREATE		
Post content into the space	No	No
READ		
Read content (messages and files) posted by its own users into the space	Yes	Yes
Read content posted by any user in the space	Yes	No
UPDATE		
Modify content posted by users into the space	No	No
DELETE		
Define retention policies for the space	Yes	No
Delete content posted by any user in the space	Yes	No
Delete content posted by its own users in the space	Yes	Yes

Enterprise Content Management

Benefits with proposed Webex Teams-ECM Solution

Let's meet soon regarding this PDF document.

Yes, let's make sure we review this tomorrow.

Hey @John

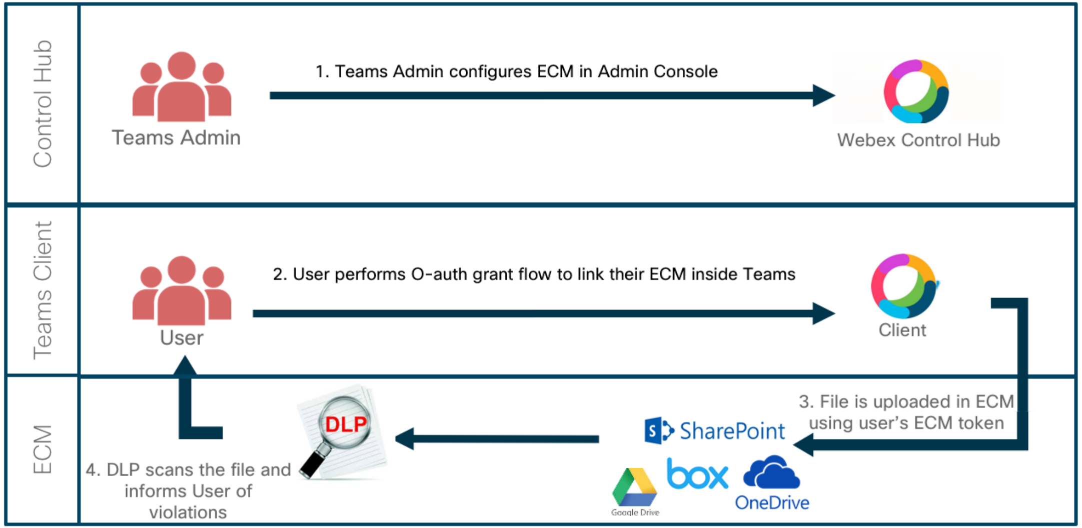
Send a message

- ✓ Keep Webex files safe and secure in ECM of your choice
- ✓ Protect via existing DLP/CASB and Anti-malware
- ✓ Easily share and sync content across apps
- ✓ Create and manage content in both ECM and Webex
- ✓ Flexibility to use ECM and/or Webex File System

Webex Teams – Enterprise Content Management

SharePoint Online/OneDrive for Business

Architecture Enterprise Content Solution to Webex Teams



Control Hub
Teams Admin
1. Teams Admin configures ECM in Admin Console
Webex Control Hub
Teams Client
User
2. User performs O-auth grant flow to link their ECM inside Teams
Client
ECM
3. File is uploaded in ECM using user's ECM token
SharePoint
box
OneDrive
Google Drive
DLP
4. DLP scans the file and informs User of violations

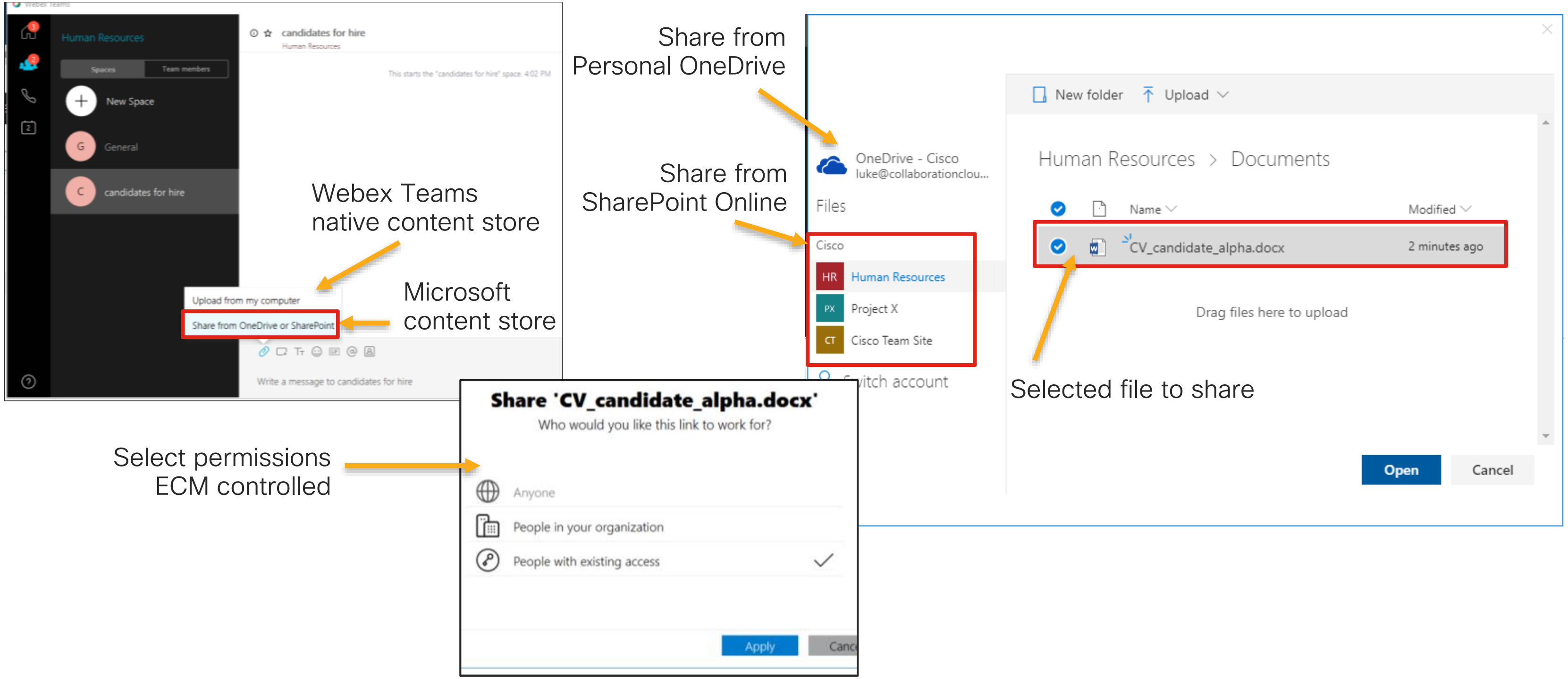
Content posted to Webex Team space is uploaded directly from the client to ECM or a reference between existing content in ECM and Webex teams space is created.

Content never passes through Cisco Webex cloud

Webex Teams – Enterprise Content Management

SharePoint Online/OneDrive for Business

User experience



Share 'CV_candidate_alpha.docx'

Who would you like this link to work for?

Webex Teams native content store

Microsoft content store

Share from Personal OneDrive

Share from SharePoint Online

Selected file to share

Select permissions ECM controlled

Webex Teams – Enterprise Content Management

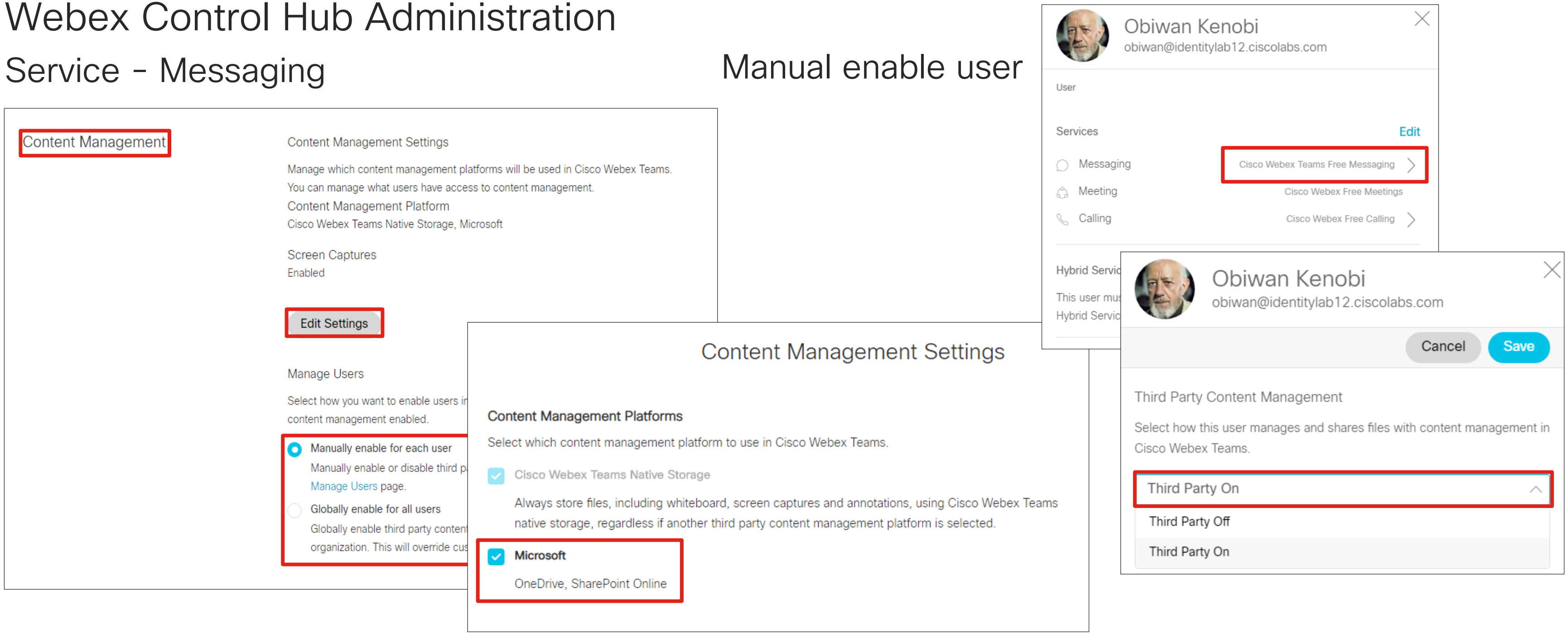
SharePoint Online/OneDrive for Business

Adding existing Enterprise Content Solution to Webex Teams

Webex Control Hub Administration

Service – Messaging

Manual enable user



Content Management

Content Management Settings

Manage which content management platforms will be used in Cisco Webex Teams.
You can manage what users have access to content management.

Content Management Platform
Cisco Webex Teams Native Storage, Microsoft

Screen Captures
Enabled

Edit Settings

Manage Users

Select how you want to enable users i
content management enabled.

● Manually enable for each user
Manually enable or disable third p
Manage Users page.

○ Globally enable for all users
Globally enable third party conten
organization. This will override cus

Content Management Settings

Content Management Platforms

Select which content management platform to use in Cisco Webex Teams.

☑ Cisco Webex Teams Native Storage

Always store files, including whiteboard, screen captures and annotations, using Cisco Webex Teams native storage, regardless if another third party content management platform is selected.

☑ Microsoft

OneDrive, SharePoint Online

Obiwan Kenobi
obiwan@identitylab12.ciscolabs.com

User

Services — Edit

Messaging	Cisco Webex Teams Free Messaging
Meeting	Cisco Webex Free Meetings
Calling	Cisco Webex Free Calling

Hybrid Servic
This user mu
Hybrid Servic

Obiwan Kenobi
obiwan@identitylab12.ciscolabs.com

Cancel — Save

Third Party Content Management

Select how this user manages and shares files with content management in Cisco Webex Teams.

Third Party On

- Third Party Off
- Third Party On

Webex Teams – Enterprise Content Management

SharePoint Online/OneDrive for Business

Office 365 Administration

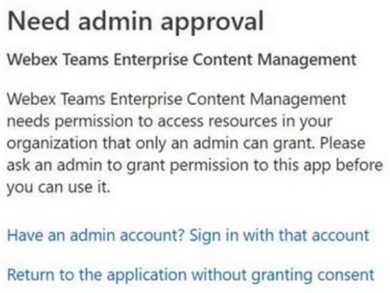
Administrators can chose to restrict certain functionalities in Office 365 which can cause the Webex Teams integration not to function properly

- Restricted access outside corporate network

  Requires users to be connected either to corporate or via VPN. With this policy in place users will get the error message: “*Your sign in was successful but does not meet the criteria to access this resource*.“

- Permissions for 3rd party applications

  By default, Azure AD tenants are configured to provide consent to third-party applications. When restricted by the administrator, an end user can’t sign in with Azure AD account in Webex Teams.



Need admin approval

Webex Teams Enterprise Content Management

Webex Teams Enterprise Content Management needs permission to access resources in your organization that only an admin can grant. Please ask an admin to grant permission to this app before you can use it.

Have an admin account? Sign in with that account

Return to the application without granting consent

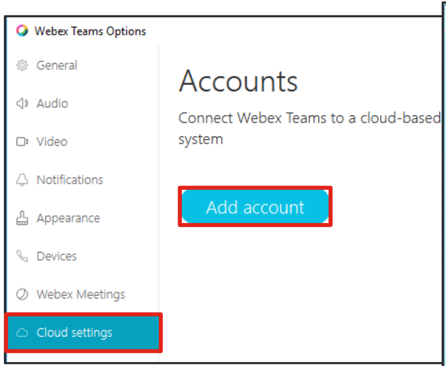
For details on how to administer the required permissions on Azure AD please check the following link
https://collaborationhelp.cisco.com/article/en-us/7501oi

Webex Teams – Enterprise Content Management

SharePoint Online/OneDrive for Business

Adding existing Enterprise Content Solution to Webex Teams

Webex Teams Client



Webex Teams Options

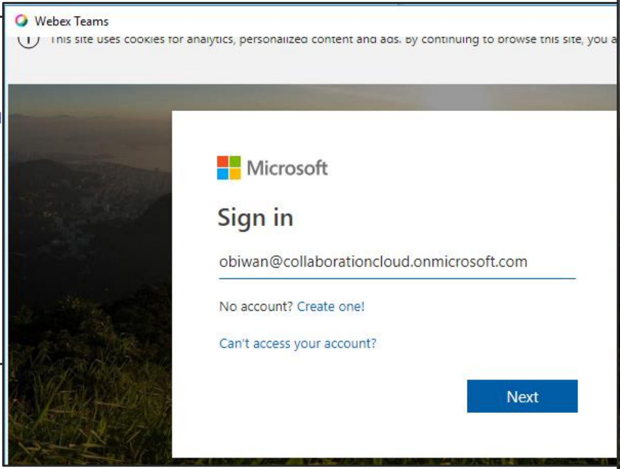
- General
- Audio
- Video
- Notifications
- Appearance
- Devices
- Webex Meetings
- Cloud settings

Accounts

Connect Webex Teams to a cloud-based system

Add account

New Cloud Settings



Webex Teams

This site uses cookies for analytics, personalized content and ads. By continuing to browse this site, you a

Microsoft

Sign in

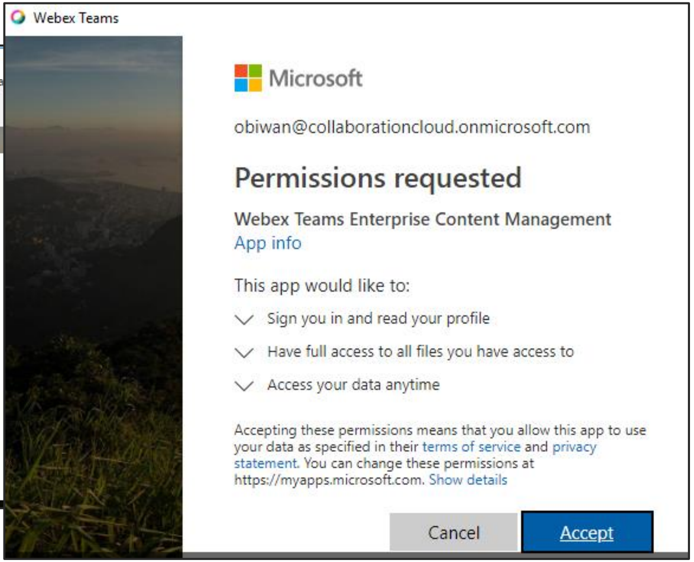
obiwan@collaborationcloud.onmicrosoft.com

No account? Create one!

Can't access your account?

Next

Login to Microsoft Office 365 will generate an OAuth Token for the user that is stored locally



Webex Teams

Microsoft

obiwan@collaborationcloud.onmicrosoft.com

Permissions requested

Webex Teams Enterprise Content Management

App info

This app would like to:

- Sign you in and read your profile
- Have full access to all files you have access to
- Access your data anytime

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Cancel Accept

Authorization for app integration
(can be pre-authorized for all users by Azure AD administrator, see reference on previous slide)

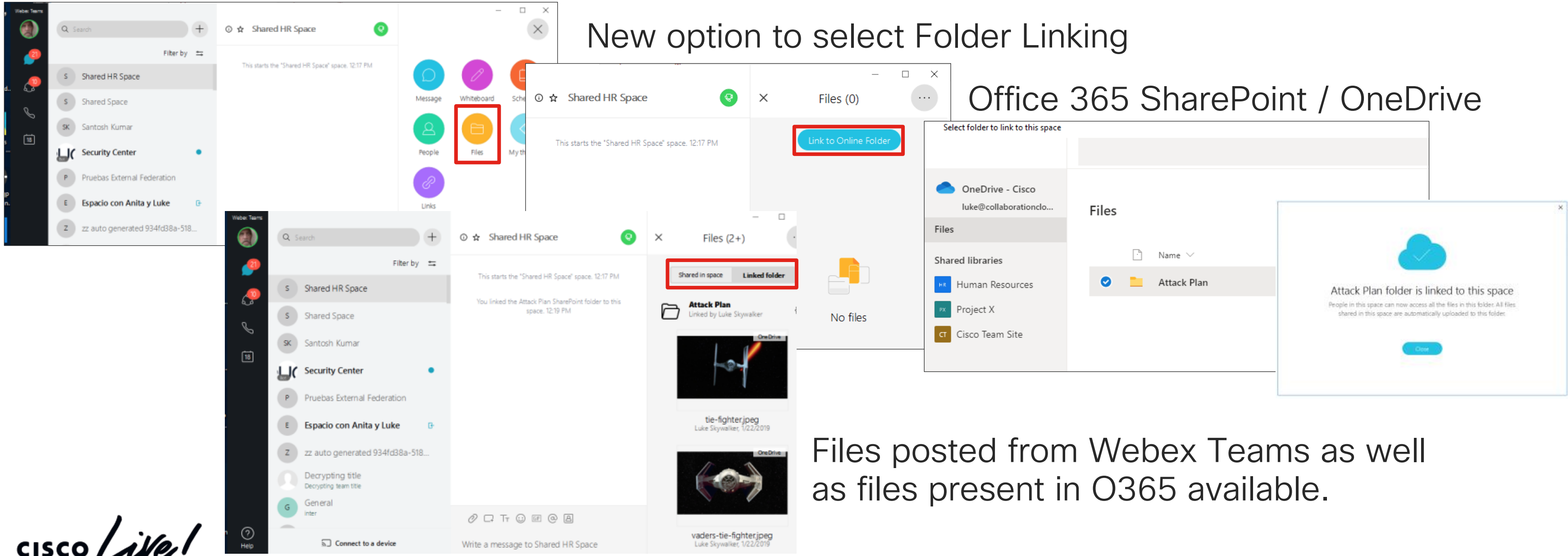
Webex Teams – Enterprise Content Management

SharePoint Online/OneDrive for Business

Linked Folders

Allows a complete content sync between Cisco Webex Teams Space and SharePoint Online / OneDrive for Business

New space created, select files activity


New option to select Folder Linking

Office 365 SharePoint / OneDrive

This starts the "Shared HR Space" space. 12:17 PM

You linked the Attack Plan SharePoint folder to this space. 12:19 PM

Select folder to link to this space

Attack Plan folder is linked to this space

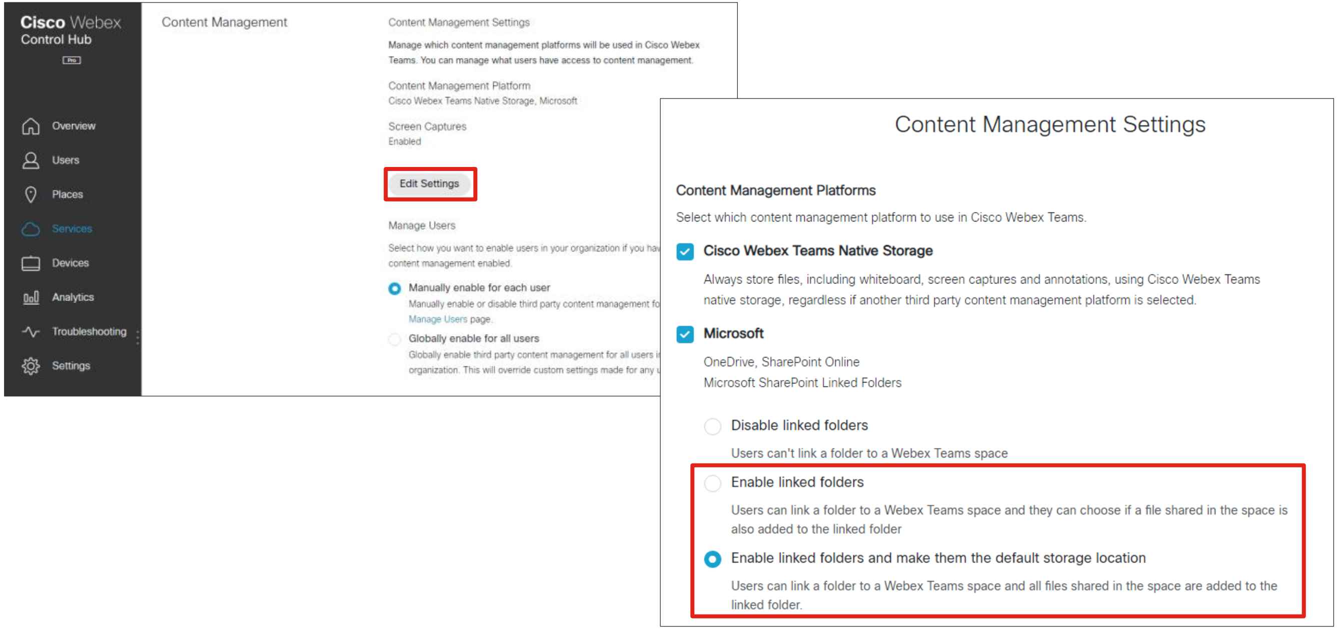
People in this space can now access all the files in this folder. All files shared in this space are automatically uploaded to this folder.

Files posted from Webex Teams as well as files present in O365 available.

Webex Teams – Enterprise Content Management

SharePoint Online/OneDrive for Business

Linked Folders – Administration



Content Management Settings

Manage which content management platforms will be used in Cisco Webex Teams. You can manage what users have access to content management.

Content Management Platform
Cisco Webex Teams Native Storage, Microsoft

Screen Captures
Enabled

Manage Users

Select how you want to enable users in your organization if you hav
content management enabled.

● Manually enable for each user
Manually enable or disable third party content management fo
Manage Users page.

○ Globally enable for all users
Globally enable third party content management for all users i
organization. This will override custom settings made for any u

Content Management Settings

Content Management Platforms

Select which content management platform to use in Cisco Webex Teams.

☑ **Cisco Webex Teams Native Storage**

Always store files, including whiteboard, screen captures and annotations, using Cisco Webex Teams native storage, regardless if another third party content management platform is selected.

☑ **Microsoft**

OneDrive, SharePoint Online
Microsoft SharePoint Linked Folders

○ Disable linked folders

Users can't link a folder to a Webex Teams space

○ Enable linked folders

Users can link a folder to a Webex Teams space and they can choose if a file shared in the space is also added to the linked folder

● Enable linked folders and make them the default storage location

Users can link a folder to a Webex Teams space and all files shared in the space are added to the linked folder.

Other Enterprise Security Capabilities

Webex Security Offers

Webex Control Hub (Existing)

- Included in all Webex subscriptions
- Administration: Provisioning and management capabilities for all Webex services
- Security: E2E encryption
- Compliance: eDiscovery, CASB integration for last 90 days data
- Analytics: 90 days reports

IT Pro Pack (Existing)

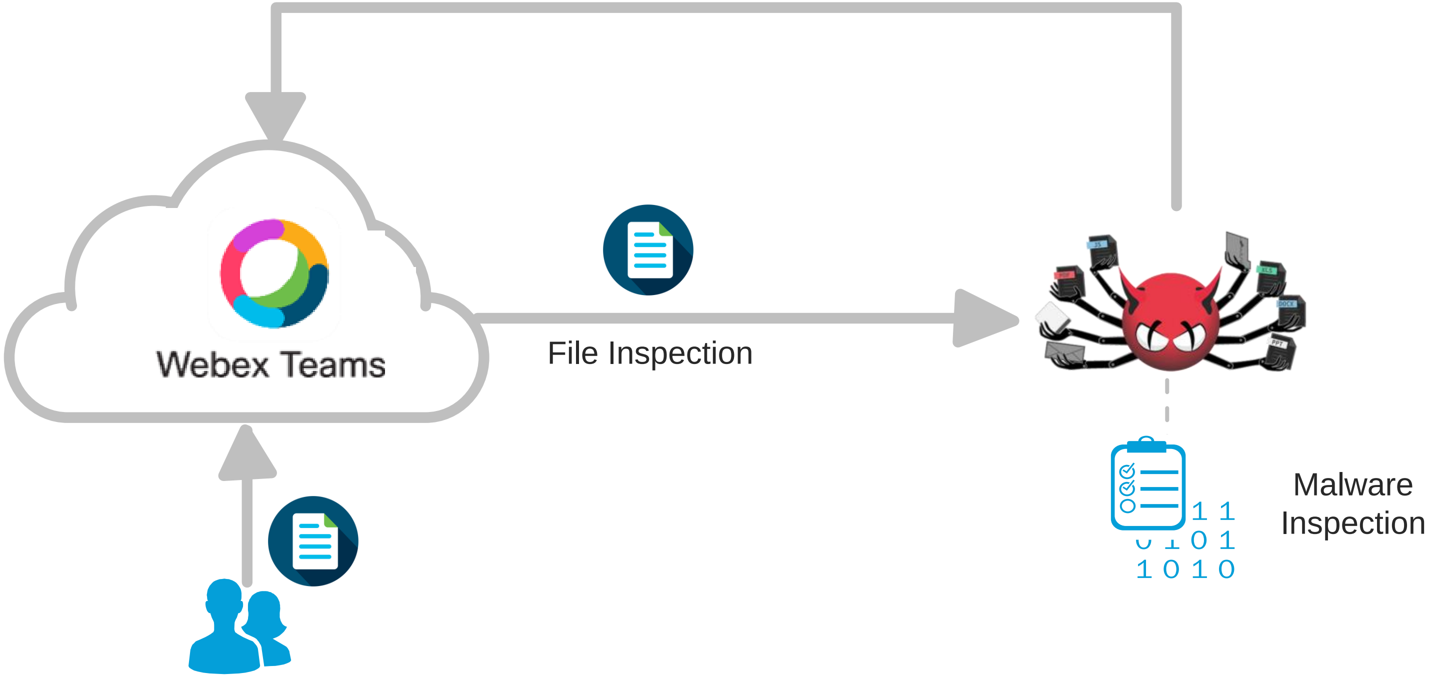
- Included in Enterprise and Active Users Flex SKUs
- Security: HDS, controls like block file share, external communication, integrations whitelisting
- Compliance: Legal Hold, unlimited data extraction for eDiscovery
- Analytics: One year reporting

Extended Security Pack (New)

- Add-on for all Flex SKUs
- Security: Anti-malware scanning for files using Cisco Talos ClamAV
- Compliance: Data Loss Prevention using full functionality Cloudlock

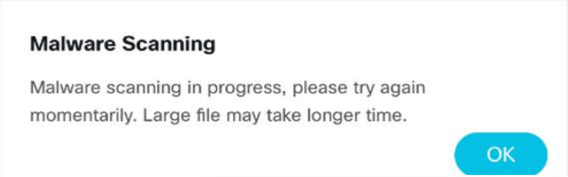
Webex Teams and Cisco Talos ClamAV Integration

Malware Protection



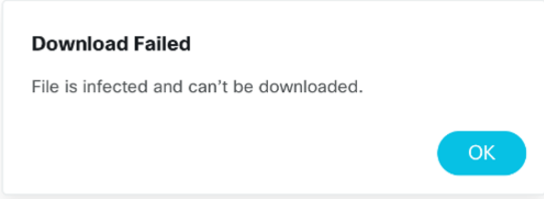
What to expect ?

- In-line Anti-virus and malware scanning of files and blocking infected files
- Malware and phishing scanning of URL’s and blocking unsafe URL’s
- Administrator control to turn-off and turn-on scanning
- Administrator visibility into Scan history



Malware Scanning

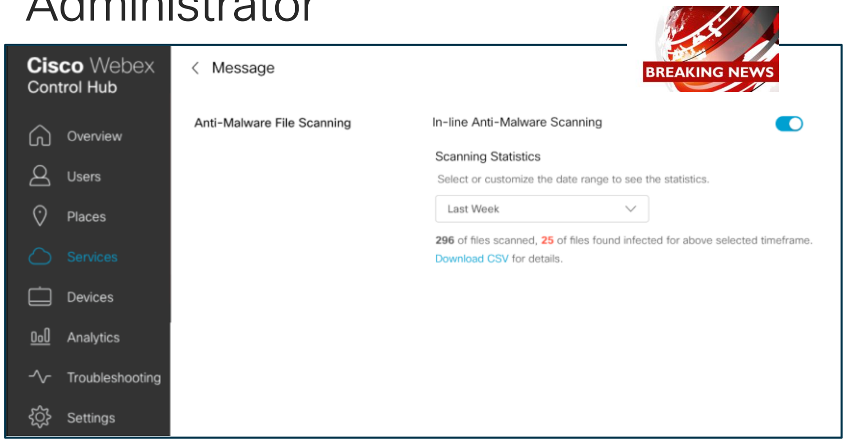
Malware scanning in progress, please try again momentarily. Large file may take longer time.



Download Failed

File is infected and can’t be downloaded.

Administrator



Anti-Malware File Scanning

In-line Anti-Malware Scanning

Scanning Statistics

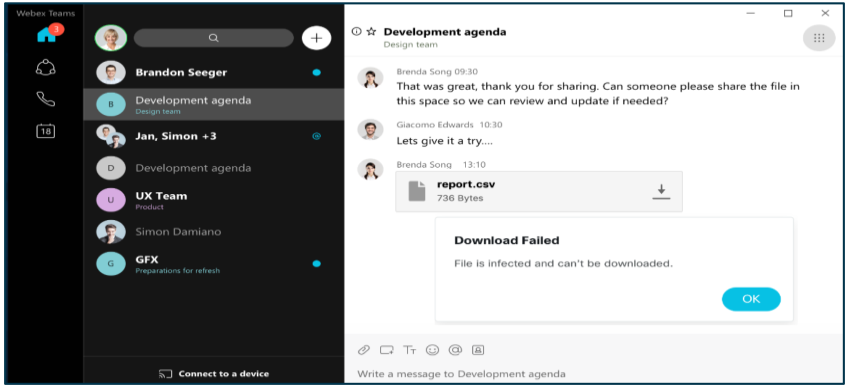
Select or customize the date range to see the statistics.

Last Week

296 of files scanned, 25 of files found infected for above selected timeframe.

Download CSV for details.

User



Brenda Song 09:30
That was great, thank you for sharing. Can someone please share the file in this space so we can review and update if needed?

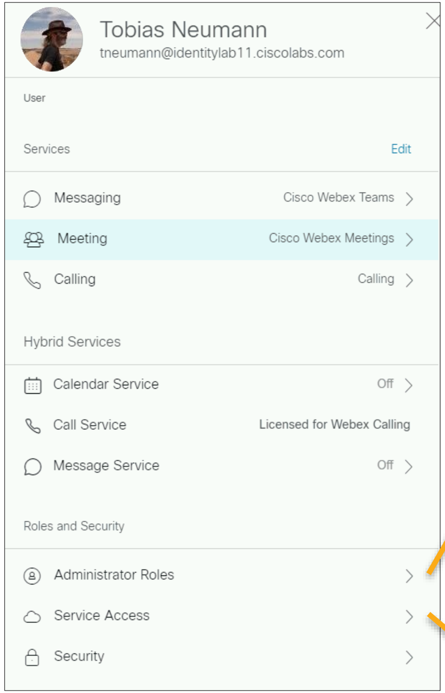
Giacomo Edwards 10:30
Lets give it a try....

Brenda Song 13:10
report.csv
736 Bytes

Download Failed

File is infected and can’t be downloaded.

Cisco Webex Pro Pack – Security Capabilities



Tobias Neumann
tneumann@identitylab11.ciscolabs.com

User

Services Edit

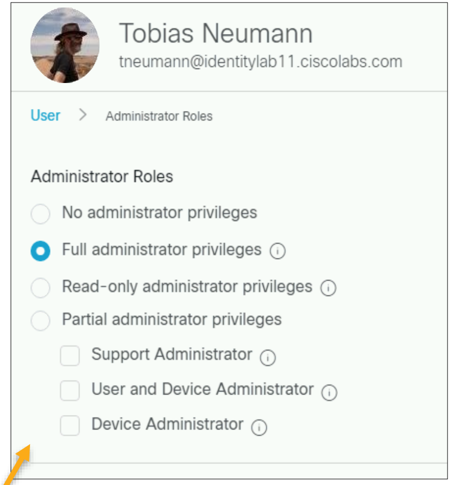
- Messaging — Cisco Webex Teams >
- Meeting — Cisco Webex Meetings >
- Calling — Calling >

Hybrid Services

- Calendar Service — Off >
- Call Service — Licensed for Webex Calling
- Message Service — Off >

Roles and Security

- Administrator Roles >
- Service Access >
- Security >

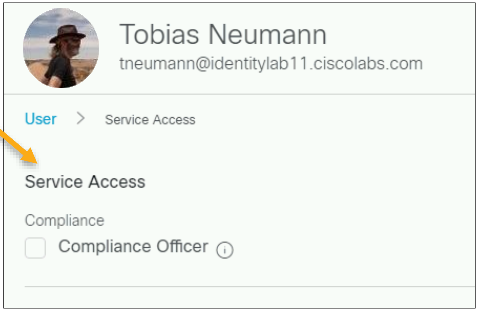


Tobias Neumann
tneumann@identitylab11.ciscolabs.com

User > Administrator Roles

Administrator Roles

○ No administrator privileges
● Full administrator privileges ⓘ
○ Read-only administrator privileges ⓘ
○ Partial administrator privileges
□ Support Administrator ⓘ
□ User and Device Administrator ⓘ
□ Device Administrator ⓘ



Tobias Neumann
tneumann@identitylab11.ciscolabs.com

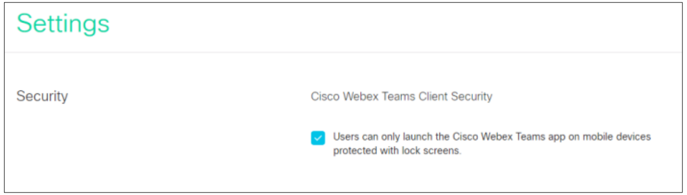
User > Service Access

Service Access

Compliance
□ Compliance Officer ⓘ

Manage User Roles and Service Access

Mobile PIN enforcement

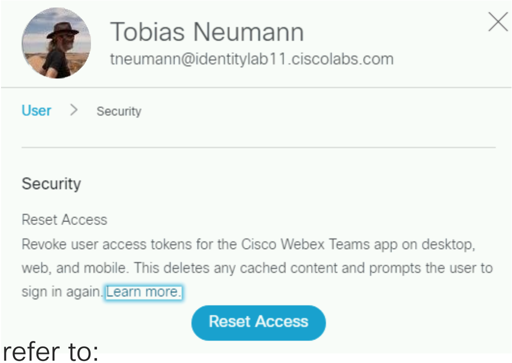


Settings

Security — Cisco Webex Teams Client Security

☑ Users can only launch the Cisco Webex Teams app on mobile devices protected with lock screens.

Reset Access and Remote Wipe



Tobias Neumann
tneumann@identitylab11.ciscolabs.com

User > Security

Security

Reset Access

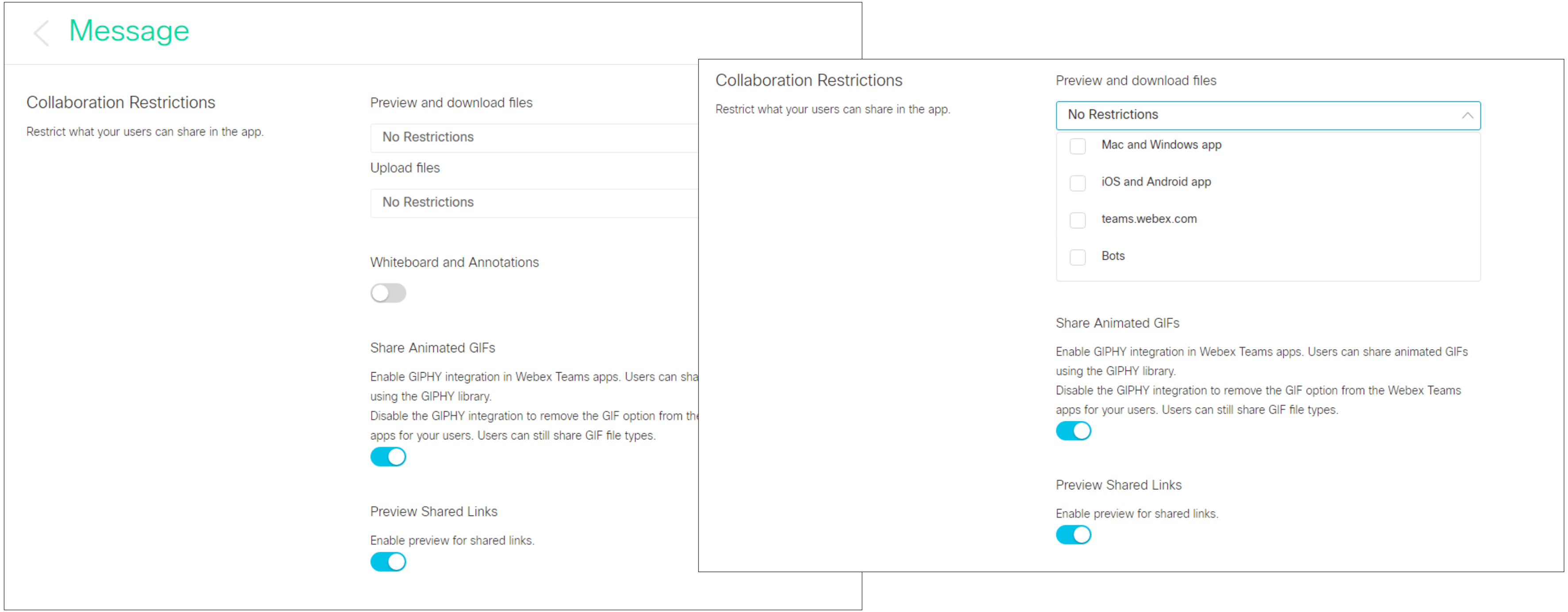
Revoke user access tokens for the Cisco Webex Teams app on desktop, web, and mobile. This deletes any cached content and prompts the user to sign in again. Learn more.

Reset Access

For detailed list of privileges associated with each role please refer to:
https://collaborationhelp.cisco.com/article/en-us/x58jl3

File Sharing Controls

Granular per device/application file and content controls



Message

Collaboration Restrictions

Restrict what your users can share in the app.

Preview and download files

No Restrictions

Upload files

No Restrictions

Whiteboard and Annotations

Share Animated GIFs

Enable GIPHY integration in Webex Teams apps. Users can sha
using the GIPHY library.
Disable the GIPHY integration to remove the GIF option from th
apps for your users. Users can still share GIF file types.

Preview Shared Links

Enable preview for shared links.

Collaboration Restrictions

Restrict what your users can share in the app.

Preview and download files

No Restrictions

- □ Mac and Windows app
- □ iOS and Android app
- □ teams.webex.com
- □ Bots

Share Animated GIFs

Enable GIPHY integration in Webex Teams apps. Users can share animated GIFs using the GIPHY library.
Disable the GIPHY integration to remove the GIF option from the Webex Teams apps for your users. Users can still share GIF file types.

Preview Shared Links

Enable preview for shared links.

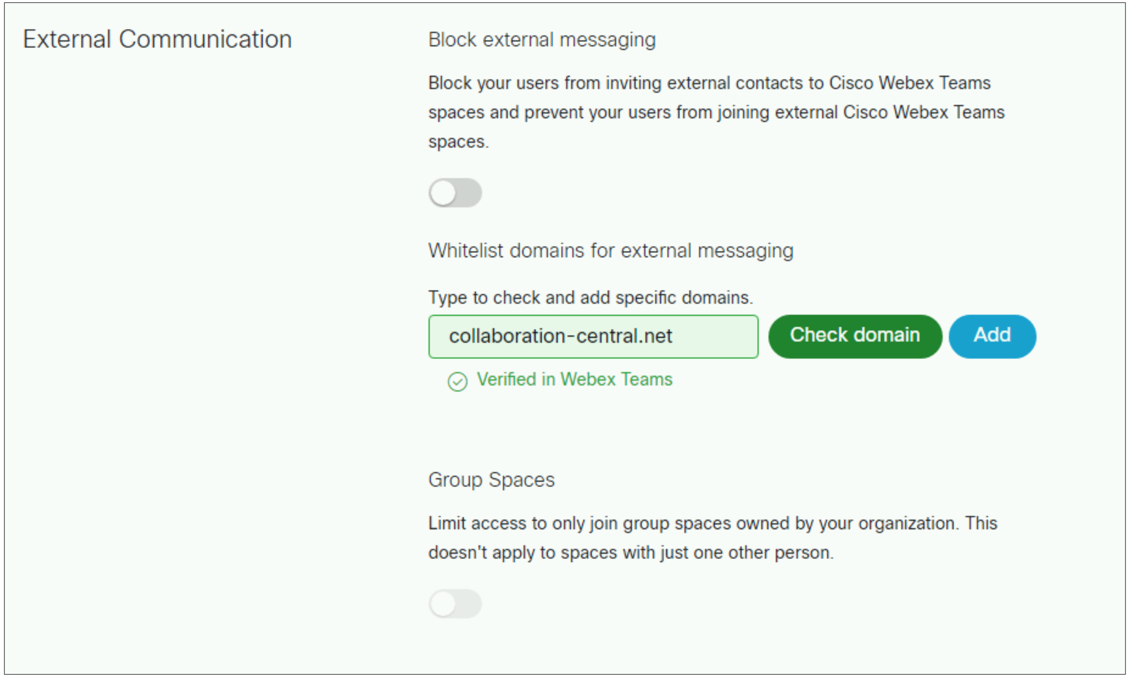
Blocking Messaging to other companies

Future

Granular controls for External Communications

Domain Whitelisting

Limit external participation to spaces owned by organization



External Communication

Block external messaging

Block your users from inviting external contacts to Cisco Webex Teams spaces and prevent your users from joining external Cisco Webex Teams spaces.

Whitelist domains for external messaging

Type to check and add specific domains.

collaboration-central.net

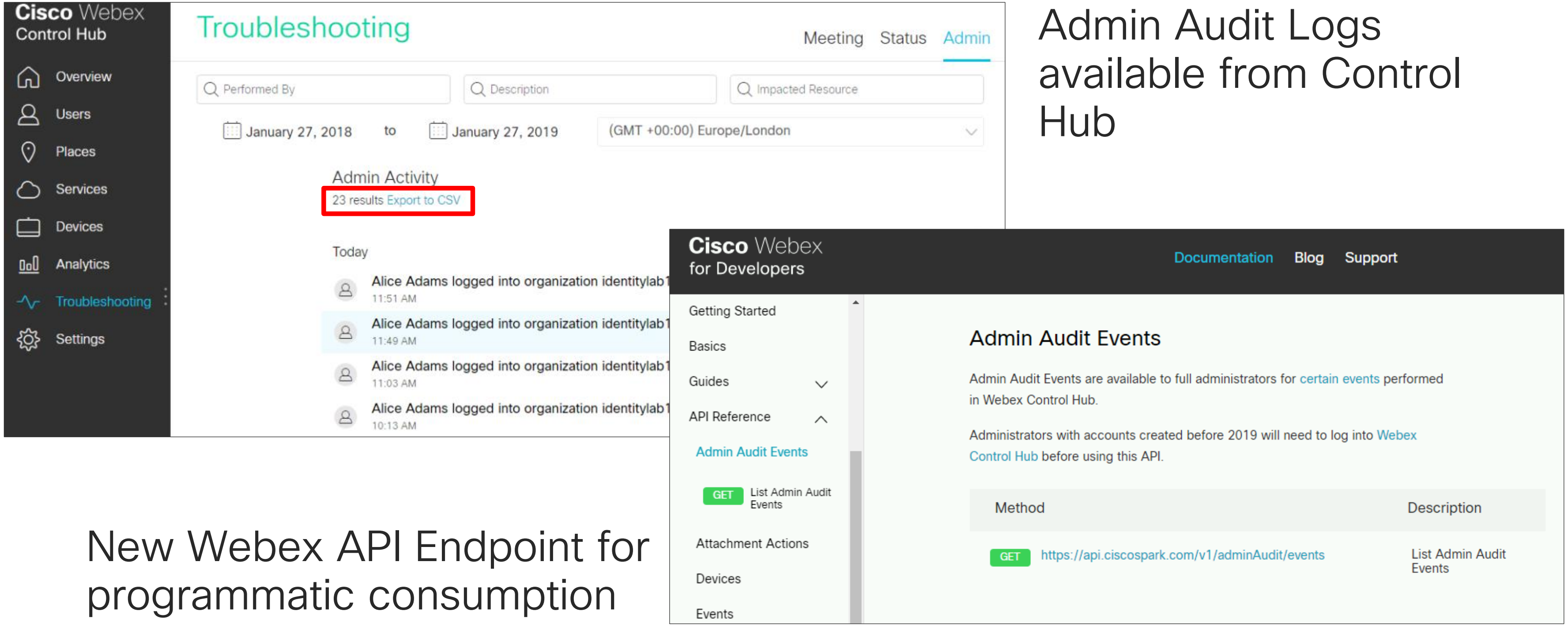
✓ Verified in Webex Teams

Group Spaces

Limit access to only join group spaces owned by your organization. This doesn't apply to spaces with just one other person.

Admin Audit Logging

Admin Audit Logs available from Control Hub



Troubleshooting

January 27, 2018 to January 27, 2019

(GMT +00:00) Europe/London

Admin Activity

23 results Export to CSV

Today

Alice Adams logged into organization identitylab1
11:51 AM

Alice Adams logged into organization identitylab1
11:49 AM

Alice Adams logged into organization identitylab1
11:03 AM

Alice Adams logged into organization identitylab1
10:13 AM

Admin Audit Events

Admin Audit Events are available to full administrators for certain events performed in Webex Control Hub.

Administrators with accounts created before 2019 will need to log into Webex Control Hub before using this API.

Method	Description
GET https://api.ciscospark.com/v1/adminAudit/events	List Admin Audit Events

New Webex API Endpoint for programmatic consumption

https://developer.webex.com/docs/api/v1/admin-audit-events

Admin Audit Log Data Dictionary
https://help.webex.com/en-us/n3b0w6x/Audit-Events-in-Cisco-Webex-Control-Hub

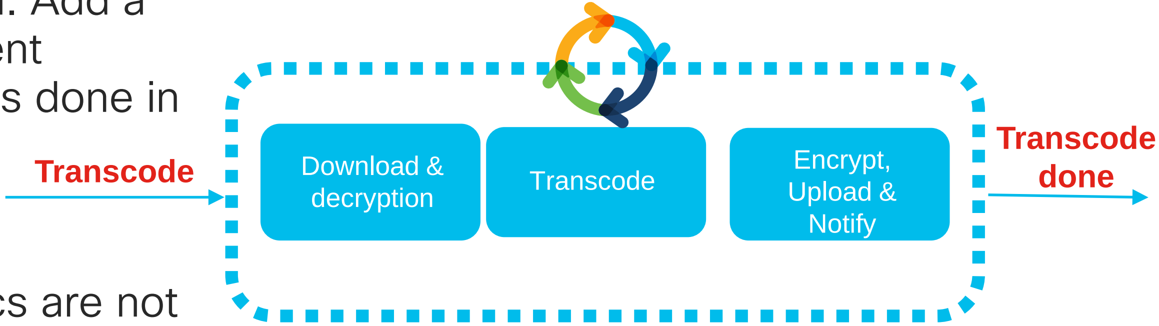
Document Transcoding in Webex Cloud

What:

- Move transcoding to Webex Cloud. Add a new transcode engine, so document transcoding and preview creation is done in Cisco Cloud

Why:

- Adds tight security process so docs are not sent to 3rd party Cloud service
- Improves load-time and performance
- Better quality previews and support on larger screen Webex Boards



Document file types: .doc, .docx, .gif, .jpeg, .pdf, .png, .ppt, .pptx, .svg, .xls, and .xlsx

Maximum 150 pages and/or 200 MB file size

Customers can open support ticket to turn off transcoding for security reasons.

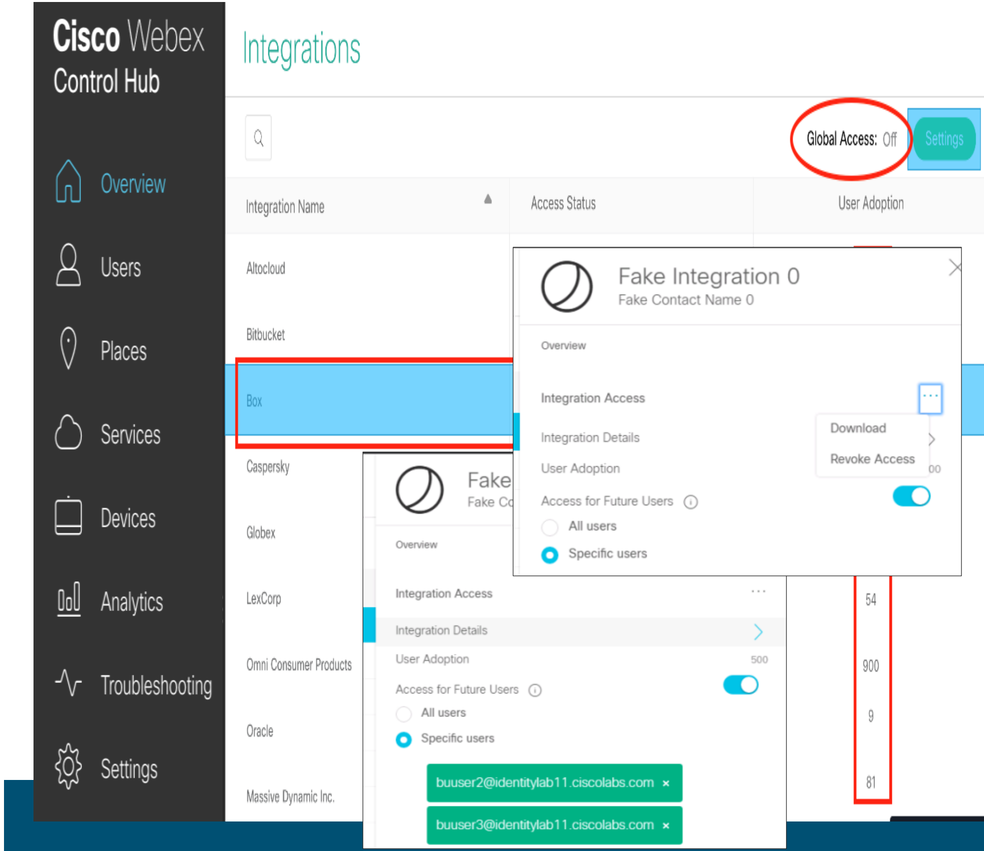
Integrations Management

What:

- Visibility of integrations available to customer’s users.
- Visibility of adoption of integrations by their users.
- Capability to allow/deny specific integrations or change the org-wide policy

Why:

- Not all integrations and bots are same.
- Customers worry about unknown privileges to non-human accounts or integrations.
- Malware and data leak concerns through unknown/unverified 3rd party code.



Cisco Webex Control Hub

Overview
Users
Places
Services
Devices
Analytics
Troubleshooting
Settings

Integrations

Global Access: Off
Settings

Integration Name | Access Status | User Adoption

Altocloud
Bitbucket
Box
Caspersky
Globex
LexCorp 54
Omni Consumer Products 900
Oracle 9
Massive Dynamic Inc. 81

Fake Integration 0
Fake Contact Name 0

Overview

Integration Access
Download
Revoke Access

Integration Details
User Adoption
Access for Future Users
○ All users
● Specific users

Fake
Fake Co

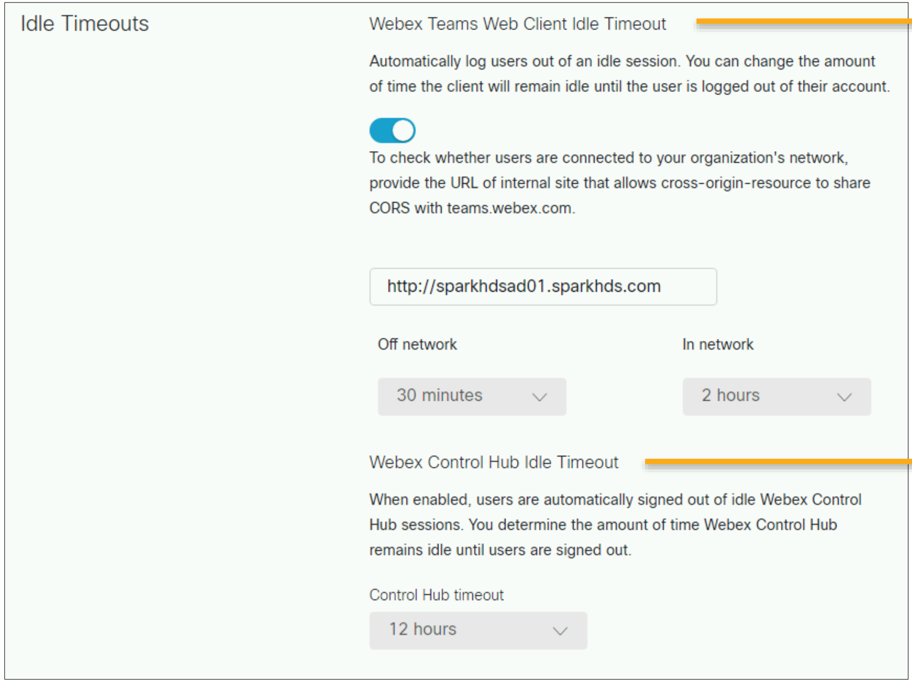
Overview

Integration Access
Integration Details
User Adoption 500
Access for Future Users
○ All users
● Specific users

buuser2@identitylab11.ciscolabs.com ×
buuser3@identitylab11.ciscolabs.com ×

cisco Live!

Idle Timeouts



Idle Timeouts

Webex Teams Web Client Idle Timeout

Automatically log users out of an idle session. You can change the amount of time the client will remain idle until the user is logged out of their account.

To check whether users are connected to your organization's network, provide the URL of internal site that allows cross-origin-resource to share CORS with teams.webex.com.

http://sparkhdsad01.sparkhds.com

Off network: 30 minutes

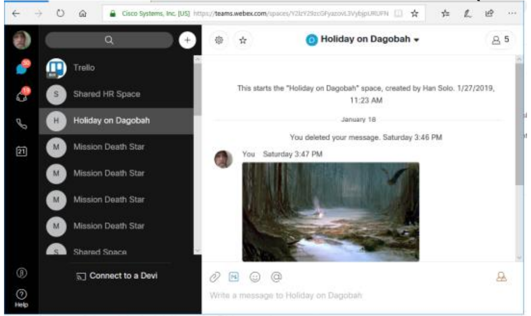
In network: 2 hours

Webex Control Hub Idle Timeout

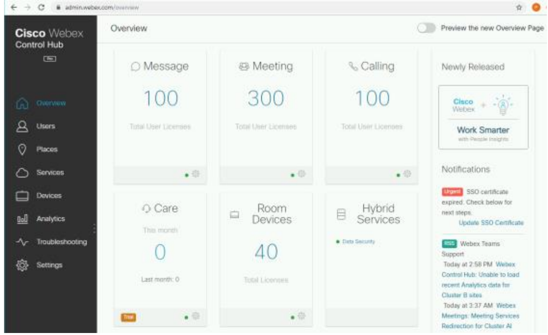
When enabled, users are automatically signed out of idle Webex Control Hub sessions. You determine the amount of time Webex Control Hub remains idle until users are signed out.

Control Hub timeout: 12 hours

Webex Teams Web Client (Browser)

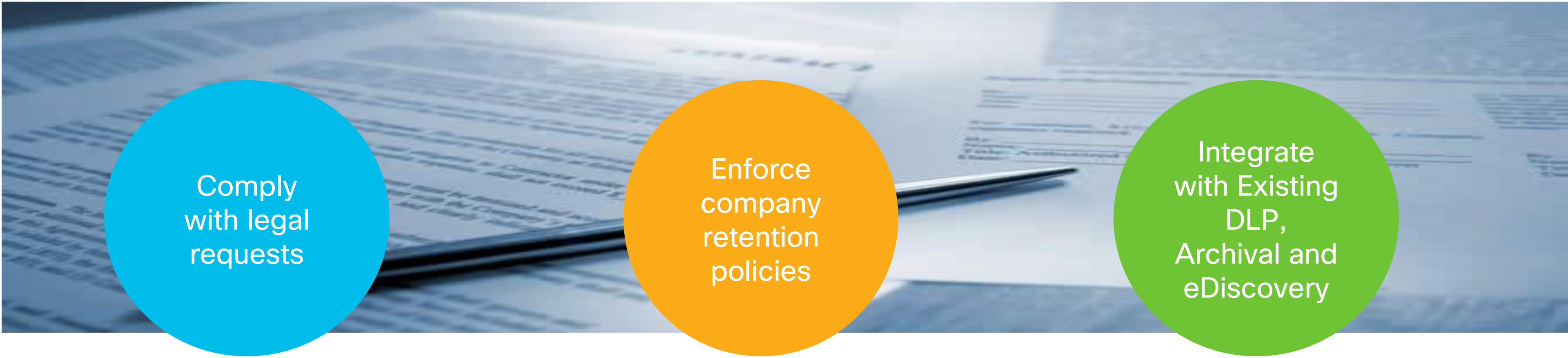


Webex Control Hub



Cisco Webex Teams Compliance

Enforce company policies



Comply with legal requests

Enforce company retention policies

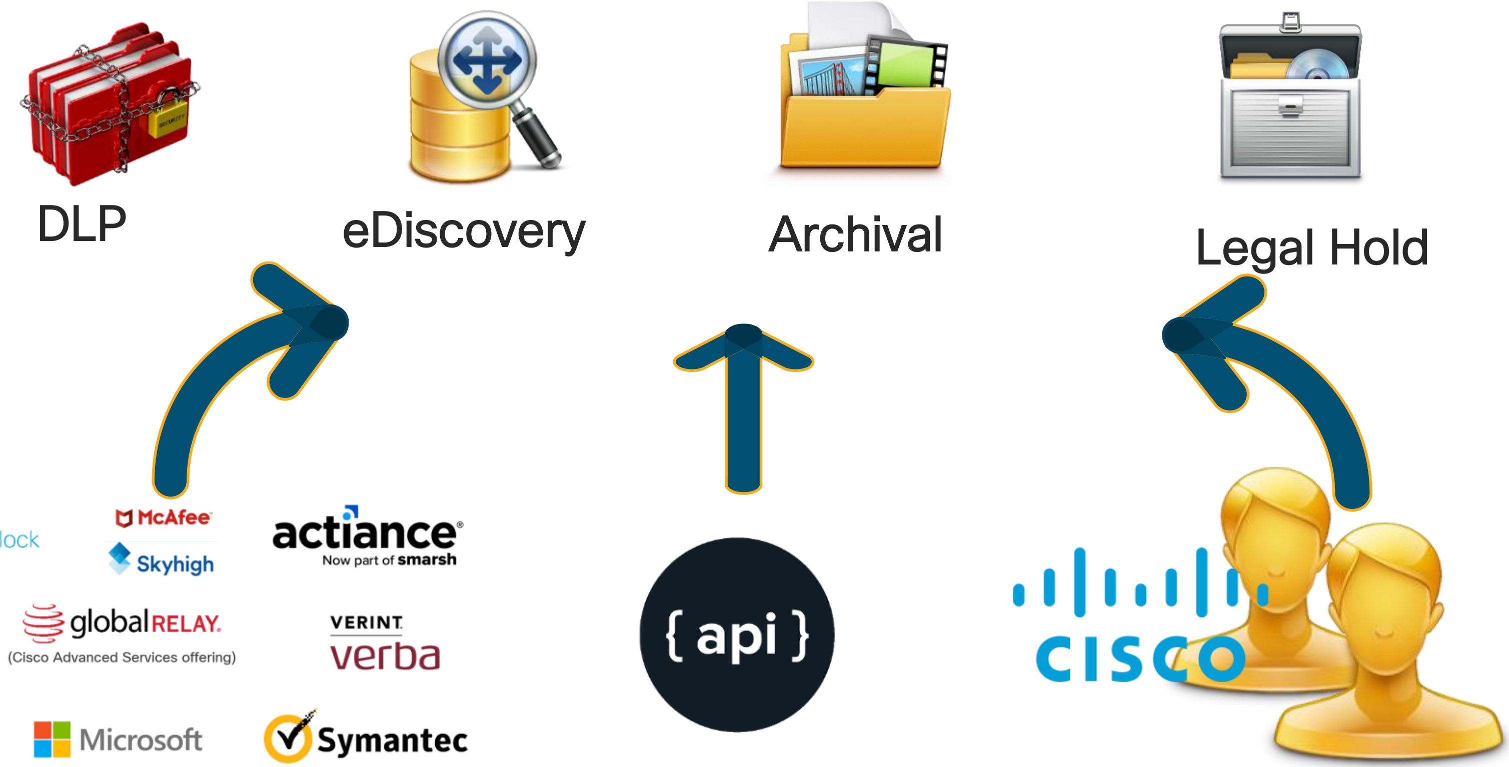
Integrate with Existing DLP, Archival and eDiscovery

eDiscovery Search and Extraction

Flexible Retention Policy Administration

Events API

Compliance Solution Strategy



DLP

eDiscovery

Archival

Legal Hold

Cisco Cloudlock

McAfee

Skyhigh

actiance
Now part of smarsh

paloalto NETWORKS

globalRELAY
(Cisco Advanced Services offering)

VERINT
verba

bitglass

Microsoft

Symantec

netskope

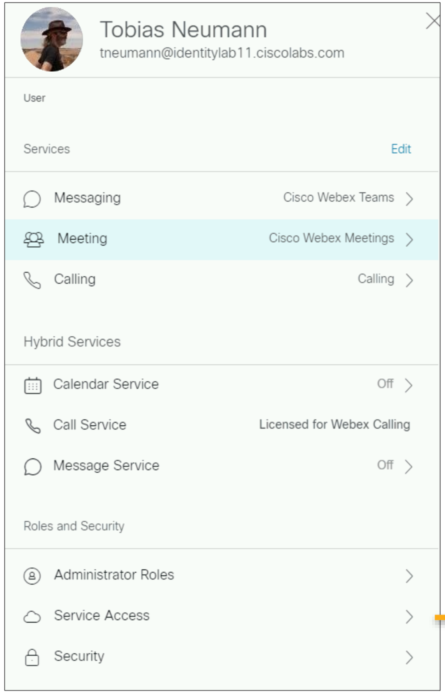
AGAT

THETALAKE

{ api }

cisco

Cisco Webex Compliance Officer Role



Tobias Neumann
tneumann@identitylab11.ciscolabs.com

User

Services Edit

Messaging	Cisco Webex Teams
Meeting	Cisco Webex Meetings
Calling	Calling

Hybrid Services

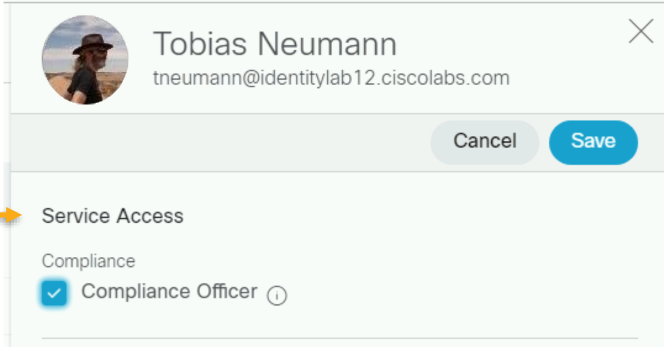
Calendar Service	Off
Call Service	Licensed for Webex Calling
Message Service	Off

Roles and Security

- Administrator Roles
- Service Access
- Security

Full Administrator privileges required to assign Compliance Officer role

Full Administrator can not assign role to self



Tobias Neumann
tneumann@identitylab12.ciscolabs.com

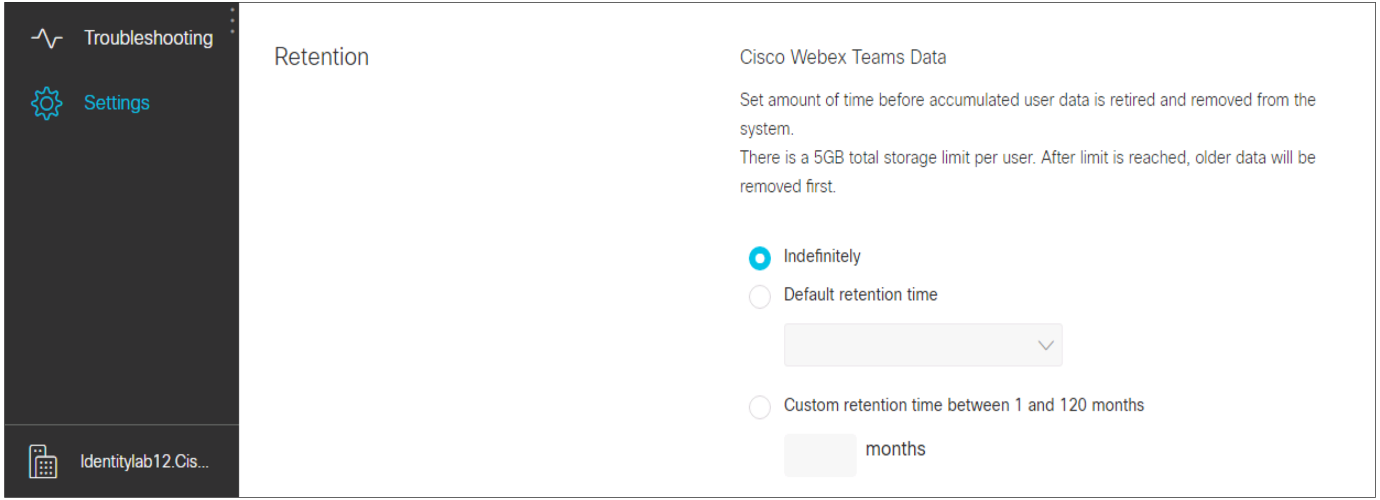
Service Access

Compliance

☑ Compliance Officer

Retention Policies

- Purge
  - Activities
  - Messages
  - Files
- Default: Indefinite subject to storage limits
- Content irretrievable

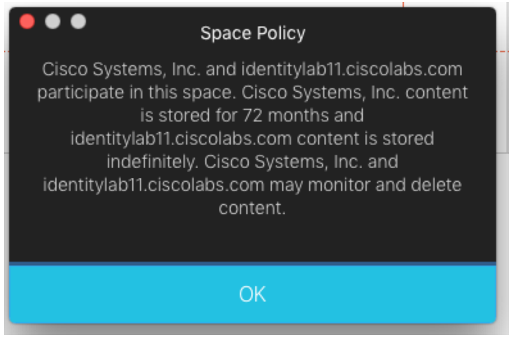


Retention

Cisco Webex Teams Data

Set amount of time before accumulated user data is retired and removed from the system.
There is a 5GB total storage limit per user. After limit is reached, older data will be removed first.

● Indefinitely
○ Default retention time
○ Custom retention time between 1 and 120 months
months



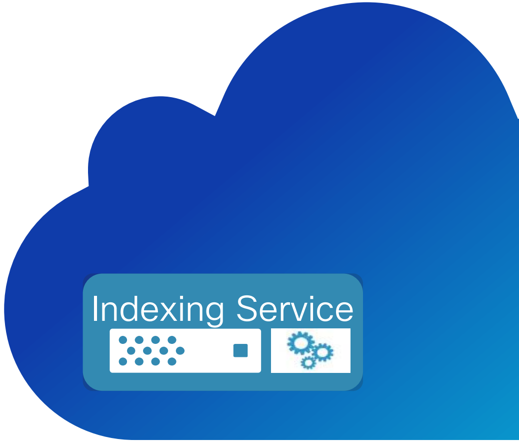
Space Policy

Cisco Systems, Inc. and identitylab11.ciscolabs.com participate in this space. Cisco Systems, Inc. content is stored for 72 months and identitylab11.ciscolabs.com content is stored indefinitely. Cisco Systems, Inc. and identitylab11.ciscolabs.com may monitor and delete content.

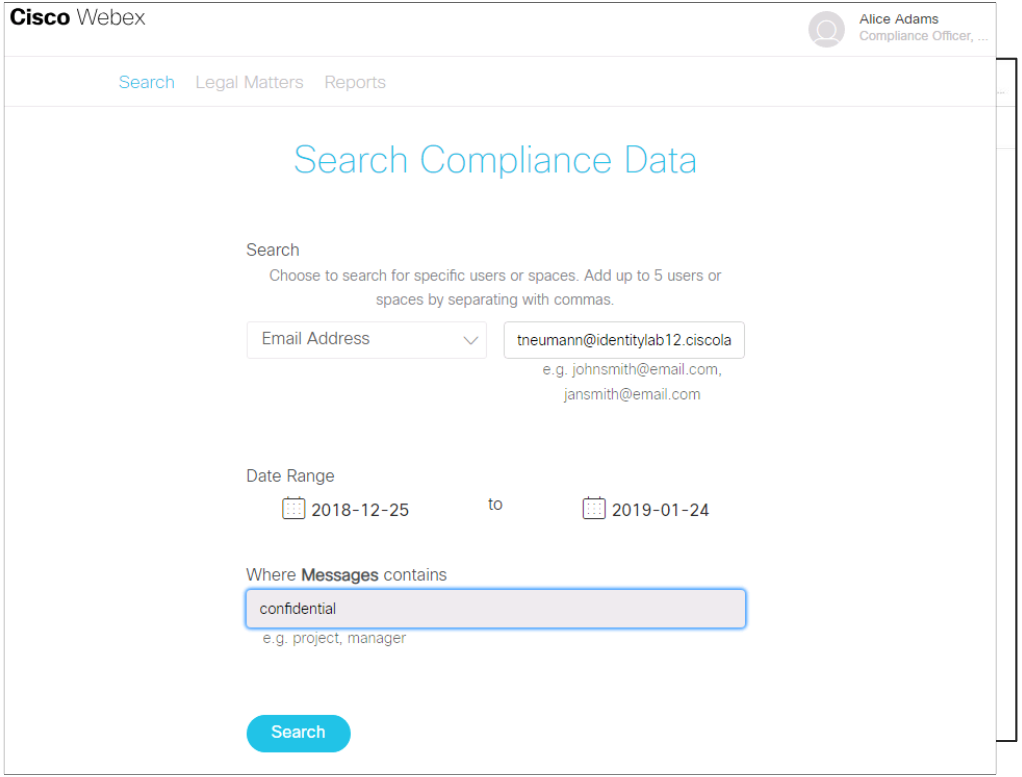
Enterprise Compliance – eDiscovery Reports

eDiscovery reports console supports investigating DLP and other compliance events with speed and accuracy

- Meet HR, GRC & Legal compliance mandates
- Only authorized members of the legal, HR and GRC teams can investigate events
- Will allow to export report to eDiscovery products



eDiscovery Search and Extraction



Search Compliance Data

Search

Choose to search for specific users or spaces. Add up to 5 users or spaces by separating with commas.

Email Address: tneumann@identitylab12.ciscola

e.g. johnsmith@email.com, jansmith@email.com

Date Range

2018-12-25 to 2019-01-24

Where **Messages** contains

confidential

e.g. project, manager

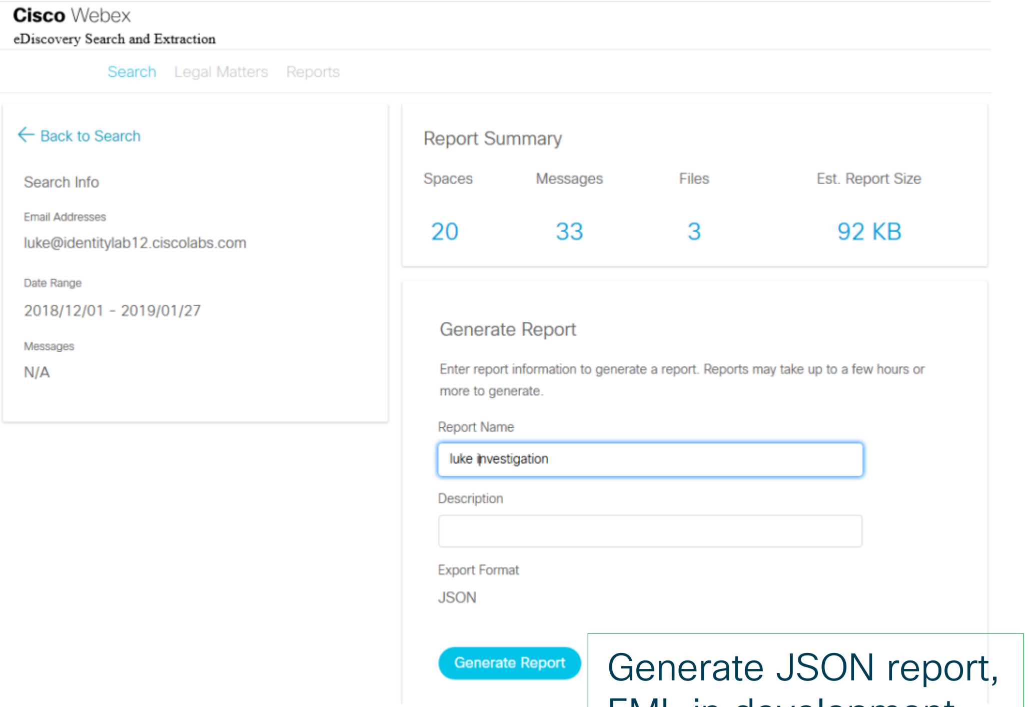
Extension of Cisco Spark Control Hub

Designed for Compliance Officer

Search on email ID, space ID, keywords

Webex Teams base offer
Any time period in Pro Pack for Cisco Webex Control Hub

eDiscovery Information Console



Cisco Webex
eDiscovery Search and Extraction

Search Legal Matters Reports

← Back to Search

Search Info

Email Addresses
luke@identitylab12.ciscolabs.com

Date Range
2018/12/01 - 2019/01/27

Messages
N/A

Report Summary

Spaces	Messages	Files	Est. Report Size
20	33	3	92 KB

Generate Report

Enter report information to generate a report. Reports may take up to a few hours or more to generate.

Report Name
luke investigation

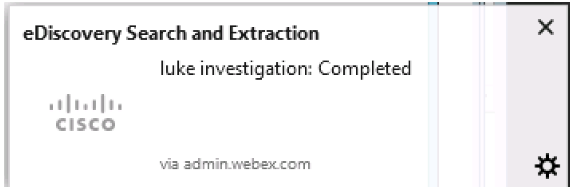
Description

Export Format
JSON

Generate Report

Generate JSON report, EML in development

Notification after report generation has completed. This might take a little …



eDiscovery Search and Extraction

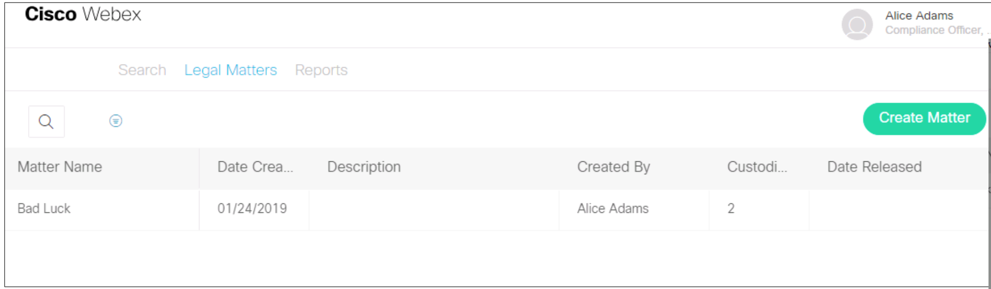
luke investigation: Completed

via admin.webex.com

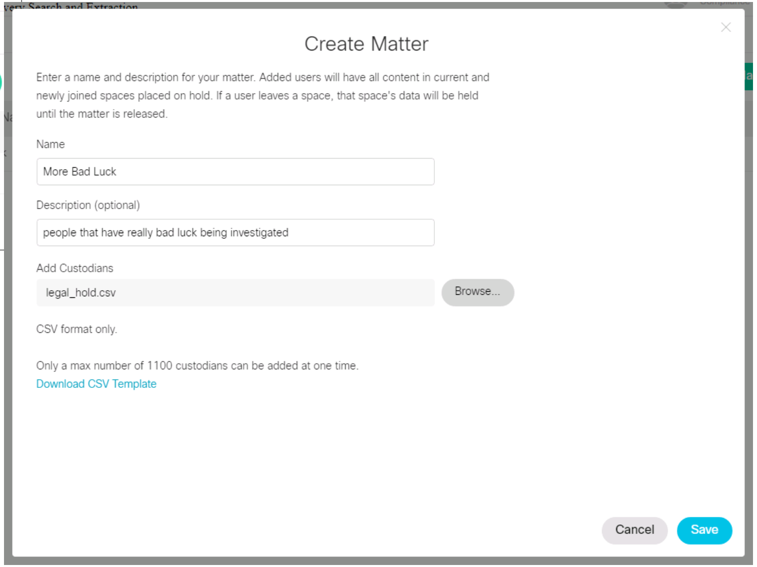
Legal Hold

Compliance Officer can create Legal Hold Matter

- Content of users flagged for legal hold will be preserved
- Retention Policy does not apply for content under legal hold



Matter Name	Date Crea...	Description	Created By	Custodi...	Date Released
Bad Luck	01/24/2019		Alice Adams	2	



Create Matter

Enter a name and description for your matter. Added users will have all content in current and newly joined spaces placed on hold. If a user leaves a space, that space's data will be held until the matter is released.

Name: More Bad Luck

Description (optional): people that have really bad luck being investigated

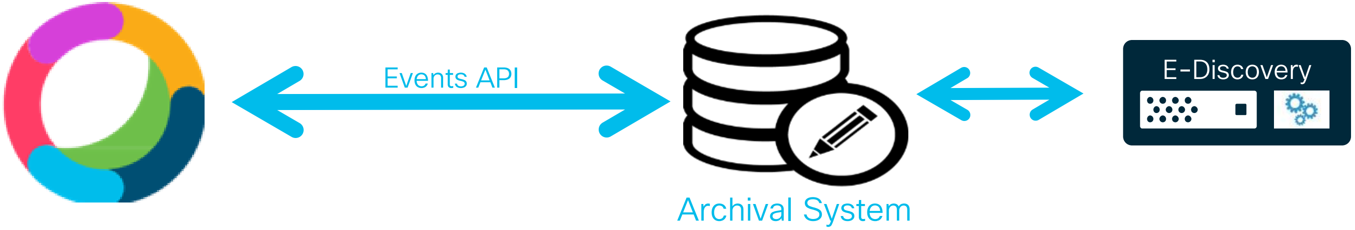
Add Custodians: legal_hold.csv

CSV format only.

Only a max number of 1100 custodians can be added at one time.

Download CSV Template

Archival Strategy

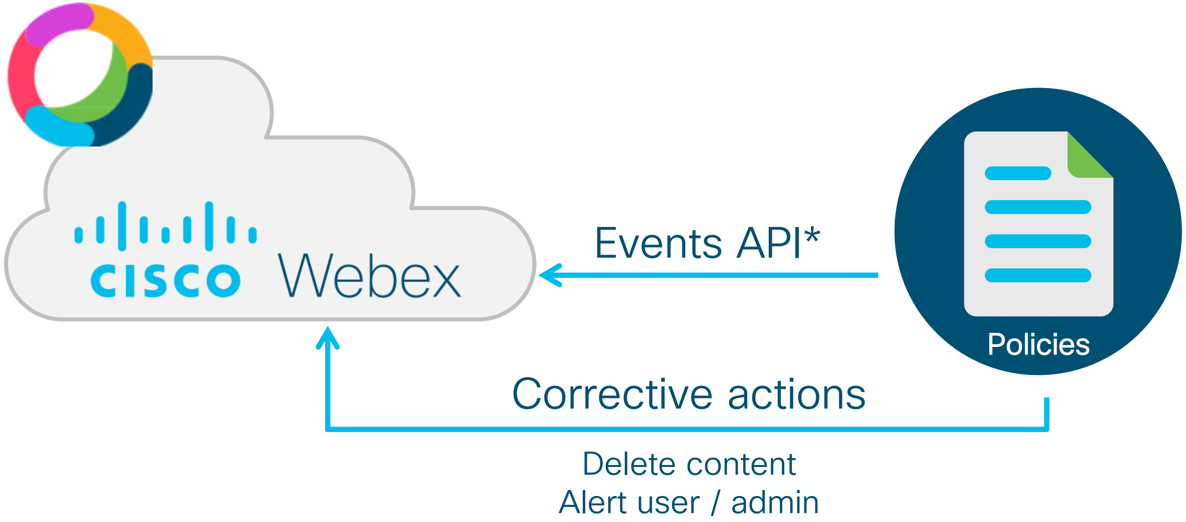


- **DIY:** Use favorite SI or self integrate Events API with Archival software
- **Out-of-the-box Solution:** Integrations with Archival partners e.g. Actiance
- **E2E Custom Solution:** Cisco Advanced Services software packages & services

- Benefits
  - Sophisticated eDiscovery
  - Legal Hold
  - Retention policies based on groups

Events API

for Data Loss Prevention, Archival, eDiscovery



Integrations

Cisco Cloudlock

globalRELAY

actiance

Symantec

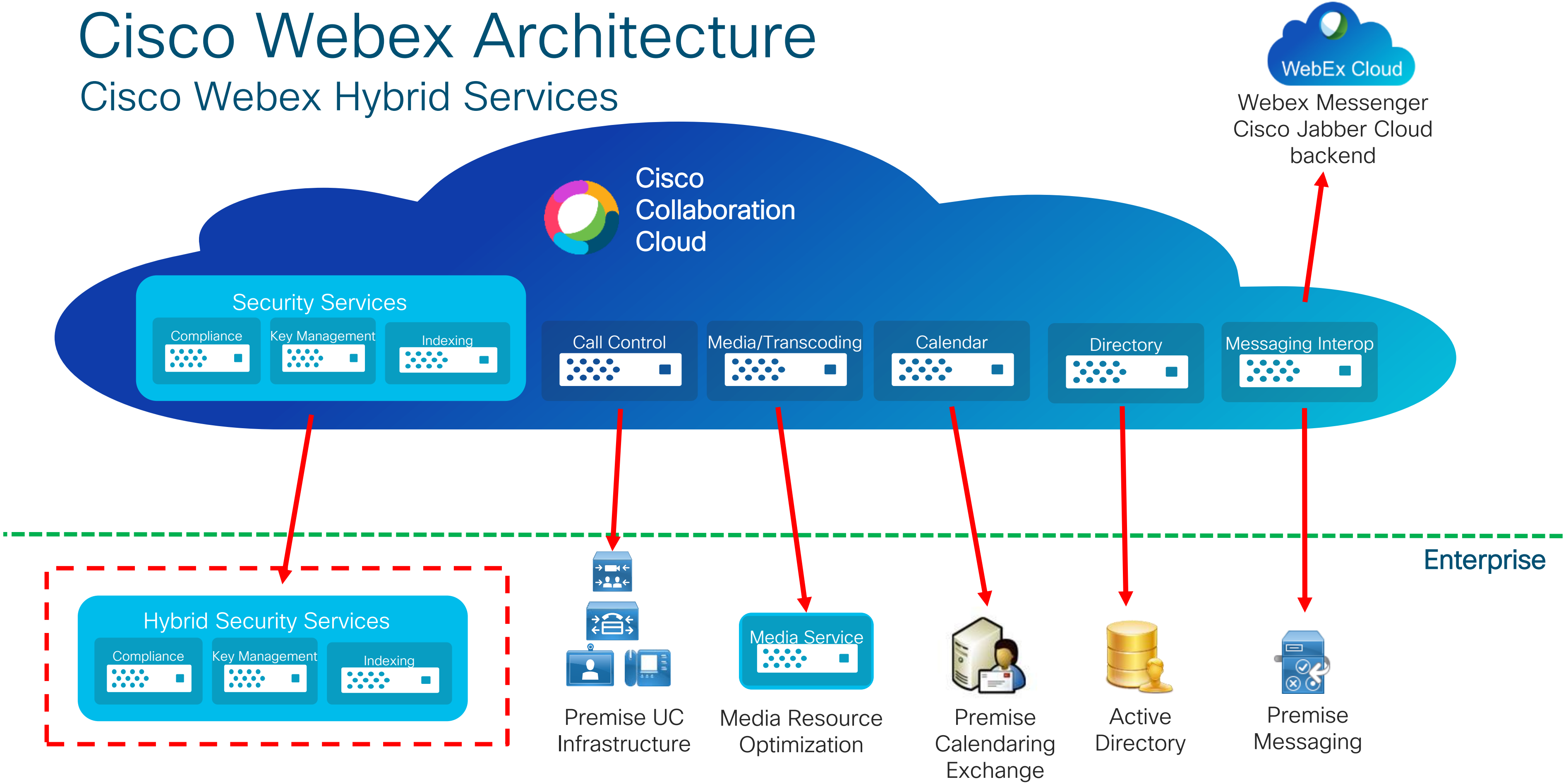
Skyhigh

*API enables polling for events and content that enables organizations to monitor and correct user behavior, preventing the loss of sensitive data

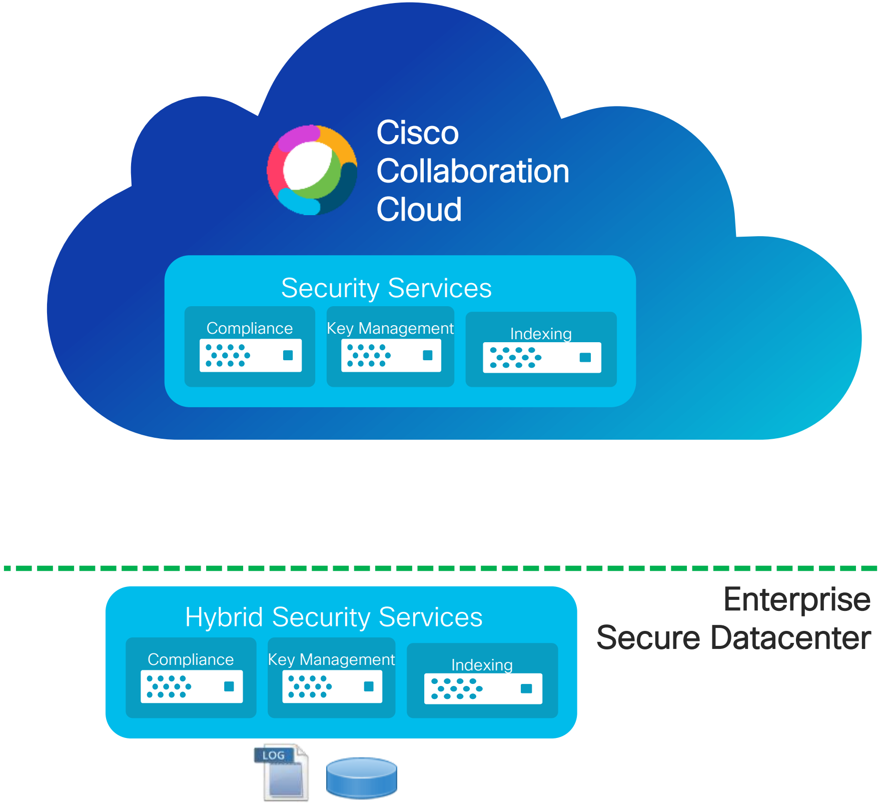
Hybrid Data Security Functionality and Architecture

Cisco Webex Architecture

Cisco Webex Hybrid Services



Cisco Webex Pro Pack – Hybrid Data Security



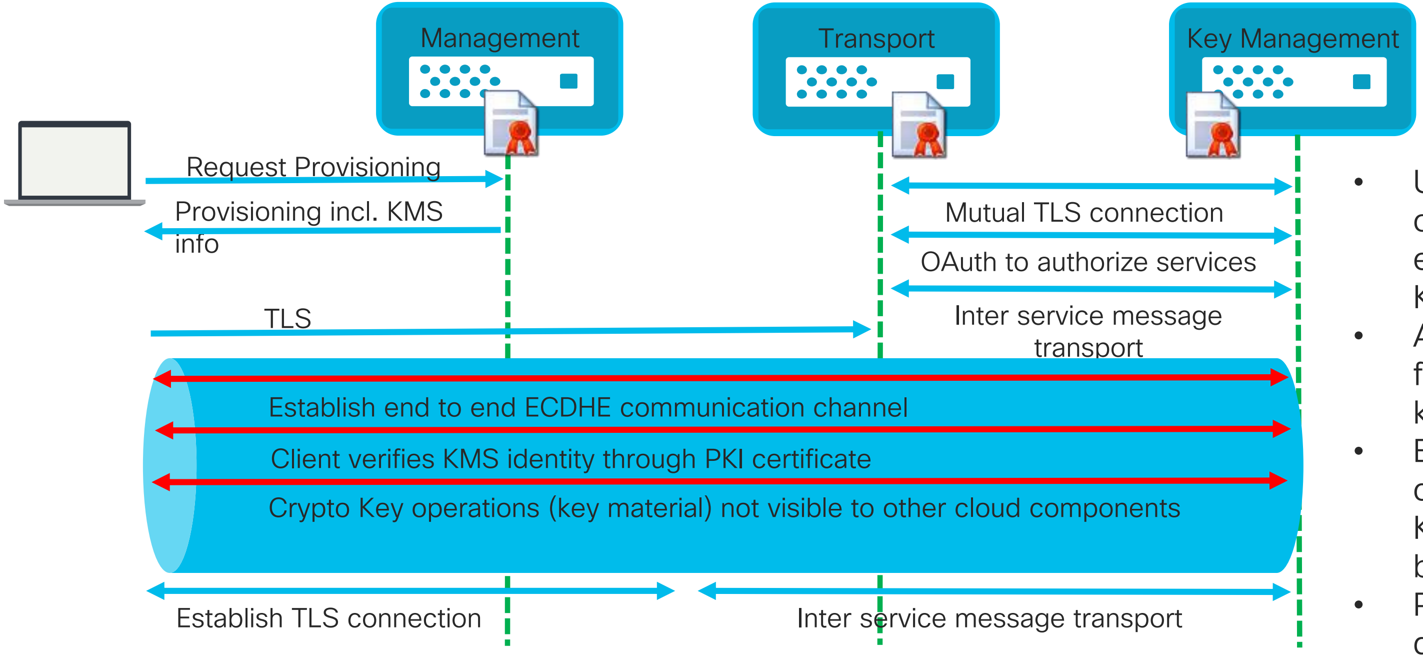
Advantages of Cisco Hybrid Data Security

- Key Management (KMS) owned by customer on premise
- Customer key material stored on premise in customer provided database
- Detailed on premise logging and transparency on access to key material
- Functions that require access to clear text information (Indexing, Compliance) operated on premise as part of HDS
- KMS Federation for secure business to business communication

- Operations and availability of HDS components and associated database crucial customer responsibility
- Backup / Disaster recovery procedures for HDS components and database required
- No plan B – if key database is lost no access to encrypted data in Cisco Webex Teams Cloud

Cisco Webex Pro Pack – Hybrid Data Security

Architecture

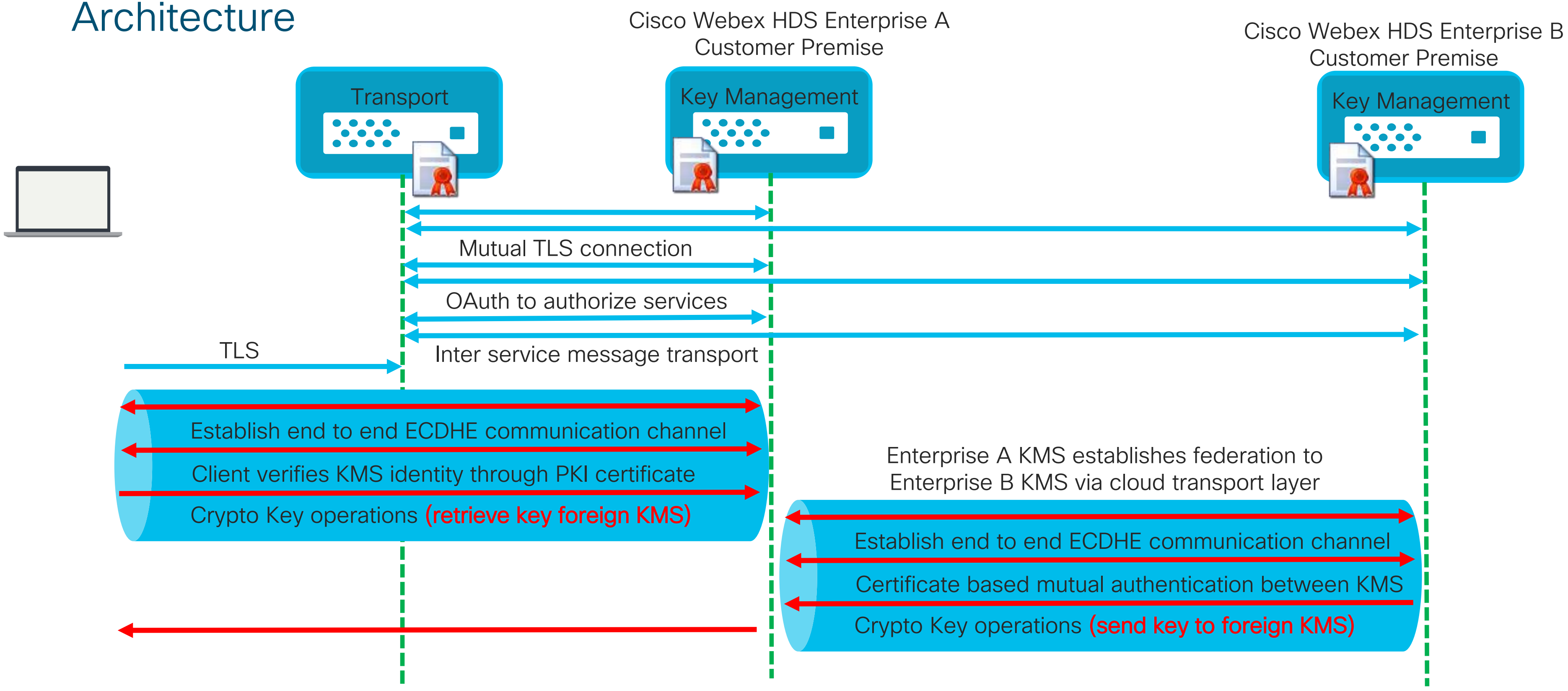


Management
Transport
Key Management
Cisco Webex Teams HDS
Customer Premise
Request Provisioning
Provisioning incl. KMS info
Mutual TLS connection
OAuth to authorize services
Inter service message transport
TLS
Establish end to end ECDHE communication channel
Client verifies KMS identity through PKI certificate
Crypto Key operations (key material) not visible to other cloud components
Establish TLS connection
Inter service message transport

- Users of Webex Teams organization with HDS enabled contact premise KMS for all requests
- After organization is enabled for HDS all newly created keys are stored on premise
- End to End encrypted channel between client and KMS ensures keys can not be intercepted in the cloud
- Public PKI certificate deployed with premise KMS validates identity and protects E2E communication from MITM attacks

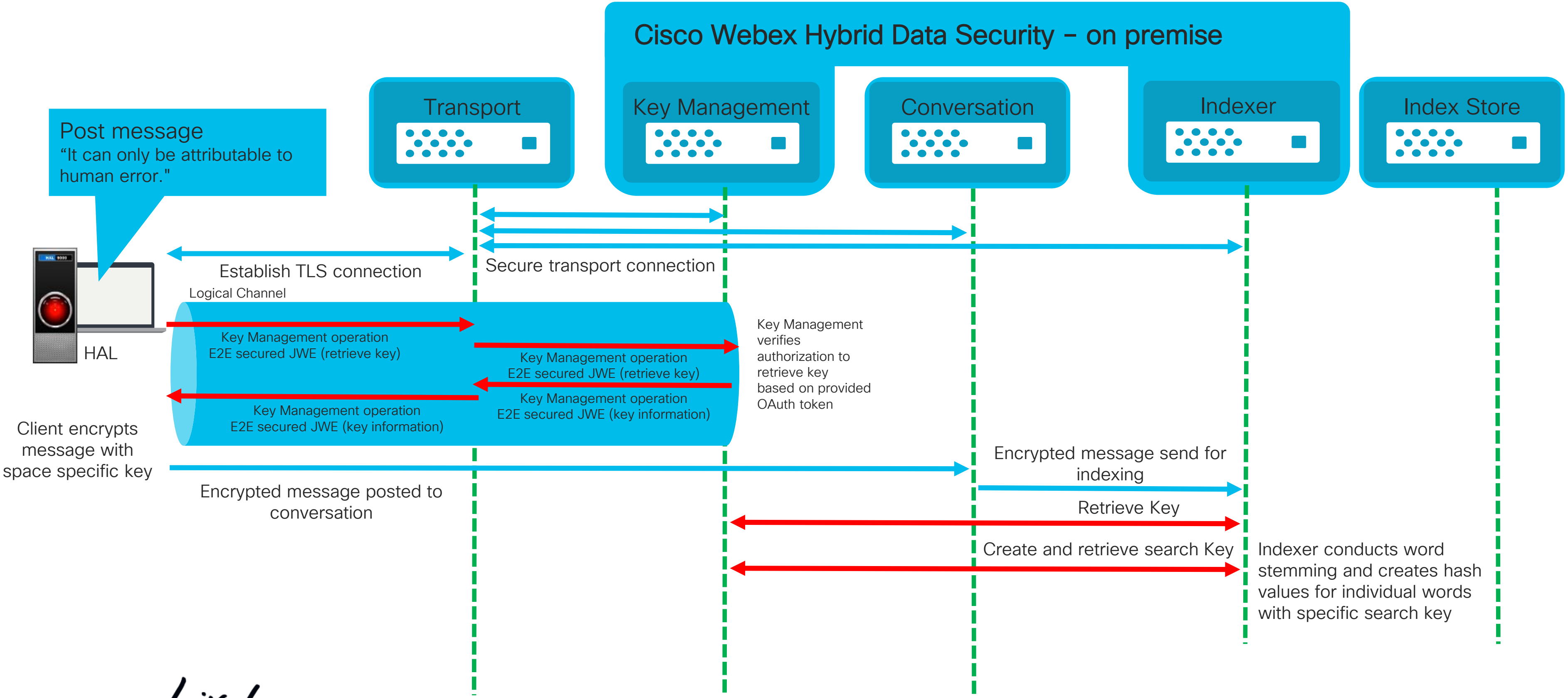
Cisco Webex Pro Pack – Hybrid Data Security

Architecture


Cisco Webex HDS Enterprise A
Customer Premise
Cisco Webex HDS Enterprise B
Customer Premise
Transport
Key Management
Key Management
Mutual TLS connection
OAuth to authorize services
TLS
Inter service message transport
Establish end to end ECDHE communication channel
Client verifies KMS identity through PKI certificate
Crypto Key operations (retrieve key foreign KMS)
Enterprise A KMS establishes federation to
Enterprise B KMS via cloud transport layer
Establish end to end ECDHE communication channel
Certificate based mutual authentication between KMS
Crypto Key operations (send key to foreign KMS)

Cisco Webex Pro Pack – Hybrid Data Security

End to End Secure Communication – How to search?



Cisco Webex Hybrid Data Security – on premise
Transport
Key Management
Conversation
Indexer
Index Store
Post message
"It can only be attributable to human error."
HAL
Establish TLS connection
Secure transport connection
Logical Channel
Key Management operation
E2E secured JWE (retrieve key)
Key Management operation
E2E secured JWE (retrieve key)
Key Management operation
E2E secured JWE (key information)
Key Management operation
E2E secured JWE (key information)
Key Management verifies authorization to retrieve key based on provided OAuth token
Client encrypts message with space specific key
Encrypted message posted to conversation
Encrypted message send for indexing
Retrieve Key
Create and retrieve search Key
Indexer conducts word stemming and creates hash values for individual words with specific search key

Cisco Webex Pro Pack Hybrid Data Security

Deployment and Configuration

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Cisco provided components requirements:

- Cisco HDS is provided as VMware OVA template download from Cisco Webex Control Hub
  - VMware requirements:
    - ✓ VMware 6.0 or higher
    - ✓ 4 vCPUs, 8 GB main memory, 50 GB local disk space
- Minimum 2 HDS virtual machines required
  - recommendation 3, maximum 5
- Cisco Webex HDS Configuration Tool
  - Docker container to create virtual ISO file that holds HDS configuration information, Windows Professional/Enterprise or Mac OS-X 10.10.3 > workstation with Docker installed

Cisco HDS network requirements:

- Outbound direct access HTTPS and WSS
  - *.wbx2.com
  - idbroker.webex.com
  - Identity.webex.com
  - Index.docker. io
- Proxy supported

Customer provided components requirements:

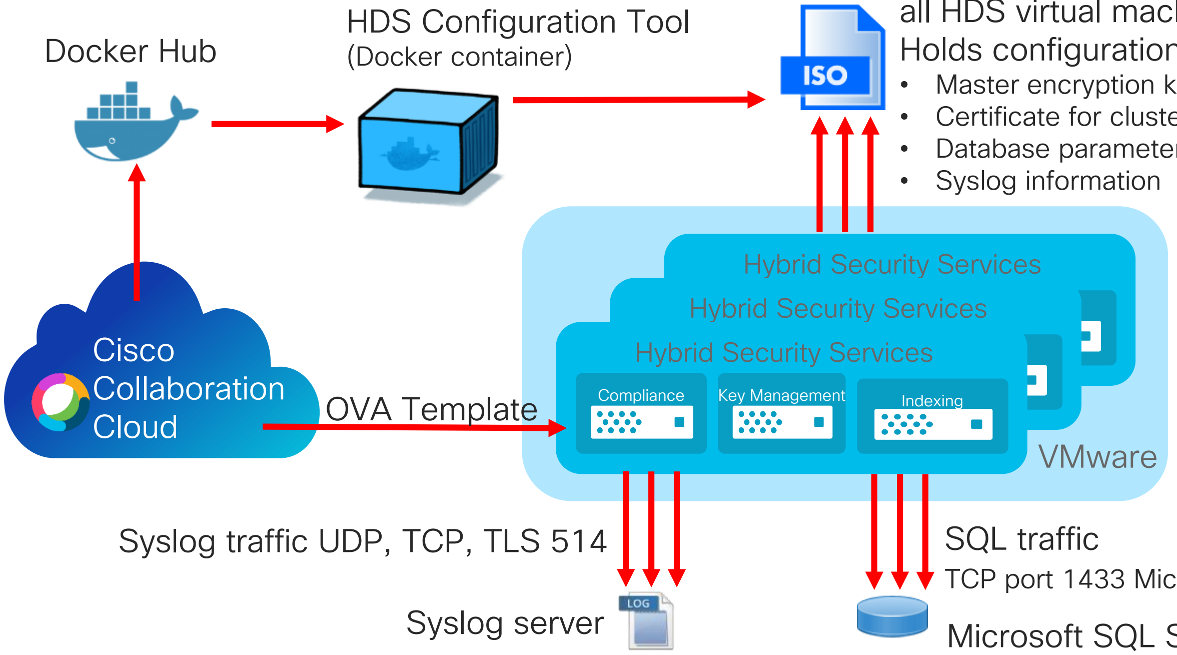
- X.509 Public Certificate
  - Signed by certificate authority on the Mozilla trust list https://wiki.mozilla.org/CA:IncludedCAs (Except WoSign & StartCom)
  - No SHA1 signature
  - Formatted as password-protected PKCS #12
  - Friendly Name kms-private-key
- **Microsoft SQL Server 2016 or later**
  - Microsoft SQL Server 2016 Enterprise
  - Microsoft SQL Server 2016 Standard

  PostgreSQL 9.6 or later database
  - Recommended resource configuration:
  - Minimum 8 vCPUs, 16 GB main memory, adequate disk space (i.e. 2 TB for long term operations without the need to increase storage configuration)
- Syslog Destination (UDP, TCP, TLS)
  - Minimum generic syslog server (i.e. running on Linux host)
  - Recommended to utilize advanced logging infrastructure for increased visibility, notification, dashboards & alarms.

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Cisco HDS components overview:



Virtual ISO image, mounted on all HDS virtual machines

Holds configuration data:

- Master encryption key
- Certificate for cluster
- Database parameters
- Syslog information

Syslog traffic UDP, TCP, TLS 514

Syslog server

SQL traffic

TCP port 1433 Microsoft SQL, 5432 PostgreSQL (TCP/TLS)

Microsoft SQL Server or PostgreSQL Database

Key information written to database is encrypted

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Deployment

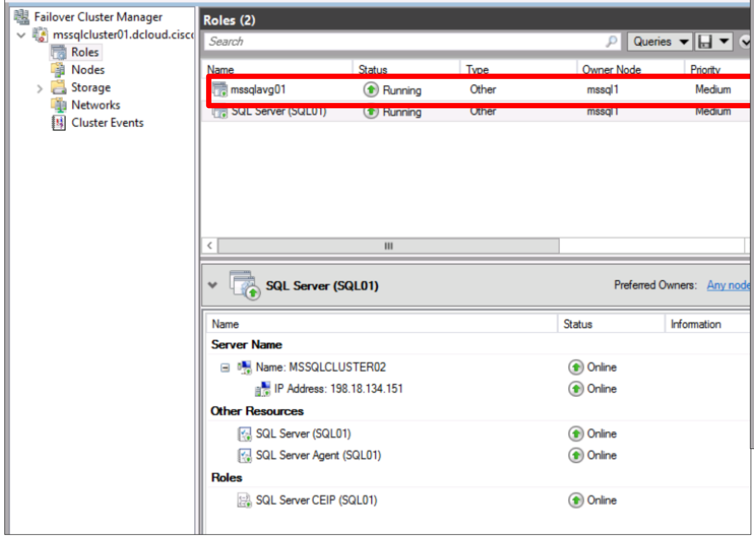
- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node

address, DNS, NTP
run HDS
on Tool
nfiguration virtual
vare data store
trial from

Microsoft SQL Install & Configuration example:

Hybrid Data Security now supports Microsoft SQL Server as a database. SQL Server Always On (Always On Failover Clusters and Always on Availability Groups) is supported by the JDBC drivers that are used in Hybrid Data Security. Added content related to deploying with SQL Server.

SQL Server Windows Failover Cluster



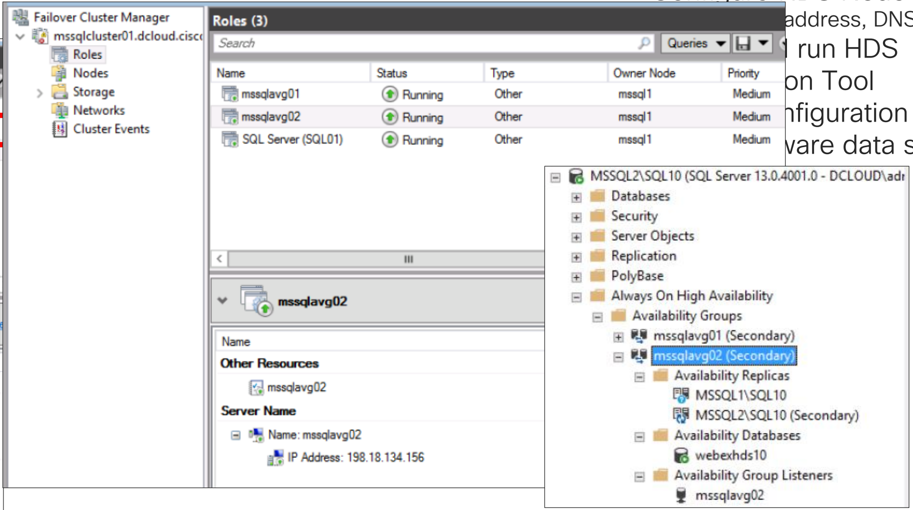
Roles (2)

Name	Status	Type	Owner Node	Priority
mssqlavg01	Running	Other	mssql1	Medium
SQL Server (SQL01)	Running	Other	mssql1	Medium

SQL Server (SQL01) — Preferred Owners: Any node

Name	Status	Information
Server Name		
Name: MSSQLCLUSTER02	Online	
IP Address: 198.18.134.151	Online	
Other Resources		
SQL Server (SQL01)	Online	
SQL Server Agent (SQL01)	Online	
Roles		
SQL Server CEIP (SQL01)	Online	

SQL Server Always On Av. Group



Roles (3)

Name	Status	Type	Owner Node	Priority
mssqlavg01	Running	Other	mssql1	Medium
mssqlavg02	Running	Other	mssql1	Medium
SQL Server (SQL01)	Running	Other	mssql1	Medium

mssqlavg02

Name
Other Resources
mssqlavg02
Server Name
Name: mssqlavg02
IP Address: 198.18.134.156

```
MSSQL2\SQL10 (SQL Server 13.0.4001.0 - DCLOUD\adr
  Databases
  Security
  Server Objects
  Replication
  PolyBase
  Always On High Availability
    Availability Groups
      mssqlavg01 (Secondary)
      mssqlavg02 (Secondary)
        Availability Replicas
          MSSQL1\SQL10
          MSSQL2\SQL10 (Secondary)
        Availability Databases
          webexhds10
        Availability Group Listeners
          mssqlavg02
```

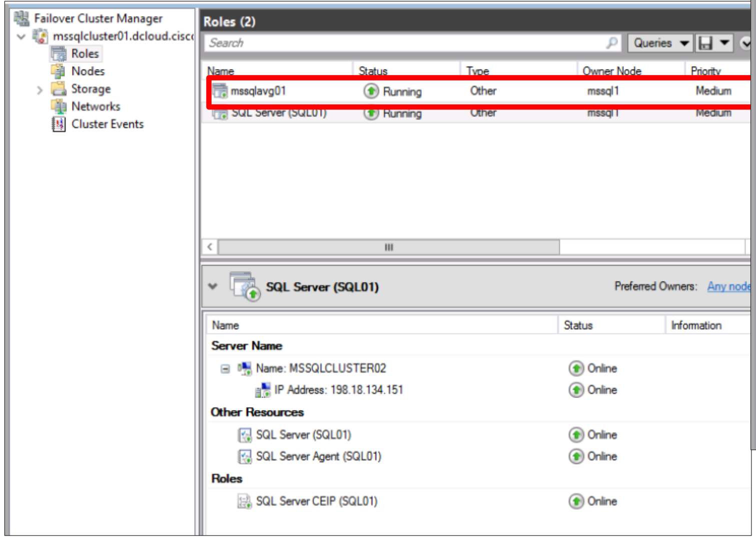
Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Microsoft SQL Install & Configuration example:

Hybrid Data Security now supports Microsoft SQL Server as a database. SQL Server Always On (Always On Failover Clusters and Always on Availability Groups) is supported by the JDBC drivers that are used in Hybrid Data Security. Added content related to deploying with SQL Server.

SQL Server Windows Failover Cluster



Failover Cluster Manager
mssqlcluster01.dcloud.cisc
Roles
Nodes
Storage
Networks
Cluster Events

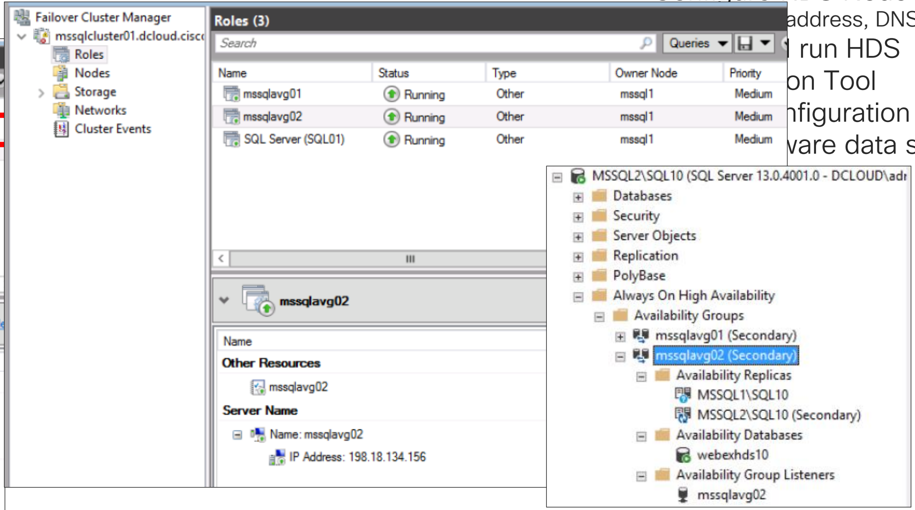
Roles (2)

Name	Status	Type	Owner Node	Priority
mssqlavg01	Running	Other	mssql1	Medium
SQL Server (SQL01)	Running	Other	mssql1	Medium

SQL Server (SQL01) Preferred Owners: Any node

Name	Status	Information
Server Name		
Name: MSSQLCLUSTER02	Online	
IP Address: 198.18.134.151	Online	
Other Resources		
SQL Server (SQL01)	Online	
SQL Server Agent (SQL01)	Online	
Roles		
SQL Server CEIP (SQL01)	Online	

SQL Server Always On Av. Group



Failover Cluster Manager
mssqlcluster01.dcloud.cisc
Roles
Nodes
Storage
Networks
Cluster Events

Roles (3)

Name	Status	Type	Owner Node	Priority
mssqlavg01	Running	Other	mssql1	Medium
mssqlavg02	Running	Other	mssql1	Medium
SQL Server (SQL01)	Running	Other	mssql1	Medium

mssqlavg02

Name
Other Resources
mssqlavg02
Server Name
Name: mssqlavg02
IP Address: 198.18.134.156

MSSQL2\SQL10 (SQL Server 13.0.4001.0 - DCLOUD\adr
- Databases
- Security
- Server Objects
- Replication
- PolyBase
- Always On High Availability
  - Availability Groups
    - mssqlavg01 (Secondary)
    - mssqlavg02 (Secondary)
      - Availability Replicas
        - MSSQL1\SQL10
        - MSSQL2\SQL10 (Secondary)
      - Availability Databases
        - webexhds10
      - Availability Group Listeners
        - mssqlavg02

Deployment

- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node

address, DNS, NTP
run HDS
on Tool
nfiguration virtual
vare data store
trial from

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

PostgreSQL Install & Configuration example (Linux):

Add repository to host

```
yum -y install https://yum.postgresql.org/9.6/redhat/rhel-7-x86_64/pgdg-redhat96-9.6-3.noarch.rpm
```

Install dependencies

```
yum -y install postgresql96-server postgresql-contrib
```

Initialize PostgreSQL database

```
/usr/pgsql-9.6/bin/postgresql96-setup initdb
```

Setup PostgreSQL database to automatically start on boot

```
systemctl start postgresql-9.6
systemctl enable postgresql-9.6
```

Create database and db user for HDS

```
CREATE USER hdsuser WITH PASSWORD '<password>';
CREATE DATABASE hdsdb OWNER hdsuser;
GRANT ALL PRIVILEGES ON DATABASE hdsdb to hdsuser;
ALTER ROLE hdsuser WITH SUPERUSER;
```

Edit PostgreSQL /var/lib/psql/9.6/data/pg_hba.conf configuration file

```
# IPv4 local network connection for HDS nodes:
host        all            all            <IP subnet or address of HDS nodes> (i.e. 192.168.0.0/24)
```

Edit PostgreSQL /var/lib/psql/9.6/data/postgresql.conf configuration file

```
listener_addresses = '*'
port = 5432
```

Restart PostgreSQL

```
service postgresql-9.6 restart
```

Check status of PostgreSQL

```
systemctl status postgresql-9.6.service
```

Deployment flow

- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node
  hostname, IP address, DNS, NTP
- Deploy and run HDS Configuration Tool
- Upload Configuration virtual ISO to VMware data store
- Activate Webex HDS trial from Control Hub
- Test environment
- Move to production

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Post
Add r
yu
Install
yu
Initializ
/us
Setup
sy
sy
Create
CR
CR
GR
AL
Edit P
I
ho
Edit P
list
po
Resta
se
Check
sy

Optional install PostgreSQL Admin (web based management):

Install HTTP server

```
yum -y install httpd
```

Setup HTTP server to automatically start on boot

```
systemctl start httpd
systemctl enable httpd
```

Install PHP and required components

```
yum -y install php php-pgsql
```

Install PostgreSQL Admin

```
yum -y install phpPgAdmin
```

Configure PostgreSQL Admin /etc/httpd/conf.d/phpPgAdmin.conf

```
Require all granted
Allow from all
```

(for production deployment this should be reviewed)

Configure PostgreSQL Admin /etc/phpPgAdmin/config.inc.php

```
$conf[‘servers’][0][‘desc’] = ‘PostgreSQL Server’
$conf[‘servers’][0][‘host’] = ‘<fqdn of postgresql server>’
$conf[‘servers’][0][‘port’] = 5432
$conf[‘servers’][0][‘sslmode’] = ‘allow’
```

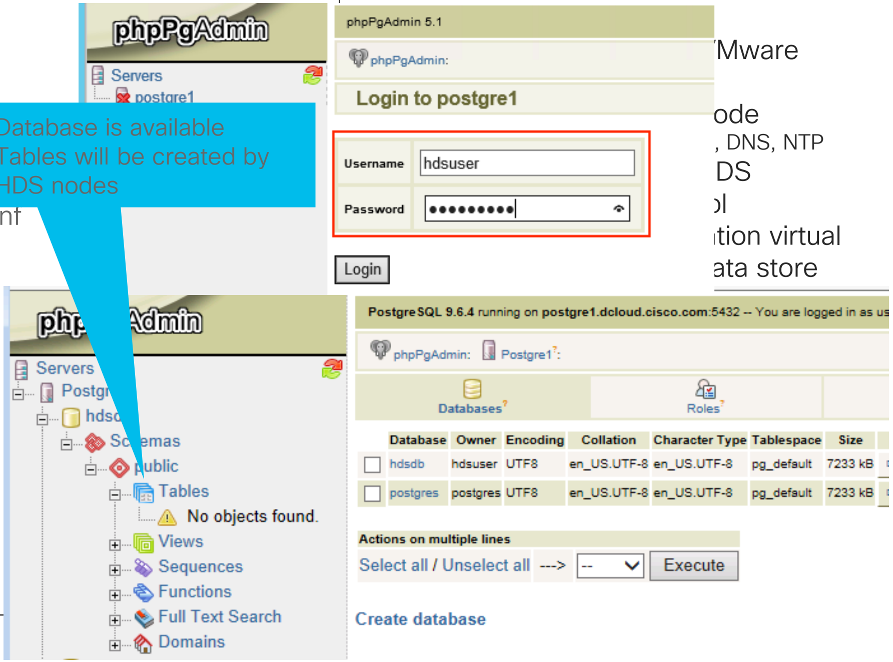
Restart PostgreSQL server

```
systemctl restart postgresql-9.6.service
```

Restart HTTP server

```
Systemctl restart httpd.service
```

Database is available
Tables will be created by HDS nodes



Login to postgre1

Username: hdsuser

Password: ●●●●●●●●●

No objects found.

PostgreSQL 9.6.4 running on postgre1.dcloud.cisco.com:5432 -- You are logged in as us

	Database	Owner	Encoding	Collation	Character Type	Tablespace	Size
□	hdsdb	hdsuser	UTF8	en_US.UTF-8	en_US.UTF-8	pg_default	7233 kB
□	postgres	postgres	UTF8	en_US.UTF-8	en_US.UTF-8	pg_default	7233 kB

Deployment flow

- Deploy & Configure Database & Syslog
- Download OVA from Webex

'Mware
ode
, DNS, NTP
DS
ol
tion virtual
ata store

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Generic Syslog Install & Configure

Install Syslog server (on some Linux distributions this might be installed by default)

```
yum -y install rsyslog
```

Configure Syslog /etc/rsyslog.conf

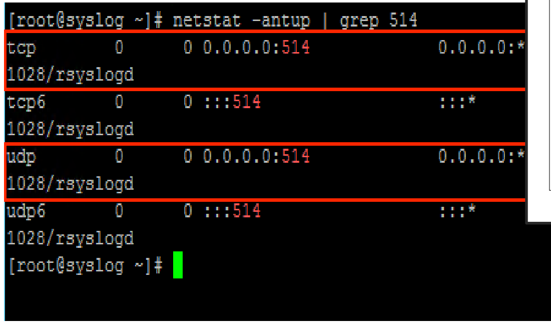
```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
# Provides TCP syslog reception
$ModLoad imtcp
$TCPServerRun 514
```

Restart Syslog server

```
Systemctl restart rsyslog.service
```

Verify Syslog server

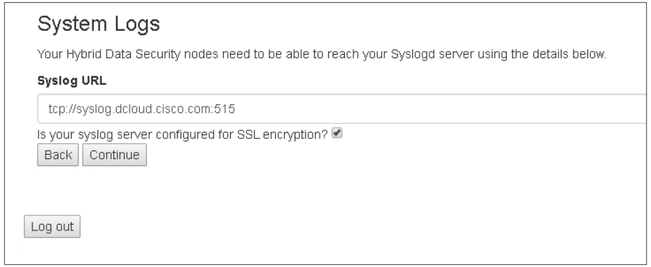
```
netstat –antup | grep 514
```



```
[root@syslog ~]# netstat -antup | grep 514
tcp        0      0 0.0.0.0:514             0.0.0.0:*
1028/rsyslogd
tcp6       0      0 :::514                  :::*
1028/rsyslogd
udp        0      0 0.0.0.0:514             0.0.0.0:*
1028/rsyslogd
udp6       0      0 :::514                  :::*
1028/rsyslogd
[root@syslog ~]#
```

Support for Syslog over TLS

- Cisco HDS allow Syslog transport over TLS
- TLS connection to Syslog server encrypted not verified
- Pending enhancement for specific Syslog servers implementation, support different line termination (CR, LF or CR/LF)



System Logs

Your Hybrid Data Security nodes need to be able to reach your Syslogd server using the details below.

Syslog URL

tcp://syslog.dcloud.cisco.com:515

Is your syslog server configured for SSL encryption? ☑

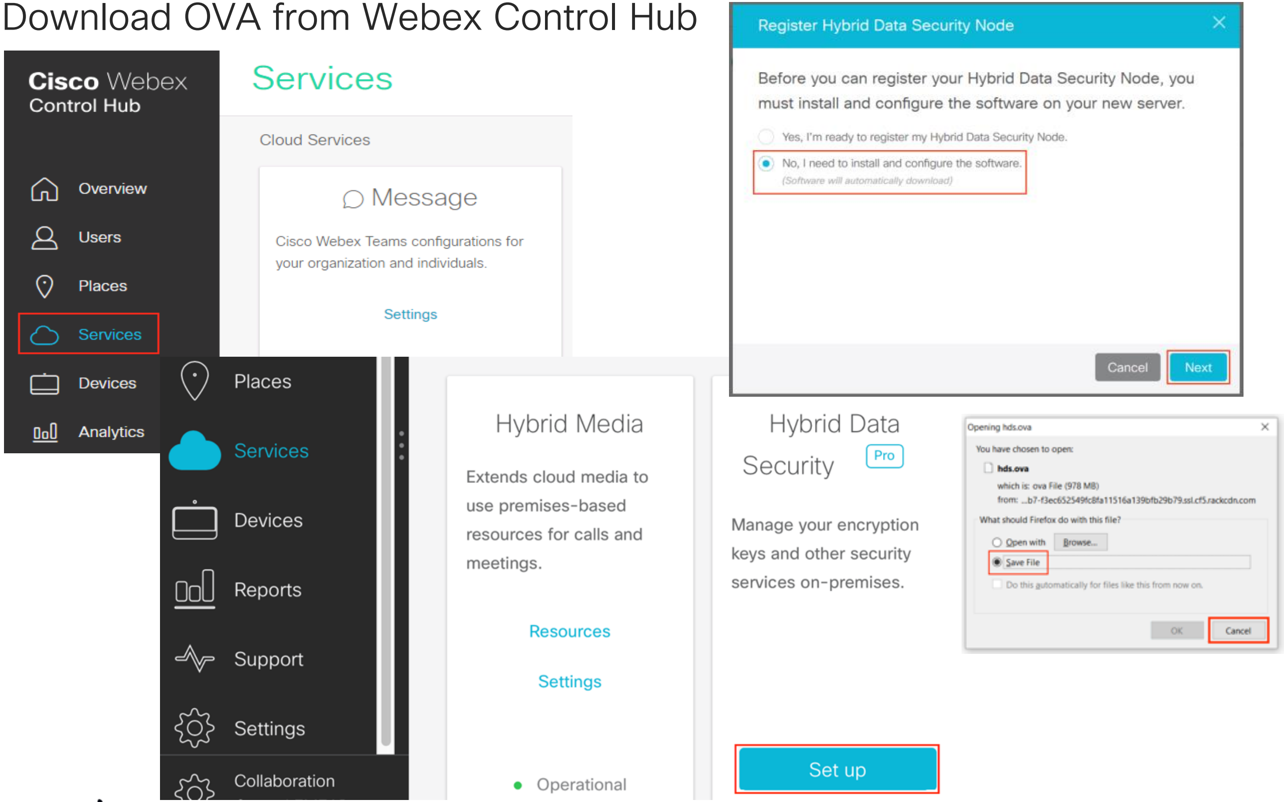
Deployment flow

- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node
  hostname, IP address, DNS, NTP
- Deploy and run HDS Configuration Tool
- Upload Configuration virtual ISO to VMware data store
- Activate Webex HDS trial from Control Hub
- Test environment
- Move to production

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Download OVA from Webex Control Hub



Cisco Webex Teams configurations for your organization and individuals.

Extends cloud media to use premises-based resources for calls and meetings.

Manage your encryption keys and other security services on-premises.

Register Hybrid Data Security Node

Before you can register your Hybrid Data Security Node, you must install and configure the software on your new server.

○ Yes, I'm ready to register my Hybrid Data Security Node.

● No, I need to install and configure the software.
(Software will automatically download)

Opening hds.ova

You have chosen to open:

hds.ova

which is: ova File (978 MB)
from: ...b7-f3ec652549fc8fa11516a139bfb29b79.ssl.cf5.rackcdn.com

What should Firefox do with this file?

○ Open with

● Save File

□ Do this automatically for files like this from now on.

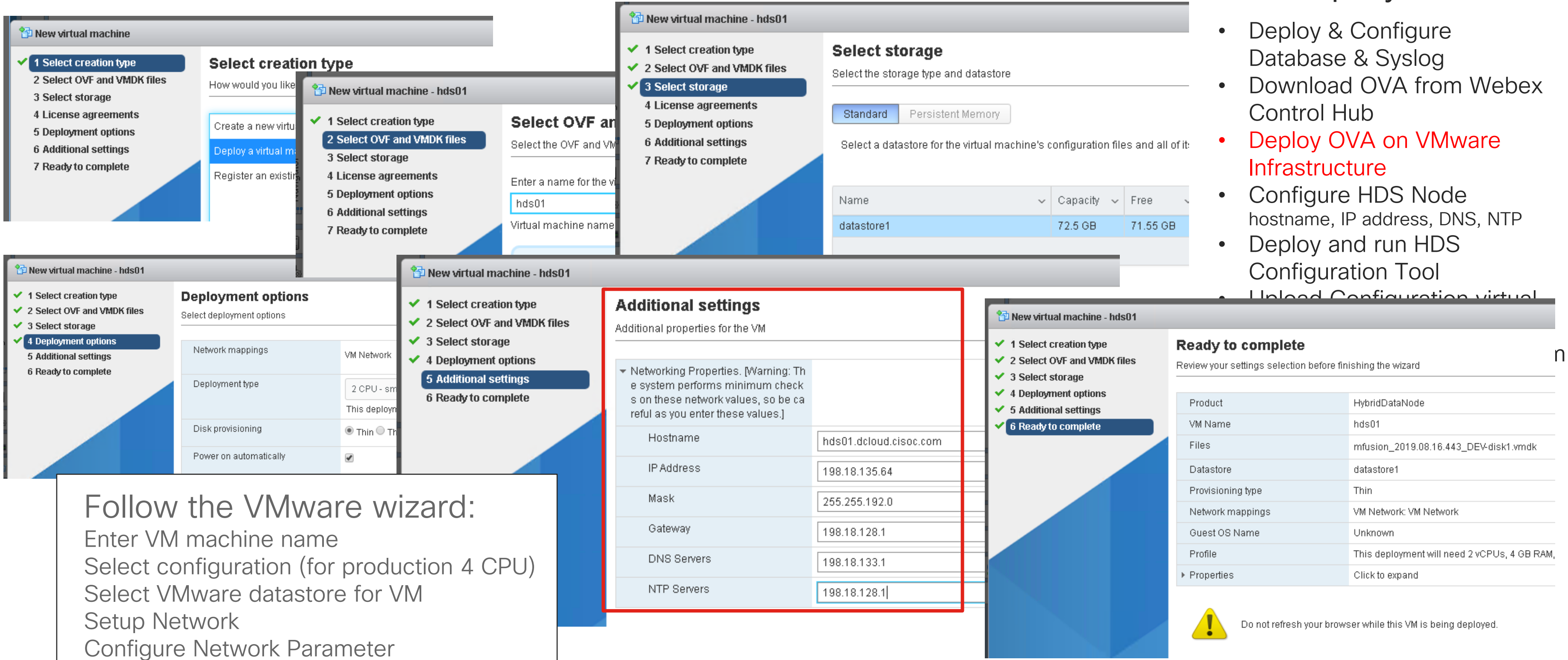
Deployment flow

- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node
  hostname, IP address, DNS, NTP
- Deploy and run HDS Configuration Tool
- Upload Configuration virtual ISO to VMware data store
- Activate Webex HDS trial from Control Hub
- Test environment
- Move to production

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Deploy OVA on VMware 6.0+ infrastructure



New virtual machine

- ✓ 1 Select creation type
- 2 Select OVF and VMDK files
- 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select creation type

How would you like

Create a new virtu

Deploy a virtual m

Register an existin

New virtual machine - hds01

- ✓ 1 Select creation type
- 2 Select OVF and VMDK files
- 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select OVF an

Select the OVF and VM

Enter a name for the vi

hds01

Virtual machine name

New virtual machine - hds01

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select storage

Select the storage type and datastore

Standard | Persistent Memory

Select a datastore for the virtual machine's configuration files and all of it

Name	Capacity	Free
datastore1	72.5 GB	71.55 GB

New virtual machine - hds01

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- 5 Additional settings
- 6 Ready to complete

Deployment options

Select deployment options

Network mappings	VM Network
Deployment type	2 CPU - sm This deploym
Disk provisioning	● Thin ○ Th
Power on automatically	☑

New virtual machine - hds01

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- 5 Additional settings
- 6 Ready to complete

Additional settings

Additional properties for the VM

Networking Properties. [Warning: The system performs minimum checks on these network values, so be careful as you enter these values.]

Hostname	hds01.dcloud.cisoc.com
IP Address	198.18.135.64
Mask	255.255.192.0
Gateway	198.18.128.1
DNS Servers	198.18.133.1
NTP Servers	198.18.128.1

New virtual machine - hds01

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Additional settings
- ✓ 6 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

Product	HybridDataNode
VM Name	hds01
Files	mfusion_2019.08.16.443_DEV-disk1.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	VM Network: VM Network
Guest OS Name	Unknown
Profile	This deployment will need 2 vCPUs, 4 GB RAM,
Properties	Click to expand

⚠ Do not refresh your browser while this VM is being deployed.

Follow the VMware wizard:

Enter VM machine name
Select configuration (for production 4 CPU)
Select VMware datastore for VM
Setup Network
Configure Network Parameter

Deployment flow

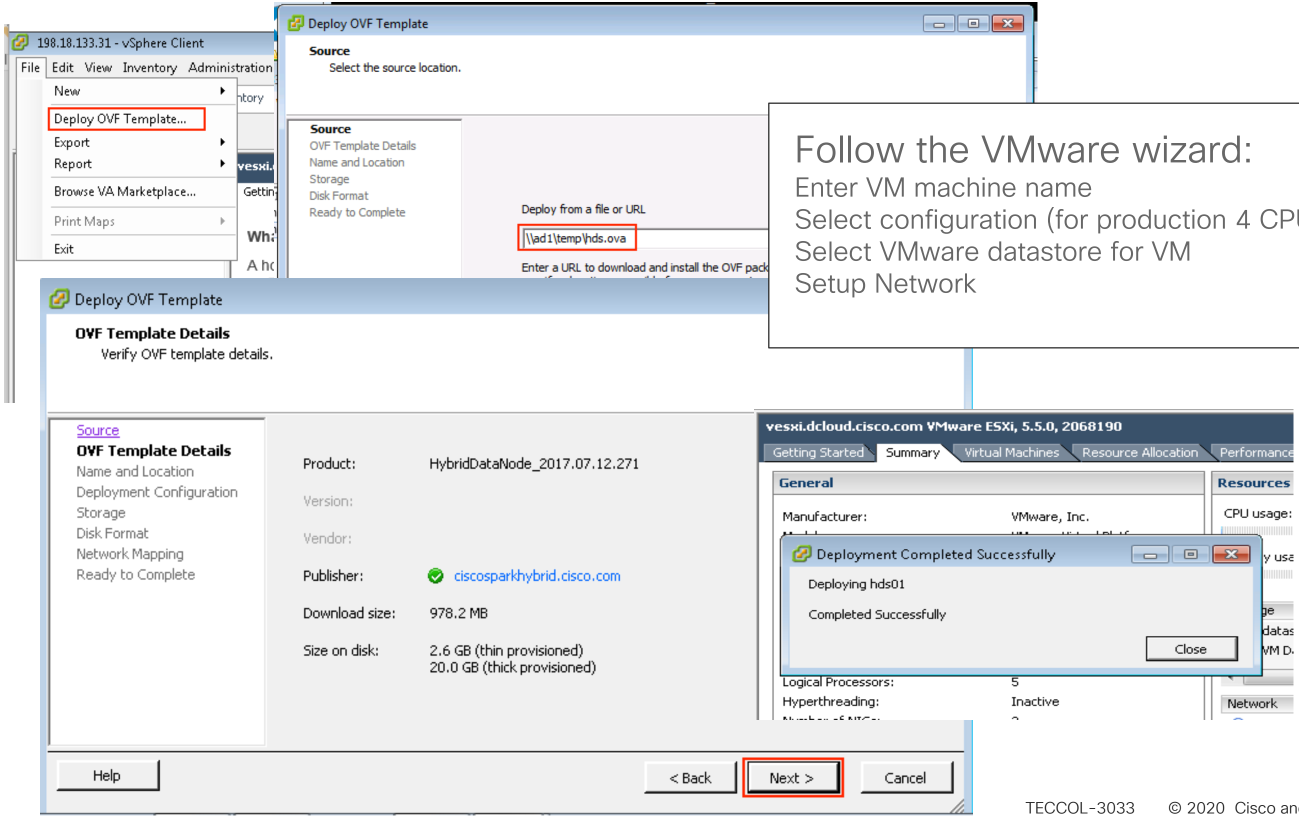
- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node hostname, IP address, DNS, NTP
- Deploy and run HDS Configuration Tool
- Upload Configuration virtual

n

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Deploy OVA on VMware 5.5 infrastructure – End of Support



Source
Select the source location.

Deploy from a file or URL
\\ad1\temp\hds.ova

Enter a URL to download and install the OVF pack

OVF Template Details
Verify OVF template details.

Product: HybridDataNode_2017.07.12.271
Version:
Vendor:
Publisher: ciscosparkhybrid.cisco.com
Download size: 978.2 MB
Size on disk: 2.6 GB (thin provisioned)
20.0 GB (thick provisioned)

vesxi.dcloud.cisco.com VMware ESXi, 5.5.0, 2068190

Manufacturer: VMware, Inc.
Logical Processors: 5
Hyperthreading: Inactive
CPU usage:

Deployment Completed Successfully
Deploying hds01
Completed Successfully

Follow the VMware wizard:
Enter VM machine name
Select configuration (for production 4 CPU)
Select VMware datastore for VM
Setup Network

Deployment flow

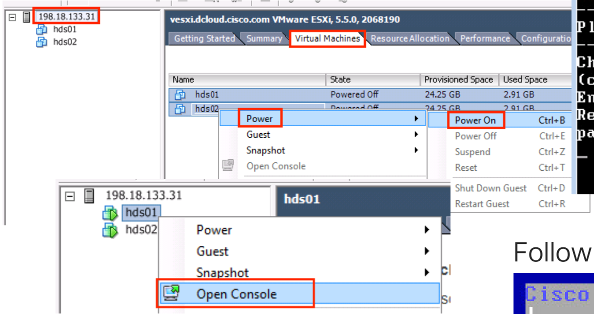
- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node
hostname, IP address, DNS, NTP
- Deploy and run HDS Configuration Tool
- Upload Configuration virtual ISO to VMware data store
- Activate Webex HDS trial from Control Hub
- Test environment
- Move to production

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Configure HDS Node

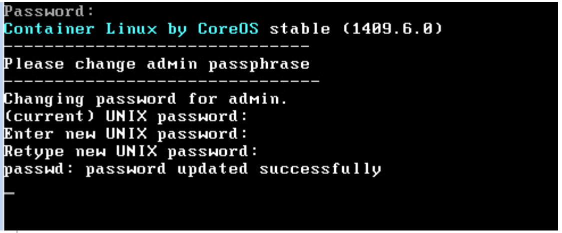
Power On HDS virtual machines



vesxi.dcloud.cisco.com VMware ESXi, 5.5.0, 2068190

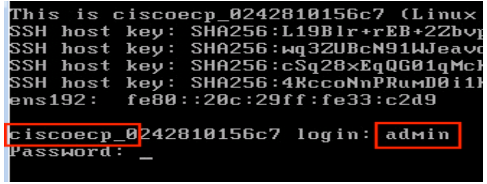
Name	State	Provisioned Space	Used Space
hds01	Powered Off	24.25 GB	2.91 GB
hds02	Powered Off	24.25 GB	2.91 GB

Follow dialog to change default password



```
Password:
Container Linux by CoreOS stable (1409.6.0)
------------------------------
Please change admin passphrase
------------------------------
Changing password for admin.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
_
```

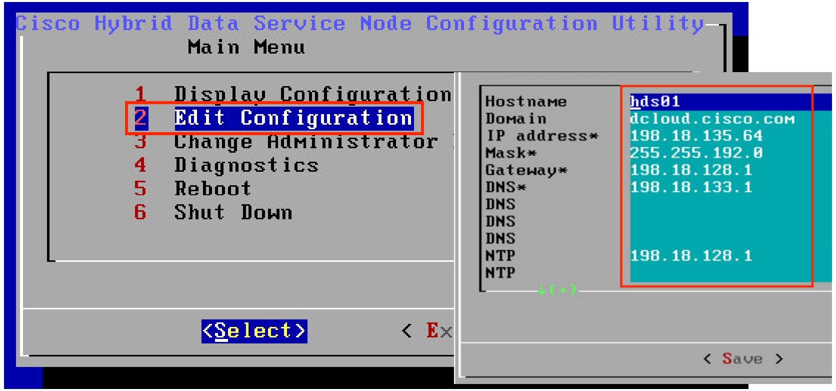
Wait for prompt to show cisco_ecp, logon with admin/cisco



```
This is ciscoecp_0242810156c7 (Linux
SSH host key: SHA256:L19Blr+rEB+2Zbvp
SSH host key: SHA256:wq3ZUBcN91WJeavc
SSH host key: SHA256:cSq28xEqQG01qMck
SSH host key: SHA256:4KccoNnPRumD0i1K
ens192:  fe80::20c:29ff:fe33:c2d9

ciscoecp_0242810156c7 login: admin
Password: _
```

Follow on screen menu to configure basic network parameter



```
Cisco Hybrid Data Service Node Configuration Utility
                     Main Menu

     1  Display Configuration
     2  Edit Configuration
     3  Change Administrator
     4  Diagnostics
     5  Reboot
     6  Shut Down

          <Select>          < Ex
```

```
Hostname     hds01
Domain       dcloud.cisco.com
IP address*  198.18.135.64
Mask*        255.255.192.0
Gateway*     198.18.128.1
DNS*         198.18.133.1
DNS
DNS
DNS
NTP          198.18.128.1
NTP
      ↓(+)
                         < Save >
```

Only required if OVA Network configuration is not utilized

Deployment flow

- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node
  hostname, IP address, DNS, NTP
- Deploy and run HDS Configuration Tool
- Upload Configuration virtual ISO to VMware data store
- Activate Webex HDS trial from Control Hub
- Test environment
- Move to production

cisco Live!

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Deploy and run HDS configuration tool

Install Docker on your admin workstation

Login Docker Hub to access Cisco Webex HDS Configuration Tool container

```
docker login -u Sparkhdsreadonly -p AtAideExertAddisDatumFlame
```

Pull Docker container

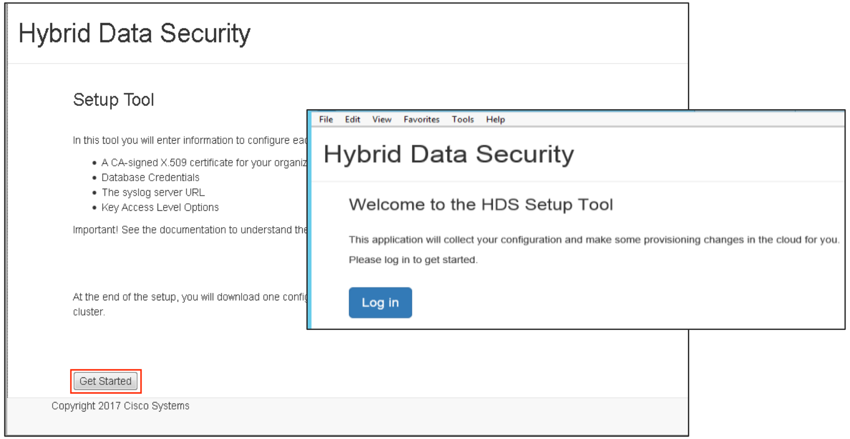
```
docker pull ciscoSparkhds/hds-setup:stable
```

make sure to repeat this step before updating ISO to always have latest version of configuration tool

Run Docker container

```
docker run -p 8080:8080 --rm -it --name ciscohds ciscoSparkhds/hds-setup:stable
```

Open browser and navigate to http://127.0.0.1:8080



Hybrid Data Security

Setup Tool

In this tool you will enter information to configure ea

- A CA-signed X.509 certificate for your organiz
- Database Credentials
- The syslog server URL
- Key Access Level Options

Important! See the documentation to understand the

At the end of the setup, you will download one confi cluster.

Get Started

Copyright 2017 Cisco Systems

Hybrid Data Security

Welcome to the HDS Setup Tool

This application will collect your configuration and make some provisioning changes in the cloud for you.

Please log in to get started.

Log in

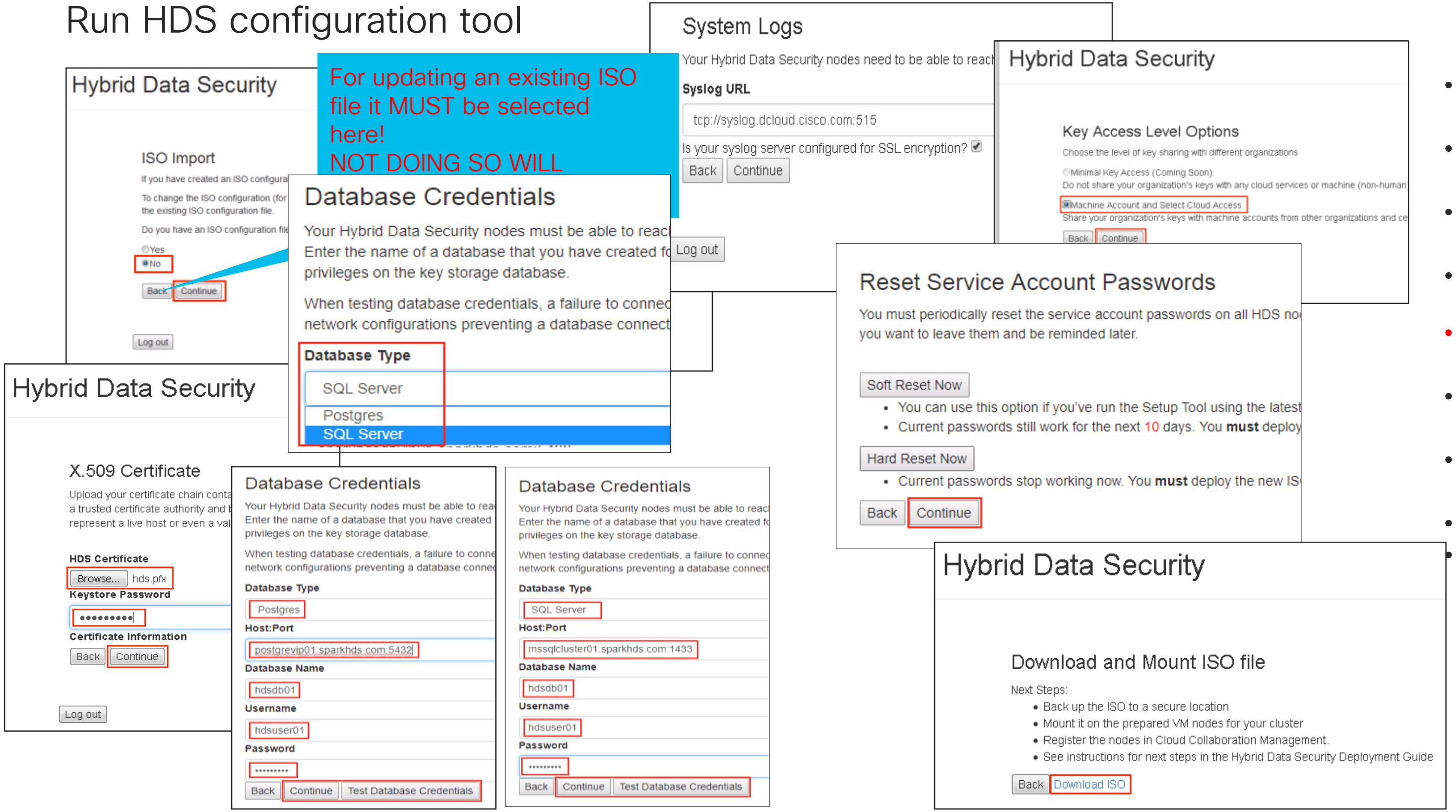
Deployment flow

- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node
  hostname, IP address, DNS, NTP
- Deploy and run HDS Configuration Tool
- Upload Configuration virtual ISO to VMware data store
- Activate Webex HDS trial from Control Hub
- Test environment
- Move to production

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Run HDS configuration tool



For updating an existing ISO file it MUST be selected here!
NOT DOING SO WILL

Hybrid Data Security

ISO Import

If you have created an ISO configura

To change the ISO configuration (for
the existing ISO configuration file.

Do you have an ISO configuration file

○ Yes
● No

Back | Continue

Log out

Database Credentials

Your Hybrid Data Security nodes must be able to reac
Enter the name of a database that you have created fo
privileges on the key storage database.

When testing database credentials, a failure to connec
network configurations preventing a database connect

Database Type: SQL Server

- Postgres
- SQL Server

System Logs

Your Hybrid Data Security nodes need to be able to reach

Syslog URL: tcp://syslog.dcloud.cisco.com:515

Is your syslog server configured for SSL encryption? ☑

Back | Continue

Log out

Hybrid Data Security

Key Access Level Options

Choose the level of key sharing with different organizations

○ Minimal Key Access (Coming Soon)
Do not share your organization's keys with any cloud services or machine (non-human

● Machine Account and Select Cloud Access
Share your organization's keys with machine accounts from other organizations and ce

Back | Continue

Hybrid Data Security

X.509 Certificate

Upload your certificate chain conta
a trusted certificate authority and b
represent a live host or even a val

HDS Certificate: Browse... hds.pfx

Keystore Password: ●●●●●●●●●

Certificate Information

Back | Continue

Log out

Database Credentials

Your Hybrid Data Security nodes must be able to rea
Enter the name of a database that you have created
privileges on the key storage database.

When testing database credentials, a failure to conne
network configurations preventing a database connec

Database Type: Postgres

Host:Port: postgrevip01.sparkhds.com:5432

Database Name: hdsdb01

Username: hdsuser01

Password: ●●●●●●●●●

Back | Continue | Test Database Credentials

Database Credentials

Your Hybrid Data Security nodes must be able to reac
Enter the name of a database that you have created fo
privileges on the key storage database.

When testing database credentials, a failure to connec
network configurations preventing a database connect

Database Type: SQL Server

Host:Port: mssqlcluster01.sparkhds.com:1433

Database Name: hdsdb01

Username: hdsuser01

Password: ●●●●●●●●●●

Back | Continue | Test Database Credentials

Reset Service Account Passwords

You must periodically reset the service account passwords on all HDS no
you want to leave them and be reminded later.

Soft Reset Now

- You can use this option if you've run the Setup Tool using the latest
- Current passwords still work for the next 10 days. You **must** deploy

Hard Reset Now

- Current passwords stop working now. You **must** deploy the new IS

Back | Continue

Hybrid Data Security

Download and Mount ISO file

Next Steps:

- Back up the ISO to a secure location
- Mount it on the prepared VM nodes for your cluster
- Register the nodes in Cloud Collaboration Management.
- See instructions for next steps in the Hybrid Data Security Deployment Guide

Back | Download ISO

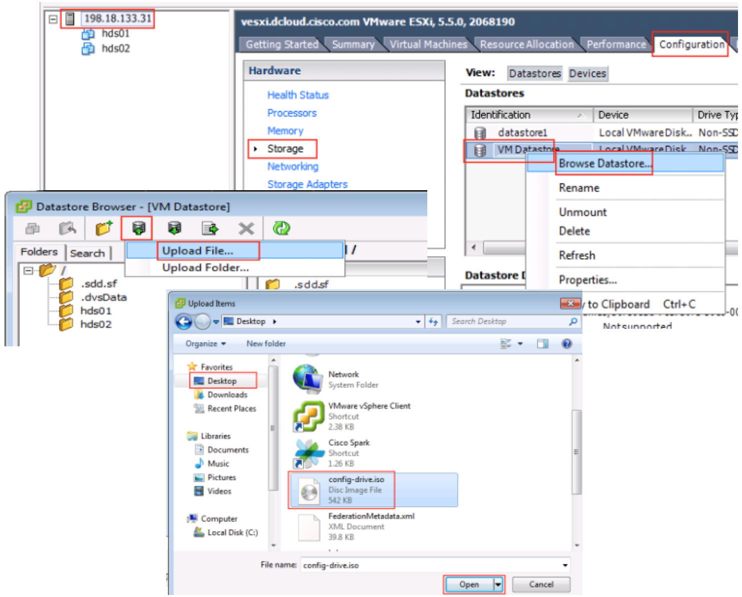
Deployment flow

- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node
  hostname, IP address, DNS, NTP
- Deploy and run HDS Configuration Tool
- Upload Configuration virtual ISO to VMware data store
- Activate Webex HDS trial from Control Hub
- Test environment
- Move to production

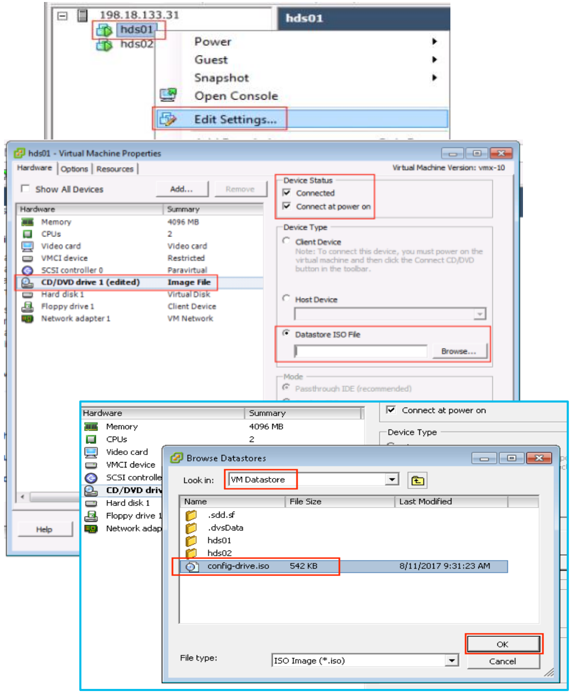
Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Upload virtual ISO to VMware data



Mount virtual ISO in HDS virtual machine



Deployment flow

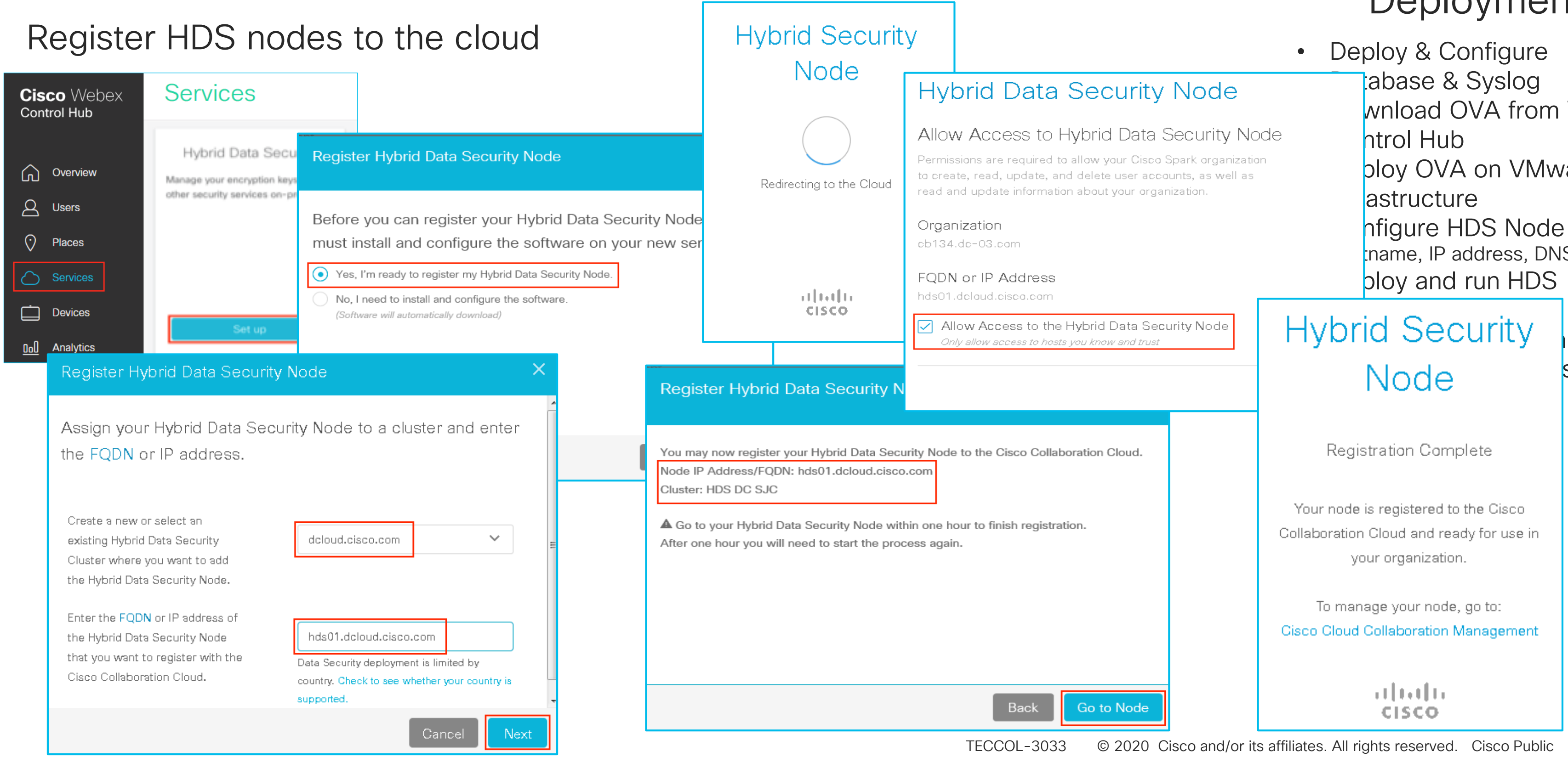
- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node
  hostname, IP address, DNS, NTP
- Deploy and run HDS Configuration Tool
- Upload Configuration virtual ISO to VMware data store
- Activate Webex HDS trial from Control Hub
- Test environment
- Move to production

The virtual ISO file hold “the keys to the kingdom”. Make sure only authorized individuals have access to the data store and ensure a backup of the file in a secure place!

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Register HDS nodes to the cloud



Cisco Webex Control Hub

Services

Hybrid Data Secu

Manage your encryption keys other security services on-pr

Register Hybrid Data Security Node

Before you can register your Hybrid Data Security Node must install and configure the software on your new ser

● Yes, I'm ready to register my Hybrid Data Security Node.

○ No, I need to install and configure the software.
(Software will automatically download)

Hybrid Security Node

Redirecting to the Cloud

Hybrid Data Security Node

Allow Access to Hybrid Data Security Node

Permissions are required to allow your Cisco Spark organization to create, read, update, and delete user accounts, as well as read and update information about your organization.

Organization
cb134.dc-03.com

FQDN or IP Address
hds01.dcloud.cisco.com

☑ Allow Access to the Hybrid Data Security Node
Only allow access to hosts you know and trust

Register Hybrid Data Security Node

Assign your Hybrid Data Security Node to a cluster and enter the FQDN or IP address.

Create a new or select an existing Hybrid Data Security Cluster where you want to add the Hybrid Data Security Node.

dcloud.cisco.com

Enter the FQDN or IP address of the Hybrid Data Security Node that you want to register with the Cisco Collaboration Cloud.

hds01.dcloud.cisco.com

Data Security deployment is limited by country. Check to see whether your country is supported.

Register Hybrid Data Security N

You may now register your Hybrid Data Security Node to the Cisco Collaboration Cloud.
Node IP Address/FQDN: hds01.dcloud.cisco.com
Cluster: HDS DC SJC

⚠ Go to your Hybrid Data Security Node within one hour to finish registration.
After one hour you will need to start the process again.

Hybrid Security Node

Registration Complete

Your node is registered to the Cisco Collaboration Cloud and ready for use in your organization.

To manage your node, go to:
Cisco Cloud Collaboration Management

Deployment flow

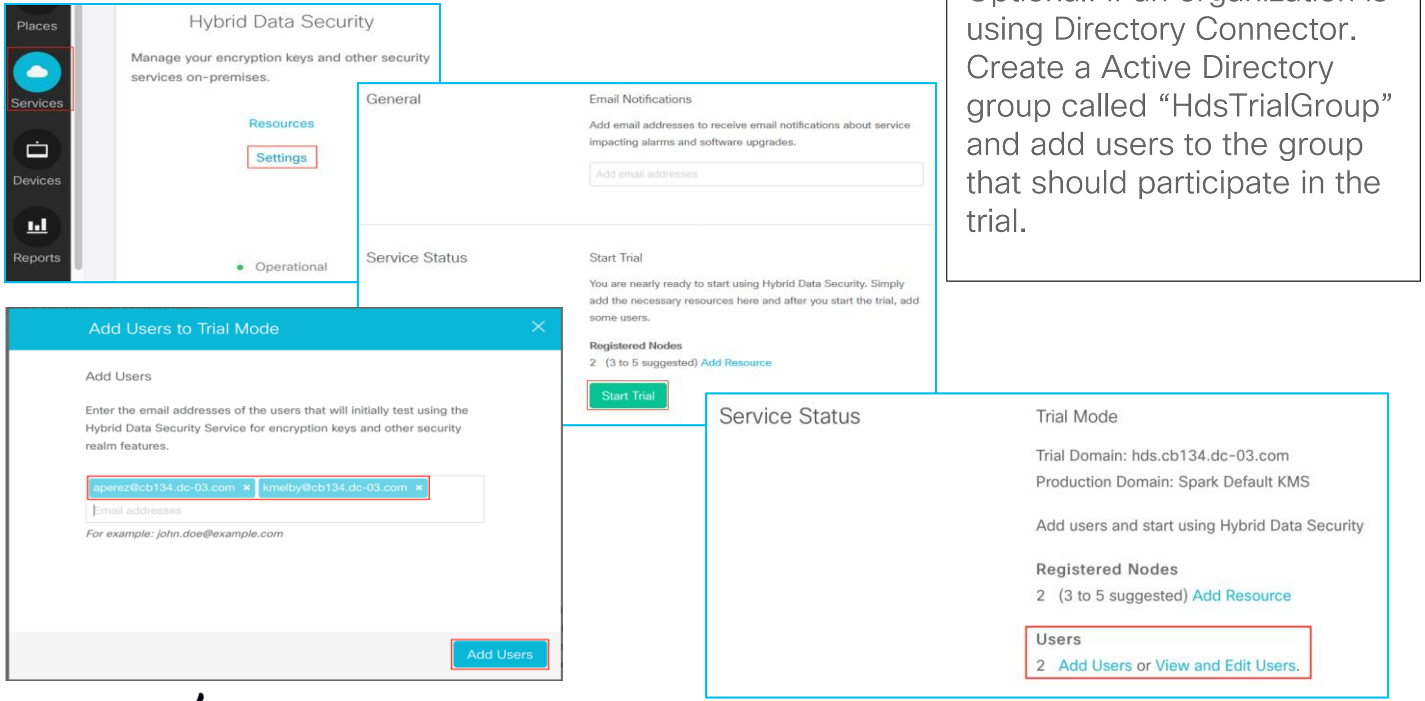
- Deploy & Configure
  tabase & Syslog
  wnload OVA from Webex
  ntrol Hub
  ploy OVA on VMware
  astructure
  nfigure HDS Node
  tname, IP address, DNS, NTP
  ploy and run HDS

virtual
store
trial from

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Active HDS trial from Control Hub



Hybrid Data Security

Manage your encryption keys and other security services on-premises.

Resources

Settings

● Operational

General

Email Notifications

Add email addresses to receive email notifications about service impacting alarms and software upgrades.

Add email addresses

Service Status

Start Trial

You are nearly ready to start using Hybrid Data Security. Simply add the necessary resources here and after you start the trial, add some users.

Registered Nodes

2 (3 to 5 suggested) Add Resource

Start Trial

Add Users to Trial Mode ×

Add Users

Enter the email addresses of the users that will initially test using the Hybrid Data Security Service for encryption keys and other security realm features.

aperez@cb134.dc-03.com × kmelby@cb134.dc-03.com ×

Email addresses

For example: john.doe@example.com

Add Users

Service Status

Trial Mode

Trial Domain: hds.cb134.dc-03.com

Production Domain: Spark Default KMS

Add users and start using Hybrid Data Security

Registered Nodes

2 (3 to 5 suggested) Add Resource

Users

2 Add Users or View and Edit Users.

Optional: if an organization is using Directory Connector. Create a Active Directory group called “HdsTrialGroup” and add users to the group that should participate in the trial.

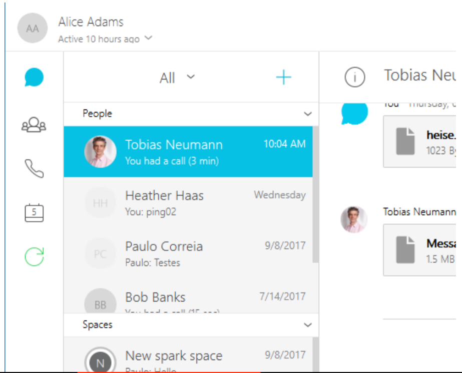
Deployment flow

- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node
  hostname, IP address, DNS, NTP
- Deploy and run HDS Configuration Tool
- Upload Configuration virtual ISO to VMware data store
- Activate Webex HDS trial from Control Hub
- Test environment
- Move to production

Cisco Webex Pro Pack – Hybrid Data Security

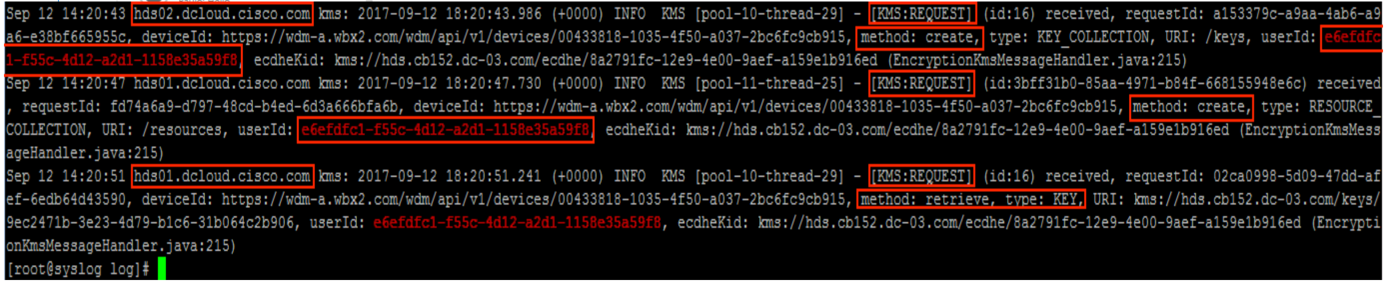
Deployment and Configuration

Test the environment



1. With a user enabled for HDS logon to Spark
2. Create a new space with one or multiple users and send some messages
3. Check your syslog for KMS messages

Example bellow shows KMS:REQUESTS send to local HDS node hds02.dcloud.com. In the example a new KMS is being created by request of a userID represented by UUID. Last line of the log file shows a key being retrieved.



```
Sep 12 14:20:43 hds02.dcloud.cisco.com kms: 2017-09-12 18:20:43.986 (+0000) INFO  KMS [pool-10-thread-29] - [KMS:REQUEST] (id:16) received, requestId: a153379c-a9aa-4ab6-a9
a6-e38bf665955c, deviceId: https://wdm-a.wbx2.com/wdm/api/v1/devices/00433818-1035-4f50-a037-2bc6fc9cb915, method: create, type: KEY_COLLECTION, URI: /keys, userId: e6efdfc
1-f55c-4d12-a2d1-1158e35a59f8, ecdheKid: kms://hds.cb152.dc-03.com/ecdhe/8a2791fc-12e9-4e00-9aef-a159e1b916ed (EncryptionKmsMessageHandler.java:215)
Sep 12 14:20:47 hds01.dcloud.cisco.com kms: 2017-09-12 18:20:47.730 (+0000) INFO  KMS [pool-11-thread-25] - [KMS:REQUEST] (id:3bff31b0-85aa-4971-b84f-668155948e6c) received
, requestId: fd74a6a9-d797-48cd-b4ed-6d3a666bfa6b, deviceId: https://wdm-a.wbx2.com/wdm/api/v1/devices/00433818-1035-4f50-a037-2bc6fc9cb915, method: create, type: RESOURCE_
COLLECTION, URI: /resources, userId: e6efdfc1-f55c-4d12-a2d1-1158e35a59f8, ecdheKid: kms://hds.cb152.dc-03.com/ecdhe/8a2791fc-12e9-4e00-9aef-a159e1b916ed (EncryptionKmsMess
ageHandler.java:215)
Sep 12 14:20:51 hds01.dcloud.cisco.com kms: 2017-09-12 18:20:51.241 (+0000) INFO  KMS [pool-10-thread-29] - [KMS:REQUEST] (id:16) received, requestId: 02ca0998-5d09-47dd-af
ef-6edb64d43590, deviceId: https://wdm-a.wbx2.com/wdm/api/v1/devices/00433818-1035-4f50-a037-2bc6fc9cb915, method: retrieve, type: KEY, URI: kms://hds.cb152.dc-03.com/keys/
9ec2471b-3e23-4d79-b1c6-31b064c2b906, userId: e6efdfc1-f55c-4d12-a2d1-1158e35a59f8, ecdheKid: kms://hds.cb152.dc-03.com/ecdhe/8a2791fc-12e9-4e00-9aef-a159e1b916ed (Encrypti
onKmsMessageHandler.java:215)
[root@syslog log]#
```

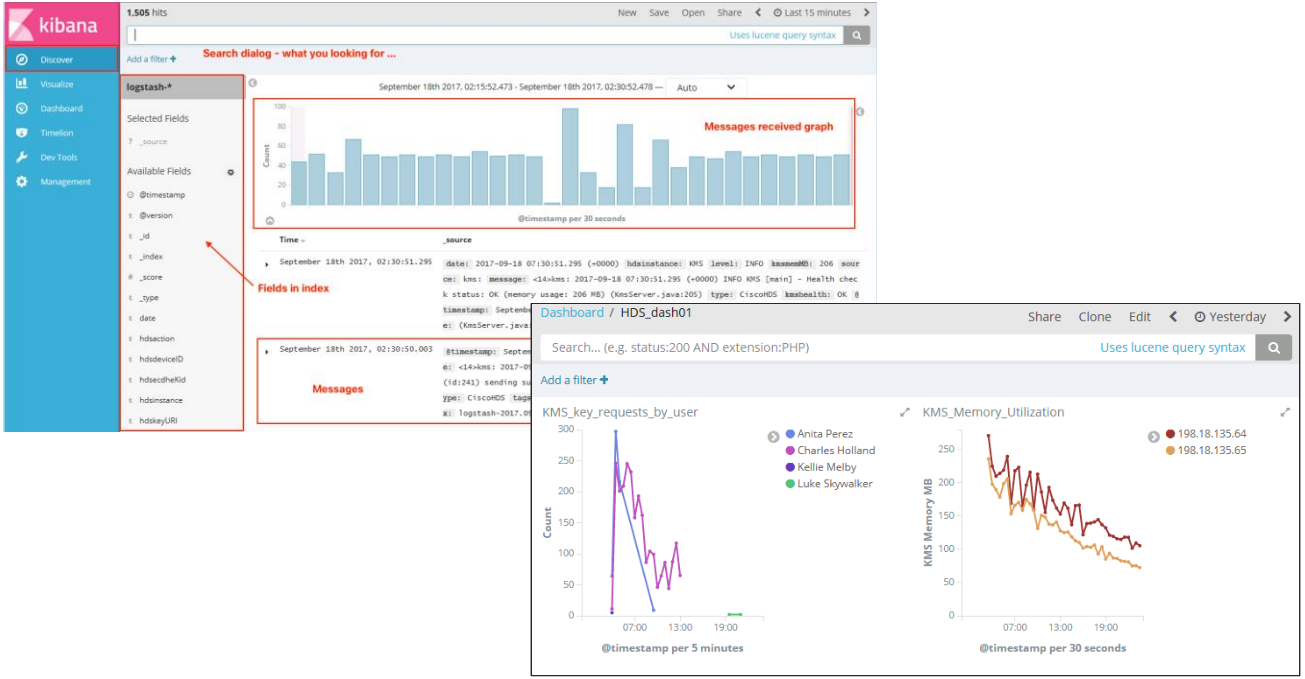
Deployment flow

- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node
  hostname, IP address, DNS, NTP
- Deploy and run HDS Configuration Tool
- Upload Configuration virtual ISO to VMware data store
- Activate Webex HDS trial from Control Hub
- Test environment
- Move to production

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Test the environment (example of utilizing extended logging facility)



Search dialog - what you looking for ...

Messages received graph

Fields in index

Messages

```
September 18th 2017, 02:30:51.295   date: 2017-09-18 07:30:51.295 (+0000) hdsinstance: KMS level: INFO kmsmemMB: 206 sour
                                    ce: kms: message: <14>kms: 2017-09-18 07:30:51.295 (+0000) INFO KMS [main] - Health chec
                                    k status: OK (memory usage: 206 MB) (KmsServer.java:205) type: CiscoHDS kmshealth: OK @
                                    timestamp: Septembe
                                    e: (KmsServer.java:

September 18th 2017, 02:30:50.003   @timestamp: Septem
                                    e: <14>kms: 2017-09
                                    (id:241) sending su
                                    ype: CiscoHDS tags
                                    x: logstash-2017.09
```

Deployment flow

- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node hostname, IP address, DNS, NTP
- Deploy and run HDS Configuration Tool
- Upload Configuration virtual ISO to VMware data store
- Activate Webex HDS trial from Control Hub
- Test environment
- Move to production

cisco Live!

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Before moving to production keep the following important things in mind:

- Key migration is not supported today with Cisco Webex HDS
  - Existing keys on KMS in the Cisco Cloud can not be migrated to HDS
  - Once HDS is deployed and in production keys can not be migrated back to the cloud
- Content preview does expose keys to the cloud
  - Cisco is currently using a 3rd party service to create preview pictures from files uploaded into Webex. As the 3rd party service needs to have access to unencrypted content keys need to be shared. Cisco plans to allow this functionality to be turned off for customers that want to limit the exposure. Mid to long term a rendering service could be envisioned as part of HDS deployment to move the creation of previews to customer premise (not committed subject to change).
- Cisco HDS nodes must be deployed in a single datacenter
- PostgreSQL database must be deployed in same datacenter as HDS nodes
- Limited high availability for PostgreSQL database and Cisco HDS

Deployment flow

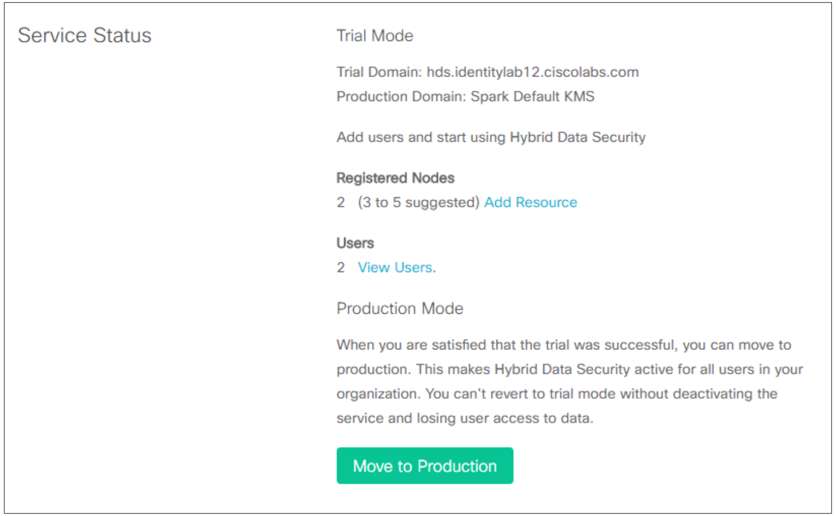
- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node
  hostname, IP address, DNS, NTP
- Deploy and run HDS Configuration Tool
- Upload Configuration virtual ISO to VMware data store
- Activate Webex HDS trial from Control Hub
- Test environment
- Move to production

Cisco Webex Pro Pack – Hybrid Data Security

Deployment and Configuration

Move to production

After successful trial of the HDS functionality and careful review of the considerations from the previous slide customer can move their Cisco Spark organization to production with HDS. This will enable the functionality for all users.



Service Status

Trial Mode

Trial Domain: hds.identitylab12.ciscolabs.com
Production Domain: Spark Default KMS

Add users and start using Hybrid Data Security

Registered Nodes
2 (3 to 5 suggested) Add Resource

Users
2 View Users.

Production Mode

When you are satisfied that the trial was successful, you can move to production. This makes Hybrid Data Security active for all users in your organization. You can't revert to trial mode without deactivating the service and losing user access to data.

Deployment flow

- Deploy & Configure Database & Syslog
- Download OVA from Webex Control Hub
- Deploy OVA on VMware Infrastructure
- Configure HDS Node
  hostname, IP address, DNS, NTP
- Deploy and run HDS Configuration Tool
- Upload Configuration virtual ISO to VMware data store
- Activate Webex HDS trial from Control Hub
- Test environment
- Move to production

Conclusion

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

- Demos in the Cisco Showcase
- Walk-In Labs
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you

You make **possible**