Exam	300-810 Exam
Title	Implementing Cisco Collaboration Applications (300-810 CLICA) Exam
Version	15.0
Product Type	184 Q&A with explanations

certexam.org

QUESTION 1
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

Answer: B

Explanation:
https://www.cisco.com/c/en/us/support/docs/unified-communications/jabber-windows773-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 2
When Cisco IM and Presence is configured to use automatic fallback, how long does the Server Recovery Manager service wait for a failed service/server to remain active before an automatic fallback is initiated?

A. 10 minutes
B. 20 minutes
C. 30 minutes
D. 1 hour

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/unified-communications/unifiedcommunications-manager-im-presence-service958-IM-and-Presence-Server-High-Availability.html
Automatic Fallback
Automatic fallback takes place when the server monitors the services and the Server Recovery Manager(SRM) service will automatically fallback users to their homed nodes. The key in this configuration is that the Server Recovery Manager(SRM) service will wait 30 minutes for a failed service/server to remain active before an automatic fallback is initiated. Once this 30 minute up time

certexam.org

is established, user sessions are moved back to their homed nodes. The Jabber client will apply the re-log in upper and lower limits for the fallback. Automatic fallback is not the default configuration, but it can be enabled. To enable automatic fallback, change the Enable Automatic Fallback parameter in the Server Recovery Manager Service Parameters to value True.

QUESTION 3
Which entity is a standard component used for authentication by SAML 2.0?

A. identity provider
B. session broker
C. Internet service provider
D. client access server

Answer: A

Explanation:

QUESTION 4
An engineer must configure a test user mailbox in a newly deployed Cisco Unity Express module. Which console command set reflects the correct configuration in this scenario?

A.
```
username testuser create
username testuser pin 12345
username testuser phonenumber 4001
voicemail mailbox owner testuser
```

B.
```
username testuser pin 12345
username testuser phonenumber 4001
voicemail mailbox owner testuser
```

C.
```
username testuser phonenumber 4001
username testuser pin 12345
voicemail mailbox owner testuser
```

D.
```
username testuser create
username testuser pin 12345
username testuser phonenumber 4001 testuser@labdomain.com
voicemail mailbox create testuser
```

CertKingdom.com
certexam.org

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:

QUESTION 5
Which two command line arguments can you specify when installing Cisco Jabber for windows?
(Choose two.)

A. CISCO_UDS_DOMAIN
B. TFTP_ADDRESS
C. VOICEMAIL_SERVER_ADDRESS
D. SERVICES_DOMAIN
E. TFTP

Answer: D, E

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber_0/CJAB_BK_D657A25F_00_deployment-installation-guide-jabber-110/CJAB_BK_D657A25F_00_deployment- installation-guide-jabber-110_chapter_01100.html#JABW_RF_CE43EF4C_00

QUESTION 6
Which description of an IdP server is true?

A. authenticates user credentials
B. provides user authorization
C. is an authentication request that is generated by a Cisco Unified Communications application
D. consists of pieces of security information that are transferred to the service provider for user authentication

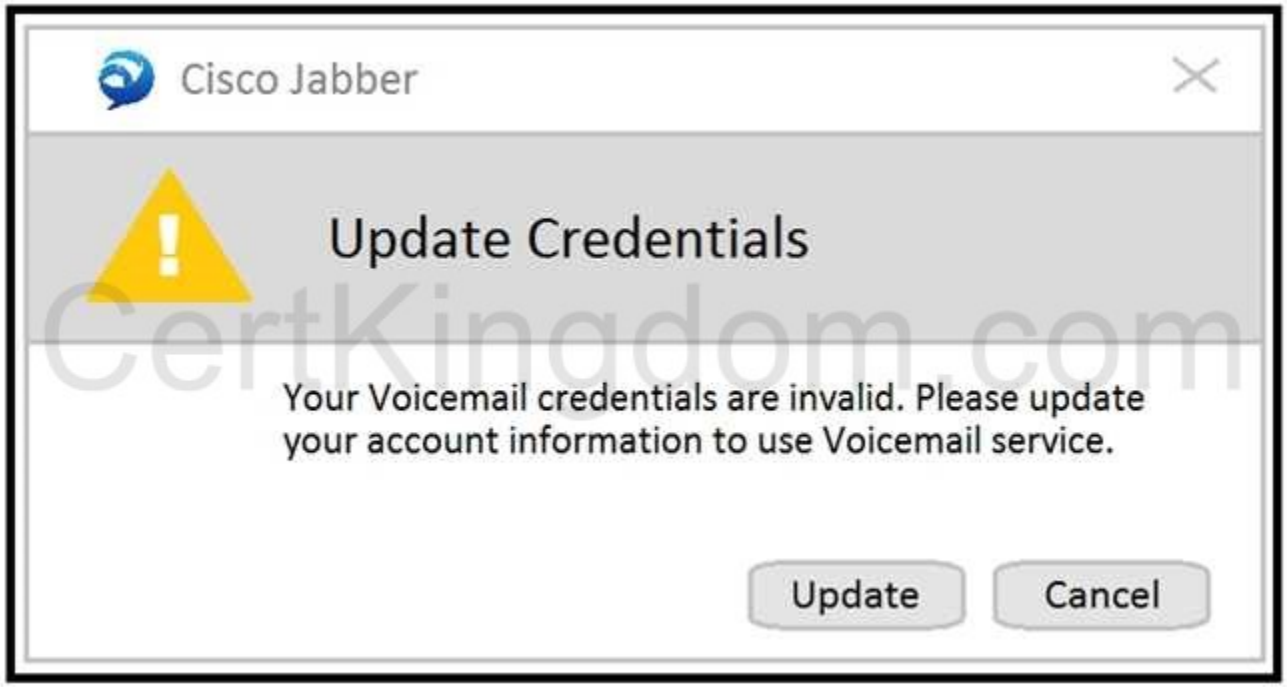
Answer: A

Explanation:
SSO uses Security Assertion Markup Language (SAML) to exchange authentication details between an Identity Provider (IdP) and a service provider. The identity provider authenticates user credentials and issues SAML assertions, which are pieces of security information transferred from the identity provider to the service provider for user authentication. Each assertion is an XML document that

certexam.org

contains trusted statements about a subject including, for example, username and privileges. SAML assertions are usually digitally signed to ensure their authenticity.
Reference:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/crs/express_11_6_2/features/guide/uccx_b_features-guide-1162/uccx_b_features-guide-1162_chapter_010.html#concept_D4C0DDEE975FE5C9416479AB5D778237

QUESTION 7
Refer to the exhibit.



Which action allows a remote Cisco Jabber user utilizing Mobile and Remote Access to automatically log in to a Cisco Unity Connection voicemail box via OAuth?

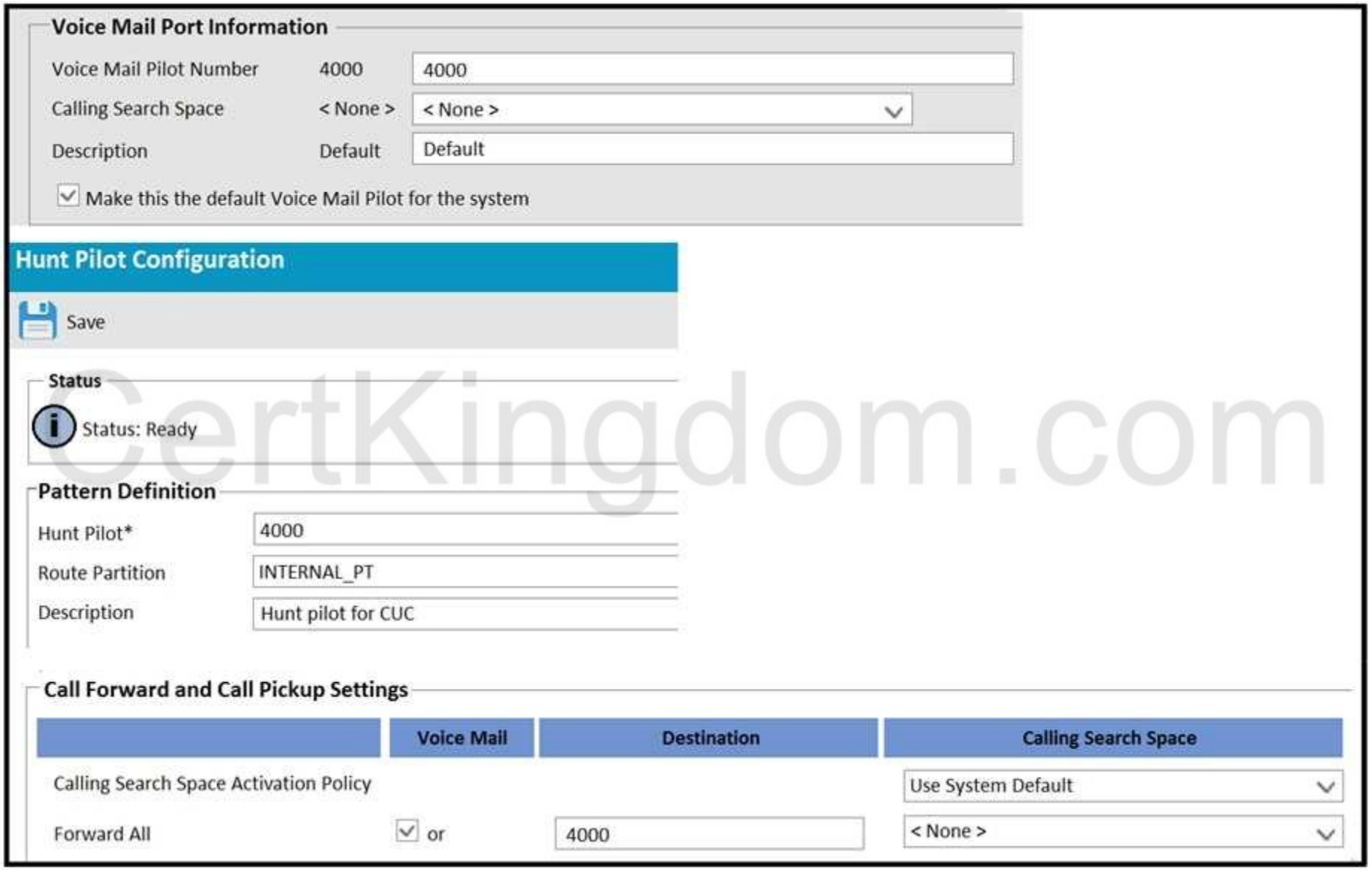
A. Add CUCM under System Settings > Authz Servers in Cisco Expressway-E.
B. Add CUCM under System Settings > Authz Servers in Cisco Expressway-C.
C. Add CUCM under System Settings > Authz Servers in Cisco Unity.
D. Add CUCM under System Settings > Authz Servers in Cisco Unity Connection.

Answer: D

Explanation:
Reference: https://community.cisco.com/t5/unified-communications/jabber-mra-unity-voice-mailintegration-issue/td-p5653

CertKingdom.com
certexam.org

QUESTION 8
Refer to the exhibit.



Cisco Unity Connection and Cisco Unified Communications Manager are integrated by using SCCP. The Voice Mail Ports are registered. Users report that calls fail when forwarded to voicemail. Which is a cause of the issue?

A. The call forward and call pickup settings do not have a CSS on Forward All.
B. The Voice Mail Port partition on the CSS of the phone is missing.
C. The Voice Mail Pilot is not configured with a CSS that contains the INTERNAL_PT.

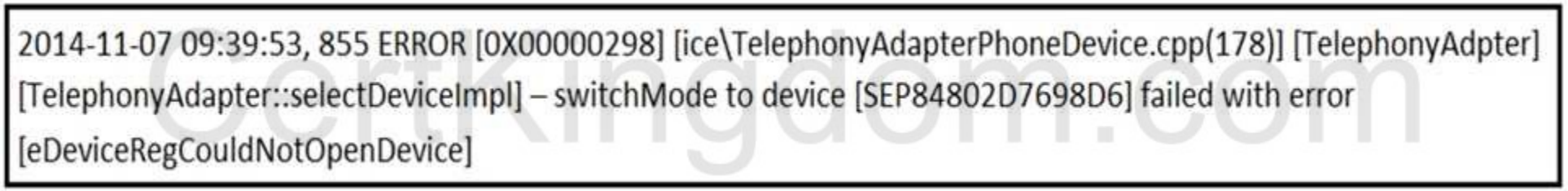
CertKingdom.com
certexam.org

D. The CSS on the Voice Mail Pilot is missing partitions for user phones.

Answer: C

Explanation:

QUESTION 9
Refer to the exhibit.



Which end-user option can resolve this issue?

A. Standard CTI Reception of SRTP Key Material
B. Standard CTI Allow Calling Number Modification
C. Standard CTI Allow Control of Phones Supporting Rollover Mode
D. Standard CTI Allow Call Monitoring

Answer: C

Explanation:
https://community.cisco.com/t5/collaboration-applications/jabber-for-windows-cannot-control-8841-desk-phone/td-p9503

QUESTION 10
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.

Answer: D

certexam.org

Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/unified-communications/unifiedcommunications-manager-im-presence-service958-IM-and-Presence-Server-High-Availability.html

---

QUESTION 11
Which Cisco IM and Presence service must be activated and running for IM Presence to successfully integrate with Cisco Unified Communications Manager?

A. Cisco DHCP Monitor Service
B. Cisco AXL Web Service
C. Self-Provisioning IVR
D. Cisco XCP Authentication Service

Answer: B

Explanation:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide_0_1/cup0_b_config-admin-guide-imp-1201/cup0_b_config-admin-guide-imp-1201_chapter_0100.html

---

QUESTION 12
Refer to the exhibit.

```
Response:
HTTP/1.1 400 Bad Request
Strict-Transport-Security: max-age=31536000
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Set-Cookie: JSESSIONID=1233ADC137E591GE144792F38123AB09; Patch=/idb/; Secure; HttpOnly
TrackingID: FOS_d0ac0d7b-f4e4-4d83-ba27-d4252e310b88
Cache-Control: no-store
Date: Mon, 06 Jan 2018 10:30:00 GMT
Accept-Ranges: bytes
Server:
Vary: Accept-Charset, Accept-Encoding, Accept-Language, Accept
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Accept,Authorization,Content-Type,TrackingID
Access-Control-Allow-Methods: POST,PUT,PATCH,HEAD,GET,TRACE,CONNECT,OPTIONS,DELETE
Pragma: no-cache
Content-Type: application/json;charset=UTF-8
Connection: close
Content-Length: 176

{"error_description":"The refresh token provided is expired, revoked, malformed, or invalid.","
error":"invalid_request","trackingID":FOS_a12b123c-d123-e123-a127-b420be310188"}
```

certexam.org

Apple Push Notification integration is configured in a Cisco Unified IM and Presence deployment and

has been working property. Administrators now report the error œPush notification settings cannot be configured. 400 Bad Request. 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:
Reference:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/push_notifications/cucm_b_pushnotifications-deployment-guide.pdf

---

QUESTION 13
Which two methods does Cisco Jabber use for contact searching in an on-premises deployment model? (Choose two.)

A. HTTP
B. XMPP
C. UDS
D. LDAP
E. SIP

Answer: CD

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11/presence.html

---

QUESTION 14
What is the maximum number of Cisco Unity Connection locations connected in a HTTPS network?

A. 50
B. 25
C. 200
D. 10

certexam.org

Answer: B

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connectionx/https_networking/guidexcuchttpsnetxxcuchttpsnet010.html

---

QUESTION 15
What is the primary mechanism in Cisco Unity Connection that is used for toll fraud prevention?

A. restriction tables
B. fraud tables
C. transfer rules
D. calling search spaces

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connectionx/security/guidexcucsecxxcucsec020.pdf

---

QUESTION 16
Which CLI command is used to collect traces from the Cisco Presence engine for seven days?

A. file build log cisco_presence_engine 7
B. file build log cisco_presence 168
C. file build log presence_engine 7
D. file build log presence_engine 168

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide_0_1/cup0_b_config-admin-guide-imp-1201/cup0_b_config-admin-guide-imp-1201_chapter_010101.html

---

QUESTION 17
SAML SSO is enabled in Cisco Unified Communications Manager. What happens when a browserbased client attempts to access a protected resource on a service provider?

A. The browser follows the redirect and issues an HTTPS GET request to the IdP.
B. The IdP checks for a valid browser session.
C. The service provider generates a SAML authentication request.
D. The SAML request is maintained as a query parameter in the GET request.

certexam.org

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/SAML_SSO_deployment_guide_5_1/cucm_b_saml-sso-deployment-guide-12_5/cucm_b_samlsso-deployment-guide-12_5_chapter_01.html

---

QUESTION 18
Which Cisco Unified Connections Manager service is required for users to control their desk phones using Cisco Jabber?

A. Cisco CTIManager
B. Cisco CTL Provider
C. Cisco Presence Engine
D. Cisco Serviceability Reporter

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber_5/CJAB_BK_D00D8CBD_00_deployment-installation-guide-cisco-jabber115/CJAB_BK_D00D8CBD_00_deployment-installation-guide-cisco-jabber115_chapter_0111.html

---

QUESTION 19
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] - Sucessfully 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 IM&P 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.

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/unified-communications/jabberwindows/116637- trouble-jabber-00.html
Certificate Authority (CA), which is the case for a self-signed certificate, the certificate needs to be

certexam.org