

CISCO *Live!*



#CiscoLive



The bridge to possible

Work From Home Contact Center Agents Using VPN-less Agent Desktop

Contact Center Enterprise

Robert W. Rogier – Technical Consulting Engineer

Maria Jose Mendez Vazquez – Technical Leader

BRKCCT-2915



#CiscoLive

Cisco Webex App

Questions?

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

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCCT-2915>



Agenda

- Introduction
- Overview
- Deployment Models
- Reverse Proxy Configuration
- CCE Configuration
- Conclusion
- Continue Your Education

Introduction



The world has **changed**.

2020 – The year it all changed

- COVID changed what work means for almost all of us
- Mandatory shutdowns, mask mandates, and employee/customer health concerns
- Companies had to scramble to deploy infrastructure

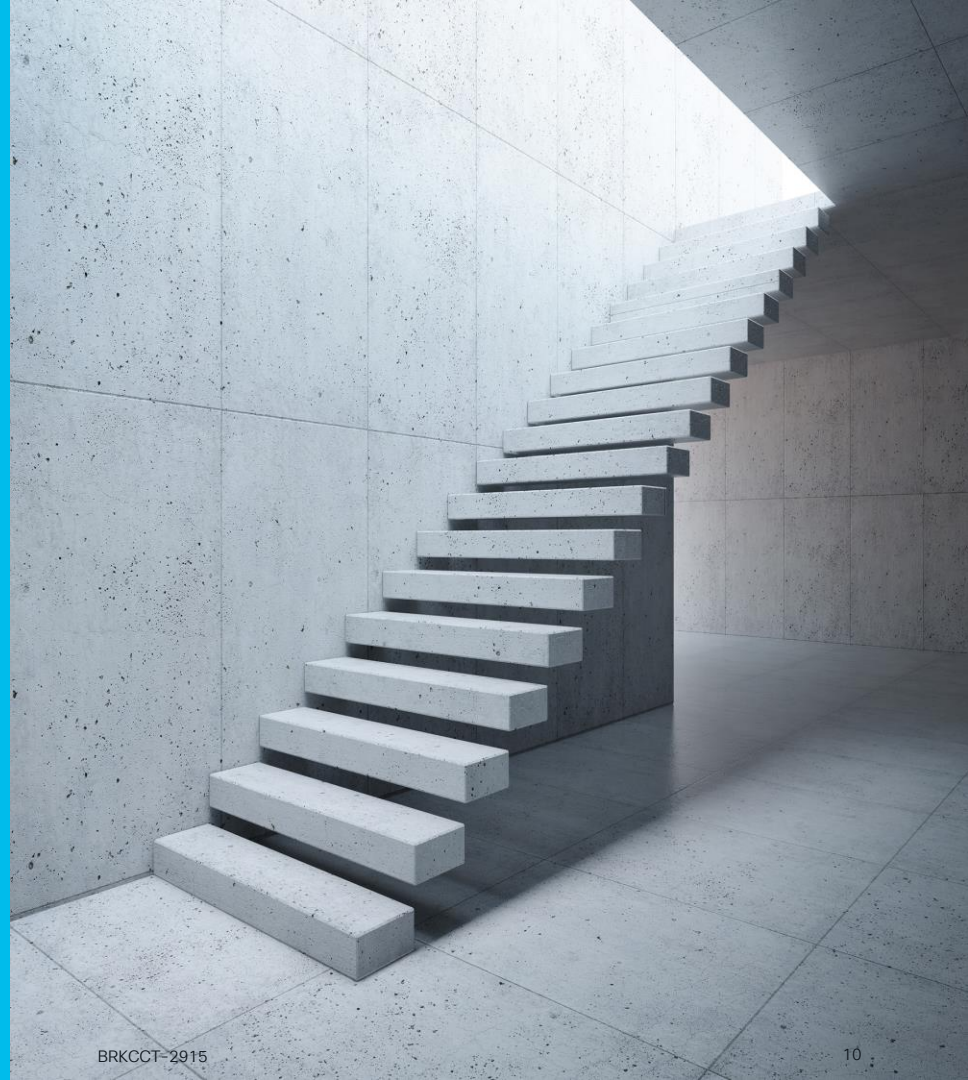
Why was this feature introduced?

- Increase in work-from-home users
- Traditional solutions require VPN infrastructure
- Allows Contact Center agents and supervisors to login from outside the company network without the cost of deploying a VPN

The past

- Previous WFH solutions were resource intensive
 - VPNs – Expensive to implement and maintain
 - VDI – Limited support and latency concerns
- Mobile Agent and MRA only provided part of the answer

The future



Overview



Requirements

VOS components must be at 12.6

- Finesse – ES02 or higher
- CUIC/IDS – ES02 or higher
- Best practice is to install latest ES available for each component
- Reverse Proxy
(Customer provided)

Version Notes

CCE components can be on 12.5

- PG, CC, AW 12.5 supported with 12.6 Finesse and CUIC, with stand-alone Live Data on 12.5
- When Finesse and CUIC are on 12.6, and Live Data is on 12.5, for Live Data gadgets to load in Finesse, install CUIC 12.5(1) ES09 or later on all Live Data stand-alone servers
- CUIC-LiveData-IdS (Coresident) needs 12.6

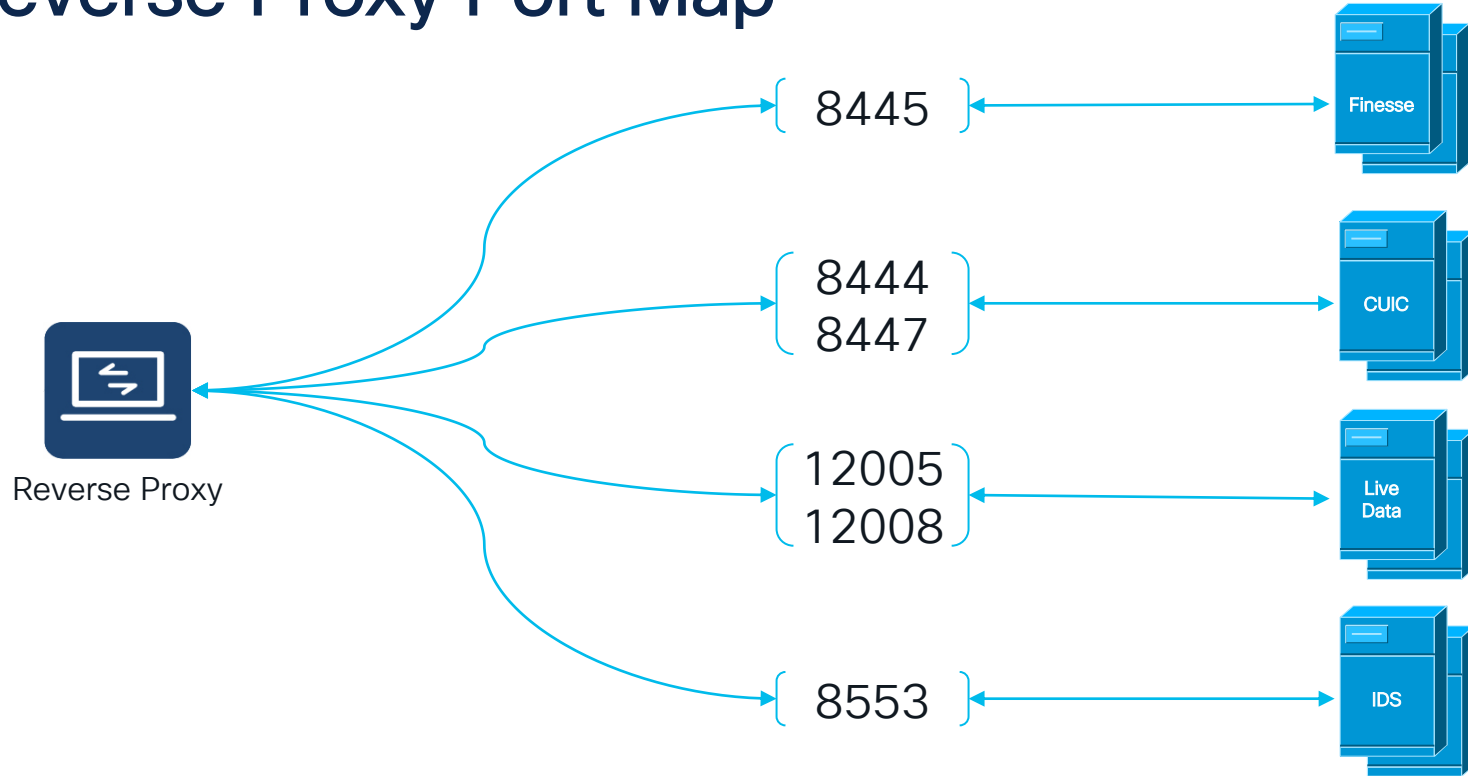
Restrictions

- FIPPA is not supported
- IDP for Single Sign-on must be externally accessible
- Gadgets must be referenced in desktop layout either:
 - On the corporate network deployed on the DMZ
 - Directly accessible from the internet
- Finesse through Reverse Proxy:
 - BOSH notification formats not supported
 - Administrative interface and corresponding API not supported

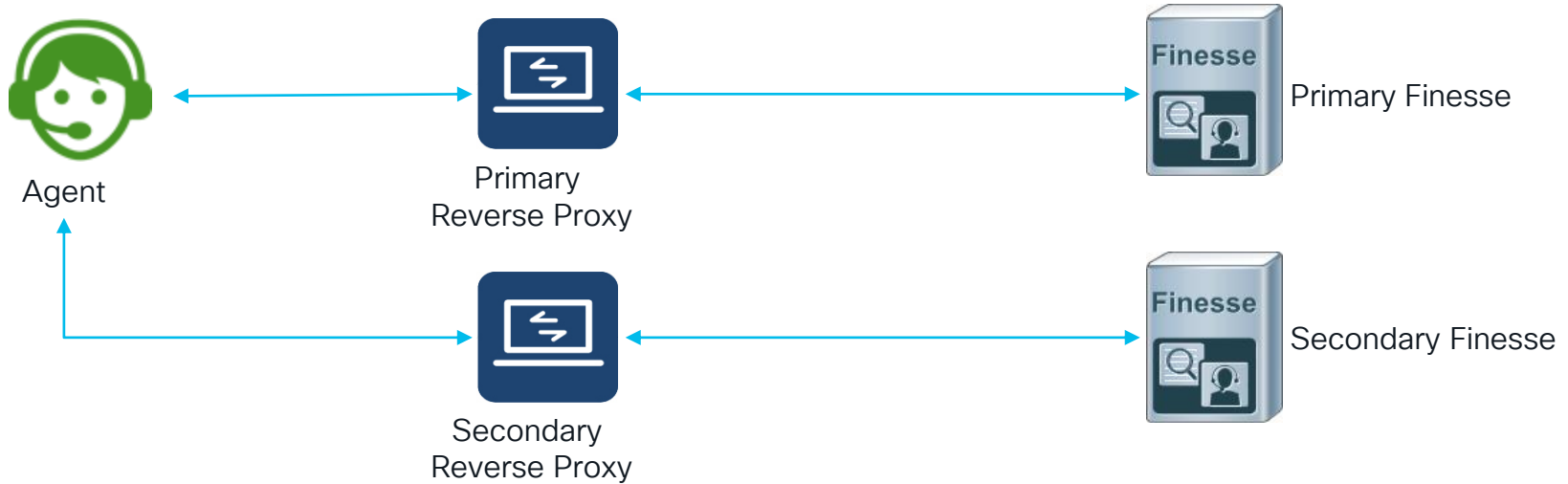
Deployment Models



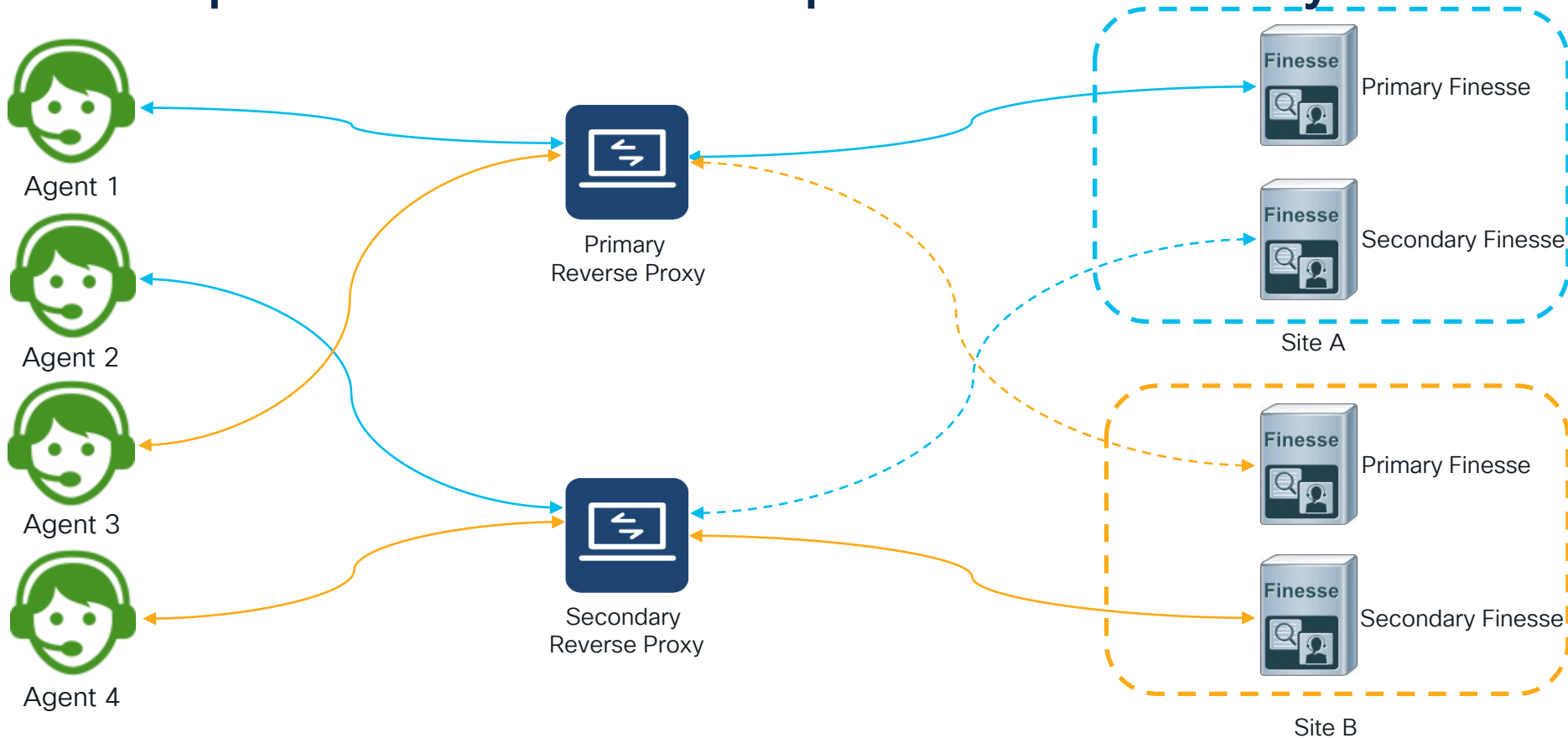
Reverse Proxy Port Map



Reverse Proxy HA per Finesse Cluster



Multiple Finesse Clusters per Reverse Proxy



Agent Login Flow

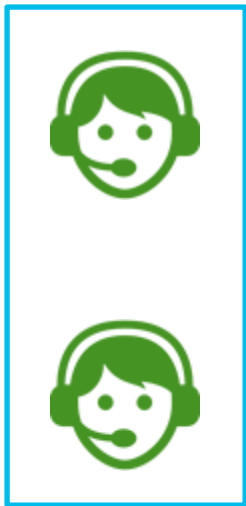
Step 1.

Finesse Administrator configures the trusted proxy hosts or IPs and proxy configuration URL.

LAN Agents/Supervisors



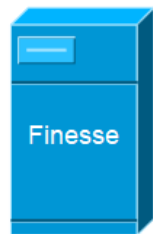
Remote Agents/Supervisors



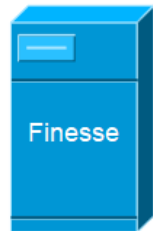
Primary
Reverse Proxy



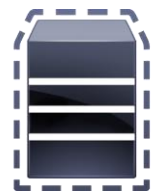
Secondary
Reverse Proxy



Primary Finesse



Secondary Finesse



Proxy Config
Lookup Server



Administrator

Agent Login Flow

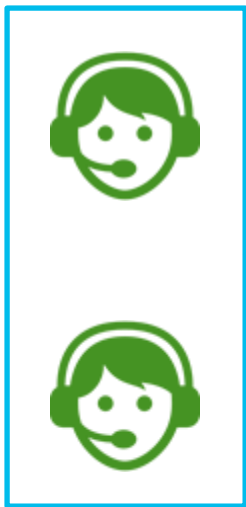
Step 2.

Remote Finesse Agents or Supervisors reach Finesse through a configured reverse proxy.

LAN Agents/Supervisors



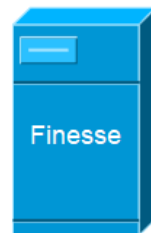
Remote Agents/Supervisors



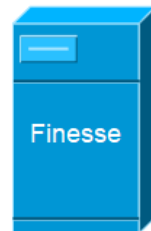
Primary
Reverse Proxy



Secondary
Reverse Proxy



Primary Finesse



Secondary Finesse



Proxy Config
Lookup Server



Administrator

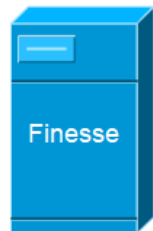
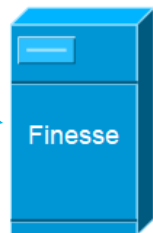
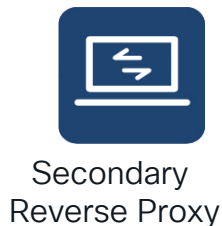
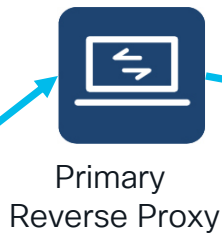
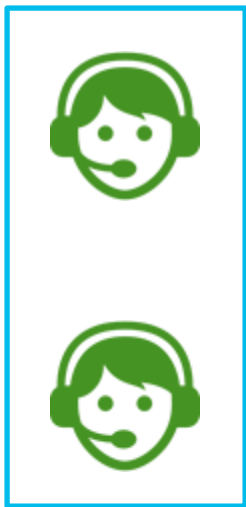
Agent Login Flow

Step 3. Reverse proxy forwards the request to the configured upstream Finesse server based on the Nginx rules.

LAN Agents/Supervisors



Remote Agents/Supervisors



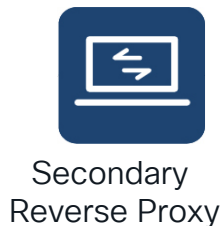
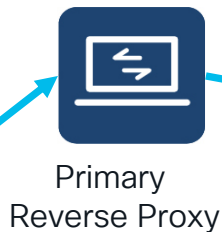
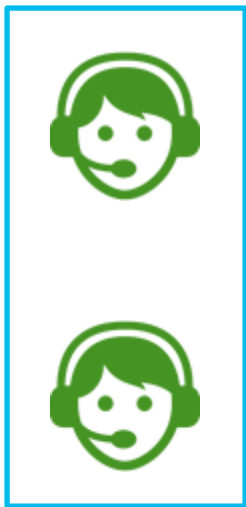
Agent Login Flow

LAN Agents/Supervisors

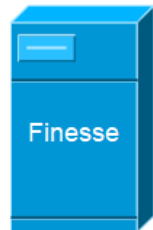


Step 4. Finesse Server looks up the proxy configuration map and takes care of replacing hostnames and port values as configured in proxy map for all the requests that come through the reverse proxy.

Remote Agents/Supervisors



Primary Finesse



Secondary Finesse



Proxy Config
Lookup Server



Administrator

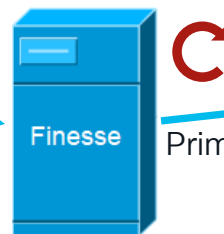
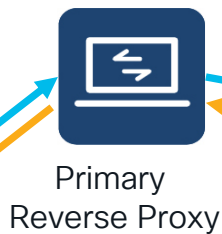
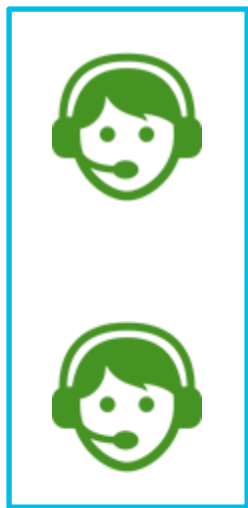
Agent Login Flow

Step 5. Request is served by Finesse through the reverse-proxy.

LAN Agents/Supervisors



Remote Agents/Supervisors

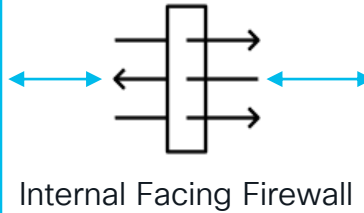
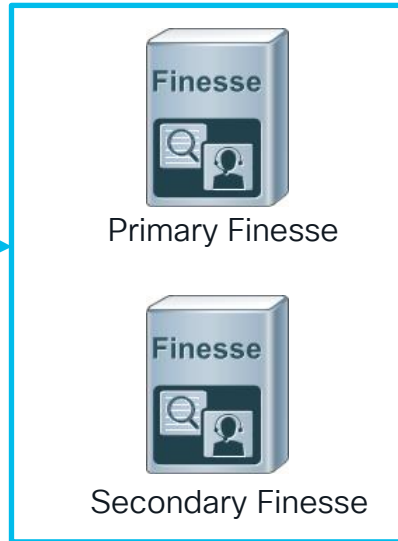


Reverse Proxy Configuration

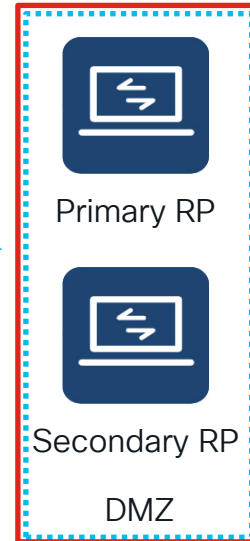


Reverse Proxy

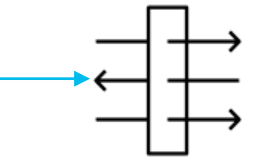
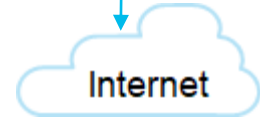
LAN Agents/Supervisors



Internal Facing Firewall



Remote Agents/Supervisors



External Facing Firewall

Proxy Selection

- Customer may choose any reverse proxy they wish
- Step-by-step instructions are given for OpenResty, but this is not a requirement
- Customer is responsible for the proxy; Cisco cannot provide support on any part of the setup or configuration
- Proxy chosen must have Lua support
- Cisco will be releasing a productized installer

Initial RP Configuration

- Install reverse proxy
- Create certificate(s) to be used for external access
- Configure reverse proxy rules
- Populate the network translation data in mapping file
- Host the mapping file on a webserver or RP
- Harden RP server

Proxy Map

```
#Finesse maps
finessel.dcloud.cisco.com:8445=pcce.vpod942.dc-05.com:8445
finessel.dcloud.cisco.com:5280=pcce.vpod942.dc-05.com:5280

#CUIC Maps
cuicl.dcloud.cisco.com:8444=pcce.vpod942.dc-05.com:8444
cuicl.dcloud.cisco.com:8447=pcce.vpod942.dc-05.com:8447

#LiveData Maps
cuicl.dcloud.cisco.com:12005=pcce.vpod942.dc-05.com:12005
cuicl.dcloud.cisco.com:12008=pcce.vpod942.dc-05.com:12008

#IDS Maps
cuicl.dcloud.cisco.com:8553=pcce.vpod942.dc-05.com:8553

#Other Gadget Maps
coeeceweb.dcloud.cisco.com:443=pcce.vpod942.dc-05.com:443
```

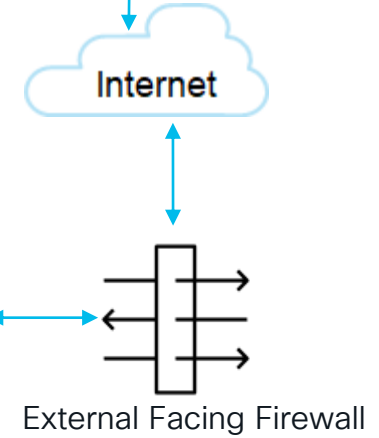
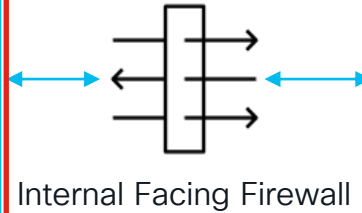
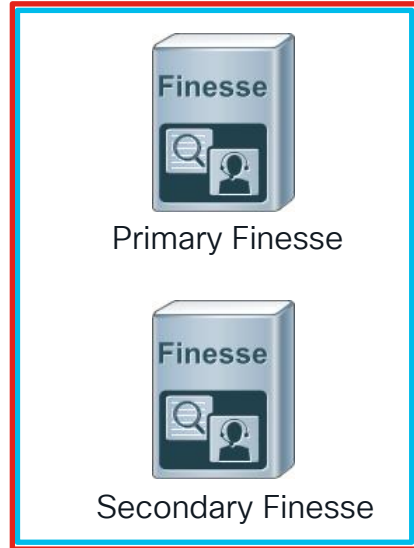
- This is the key file for this solution to work
- Simple, plain-text properties file
- Left-hand entries are internal, right-hand entries are external
- Hosted on proxy server or another web server
- Entries are case sensitive
- Port MUST be specified on both sides of the 'equation'

CCE Configuration



Finesse

LAN Agents/Supervisors



Remote Agents/Supervisors



Configure VOS Servers: Overview

- Proxy server(s) certificate(s) must be in tomcat-trust on each component
- Add the proxy server IP and name to allowed-hosts
- Set the config-uri where the proxy map is hosted
- Update CORS to include proxy server
- Update IdS configuration if SSO is used

Finesse, CUIC and IdS: Certificates

- The SSL Certificates used on the Reverse Proxy must be uploaded to the tomcat-trust store on all three VOS products
- Certificates from VOS products need to be trusted by the Linux server

Finesse, CUIC and IdS: RP CLI Commands

- Add the list of trusted reverse-proxy IP addresses and their corresponding hostnames with the CLI command:

```
utils system reverse-proxy  
allowed-hosts add <IP, FQDN>
```

- Configure the proxy-config map URL with the CLI command:

```
utils system reverse-proxy  
config-uri add <proxymap.txt  
URL>
```

- Restart Service
 - Cisco Web Proxy Service

Finesse: CORS CLI Commands

- Add external FQDN of RP to CORS:

```
utils finesse cors  
allowed_origin add  
https://<EXT FQDN>:8444
```

```
utils finesse cors  
allowed_origin add  
https://<EXT FQDN>:8447
```

- Restart services
 - Cisco Finesse Tomcat
 - Cisco Finesse Tomcat Notification Service

CUIC: CORS CLI Commands

- Add external FQDN of RP to CORS:
utils cuic cors allowed_origin
add https://<EXT
FQDN>:8444

```
utils cuic cors allowed_origin  
add https://<EXT  
FQDN>:8445
```

```
utils cuic cors allowed_origin  
add https://<EXT FQDN>
```

- Restart Service
 - Intelligence Center
Reporting Service

Live Data: CLI Commands

- Add external FQDN of RP to CORS:

```
utils live-data cors  
allowed_origin add  
https://<EXT FQDN>:8444
```

```
utils live-data cors  
allowed_origin add  
https://<EXT FQDN>:8445
```

```
utils live-data cors  
allowed_origin add  
https://<EXT FQDN>
```

- Restart Service
 - Cisco Web Proxy Service

RP / IDP: Single Sign-On

- Ensure IDP is accessible from the internet
- Cisco provided RP configuration does not include IDP maps
- RP configuration must be updated to decrypt token
 - From IDS, execute:
show ids secret
 - Update maps.conf

```
map $host $jwt_secret {~
...## Must-change Replace below value with output of IdS CLI -- show ids secret~
...default "xwUP8GjDxPS0Mhy/9g7PVk/gkW+pUkcpglwjycQX0wQ=";~
}~
~
```

IDS: Redirect URL

Identity Service Management

administrator

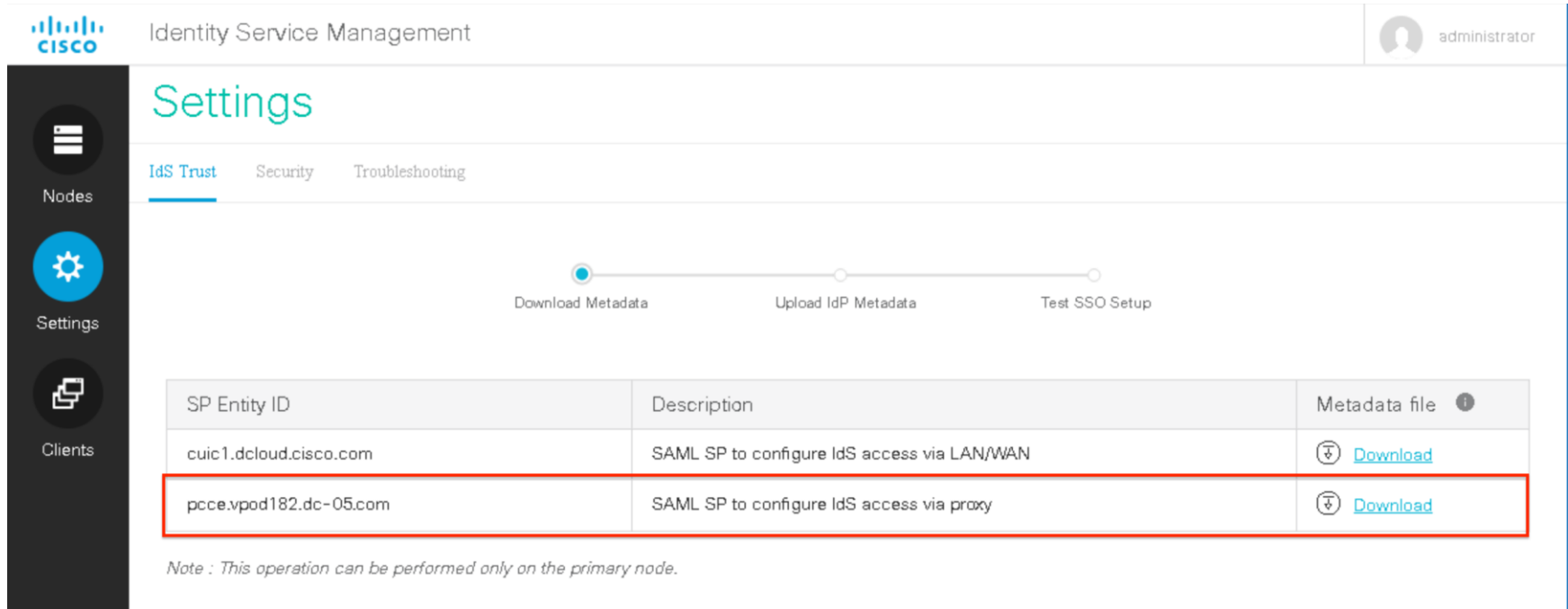
Clients

Search: All New

Client Name	Client ID	Redirect URL	Actions
UNIFIED_CCE_ADMINISTR...	82ffb6c5886b90e6335e27dcc9fa48776148abb5	https://ccedata.dcloud.cisco.com:443	...
FINESSE	f6fb0f4067098b7940be2df538875e42f6e72b50	https://finesse1.dcloud.cisco.com https://pcce.vpod1036.dc-05.com:8445/desktop/sso/authcode	...
CUIC	c48247bf1ce0b6f1555676cb97fab3f4642325af	https://cuic1.dcloud.cisco.com:8444	...

- Add external redirect URL to “FINESSE” Client
- URL: `https://{EXTERNAL_RP_FINESSE_FQDN}:{EXTERNAL_RP_FINESSE_PORT}/desktop/sso/authcode`

IDS: SP Metadata



Identity Service Management

administrator

Settings

IdS Trust Security Troubleshooting

Download Metadata Upload IdP Metadata Test SSO Setup

SP Entity ID	Description	Metadata file ⓘ
cuic1.dcloud.cisco.com	SAML SP to configure IdS access via LAN/WAN	⬇ Download
pcce.vpod182.dc-05.com	SAML SP to configure IdS access via proxy	⬇ Download

Note : This operation can be performed only on the primary node.

- SP Entity is automatically added when relevant CLI commands have been executed
- Metadata file is used to build the Relying Party Trust on customer IDP

IDP / IDS: Single Sign-On

- Configure Relying-Party Trust on IDP for proxy entity
- Upload IDP Metadata to IDS
- Test SSO Login

Gadgets

- Gadgets are rendered the same way as without proxy
- Customer must ensure that gadget server can be accessed from outside the network
- ECE is supported but URL must be accessible from the internet

Conclusion



Planning

Effective planning and discovery is the key to a successful implementation

Gather

Gather a complete inventory of non-Cisco gadgets used in Finesse

- Ensure each gadget can be accessed directly from the Internet or supports VPN-less access (Contact vendor)
- ECE requires the web server be internet accessible, even in an email-only deployment

Verify

Verify your Single Sign-On configuration is ready for VPN-Less use

- IdP must be able to be accessed from the Internet (Cisco Reverse Proxy does NOT include any mappings for the IdP)
- SSO setup may need to be changed if IdP URL is not accessible

Ensure

Ensure that you understand your full topology

- Ensure that you have planned for firewalls and routing and security

Know

Know how your agents will use this feature

- Will you use Mobile Agent or MRA
- Ensure your agents can access all resources required

Best Practices

Reverse-Proxy

- Configure TLS 1.2 and turn off other TLS protocols
- Allow only secure HTTP/2 based access
- Turn off default access and default rules
- Ensure that direct outbound connections to the internet are not allowed
- Ensure API paths other than those explicitly exposed are not available via the configured rules
- Validate the HOST headers
- Maintain security hardened golden images with updated patches and configuration changes

Best Practices

Reverse-Proxy Continued

- Monitor and deploy updated reverse proxy server and proxy configuration whenever there are security updates
- Subscribe to OS security patch updates for proxy hos
- Harden the reverse proxy host following CIS guidelines
- Add effective iptables and rate limits as recommended in the security guide
- Deploy with a Web Application Firewall (WAF)/ Content Delivery Network (CDN) that provides attack prevention

Best Practices

Firewall

- Internal Facing Firewall
- External Facing Firewall

Finesse, IdS, and CUIC servers

- Validate resources periodically
- Regulate the Websocket connections

Keep all servers up to date with patches

Conduct regular security audits

Key Takeaways

New in 12.6

Hybrid work

Reduce costs
(no VPN)

Planning is
KEY

Reference

UCCE 12.6 Features Guide, Mobile Agent, VPN-Less Finesse:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/configuration/ucce_b_features-guide-1261/ucce_m_mobile_agent-1261.html#Cisco_Generic_Topic.dita_48bfd918-9612-4187-be17-58

PCCE 12.6 Features Guide, Mobile Agent, VPN-Less Finesse:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/configuration/ucce_b_features-guide-1261/ucce_m_mobile_agent-1261.html#Cisco_Generic_Topic.dita_48bfd918-9612-4187-be17-58eadec559b4

Configure Nginx Reverse Proxy for VPN Less Access to Cisco Finesse:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/configuration/ucce_b_features-guide-1261/rcct_m_vpnless_1261es04_appendix.html

Security Guidelines for Reverse-Proxy Deployment:

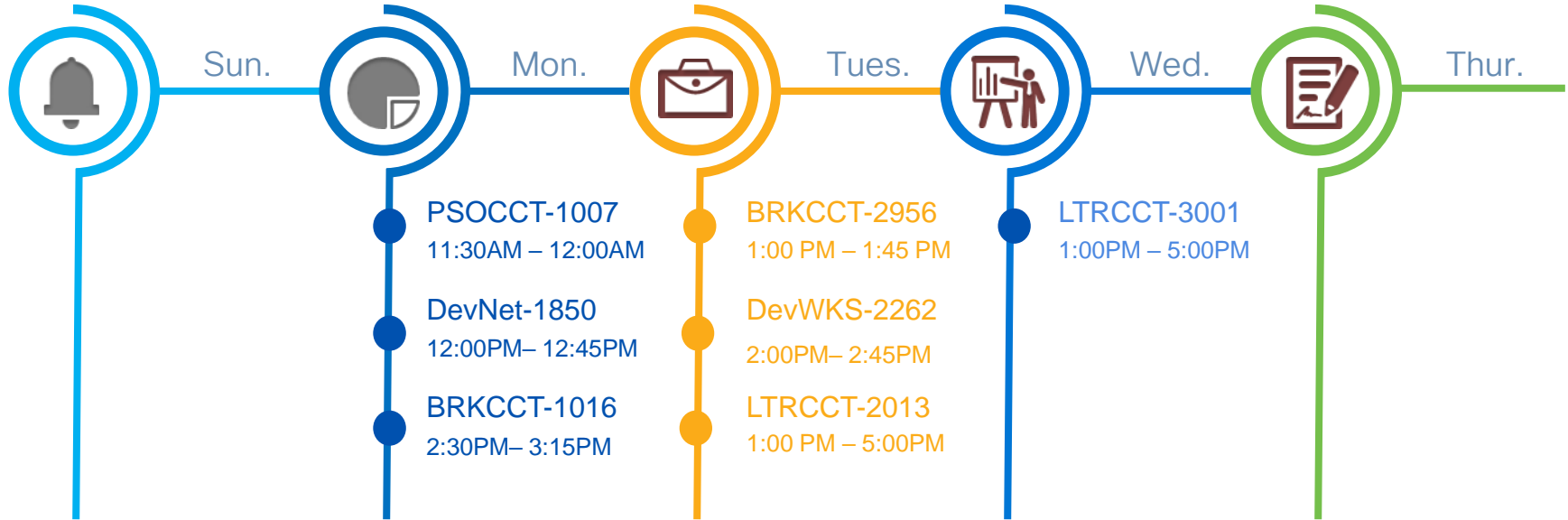
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/configuration/guide/ucce_b_security-guide_12_6_1/rcct_m_1261es2_security-considerations-for-mobile-agent-deployments.html



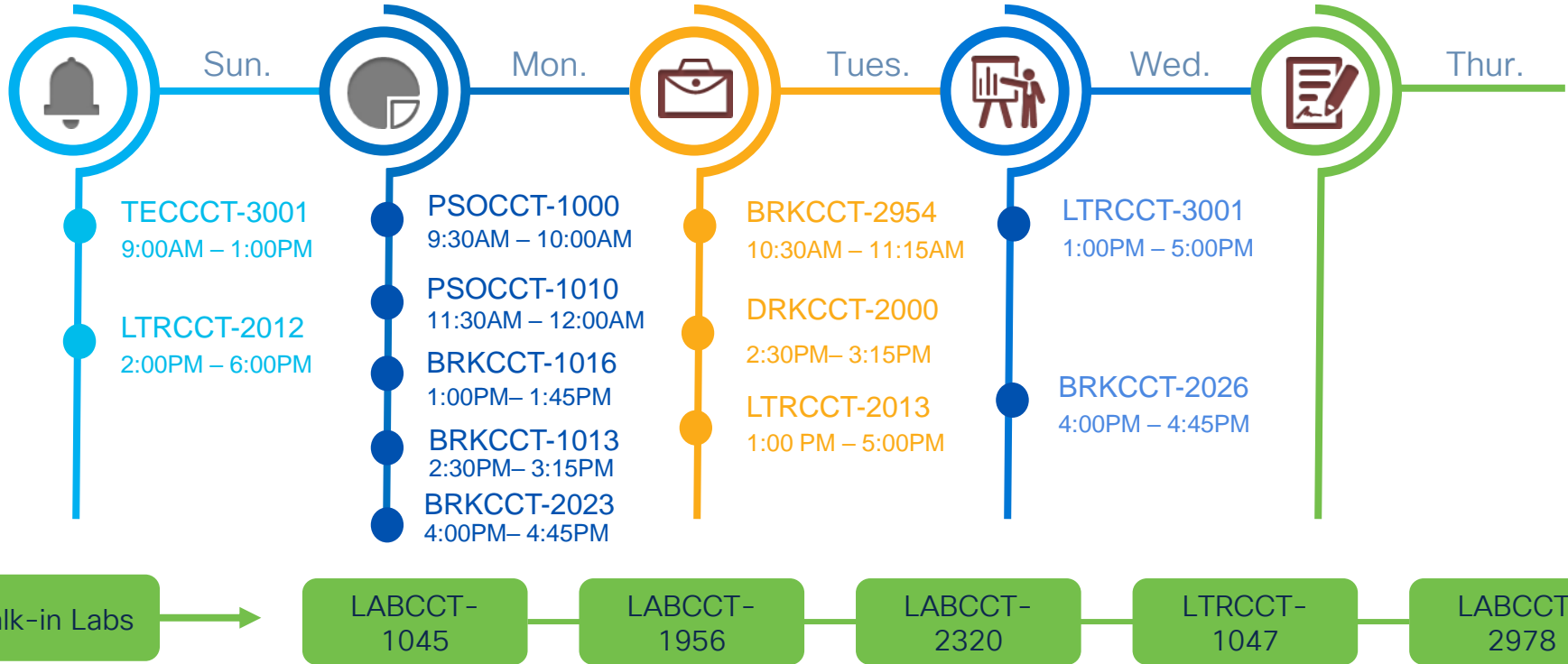
Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

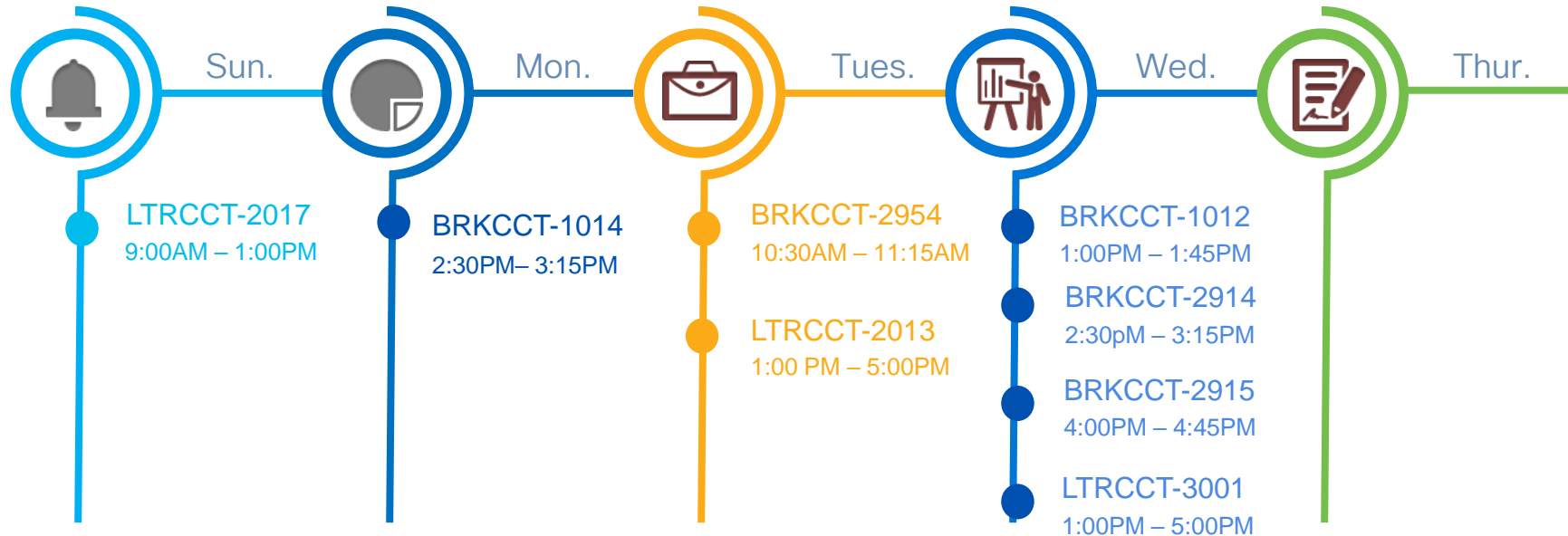
Webex Connect Learning Map



Webex Contact Center Learning Map



Webex Contact Center Enterprise & UCCE Learning Map



Walk-in Labs

LABCCT-
2978

LABCCT-
2392

LABCCT-
2004

LABCCT-
2002

LABCCT-
1555

Schedule



Sunday June 12th

TECCCT-3001

Webex Contact Center Workshop: Differentiating your Customer Experience
Sunday Jun 12
9:00AM – 1:00PM

LTRCCT-2017

Cisco Webex Contact Center & Contact Center Enterprise New Feature Deep Dive Lab
Sunday Jun 12
9:00AM – 1:00PM

LTRCCT-2012

Webex Contact Center Flow Designer: Orchestrating Customer Experiences
Sunday Jun 12
2:00PM – 6:00PM

Monday June 13th

Morning

PSOCCT-1000

The Future of Customer Experience,
today, with Webex Contact Center
Monday Jun 13
9:30AM – 10:00AM

PSOCCT-1007

Orchestrating & automating customer
interactions with Webex Connect
Monday Jun 13
10:30AM – 11:00AM

PSOCCT-1010

Proactive, contextual customer
engagement with Webex Contact
Center and Webex Connect
Monday Jun 13
11:30AM – 12:00AM

Afternoon

DevNet-1850

Introducing Webex Connect and
CPaaS APIs
Monday Jun 13
12:00PM– 12:45PM

BRKCCT-1016

Webex Contact Center Solution
Updates
Monday Jun 13
1:00PM– 1:45PM

BRKCCT-1013

Migrating the Premise Contact Center
to the Cloud
Monday Jun 13
2:30PM– 3:15PM

BRKCCT-1014

Webex Contact Center Enterprise
Solution Updates
Monday Jun 13
2:30PM– 3:15PM

BRKCCT-2023

Understanding your PSTN options for
the Cisco Webex Contact Center
Monday Jun 13
4:00PM– 4:45PM

Tuesday June 14th

BRKCCT-2954

Integrating Digital Channels to Cisco
Contact Center Enterprise and Webex
Contact Center
Tuesday Jun 14th
10:30AM-11:15AM

BRKCCT-2956

Implementing Customer Interaction
Automation Using Webex Connect
Tuesday Jun 14th
1:00 PM – 1:45 PM

BRKCCT-2000

New Webex Contact Center Analyzer
– Data, Analytics, & Insights
Tuesday Jun 14th
2:30 PM – 3:15 PM

DevWKS-2262

Webex Connect and CPaaS
Workshop
Tuesday Jun 14
2:00PM- 2:45PM

LTRCCT-2013

Dip into NEW Digital Channels for Contact Center
Tuesday Jun 14th
1:00 PM – 5:00PM

Wed June 15th

BRKCCT-1012
Contact Center security
Wed. June 15th
1:00PM – 1:45PM

BRKCCT-2914
Managing and Monitoring Contact Center
Enterprise Using AppDynamics
Thursday June 16th
2:30PM – 3:15PM

BRKCCT-2915
Work From Home Contact Center Agents
Using VPN-less Agent Desktop
Wed. June 15th
4:00PM – 4:45PM

BRKCCT-2026
Intelligently Handling Call Traffic Between
Premise & Cloud Contact Center
Wed. June 15th
4:00PM – 4:45PM

LTRCCT-3001
Webex Contact Centre New Digital Channels Bot Capabilities
Wed. June 15th
1:00PM – 5:00PM

Thursday June 16th

No Contact Center/CPaaS track breakout sessions or paid labs for
Thursday June 16th
Walk-in labs are still available

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



Learn

Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning



Train

Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



Certify

Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive