

## 300-810<sup>Q&As</sup>

Implementing Cisco Collaboration Applications (CLICA)

### Pass Cisco 300-810 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/300-810.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco  
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



## QUESTION 1

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

Correct Answer: A

---

## QUESTION 2

An administrator must configure a system distribution list for the IT staff that must be reachable via voice recognition using either the phrases "service desk" or "Help desk". Which advanced distribute list feature should be used to accomplish this task?

- A. Alternate Greeting
- B. Alternate Extension
- C. Alternate Name
- D. Alternate Diction

Correct Answer: C

---

## QUESTION 3

Which SSO authentication method requires no action from the user when the session token times out?

- A. web form
- B. smart card
- C. external database
- D. local authentication

Correct Answer: A

---

## QUESTION 4

DRAG DROP

Drag and drop the steps of the SAML SSO process from the left into the order on the right.

Select and Place:

The browser issues an HTTPS GET request to the IdP.	step 1
The IdP checks for a valid browser session.	step 2
The IdP generates a SAML response.	step 3
The service provider generates a SAML authentication request.	step 4
The service provider redirects the request to the browser.	step 5
The service provider validates the digital signature.	step 6

Correct Answer:

	The service provider generates a SAML authentication request.
	The service provider redirects the request to the browser.
	The browser issues an HTTPS GET request to the IdP.
	The IdP checks for a valid browser session.
	The IdP generates a SAML response.
	The service provider validates the digital signature.

## QUESTION 5

An engineer is configuring SAML SSO for a Cisco Unified Communications Manager. After completing all required

steps, the engineer wants to verify the status. Which CLI command provides the status of SAML SSO?

- A. `utils sso status`
- B. `show sso status`
- C. `show saml status`
- D. `utils saml status`

Correct Answer: A

Reference: <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/213293-troubleshoot-ss0-in-cucm.html>

---

## QUESTION 6

Which function of the Cisco IM and Presence high availability solution is true?

- A. When the server has been restored to a normal state, user sessions remain on the backup server.
- B. When an event takes place, the end user sessions are not moved from the failed server to the backup.
- C. When the server has been restored, the server automatically fails back.
- D. When a high availability event takes place, the end user sessions are moved from the failed server to the backup.

Correct Answer: D

Reference: <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-im-presence-service/200958-IM-and-Presence-Server-High-Availability.html>

---

## QUESTION 7

Which authentication method allows a user to log in to an SSO-enabled Cisco Unified Communications application by utilizing a Microsoft Windows login, thereby not requiring any credentials to be entered?

- A. Smart Card
- B. OAuth
- C. form-based
- D. Kerberos

Correct Answer: D

<https://www.cisco.com/c/en/us/support/docs/unified-communications/jabber-windows/118773-configure-kerberos-00.html> The main advantage of Kerberos authentication compared to the other authentication methods is that you do not need to provide your credentials when you log in to Cisco Jabber. If you use Kerberos, the client does not prompt users for credentials, because authentication was already provided to gain access to the Windows desktop. This authentication method allows you to log in to Cisco Jabber with your Microsoft Windows login.

---

## QUESTION 8

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

Correct Answer:

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

Reference: [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/SAML\\_SSO\\_deployment\\_guide/12\\_5\\_1/cucm\\_b\\_saml-ss0-deployment-guide-12\\_5/cucm\\_b\\_saml-ss0-deployment-guide-12\\_5\\_chapter\\_01.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/SAML_SSO_deployment_guide/12_5_1/cucm_b_saml-ss0-deployment-guide-12_5/cucm_b_saml-ss0-deployment-guide-12_5_chapter_01.html)

## QUESTION 9

An administrator is configuring Cisco Unity Express and is using the default Auto-Attendant script, aa aef. Which script parameter prevents the script from transferring callers to external numbers?

- A. allowExternalTransfers
- B. disallowExternalTransfers
- C. disableExternalTransfers
- D. disableToli Fraud

Correct Answer: A

## QUESTION 10

Refer to the exhibit.

```
[csf.cert.] [csf::cert::BaseCertVerifier:doVerifyCertificate] - About to verify the certificate.
[csf.cert.win32] [csf::cert::Win32CertVerifier:loadCertificateChain] - Certificate Chain status 0x20
[csf.cert.win32] [csf::cert::Win32CertVerifier:verifySslPolicy] - Ignoring errors due to Invalid CN
[csf.cert.win32] [csf::cert::Win32CertVerifier:verifyPolicies] - SSL Policy status 0x2148204809
[csf.cert.win32] [csf::cert::win32CertVerifier:verifyPolicies] - Basic Constraints Policy status 0x0
[csf.cert.win32] [csf::cert::win32CertVerifier:verifyCertificate] - Certificate validation response is 'invalid'
[csf.cert.] [csf::cert::BaseCertVerifier:doVerifyCertificate] - Result of platform cert verification: [UNTRUSTED_ROOT]
[csf.cert.] [csf::cert::BaseCertVerifier:checkIdentity] - About to check for an Identity Match.
[csf.cert.xmpp] [csf::cert::XmppCertVerifier:checkIdentifier] - Verifying XMPP Identity 'example.com'
[csf.cert.utils] [csf::cert::AltNameParserImpl:verifyXmpp] - Xmpp match was not found for: 'example.com'
[csf.cert.utils] [csf::cert::AltNameParserImpl:verify] - Match for 'example.com' found in dnsNames index: 1
[csf.cert.] [csf::cert::BaseCertVerifier::checkIdentifiers] - Verification of identity succeeded. Matched identifier : 'example.com'
[csf.diagnostics] [CSFDiagnostics::DiagnosticsImpl::AddRecord] - Add record task enqueued: example.com
[csf.common.PolicySet] [csf::common:PolicySet::getPolicy] - Successfully found Policy with nature IGNORE_INVALID_CERT_CONDITION
[IGNORE_REVOCATION_INFO_UNAVAILABLE_ERRORS]
[csf.cert.] [csf::cert::BaseCertVerifier::applyIgnoreInvalidCertConditionPolicy] - About to enforce ignore invalid cert condition policy.
[csf.cert] [csf::cert::IgnoreInvalidCertConditionPolicy::removeIgnoredStatuses] - No statuses have been removed from the verification status.
[csf.cert] [csf::cert::IgnoreInvalidCertConditionPolicy::enforce] - Policy enforced
[csf.cert.] [csf::cert::BaseCertVerifier::verifyCertificateAsync] - Certificate initially verified, result: FAILURE
[csf.cert] [csf::cert::CertificateDataImpl::parseSubjectCNField] - size of Subject CN field : 16
[csf.cert] [csf::cert::CertificateDataImpl::parseSubjectCNField] - Sybject CN field : impa.example.com
[csf.common.PolicySet] [csf::common:PolicySet::getPolicy] - Successfully found Policy with nature INVALID_CERT_MANAGEMENT [PROMPT_USER]
```

Users report that they are prompted to accept server certificates when they initially run Cisco Jabber. An engineer removes these prompts to prevent confusion. Which statement about this scenario is true?

- A. Presentation of the certificates can be disabled by setting up Cisco IMandP servers into nonsecure mode.
- B. Nothing can be done to resolve this issue because certificates must be accepted by each Jabber user, per Cisco policy.
- C. These certificates are self-signed certificates, so they must be added manually to the user OS certificate stores.
- D. The behavior is a security breach because certificates are considered untrusted and as not coming from Cisco Collaboration servers.

Correct Answer: C

Reference: <https://www.cisco.com/c/en/us/support/docs/unified-communications/jabber-windows/116637-trouble-jabber-00.html>

Certificate Authority (CA), which is the case for a self-signed certificate, the certificate needs to be loaded into the client

OS certificate store. Otherwise, Jabber users will be prompted to accept or decline individual server certificates when they initially connect.

---

## QUESTION 11

What are two characteristics of HTTPS networking for Cisco Unity Connection? (Choose two)

- A. HTTPS single-site networks are joined via an intersite link
- B. HTTPS networking uses a ring topology
- C. HTTPS networking supports a maximum of 25 locations
- D. HTTPS networking uses the SMTP protocol
- E. HTTPS networking supports multisite networks

Correct Answer: CD

---

## QUESTION 12

An engineer must configure open SIP Federation on cisco IM and presence using cisco Expressways with the additional requirement not to allow a specific list of domains and allow all other domains that are not specified. How is this additional requirement met?

- A. Configure default static routes for each blocked domain with an invalid next-hop IP address.
- B. Add a static route for each blocked domain and keep the "Block Route" checkbox checked.
- C. Block the specified SIP domains on the Expressway
- D. Add each allowed domain as a SIP Federated domain.

Correct Answer: D

---

## QUESTION 13

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 > click Restart Services
- C. BLF Presence Group Configuration > High Availability > click Fallback
- D. Presence Redundancy Group Configuration > High Availability > click Fallback

Correct Answer: D

---

## QUESTION 14

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.

Correct Answer: CD

---

## QUESTION 15

What are two authentication mechanisms for identity provider authentication? (Choose two.)

- A. UID
- B. PKI/CAC
- C. ACS
- D. Password only
- E. Kerberos

Correct Answer: BE

[300-810 PDF Dumps](#)

[300-810 VCE Dumps](#)

[300-810 Practice Test](#)