PassQueen
a.k.a dumpsqueen.com

# Implementing Cisco Collaboration Applications (CLICA)

## Cisco 300-810

**Version Demo**

**Total Demo Questions: 27**

**Total Premium Questions: 274**

**Buy Premium PDF**

https://passqueen.com

support@passqueen.com

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Cisco Unified IM and Presence | 130 |
| Topic 2, Cisco Unity Connection | 83 |
| Topic 3, Cisco Expressway | 9 |
| Topic 4, Cisco Collaboration applications security | 15 |
| Topic 5, Single Sign-On (SSO) for Cisco Collaboration Applications | 29 |
| Topic 6, Mix Questions | 8 |
| Total | 274 |

QUESTION NO: 1

An engineer must configure XMPP federation on a Cisco Instant Messaging and Presence Service node, but the XCP XMPP Federation Connection Manager service fails to start. Which action must the engineer take to resolve the issue?

**A.** Activate XMPP federation service

**B.** Enable TLS m the XMPP Federation settings.

**C.** Restart the Cisco XCP Router service

**D.** Restart the Cisco IM and Presence service.

**ANSWER: C**

**Explanation:**

Restart the Cisco XCP Router service is the required action because the XCP XMPP Federation Connection Manager relies on the Cisco XCP Router as part of the IM and Presence XMPP service architecture. The XCP Router provides the routing framework used by XMPP components on the node, including components that establish and manage federation connectivity with external XMPP domains. If the router service is not running properly, is stalled, or has failed during initialization, its dependent federation connection-management process cannot start successfully. Restarting Cisco XCP Router restores the underlying XMPP routing function and allows the XCP XMPP Federation Connection Manager to initialize and register its required connectivity. The engineer should perform the restart from Cisco Unified Serviceability on the affected IM and Presence node, then confirm that both services reach a running state before continuing the federation configuration. Cisco documentation identifies Cisco XCP Router as a core IM and Presence service and provides service-management guidance through Unified Serviceability. See Cisco's IM and Presence Service configuration guides and the IM and Presence Service technical support documentation.

**QUESTION NO: 2**

Digital networking is configured between two Cisco Unity Connection clusters using an HTTPS connection. Which two objects are replicated between these two clusters? (Choose two.)

**A.** partitions and search spaces

**B.** user greetings

**C.** user templates and user greetings

**D.** call handlers

**E.** users and their corresponding mailboxes

**ANSWER: A E**

**Explanation:**

In Cisco Unity Connection HTTPS networking, replication synchronizes the addressing and subscriber information needed for the connected clusters to function as one digital voicemail network. **partitions and search spaces** are replicated so that each cluster has consistent dialing and object-addressing context when resolving networked subscribers and other replicated directory objects. This consistency is necessary for correct addressing and routing of voicemail across the network.

**users and their corresponding mailboxes** are also replicated. A user remains homed on the cluster where the mailbox is stored, but the user's replicated directory information enables subscribers on another connected cluster to address that user and send messages transparently. The mailbox itself remains associated with its home cluster; replication makes the user and mailbox relationship available throughout the HTTPS digital network rather than creating an independently administered mailbox on every cluster.

Cisco documents HTTPS networking as a digital-networking method that replicates selected Unity Connection data between locations to support cross-cluster subscriber addressing and messaging. See Cisco's HTTPS Networking Guide and the Cisco Unity Connection Networking Guide.

## QUESTION NO: 3

An engineer is configuring toll fraud prevention on a Cisco Unity Connection system. The Unity Connection system is integrated with two phone systems each with its own trunk access code Which figuration blocks attempts to bypass the restriction table by dialing trunk access codes?

**A.** Add restriction table patterns to match applicable trunk access codes for both phone system integrations

**B.** Restrict the numbers that can be used for system transfers

**C.** Set up all restriction tables to block calls to the international operator

**D.** Set up restriction tables to block all calls to international numbers.

## ANSWER: A

**Explanation:**

Add restriction table patterns to match applicable trunk access codes for both phone system integrations is correct because Cisco Unity Connection restriction tables evaluate the digits entered for call transfers and can block dialing patterns that represent external-access prefixes. A trunk access code, such as a digit used to obtain an outside line, must be included in the restriction patterns so that a caller cannot evade the intended controls merely by prepending the phone-system-specific access code to a destination number. Because this Unity Connection deployment integrates with two phone systems and each has its own code, the restriction table must contain patterns for every applicable trunk access code. The patterns should be associated with the relevant transfer restrictions so that Unity Connection applies them before completing a supervised or released transfer. This approach protects the transfer feature at the point where Unity Connection processes the dialed digit string, rather than relying on users to omit an external-access prefix. Cisco documents restriction tables as the mechanism for restricting the numbers that callers and users can dial during transfers, including patterns designed to prevent toll fraud. See Cisco's Restriction Tables and Toll Fraud Prevention documentation and the Cisco Unity Connection Administration Guide.

## QUESTION NO: 4

Which two certificate requirements apply to Cisco Expressway-E when Mobile and Remote Access is deployed? (Choose two.)

**A.** The certificate SAN must include the Expressway-E FQDN returned by the _collab-edge SRV record.

**B.** The certificate must be trusted by remote clients.

**C.** The certificate must contain the IP address of every Unified CM node.

**D.** The certificate must be installed only in the Unified CM tomcat-trust store.

**E.** The certificate common name must be the internal domain controller name.

## ANSWER: A B

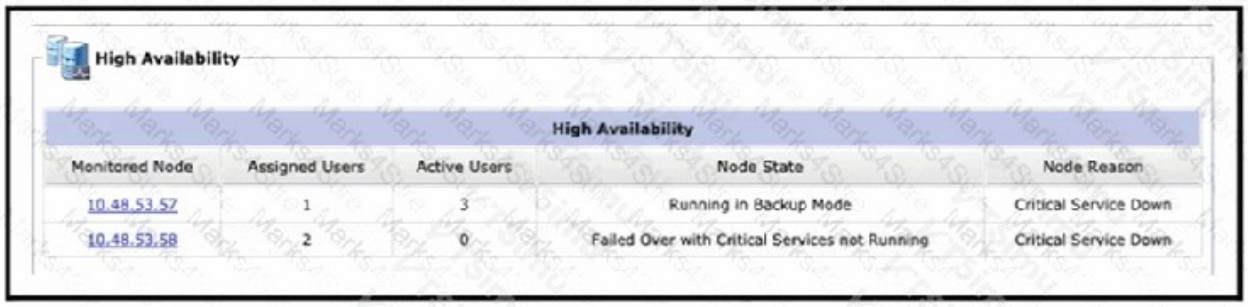
**Explanation:**

The certificate installed on Cisco Expressway-E must contain the externally discoverable collaboration edge name in its subject alternative name. Remote clients use the target returned by the `_collab-edge._tls` SRV record to connect to Expressway-E, and the client validates that the server certificate identity matches that hostname.

The certificate must also be issued by a certificate authority trusted by the remote clients. A client that cannot validate the issuer chain or hostname cannot establish the required TLS connection for Mobile and Remote Access. Cisco documents certificate and DNS requirements in the Cisco Expressway installation and configuration guides.

## QUESTION NO: 5

Refer to the exhibit.




An organization is moving from on-premise Exchange to Microsoft Office 365 for email and calendaring. The administrator would like to maintain meeting presence functionality in Jabber clients connected to Cisco IM and Presence after this move. Office 365 certificates must be installed to accomplish this. Which two trust stores should these certificates be uploaded to on Cisco IM and Presence? (Choose two.)

**A.** cup-xmpp- trust

**B.** xmpp-fed-trust

**C.** cup-trust

**D.** tomcat-trust

**E.** xmpp- rust

**ANSWER: A C**

**Explanation:**

Meeting presence lets Cisco Jabber obtain calendar-based availability and meeting details through the Cisco IM and Presence Service integration with Exchange Online (Office 365). To establish the required TLS trust relationship after the mailbox and calendaring services move to Office 365, the relevant Microsoft certificate chain must be trusted by both the Cisco Unified Presence service components and the XMPP-related service components that support Jabber presence. Cisco documents this requirement as importing the Office 365 certificates into the **cup-trust** and **cup-xmpp-trust** certificate stores on every applicable IM and Presence node. The certificate chain should include the appropriate issuing CA certificates needed to validate the Office 365 endpoint certificate, rather than only an unrelated local server certificate. Once the certificates are installed and the Exchange integration is configured with the Office 365 service details, IM and Presence can securely query calendar information and publish the resulting meeting presence to Jabber users. Cisco's IM and Presence administration guidance describes certificate-store management and the Exchange calendar integration requirements in the IM and Presence Service Administration Configuration Guide. Microsoft also documents the certificate and TLS requirements for Exchange client-access services at Microsoft Learn.

**QUESTION NO: 6**

Which two steps are needed to configure high availability in Cisco IM and presence? (choose two.)

**A.** Enable the Failover Check box

**B.** Configure CUP administrator

**C.** Assign the subscriber to the redundancy group

**D.** Select the enable high availability checkbox and save the configuration change

**E.** Configure the CUP AXL user.

**ANSWER: C D**

**Explanation:**

Cisco IM and Presence high availability is configured by first enabling the high-availability function for the deployment and then defining how the participating servers provide redundancy. Selecting the enable high availability checkbox and saving the configuration change activates the high-availability configuration on the IM and Presence deployment. This is the administrative action that permits the service to use redundant-node behavior rather than operating solely as independent nodes.

After high availability is enabled, assigning the subscriber to the redundancy group establishes its relationship with the corresponding publisher node. A redundancy group is the logical pairing used by IM and Presence for failover and service continuity. It determines the server pair that supports users and services if the active server becomes unavailable. Together, enabling high availability and placing the subscriber into the appropriate redundancy group complete the essential configuration required for an IM and Presence redundant deployment. Cisco documents redundancy groups and the high-availability setup workflow in the IM and Presence administration guidance, available from the Cisco IM and Presence configuration guides and the Cisco IM and Presence documentation portal.

## QUESTION NO: 7

An engineer is asked to configure cisco jabber for windows on-premises, in phone-only mode and later with cisco IM and presence. In the configuration steps, which two DNS records will be needed, assuming the jabber client is in “domain.com?’ (Choose two.)


**A.** _cisco-uds._tcp.domain.com

**B.** Option B

**C.** Option C

**D.** Option D

**E.** _cuplogin._tcp.domain.com

## ANSWER: A E

**Explanation:**

For on-premises Cisco Jabber service discovery, the required DNS SRV records are `_cisco-uds._tcp.domain.com` and `_cuplogin._tcp.domain.com`. The Cisco UDS record enables the Jabber client to discover Cisco Unified Communications Manager and access the User Data Service. This discovery mechanism supports the initial phone-only deployment because Jabber can locate its calling services without requiring a manually specified server address in the client configuration. The record should point to the Unified CM publisher or other appropriate Unified CM node that provides UDS.

When Cisco IM and Presence is introduced, the CUPS login record enables Jabber to locate the IM and Presence service for instant messaging and presence registration. It should target the IM and Presence service node designated to accept client logins. Both records are created in the DNS forward-lookup zone corresponding to the users’ email/domain suffix, here `domain.com`, and use the appropriate TCP service port specified for the relevant Cisco service. Cisco documents these records as the standard on-premises service-discovery method for Jabber clients. See the Cisco Jabber installation and configuration guide and Cisco’s Jabber DNS service-discovery documentation.

## QUESTION NO: 8

Which two Cisco Unified Communications Manager services are involved in generating and collecting call detail records for a cluster? (Choose two.)

**A.** Cisco CallManager

**B.** Cisco CDR Repository Manager

**C.** Cisco TFTP

**D.** Cisco RIS Data Collector

**E.** Cisco SOAP - CDROnDemand

**ANSWER: A B**

**Explanation:**

**Cisco CallManager** is involved because it processes calls and generates call detail record information when CDR is enabled through the applicable service parameters. The resulting records contain call-related information that can be used for reporting, troubleshooting, and billing analysis.

**Cisco CDR Repository Manager** collects CDR files from cluster nodes and manages the repository from which records can be retrieved. In a standard deployment, this service runs on the Unified CM publisher and provides the collection function for the cluster.

Cisco RIS Data Collector gathers real-time registration and device-status information, rather than CDR files. Cisco TFTP distributes configuration files to endpoints and does not participate in CDR generation or repository collection.

See the Cisco Unified Communications Manager Serviceability Administration Guide.

**QUESTION NO: 9**

An end user opened a ticket, stating that before logging in to Jabber for Windows, a warning is displayed that a server certificate has expired. Which two certificates must be verified on the Cisco Unified Communications Manager and IM&P deployment? (Choose two.)

**A.** capf on Cisco Unified CM

**B.** cup-xmpp on IM&P

**C.** callmanager on Cisco Unified CM

**D.** tomcat on Cisco Unified CM

**E.** cup on IM&P

**ANSWER: B D**

**Explanation:**

The certificates to verify are **cup-xmpp on IM&P** and **tomcat on Cisco Unified CM**. Jabber for Windows uses HTTPS services on Unified Communications Manager during sign-in and service discovery, so the Unified CM Tomcat certificate must be valid, current, and trusted by the client. The Tomcat certificate secures the web-based interfaces and service requests that Jabber uses to obtain configuration and authenticate against the collaboration deployment.

After Jabber is directed to the IM&P service, it establishes its XMPP client connection with the IM&P node. The IM&P *cup-xmpp* certificate secures that XMPP service. An expired certificate in either of these client-facing paths can therefore trigger a server-certificate expiration warning before the user completes sign-in. Administrators should check the expiration dates in Cisco Unified OS Administration, renew certificates where necessary, and ensure that the renewed certificate chain is trusted by Jabber clients. Cisco documents these Jabber certificate dependencies and the relevant IM&P and Unified CM certificates in its Jabber certificate troubleshooting guidance and Jabber certificate planning documentation.

## QUESTION NO: 10

Refer to the exhibit.

A Jabber user is unable to access voicemail. During troubleshooting, an administrator captures this screenshot. What are the two ways to resolve this issue? (Choose two.)

**A.** Ask the user to click on the Connect to a device" button and use the correct username and password.

**B.** Ensure the user is not locally created on Cisco Unity Connection with a password expiring separately from the password that is used for Jabber.

**C.** Make sure the Jabber service profile created in Cisco UCM contains Unity Connection UC service with a voicemail server configured.

**D.** Ask an administrator to create an account for this user in Cisco Unity Connection but remove the Unity Connection UC service from the Cisco UCM Jabber service profile.Check if "OAuth with Refresh Login Flow" is enabled on Cisco Unity Connection but disabled in Cisco UCM.

## ANSWER: B C

**Explanation:**

Ensuring that the user is not locally created on Cisco Unity Connection with a separately expiring password addresses a common voicemail-authentication issue. When Jabber accesses Unity Connection, the voicemail credentials must remain valid and consistent with the identity and authentication design. A locally managed Unity Connection account can have an independently expired or changed password, preventing Jabber from authenticating to voicemail even while the user can sign in to Jabber successfully. Using directory-integrated users and maintaining the intended password synchronization or authentication configuration prevents this condition.

The Jabber service profile in Cisco Unified CM must also contain a Unity Connection UC service that points to a configured voicemail server. Jabber obtains voicemail-server information through the assigned service profile and its UC service configuration. Without that association, Jabber has no valid Unity Connection destination for voicemail features such as visual voicemail, message retrieval, and calling voicemail. The UC service must specify the appropriate Unity Connection server details and be included in the service profile assigned to the affected user. Cisco documents Unity Connection service assignment as part of Jabber voicemail integration and deployment. See the Cisco Jabber Feature Configuration Guide and the Cisco Unity Connection User Setup Guide.

## QUESTION NO: 11

What prevents toll fraud on voicemail ports?

**A.** IP address trusted list on the PSTN gateway

**B.** CSS

**C.** Block OffNet to OffNet Transfer service parameter

**D.** FAC

## ANSWER: B

**Explanation:**

CSS is correct because the calling search space assigned to Cisco Unity Connection voicemail ports controls the destinations that those ports are allowed to reach when Unity Connection transfers or places a call through Cisco Unified Communications Manager. Toll-fraud protection depends on applying a deliberately restrictive CSS to the voicemail ports: it should include only the partitions required for legitimate internal extensions, voicemail-related destinations, and any explicitly approved services. It must not provide access to route patterns, translation patterns, or other dial-plan objects that can send a call to the PSTN unless that capability is specifically required and protected. This limits the ability of an outside caller who reaches voicemail to exploit transfer functionality to create unauthorized outbound calls. Cisco's Unity Connection toll-fraud guidance identifies the voicemail-port calling search space as a key control and recommends restricting it to the minimum

necessary calling privileges. This approach follows the Cisco dial-plan best practice of using partitions and calling search spaces to enforce least-privilege calling permissions at the originating device or application port. See Cisco's Unity Connection toll-fraud prevention guidance and the Cisco Unified Communications Manager Security Guide.

## QUESTION NO: 12

A collaboration engineer is configuring SIP interdomain federation for Cisco IM and Presence. The external domain cannot be discovered using DNS SRV. If the external enterprise domain is ciscocollab.com, what destination pattern should the engineer use for a static route?

**A.** com.ciscocollab.*

**B.** _sipfederationtls._tcp.ciscocollab.com

**C.** *.ciscocollab.com,*

**D.** .ciscocollab.com

## ANSWER: A

**Explanation:**

`com.ciscocollab.*` is the appropriate static-route destination pattern because Cisco IM and Presence Service expresses federated SIP destination domains in reverse-domain notation. The DNS-style enterprise domain `ciscocollab.com` is therefore represented with the top-level domain first, followed by the organization label: `com.ciscocollab`. Appending `.*` makes the pattern applicable to the matching federation destination namespace. This static route supplies an explicitly configured next hop when the normal DNS SRV discovery process cannot locate the remote federation service. In this situation, the route pattern identifies the remote SIP domain to which federation traffic is addressed, while the static-route configuration also defines the remote server or proxy details used to forward that traffic. Cisco's IM and Presence Service federation configuration documentation describes static SIP federation routes as the method to use when DNS-based discovery is unavailable and documents the required destination-pattern format. Review the Cisco IM and Presence Service installation and configuration guides and the Cisco IM and Presence Service product documentation for the release-specific static federation routing workflow.

## QUESTION NO: 13

Refer to the exhibit.

A company deployed the Cisco Webex calling with Cisco Unified Border Element as a local gateway for PSTN calls and a firewall to restrict and control the HTTP-based traffic that leaves and enters the network. However, Alice in LA cannot dial 82024001 to reach Charlie in NY. Which action must an administrator take to resolve the issue?

**A.** Open UDP port 5062 outbound on the firewall.

**B.** Open TCP port 5062 outbound on the firewall.

**C.** Open TCP port 8934 outbound on the firewall.

**D.** Open UDP port 8934 outbound on the firewall.

## ANSWER: B

**Explanation:**

Open TCP port 5062 outbound on the firewall. A Cisco Unified Border Element operating as a Webex Calling Local Gateway must establish outbound SIP signaling connectivity to the Webex Calling cloud. That signaling connection uses SIP over TLS, which runs over TCP destination port 5062. Allowing this outbound connection enables the Local Gateway to register or maintain its trunk signaling relationship with the Webex Calling platform and exchange the SIP call-control messages required to route a call between users at different locations. The firewall policy must permit the connection from the Local Gateway to the Cisco Webex Calling signaling infrastructure; return traffic for the established TCP session must also be

allowed by the firewall's stateful inspection behavior. This requirement is specifically distinct from HTTP-based web access: the call setup path for the Local Gateway uses secured SIP signaling, not ordinary HTTP. Cisco's Webex Calling network requirements identify TCP 5062 as the secure SIP signaling port used by Local Gateways. Cisco's Local Gateway configuration guidance also describes the TLS-based SIP connection between Cisco IOS XE CUBE and Webex Calling. See Webex Calling network requirements and Configure Local Gateway on Cisco IOS XE for Webex Calling.

## QUESTION NO: 14 - (DRAG DROP)

DRAG DROP

Drag and drop the steps for SAML SSO authentication from the left into the order on the right.

**Select and Place:**

| | |
|---|---|
| The client attempts to access a resource. | step 1 |
| The client sends an authentication request to an IdP. | step 2 |
| The client sends a signed response to the service provider. | step 3 |
| The IdP authenticates the client by using a signed response. | step 4 |
| The service provider redirects the client to the IdP. | step 5 |

## ANSWER:

| | |
|---|---|
| The client attempts to access a resource. | The client attempts to access a resource. |
| The client sends an authentication request to an IdP. | The service provider redirects the client to the IdP. |
| The client sends a signed response to the service provider. | The client sends an authentication request to an IdP. |
| The IdP authenticates the client by using a signed response. | The IdP authenticates the client by using a signed response. |
| The service provider redirects the client to the IdP. | The client sends a signed response to the service provider. |

**Explanation:**

The correct SAML single sign-on sequence begins when the client attempts to access a protected resource at the service provider. Because the client does not yet have an authenticated session for that resource, the service provider initiates the federation process by redirecting the client to the identity provider. This browser redirect is important because the client acts as the transport mechanism between the two federation endpoints.

After reaching the identity provider, the client submits the authentication request to it. The identity provider then performs the user authentication process and creates the signed SAML response that represents the successful authentication result.

Signing protects the integrity and authenticity of the SAML information so that the service provider can trust the assertion when it receives it.

Finally, the client sends the signed response to the service provider. The service provider validates the response and can establish the authenticated session that permits access to the requested resource. Thus, the placed order correctly represents the client's initial resource request, redirection to the identity provider, authentication exchange, generation of the signed authentication result, and delivery of that result back to the service provider. Cisco documents this browser-based SAML SSO interaction in its SAML SSO Deployment Guide.

## QUESTION NO: 15

Which type of protocol is OAuth 2.0?

**A.** single sign-on

**B.** authorization

**C.** accounting

**D.** authentication

## ANSWER: B

**Explanation:**

OAuth 2.0 is an **authorization** framework. It enables a resource owner to delegate limited, scoped access to protected resources—such as APIs, user profiles, calendars, or collaboration data—to an application without disclosing the resource owner's password to that application. Instead of sharing credentials, the application obtains an access token from an authorization server and presents that token to the resource server. The token represents the granted permissions and is normally limited by scopes, lifetime, and the authorization flow used.

This delegated-access model is especially relevant to Cisco collaboration integrations, where an external application may need permission to call a service API on a user's behalf while preserving credential security and allowing access to be constrained or revoked. OAuth itself does not define a standard way to convey a user's identity; protocols such as OpenID Connect can layer identity capabilities on top of OAuth 2.0 when authentication information is needed. The OAuth 2.0 framework and its roles, grant mechanisms, access tokens, and scopes are defined in RFC 6749. For a practical standards-based overview of OAuth's delegated authorization purpose, see the OAuth 2.0 documentation.

## QUESTION NO: 16

Refer to the exhibit.

Apple Push Notification integration is configured in a Cisco Unified IM and Presence deployment and has been working property. Administrators now report the error â€œPush notification settings cannot be configured. 400 Bad Request.â€ in the GUI, and HTTP logs are displaying the errors that are shown in the exhibit. Which action solves this issue?

**A.** Fix the network connectivity to Apple iCloud.

**B.** Reboot the IM&P cluster.

**C.** Change the HTTP proxy settings to remove errors in request syntax.

**D.** Update Refresh Token Manually.

## ANSWER: D

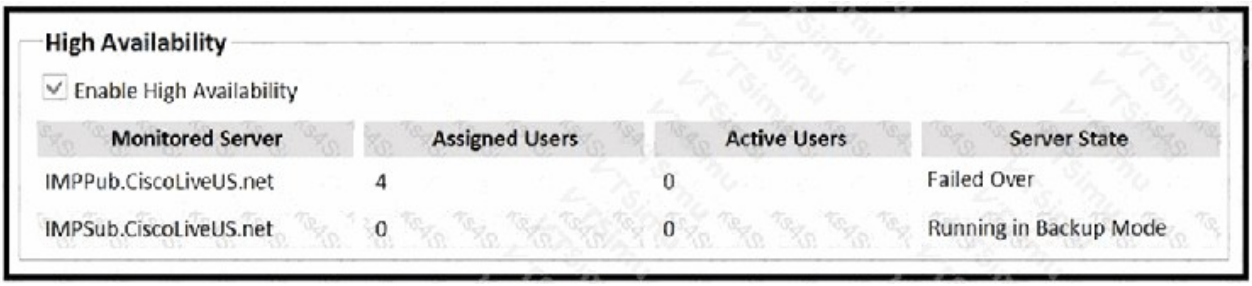
**Explanation:**

Update Refresh Token Manually is the appropriate remediation when a previously functioning Apple Push Notification deployment begins returning an HTTP 400 Bad Request while the administrator attempts to view or configure the push-notification settings. Cisco Unified IM and Presence uses the configured OAuth refresh token to obtain access tokens

required for its push-notification service integration. If that refresh token has expired, been revoked, or otherwise become invalid, the token-refresh request is rejected and the administration interface cannot successfully retrieve or save the associated configuration. Generating a replacement refresh token through the required Cisco process and entering it manually restores the authentication relationship, allowing the system to obtain valid access tokens again. This is a credential-lifecycle issue rather than an indication that the IM and Presence nodes require a restart. Cisco's Push Notifications Deployment Guide documents the refresh-token configuration workflow and the procedure for manually updating the token when required. See the Cisco Push Notifications Deployment Guide and Cisco's Unified Communications Manager documentation resources.

## QUESTION NO: 17

Refer to the exhibit.




A customer reports that after a network failure, all of the Cisco Jabber clients are not switched back to their home nodes. An engineer determines that the primary Cisco IM & P server is in Failed Over state. Which two actions should be performed to bring the system back to operational state and to prevent future occurrences? (Choose two.)

**A.** Advise all users to re-login to their Jabber clients.

**B.** Confirm that both IM & P servers are configured in the Presence Redundancy Group configuration pane.

**C.** Perform a restart of the IM & P primary server to force fallback.

**D.** Click the Fallback button in the Server Action pane.

**E.** Set the Automatic Failover parameter in the Server Recovery Manager Service Parameters to the value True.

## ANSWER: B D

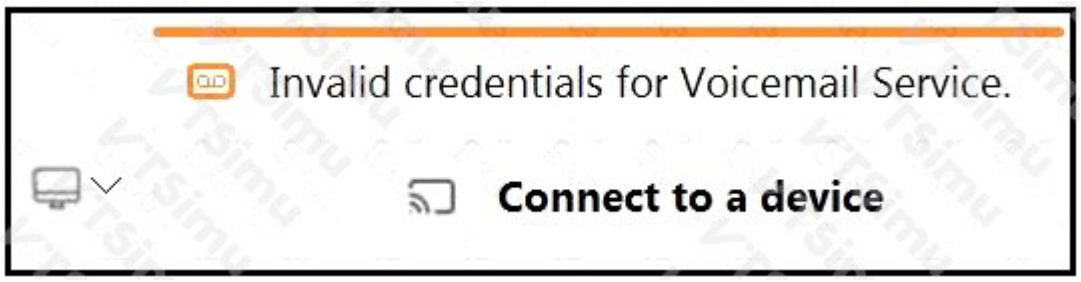
**Explanation:**

**Confirm that both IM & P servers are configured in the Presence Redundancy Group configuration pane** is required because an IM and Presence redundancy group defines the paired primary and backup servers that provide high availability for the users assigned to the group. Correctly establishing and validating that pairing ensures the deployment has the intended recovery relationship and allows users to be served by the surviving node during a failure.

**Click the Fallback button in the Server Action pane** is the appropriate recovery action once the original primary node is healthy. A node in the Failed Over state continues to operate with services active on the backup node until an administrator explicitly initiates fallback. The Fallback action returns service responsibility to the home, or primary, node and restores the normal primary/backup operating model without requiring each Jabber user to sign in again. Cisco documents that administrators manage IM and Presence high-availability state, including failover and fallback, through the System Configuration and Server Action controls. See Cisco's IM and Presence high-availability configuration guidance and the Cisco Unified Communications maintenance documentation.

## QUESTION NO: 18

Refer to the exhibit.




A Jabber user is unable to access voicemail. During troubleshooting, an administrator captures this screenshot. What are the two ways to resolve this issue? (Choose two.)

**A.** Ask the user to click on the Connect to a device " button and use the correct username and password.

**B.** Ensure the user is not locally created on Cisco Unity Connection with a password expiring separately from the password that is used for Jabber.

**C.** Make sure the Jabber service profile created in Cisco UCM contains Unity Connection UC service with a voicemail server configured.

**D.** Ask an administrator to create an account for this user in Cisco Unity Connection but remove the Unity Connection UC service from the Cisco UCM Jabber service profile.Check if " OAuth with Refresh Login Flow" is enabled on Cisco Unity Connection but disabled in Cisco UCM.

**ANSWER: B C**

**Explanation:**

Ensure the user is not locally created on Cisco Unity Connection with a password expiring separately from the password that is used for Jabber. Jabber normally authenticates the user to Unity Connection with the enterprise credentials established during Jabber sign-in. A Unity Connection user that is locally authenticated can have an independent Unity Connection password, password-expiration policy, or locked/expired credential state. Synchronizing the Unity Connection user with the directory-backed identity used by Jabber, or otherwise ensuring that the Unity Connection credential remains valid and aligned with the user's Jabber authentication, restores voicemail access.

Make sure the Jabber service profile created in Cisco UCM contains Unity Connection UC service with a voicemail server configured. Cisco Unified Communications Manager supplies Jabber's service-profile configuration, including the selected voicemail UC service. That UC service must identify the appropriate Cisco Unity Connection voicemail server so that Jabber can discover and connect to the voicemail service for the user. After the service is assigned in the user's Jabber service profile, the client can use the configured Unity Connection destination for visual voicemail and message retrieval. Cisco documents the voicemail-service assignment process in its Jabber feature configuration guide and Unity Connection authentication behavior in the Cisco Unity Connection Administration Guide.

## QUESTION NO: 19

An administrator is configuring call handlers in Cisco Unity Connection. The administrator must ensure that internal extensions are restricted so that callers must go through the company operator to reach employees, and so that callers hear an error message if they attempt to dial extensions directly. Which setting is configured to accomplish this task?

**A.** Transfer Rules

**B.** Caller Input

**C.** Greetings

**D.** Message Settings

**ANSWER: B**

**Explanation:**

**Caller Input** is the correct setting because it controls how Cisco Unity Connection processes digits that a caller enters while interacting with a call handler. In the call handler's Caller Input configuration, an administrator defines the actions associated with keypad entries and the behavior for invalid or otherwise disallowed entries. This is where the call flow can direct callers to the company operator rather than permit unrestricted direct dialing to internal extensions. When a caller attempts an extension-dialing action that is not allowed by the configured caller-input behavior, Unity Connection applies the relevant invalid-entry handling and plays the configured error prompt or routes the call according to the call handler's settings. As a result, the restriction is enforced at the point where the caller enters digits, which is precisely the required call-handler behavior. Cisco's Unity Connection administration guidance identifies Caller Input as the call-handler area used to configure caller keypad actions and invalid-entry processing. See the Cisco Unity Connection Administration Guide and Cisco's Unity Connection configuration documentation.

## QUESTION NO: 20

Which dial-peer configuration routes calls from SIP-based phones on Cisco Unified Communications Manager Express to Cisco Unity Express?

**A.** dial-peer voice 7000 voip destination-pattern 7000 session protocol sipv2 session target ipv4: 10.3.6.127 codec g711alaw

**B.** dial-peer voice 7000 voip destination-pattern 7000 session protocol sipv2 session target ipv4: 10.3.6.127 codec ilbc

**C.** dial-peer voice 7000 voip destination-pattern 7000 session protocol sipv2 session target ipv4: 10.3.6.127 codec g711ulaw

**D.** dial-peer voice 7000 voip destination-pattern 7000 session protocol sipv2 session target ipv4: 10.3.6.127 codec g729r8

## ANSWER: C

**Explanation:**

The configuration **dial-peer voice 7000 voip destination-pattern 7000 session protocol sipv2 session target ipv4: 10.3.6.127 codec g711ulaw** correctly defines a VoIP dial peer for calls placed to the Cisco Unity Express pilot number. The `destination-pattern 7000` matches calls dialed to extension 7000, allowing Cisco Unified Communications Manager Express to select this peer for voicemail or auto-attendant routing. `session protocol sipv2` specifies SIP signaling, which is required for communication with a SIP-integrated Cisco Unity Express system. The `session target ipv4:10.3.6.127` then directs the SIP session to the Unity Express server address. Finally, `codec g711ulaw` selects G.711 μ-law media, the codec used in Cisco's documented SIP dial-peer example for this CME-to-CUE call flow. This combination supplies the essential dial-plan match, SIP transport, Unity Express destination, and compatible media selection needed to route incoming voicemail calls successfully. Cisco's Unity Express configuration guidance shows this SIP dial-peer structure and the use of G.711 μ-law for the CUE session target. See Cisco's Unity Express and CME configuration example and the Cisco Unity Express codec information.

## QUESTION NO: 21

Which component of SAML SSO defines the transport mechanism that is used to deliver the SAML messages between entities?

**A.** assertions

**B.** profiles

**C.** bindings

**D.** metadata

## ANSWER: C

**Explanation:**

**bindings** is correct because SAML bindings define how SAML protocol messages are packaged and transported between SAML entities, such as an identity provider and a service provider. A binding specifies the communication mechanism used to convey the message, including mechanisms such as HTTP Redirect, HTTP POST, HTTP Artifact, and SOAP. For

example, an HTTP Redirect binding carries a SAML request or response through a URL query string, whereas an HTTP POST binding sends the message in an HTML form submitted through the user's browser. The binding therefore provides the concrete transport and encoding rules that allow the SAML single sign-on exchange to move between participating systems. In a Cisco collaboration SSO deployment, the identity provider and application/service-provider configuration must support compatible bindings so authentication requests and SAML assertions can be exchanged successfully. The SAML technical overview distinguishes bindings from the message content itself and identifies bindings as the defined mechanisms for transmitting protocol messages. See the OASIS SAML V2.0 Bindings specification and Cisco's SAML SSO Deployment Guide.

## QUESTION NO: 22

An engineer is importing users into Cisco Unity Connection using AXL and discovers that some users are not listed in the import view. Which action should be taken to resolve this issue?

**A.** Configure the user access control group assignment to Standard CTI Enabled.

**B.** Configure the user digest credentials to match the user password.

**C.** Configure the username and password in LDAP.

**D.** Configure the user primary extension to their directory number.

## ANSWER: D

**Explanation:**

Configure the user primary extension to their directory number. When Cisco Unity Connection imports users from Cisco Unified Communications Manager through AXL, it uses information returned by Unified CM to identify eligible users and associate them with their telephone extensions. A primary extension is a key part of that association. If a Unified CM end user does not have a primary extension configured, the user can be omitted from the Unity Connection import view because Connection cannot reliably establish the user's extension relationship for import.

In Unified CM Administration, the administrator should associate the appropriate device and directory number with the end user as needed, then set that directory number as the user's primary extension. After the Unified CM user record is updated, refresh or repeat the Unity Connection AXL import so that the user appears in the available import list. This configuration also supports correct mailbox extension assignment and integration behavior after the user is imported. Cisco documents primary extensions as part of the Unified CM end-user configuration used by integrated applications and Unity Connection user-import workflows. See the Cisco Unity Connection Administration Guide and the Cisco Unified CM System Configuration Guide.

## QUESTION NO: 23

A network engineer needs to configure high availability on the Cisco IM and presence cluster. After the configuration was completed and tested, the engineer noticed on Cisco UCM that the IM and Presence publisher is in "Failed Over" state. Which set of steps must be taken to resolve this issue?

**A.** Cisco UCM Group Configuration > High Availability > click Fallback

**B.** BLF Presence Group Configuration > High Availability > select the publisher server > cl i ck Restart Services

**C.** BLF Presence Group Configuration > High Availability > click Fallback

**D.** Presence Redundancy Group Configuration > High Availability > click Fallback

## ANSWER: D

**Explanation:**

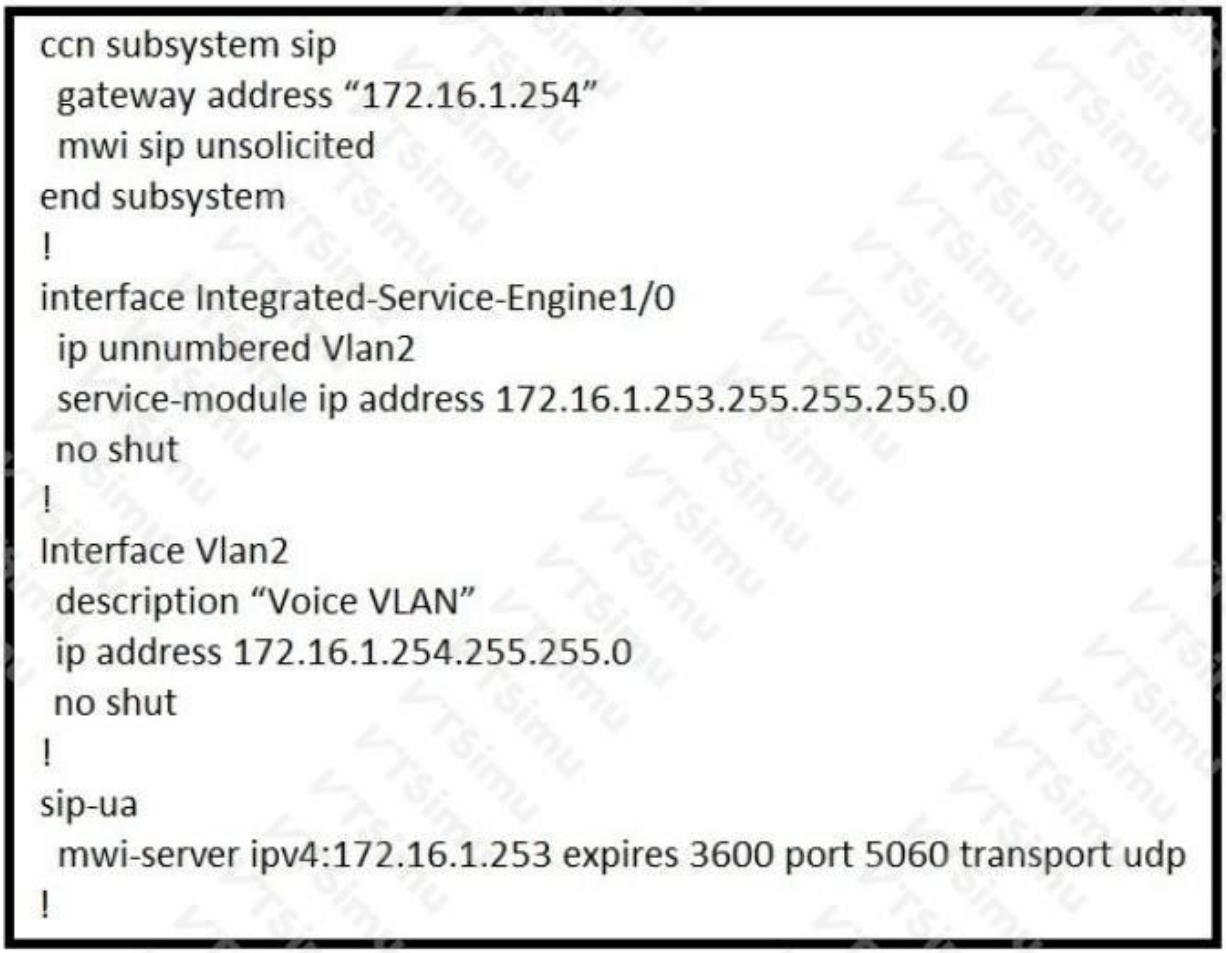
**Presence Redundancy Group Configuration > High Availability > click Fallback** is the correct procedure. In Cisco IM and Presence Service high availability, a publisher can enter the Failed Over state after a redundancy event, such as a

publisher outage or a deliberate failover test. Even after the publisher has recovered and is operational, the cluster does not necessarily move services back automatically. The administrator must initiate a fallback operation to restore the normal active/standby role arrangement and return the publisher to its intended active state.

The fallback action is performed from the relevant Presence Redundancy Group because that object defines the high-availability relationship between the IM and Presence publisher and subscriber. Selecting *Fallback* triggers the controlled return of responsibility to the recovered publisher and updates the high-availability status shown in Unified CM. This is the appropriate post-test recovery action when the publisher remains listed as Failed Over. Cisco documents IM and Presence redundancy-group administration and high-availability operations in its IM and Presence Service administration documentation: Cisco IM and Presence Service Documentation and Cisco Unified Communications Manager Maintenance Guides.

## QUESTION NO: 24

Refer to the exhibit.




A collaboration engineer has integrated Cisco Unity Express with Cisco Unified Communications Manager Express and is experimenting with the MWI feature. With the current configuration, no

MWI change occurs when leaving new messages or after playing new messages. Which two changes are needed to correct the configuration? (Choose two.)

**A.** ccn subsystem sip mwi sip outcall

**B.** ccn subsystem sip mwi envelop-info

**C.** sip-ua no mwi-server
mwi-server ipv4:172.16.1.254 expires 3600 port 5060 transport udp

**D.** ccn subsystem sip mwi sub-notify

**E.** sip-ua no mwi-server
mwi-server ipv4:172.16.1.253 expires 3600 port 5060 transport tcp notify

**F.** sip-ua no mwi-server mwi-server ipv4:172.16.1.253 expires 3600 port 5060 transport udp unsolicited

**ANSWER: A F**

**Explanation:**

`ccn subsystem sip mwi sip outcall` enables the Cisco Unity Express SIP subsystem to generate message-waiting indication updates using SIP outcalls. This gives Unity Express the required signaling behavior to originate MWI state changes when a mailbox gains a new message or when all new messages have been reviewed.

`sip-ua no mwi-server mwi-server ipv4:172.16.1.253 expires 3600 port 5060 transport udp unsolicited` replaces the existing MWI-server setting with the Unity Express address and configures Cisco Unified Communications Manager Express for unsolicited UDP MWI signaling. “Unsolicited” is essential in this integration model because Unity Express sends the MWI update without relying on a prior SIP subscription from the message-waiting endpoint. Together, these settings align the Unity Express notification method with the CME SIP user-agent MWI handling, allowing the phone message lamp to be activated for new voicemail and cleared after the new-message state is removed.

Cisco’s Unity Express configuration resources are available in the Cisco Unity Express installation and configuration guides. Related SIP and voicemail integration guidance is available in the Cisco Unified Communications Manager Express configuration guides.

**QUESTION NO: 25**

An engineer Is troubleshooting an MWI Issue between Unity Express and CallManager Express. In the debug SIP logs, the engineer can see CallManager Express responding to Unity Express with a 488 Not Acceptable Media message. Which action resolves the issue?

**A.** Ensure that codec G.722 Is configured In the dial peer.

**B.** Ensure that codec G.711ulaw is configured in the dial peer.

**C.** Ensure that codec G.711alaw is configured In the dial peer.

**D.** Ensure that codec G.729 is configured In the dial peer.

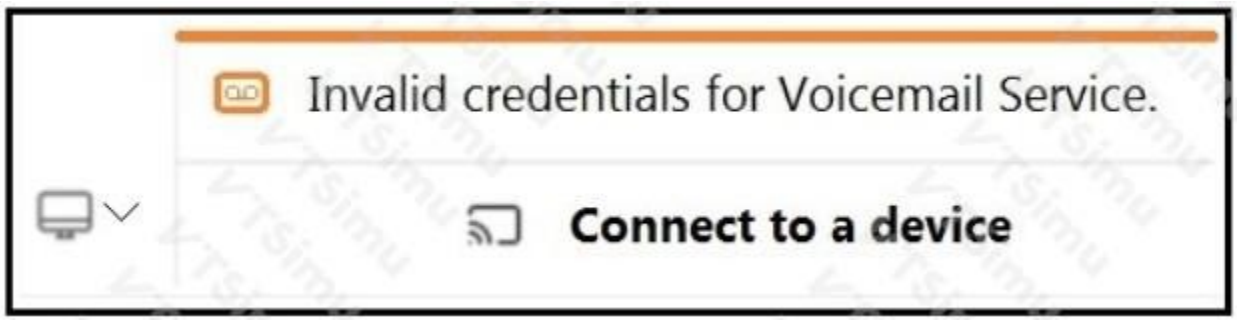
**ANSWER: B**

**Explanation:**

Ensure that codec G.711ulaw is configured in the dial peer. Cisco Unity Express and Cisco Unified Communications Manager Express use SIP signaling for message-waiting indicator integration, and the relevant dial peers must negotiate media characteristics that both endpoints support. A SIP `488 Not Acceptable Media` response means that the session description presented in the SIP message contains media parameters that Cisco Unified Communications Manager Express cannot accept for that call leg. In this integration scenario, configuring G.711 μ-law on the applicable dial peer provides the expected codec capability and allows the SIP exchange associated with message-waiting indication processing to complete successfully. Verify the codec statement on the dial peer used for calls and SIP messaging between the Cisco Unity Express module and Cisco Unified Communications Manager Express, then confirm that the dial-peer destination pattern and session target select that peer. After applying the configuration, reproduce the condition and review SIP debugging to confirm that the codec is offered and accepted rather than generating a 488 response. Cisco Unity Express configuration guidance is available in the Cisco Unity Express installation and configuration guides; Cisco IOS voice configuration references are available through the Cisco IOS Voice command reference.

**QUESTION NO: 26**

Refer to the exhibit.




A Jabber user is unable to access voicemail. During troubleshooting, an administrator captures this screenshot. What are the two ways to resolve this issue? (Choose two.)

**A.** Ask the user to click on the "Connect to a device" button and use the correct username and password.

**B.** Ensure the user is not locally created on Cisco Unity Connection with a password expiring separately from the password that is used for Jabber.

**C.** Make sure the Jabber service profile created in Cisco UCM contains Unity Connection UC service with a voicemail server configured.

**D.** Ask an administrator to create an account for this user in Cisco Unity Connection but remove the Unity Connection UC service from the Cisco UCM Jabber service profile.

**E.** Check if "OAuth with Refresh Login Flow" is enabled on Cisco Unity Connection but disabled in Cisco UCM.

**ANSWER: B C**

**Explanation:**

Jabber visual voicemail requires a working Unity Connection voicemail service assignment and credentials that Unity Connection can authenticate for the individual user. “Make sure the Jabber service profile created in Cisco UCM contains Unity Connection UC service with a voicemail server configured.” is required because the UC service supplies Jabber with the Unity Connection server details it needs to discover and access visual voicemail. The UC service must be assigned through the user’s Jabber service profile, and its voicemail-server setting must point to the appropriate Unity Connection deployment.

“Ensure the user is not locally created on Cisco Unity Connection with a password expiring separately from the password that is used for Jabber.” is also a valid resolution. When Jabber relies on the enterprise user’s credentials for voicemail access, a separately managed local Unity Connection account can have a different or expired password and prevent authentication. Using directory-integrated user identity and aligned credential lifecycle management avoids that mismatch. Cisco’s Jabber planning guidance describes configuring voicemail through a Unity Connection UC service and service profile, while Unity Connection documentation covers LDAP-based user integration and authentication behavior. See Cisco Jabber Planning Guide and Cisco Unity Connection configuration guides.

**QUESTION NO: 27**

A collaboration engineer is installing Jabber for Windows via the CLI Which two authentication command line arguments ensure that the client authenticates to a Cisco UCM server? (Choose two.)

**A.** CCMCIP=10.10.10.99

**B.** CUP_ADDRESS=10.10.10.98

**C.** CTI=10.10.10.97

**D.** REGISTRATION_SERVER=CUCM

**E.** EXCLUDED_SERVICES=Webex

**ANSWER: A B**

**Explanation:**

**CCMCIP=10.10.10.99** and **CUP_ADDRESS=10.10.10.98** are Jabber for Windows bootstrap parameters that provide the client with the locations of the collaboration servers required during initial sign-in and service discovery. CCMCIP identifies the Cisco Unified Communications Manager Cisco CallManager IP Phone service endpoint. Jabber can use this endpoint to obtain the configuration and service information associated with the user's Unified CM environment. CUP_ADDRESS identifies the Cisco Unified Communications Manager IM and Presence Service address. This enables the client to locate the IM and Presence service and complete the associated sign-in and presence-service discovery workflow using the Unified CM deployment credentials. These parameters are especially useful when DNS-based service discovery is unavailable, incomplete, or intentionally bypassed during a managed installation. The CCMCIP address has been corrected to a valid IPv4 format by removing the embedded space. Cisco documents CCMCIP and CUP_ADDRESS as installer/bootstrap parameters for supplying Unified CM and IM and Presence server information to Jabber clients. See the Cisco Jabber Deployment and Installation Guide and the Cisco Jabber for Windows installation guides.