Cisco Finesse Release 10.5(1) ES10

Contents

Cisco Finesse Release 10.5(1) ES10

File Name	MD5 Checksum
ccd-finesse.1051.ES10.10000.cop.sgn	0ea4038b186ee65888b0ee6634ef4497
ccd-finesse.1051.ES.Rollback.cop.sgn	2facd78d7472f630e8edb6e3fb824d6d

Cisco Finesse Release 10.5(1) ES10 is cumulative. It contains fixes for all Cisco Finesse Releases from 10.5(1) ES01 to 10.5(1) ES09.

Valid Upgrade Paths

Cisco Finesse Release 10.5(1) ES10 is delivered as a Cisco Option Package (COP) file. If you are using any other 10.5 ES versions, you must upgrade to 10.5(1) ES09 or rollback to 10.5(1) and then install ES10.

The supported upgrade paths for 10.5(1) ES10 are the following:

- 10.5(1)
- 10.5(1) ES09

Installing Cisco Finesse Release 10.5(1) ES10

You must perform the following procedure, first on the primary Finesse node and then on the secondary Finesse node.

IMPORTANT: You must use the CLI to perform this upgrade. Do not use the Cisco Unified Operating System Administration page to perform this upgrade as the installation may not proceed. Installing this patch or performing a rollback stops and restarts certain Cisco Finesse services. To avoid interruption to agents, perform the installation or rollback during a maintenance window.

1. Download **ccd-finesse.1051.ES10.10000.cop.sgn** to an SFTP server that can be accessed by the Cisco Finesse system.
2. Use SSH to sign in to your Cisco Finesse system with the platform administration account.
3. Access the CLI and run the following command:
   utils system upgrade initiate
4. Follow the instructions that appear on your screen. When prompted, provide the location and credentials for the remote file system (SFTP server).
   Note: The COP file performs a check to ensure that Cisco Finesse Release 10.5(1) is installed. If this release is not found on your system, an error is displayed and the installation does not proceed.
5. When the installation is complete, you are prompted to reboot the server. However, for this installation no reboot is required and you can ignore this message.
6. To verify if Cisco Finesse is now running the correct release, access the CLI using the Administrator User credentials and enter the following command:
   show version active
   The result should contain the following:
   - Active Master Version: 10.5.1.10000-3

- Active Version Installed Software Options
- ccd-finesse.1051.ES10.10000.cop

7. Check if the installation was successful by signing in to Cisco Finesse ((http://IP-Address or hostname of Cisco Finesse server or desktop).

Rollback

If there is a problem with the installation, you can roll back to the previous version as follows:

1. Download the file **ccd-finesse.1051.ES.Rollback.cop.sgn** to an SFTP server that can be accessed by Cisco Finesse system.
2. Use **SSH** to sign in to your Cisco Finesse system with the platform administration account.
3. Access the CLI and run the following command:
   utils system upgrade initiate
4. Follow the instructions that appear on your screen. When prompted, provide the location and credentials for the remote file system (SFTP server).
5. To verify if Cisco Finesse is now running the correct release, access the CLI using the Administrator User credentials and enter the following command:
   show version active
   The result should contain the following:
   - Active Master Version: 10.5.1.10000-3
   - Active Version Installed Software Options
   - ccd-finesse.1051.ES.Rollback.cop

Note: The Cisco Finesse Rollback COP file restores your system to the base Cisco Finesse version (in this case, Cisco Finesse Release 10.5(1)). If you want to revert to a different Release 10.5(1) ES, you can install the desired ES only after you perform the rollback to Release 10.5(1).

Resolved Caveats in Cisco Finesse Release 10.5(1) ES10

Defect ID: CSCvb63177

Headline: Cisco Finesse 10.5(1) - agent stays signed when user closes the browser.

Symptoms: When an agent closes the browser (by clicking on browser close button), Cisco Finesse may take more than 60 seconds to sign out the agent.

Workaround: Agents should do sign out from the Cisco Finesse client. They should not directly close the browser.

Defect ID: CSCve59504

Headline: After installing ES09 on Cisco Finesse 10.5(1), the Mobile Agent check box is missing in compatibility mode.

Symptoms: Cannot sign in to Cisco Finesse with mobile agent because Mobile Agent check box is missing.

Workaround: Do not use compatibility mode to sign in so that Mobile Agent check box is present.

Defect ID: CSCve11977

Headline: Cisco Finesse agent state change is delayed.

Symptoms: Cisco Finesse agent state change is delayed.

Workaround: None.
However, the situation can be avoided by processing "ClearConnectionReq" in a timely manner from CUCM.

Defect ID: CSCvc90295

Headline: Team configurations are lost after CTI Server Disconnect.

Symptoms: After Ctisvr failover when Cisco Finesse connects to the active side, intermittently in the Team performance gadget, when a supervisor selects the team, agent data is not populated. The following error message is displayed - "No Members on this Team."

However, it is important to note that the team agent mapping does not go away and agent and supervisor can still sign in and are able to change states and take calls.

Workaround: Restart the primary Cisco Finesse server followed by the secondary server by using the **"utils system restart"** command.

Resolved Caveats in Cisco Finesse Release 10.5(1) ES09

Defect ID: CSCvb30767

Headline: Openfire closes session to CTISRV when receiving non-XML symbols.

Symptoms: When Openfire receives non-printable XML symbols in variables fields, Cisco Finesse Openfire service crashes.

Workaround: None.

Defect ID: CSCva98038

Headline: In Cisco Finesse, the IVR port number is displayed if wrap-up is configured after transfer.

Symptoms: Cisco Finesse agent sees a CUCM CTI RP number as the calling number for transferred calls.

Workaround: None.

Defect ID: CSCvb09547

Headline: Missing call data in Cisco Finesse agent screen after blind transfer to IP-IVR RP.

Symptoms: When transferring a call from one Cisco Finesse agent to another through CTI RP on CUCM (using single step transfer), the second agent does not get the call variables and

ANI of the caller. This occurs when an agent is using **Required** work mode in the agent desktop settings.

Workaround: To use **Optional** work mode in agent desktop settings.

Defect ID: CSCva10637

Headline: Cisco Finesse displays ConnectionDeviceID instead of ANI during a transfer.

Symptoms: When transferring a call from one Cisco Finesse agent desktop to another in a CVP comprehensive call flow, Cisco Finesse displays ConnectionDeviceID on the desktop instead of ANI.

As Cisco Finesse uses the ConnectionDeviceID to display customer data, the second agent is unable to determine the customer's identity due to incorrect information.

Workaround: None.

Defect ID: CSCut16568

Headline: In Unified CCE, Precision Queues do not show in the agent's queue statistic gadget.

Symptoms: During sign in, Precision Queues (PQ's) may not show in the agent queue statistic gadget intermittently.

Workaround: Try to sign in again.

Defect ID: CSCvb54353

Headline: MID call state transition from Talking>Held>Not Ready>Reserved>Talking is not handled in Cisco Finesse.

Symptoms: MID call state transition from Talking>Held>Not Ready>Reserved>Talking is not handled in Cisco Finesse for an agent available in wrap up mode.

Workaround: None.

Defect ID: CSCva72280

Headline: Cisco Finesse Tomcat and Openfire crash due to invalid XML characters.

Symptoms: When Openfire receives non-printable XML symbols in variables fields, Cisco Finesse Openfire service crashes.

Workaround: None.

Defect ID: CSCvc41711

Headline: Cisco Finesse returns incorrect line state.

Symptoms: Typically when VOIP inbound calls from Skype, Viber or other internet service providers are received, Cisco Finesse intermittently returns the incorrect LINE state. This while IVR APP is designed to drop the call if customer is not ACTIVE.

Workaround: None.

Defect ID: CSCvd00580

Headline: When the REST proxy authentication is enabled, Cisco Finesse cannot operate in HTTP mode.

Symptoms: When the REST proxy authentication is enabled, Cisco Finesse cannot operate in HTTP mode.

Workaround: Enable HTTPS redirection for REST proxy authentication to work or disable HTTPS redirection to work in HTTP mode.

Known Caveats

Defect ID: CSCvd19469

Headline: Conference call missing on Agent Desktop.

Symptoms: When an agent does a direct transfer of a conference call, and if one agent ends the call, the second agent is unable to end the call.

Workaround: None.

Resolved Caveats in Cisco Finesse Release 10.5(1) ES08

Defect ID: CSCux28810

Headline: Cisco Finesse server crashes if there are any non-printable characters in Openfire.

Symptoms: All agents show a red banner intermittently that says disconnected from Cisco Finesse server. Agents will not be able to sign in to Cisco Finesse during this time.

Workaround: Manually remove the control character from the agent's name field in Config Manager.

Defect ID: CSCuz11421

Headline: CTI-4047 error causes Cisco Finesse desktop to freeze for a couple of seconds.

Symptoms: When CTI-4047 error occurs, a few seconds delay is seen in the Cisco Finesse desktop.

Workaround: The agent has to click in any area on the browser window to release the Cisco Finesse desktop or wait for a few seconds.

Defect ID: CSCuz97228

Headline: ConnectionDeviceID is being set to unknown.

Symptoms: This issue occurs when connectionDeviceId in *all* CTIBeginCallEvents is set to “unknown" OR "anonymous".

Workaround: None.

Defect ID: CSCuz00782

Headline: Cisco Finesse fails to execute condition based workflows for dialer calls.

Symptoms: For outbound dialer calls, the workflow holds true and is executed when no condition is applied. However, in the workflow, if any condition is applied (Example: BAStatus "is not Empty") the workflow fails to execute.

Workaround: None.

Defect ID: CSCuw86623

Headline: Cisco Finesse SSRF Vulnerability.

Symptoms: A vulnerability in the web interface of Cisco Finesse could allow an unauthenticated, remote attacker to trigger the Cisco Finesse server to perform an HTTP request to an arbitrary host. This type of attack is commonly referred to as Server Side Request Forgery (SSRF).

The vulnerability is due to insufficient access controls to the Cisco Finesse API for gadgets integration. An attacker could exploit this vulnerability by submitting a HTTP request to the Cisco Finesse server.

Workaround: None

Note: This fix ensures that gadgets that invoke 3rd party REST APIs proxied through Cisco Finesse shindig are authenticated by Shindig. After installation of 10.5(1) ES08, the REST proxy authentication is enabled by default. Cisco Finesse provides new utils commands which can be used to disable or enable the authentication for the proxied REST request.

- utils finesse rest_proxy_auth enable
- utils finesse rest_proxy_auth disable
- utils finesse rest_proxy_auth status

If HTTPS redirect is enabled, users can set the REST proxy authentication to either disabled or enabled. However, if HTTPS redirect is disabled users must set the REST proxy authentication to disabled.

For more details about SSRF, see https://cwe.mitre.org/data/definitions/918.html. Also, see the defect notes in the bug search tool.

Defect ID: CSCuz19136

Headline: Shindig Authentication Redirect.

Symptoms: Agent state is out of sync after Cisco Finesse failover. An agent who has signed out is shown as signed in and the agent state change is not reflected. Agent state is reflected properly only after the agent state changes after failover.

Workaround: This issue is resolved by disabling the internal redirect.

After obtaining root access, the following command is issued **"FinesseRestProxyAuth.sh disable"** in **/opt/cisco/desktop/bin**

Restart Cisco Finesse Tomcat service on both Finesse nodes.

Defect ID: CSCuz38289

Headline: Cisco Finesse agent is unable to change state after being idle for 30 minutes.

Workaround: Disable RestProxy Authentication to revert back to old behavior. Rollback ES03 COP file or sign in as a root and execute the below command: **/opt/cisco/desktop/bin/FinesseRestProxyAuth.sh disable**. Now, stop and restart TOMCAT.

Defect ID: CSCuy94569

Headline: Unable to turn on Openfire debug logging after 10.5(1) ES07.

Workaround: Remove 10.5(1) ES07 or revert default Openfire password in the backend.

Resolved Caveats in Cisco Finesse Release 10.5(1) ES07

Defect ID: CSCuw86228

Headline: Cisco Finesse dial-pad in IE recognizes double click and enters three digits.

Symptoms: PhonePad.xd.js has event handlers for the dial-pad mouse and keyboard events. There is an IE specific double click event handler in addition to the generic single click handler. So when we click fast twice, two single clicks and double click (only for IE) will be processed which results in 3 digits being displayed. Since there is no double click event handler for Firefox, the digit is not displayed for the third time.

Workaround: Enter digits from the keyboard directly.

Defect ID: CSCuy14779

Headline: Cisco Finesse supervisor cannot see an agent status update after PG failover.

Symptoms: Agent state is out of sync after Cisco Finesse failover. An agent who has signed out is shown as signed in and the agent state change is not reflected. Agent state is reflected properly only after the agent state changes after failover.

Workaround: None.

Defect ID: CSCuu83970 (CSCuv66158)

Headline: OutOfMemoryError - ConnectionHandler reports unexpected exception.

Symptoms: During high load conditions Cisco Finesse notification service runs out of memory.

Workaround: None

Resolved Caveats in Cisco Finesse Release 10.5(1) ES06

Defect ID: CSCuy52732

Headline: sha256 support on 10.0(1) and 10.5(1) versions.

Note: Procedure for certificate regeneration.

Resolved Caveats in Cisco Finesse Release 10.5(1) ES05

Defect ID: CSCux13711

Headline: PCCE 10.5.2 validation fails with Cisco Finesse 10.5_ES4.

Symptoms: PCCE validation fails with error "Finesse" Side A and B servers DIAGNOSTIC_PORTAL&userName=appadmin&password=********, privateAddress=

Cisco Finesse servers are functional on Cisco Finesse agent desktops. While Finesse appadmin can sign in with the same credentials, passwords could be corrupted in the PCCE inventory DB. Issue seems to occur with 10.5.2_ES4 on Cisco Finesse.

Workaround: Modify Server.xml file on Finesse 10.5.1_ES4 version.
Root to Finesse Server and navigate to folder **/usr/local/thirdparty/apache-tomcat-6.0.29/conf/server.xml**.
Launch Server.xml and modify protocols="TLSv1" with sslEnabledProtocols="TLSv1".
Restart Cisco Finesse Tomcat and revalidate Packaged CCE.

Defect ID: CSCuw79085

Headline: XMPP port 5222 can be accessed with default username and password.

Symptoms: The fact that admin can enter via 5222 is an OpenFire vulnerability. The default admin password cannot be changed post-install.

Workaround: None.

Resolved Caveats in Cisco Finesse Release 10.5(1) ES04

Defect ID: CSCur36742

Headline: Evaluation of SSLv3 Poodle Vulnerability CVE-2014-3566.

Symptoms: This product includes a version of SSL that is affected by the vulnerability identified by the – Common Vulnerability and Exposures (CVE) IDs: CVE-2014-3566.

Conditions: Exposure is not configuration dependent.

Workaround: None.

Defect ID: CSCuv28457

Headline: Openfire crashes when non-valid XML 1.0 characters are passed to Cisco Finesse.

Symptoms: ++ Openfire crashes when non-valid XML 1.0 characters are passed to Cisco Finesse. ++ Agent loses connectivity to Finesse Server and ++ Agent cannot sign in until

services are restarted.

Conditions: When non-valid XML 1.0 characters are passed to Cisco Finesse.

Workaround: Restart Cisco Finesse Notification and Tomcat Service.

Defect ID: CSCuv76434

Headline: Cisco Finesse Logjam Vulnerability.

Symptoms: Cisco Finesse is susceptible to the Logjam vulnerability documented here: http://blogs.cisco.com/security/understanding-logjam-and-future-proofing-your-infrastructure

Firefox, in version 39, blocked access to websites using DH ciphers susceptible to Logjam documented here:

https://support.mozilla.org/en-US/questions/1066238 includes a version of OpenSSL that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2015-4000.

Conditions: Using Cisco Finesse in a Unified CCE environment or Unified CCX with co-resident Cisco Finesse.

Workaround: No workarounds currently exist to change Cisco Finesse to be protected from Logjam exploitation, but users of Firefox can perform the following workaround to regain access to Cisco Finesse web pages:

1. In FireFox, enter "about: config" in the URL field and press enter.
2. Accept the "This might void your warranty!" warning.
3. In the search field at the top, enter "security.ssl3.dhe_rsa_aes".
4. Double click each result (128 and 256) to toggle the Value to "false".

Resolved Caveats in Cisco Finesse Release 10.5(1) ES03

Defect ID: CSCus78964

Headline: Unified CCX and Unified CCE: Team performance gadget refresh.

Symptoms: When an agent makes a state change, it triggers a refresh of the Team Performance gadget on the supervisor's desktop. If the focus is at the bottom of the list, the state change moves the focus to some other row.

Conditions: In Cisco Finesse 10.5(1) ES02, when the supervisor focuses on an agent in the team performance gadget, one of the other agents in the same team changes state.

Workaround: None

Defect ID: CSCus11350

Headline: Cisco Finesse clients take 3 minutes to detect server NIC is disabled or offline.

Symptoms: Agent or Supervisor gadgets take close to 3 minutes to detect that Finesse server NIC is offline.

Conditions: Consider the following scenario:

Finesse A and Finesse B side servers are up and running. Agent signs in to Cisco Finesse and is in READY\NOT READY state. Using vSphere client, go in to the virtual machine properties and disable\disconnect the NIC card. Using Ping, confirm that the server NIC is not responding. Agent\Supervisor takes at least 3 minutes to detect that the Cisco Finesse server is not responding before attempting to connect to the B side server.

Workaround: None.

Changes in Cisco Finesse Release 10.5(1) ES02

NTLMv2 Support for Finesse Authentication to AWDB

With Release 10.5(1) ES02, Cisco Finesse is now configured to use only NTLMv2 for authentication to the AWDB. Cisco Finesse no longer supports the NTLMv1 authentication. As all releases of Unified CCE supported by Cisco Finesse 10.5(1) support NTLMv2, no additional configuration is required to support this feature.

Resolved Caveats in Cisco Finesse Release 10.5(1) ES02

Defect ID: CSCuq94553

Headline: Cisco Finesse XMPP connection is lost in IE9 and IE10.

Symptoms: The Salesforce.com integration of the Cisco Finesse API uses the tunnel IFrame hosted in the Cisco Finesse server to establish a connection to the Open Fire Service of Cisco Finesse to receive Events. This is outside the standard Cisco Finesse Desktop and therefore a non-Gadget.

In case the user is following any link, the connection to Cisco Finesse Openfire Service is terminated in the tunnel frame provided by Cisco.

The link causing the connection to abort*: clear*

This links triggers the onbeforeunload event in IE9 and IE10 and the Cisco tunnel catches this event and sends a XMPP terminate request to Cisco Finesse Server.

Conditions: B&H Connector + SalesForce.com integration on IE9 and IE10 browsers.

Workaround: None.

Defect ID: CSCur32699

Headline: Dynamic sorting not working in Supervisor.

Symptoms: Dynamic sorting does not work for team performance and queue statistics gadgets in Cisco Finesse supervisor.

Workaround: None. However, sorting again would put them in the right order.

Defect ID: CSCur35372

Headline: Cisco Finesse Tomcat crashes with OOM.

Symptoms: Cisco Finesse Tomcat service crashes and agents cannot sign in.

Conditions: This issue occurs after some undetermined period of running and depends on types of gadgets being hosted in Cisco Finesse. It is likely to occur with Live Data Gadgets due to their larger HTTP Responses.

Workaround: Restart the Cisco Finesse Tomcat service.

Defect ID: CSCur46146

Headline: Cisco Finesse 10.5(1) Failover Tool does not load completely.

Symptoms: Finesse Desktop Failover Tool does not load completely when following the **Ensure Failover Functions Correctly** section of the Cisco Finesse 10.5(1) installation guide.

However, failover does work if you conduct a manual failover test.

Conditions:

1. Cisco Finesse is installed and in service.
2. Failover test is attempted.

Workaround: None.

Note: This is a failover test tool issue and has no impact on actual failover functionality of agent or supervisor desktop.

Defect ID: CSCur53045

Headline: Cisco Finesse does not decode internationalized named vars and arrays correctly.

Symptoms: Within the context of outbound, if BABuddyName is given internationalized characters, they may not render correctly on the Cisco Finesse desktop.

This includes if ECC named vars and named arrays with internationalized characters are used within any other context (other than outbound).

Workaround: None.

Changes in Cisco Finesse Release 10.5(1) ES01

Cisco Finesse Release 10.5(1) ES01 introduces support for Internet Explorer 10.0, and also supports the use of Compatibility View for the Finesse agent and supervisor desktop with Internet Explorer 9.0, 10.0, and 11.0. When Compatibility View is enabled in IE9, IE10, or IE11, the browser renders in IE8 mode.

Note: The banner that appears on the Cisco Finesse desktop which warns agents that their browser is running in Compatibility View has been removed in this ES.

Resolved Caveats in Cisco Finesse Release 10.5(1) ES01

Defect ID: CSCuo34735

Headline: EIM or WIM 9.0(2) Gadget and Cisco Finesse Version 10.0(1) incompatible.

Symptoms: The gadget is provided with EIM or WIM 9.0(2) for use within Cisco Finesse Release 10.0(1). Through EIM or WIM gadget, the EIM or WIM UI fails to produce Username and Password entry options within Cisco Finesse version 10.0(1), the logo and butterfly is

displayed but there are no input areas. However, Cisco Finesse Release 9.0(1) with EIM or WIM gadget installed running IE9 in compatibility mode works properly and displays input fields.

Conditions: Because of the conditions that has changed, Finesse Release 10.0(1) cannot be used with IE in compatibility mode and requires non-Compatibility mode which causes the gadget to be non- functional. Therefore the two are incompatible. Despite the fact that the compatibility matrix displays Cisco Finesse 10.0(1) compatible with EIM or WIM 9.0(2).

Workaround: None at this time, to run EIM or WIM 9.0(2) gadget within Cisco Finesse. But the EIM or WIM 9.0(2) application can be launched as a separate browser application independent of Cisco Finesse.

Defect ID: CSCup21532

Headline: Warning exception repeated in Tomcat Catalina logs.

Symptoms: The following message repeats itself and fills Finesse catalina.out log file: com.sun.jersey.core.impl.provider.xml.SAXParserContextProvider getInstance

WARNING: JAXP feature XMLConstants.FEATURE_SECURE_PROCESSING cannot be set on a SAXParserFactory. External general entity processing is disabled but other potential security related features will not be enabled.

org.xml.sax.SAXNotRecognizedException: Feature 'http: //javax.xml.XMLConstants/feature/secure- processing' is not recognized.

Conditions: This message occurs in the log files due to a jar upgrade with the Cisco Finesse 10.5(1) release. The jar upgrade was to fix CDET CSCuo27571. So any Cisco Finesse deployment running Cisco Finesse version 10.5(1) will experience this issue.

Workaround: None.

Defect ID: CSCup22195

Headline: Smarter failover issue while restarting Cisco Finesse Tomcat.

Symptoms: In the following scenario, agents fail to sign in to the desktop after restarting Cisco Finesse Tomcat.

1. Sign in an agent and receive either an inbound or outbound call.
2. When the agent is in TALKING state stop Cisco Finesse Tomcat. A red disconnected bar appears on top of the desktop.
3. Start Cisco Finesse Tomcat.
4. Desktop is trying to reconnect and it is failing.
5. Reconnect is failing with the Sign Out notification message "You have been signed out and will redirected to the sign in page."

Conditions: Restart Cisco Finesse Tomcat when the agent is in TALKING state for an inbound or outbound call.

Workaround: Agent can sign in again and continue all normal call control operations.

Defect ID: CSCup26212

Headline: Meta tags in head tag are not rendered in order in gadget.

Symptoms: When a gadget renders an HTML, the meta tags in the head tag of the HTML contained in the CDATA section in DgridViewer.jsp is not maintained.

Conditions: Add a meta tag such as <meta http-equiv="X-UA-Compatible" content="IE=9" /> just below the <head> tag in the DgridViewer.jsp and check the output HTML rendered by the gadget container in Finesse.

Workaround: None.

Defect ID: CSCup29927

Headline: Insufficient logging in Queue stats polling.

Conditions: Always.

Workaround: None.

Defect ID: CSCup40082

Headline: Cisco Finesse memory leak from duplicate CTI requests.

Conditions: Requests are coming from CTI fail over which accumulate over time.

Workaround: Restart Tomcat service.

Defect ID: CSCup70092

Headline: Cisco Finesse wrap-up API does not handle single extended ASCII code character.

Symptoms: Currently, Cisco Finesse does not handle the wrap-up reason properly from a REST API request when there is only a single extended ASCII code character in the wrap-up reason and the extended ASCII code character is the last character in the wrap-up reason, which results in an ArrayIndexOutOfBoundsException being thrown in one of our helper classes, that leads to the Internal Server Error.

Conditions: REST API request when there is only a single extended ASCII code character in the wrap-up reason and the extended ASCII code character is the last character in the wrap-up reason.

Workaround: Do not use single extended ASCII code character in the wrap-up reason when the extended ASCII code character is the last character in the wrap-up reason.

Defect ID: CSCup78848

Headline: Barge of a conference call with UCCE 10.5(1).

Symptoms: Supervisor receives a generic error - "Call could not be completed as dialed" while trying to barge into a conference call.

Conditions: Supervisor is trying to barge in to an agent's call who is not the conference

controller.

Workaround: Supervisor cannot barge into a conference call through non-conference controller agent.

Defect ID: CSCup81268

Headline: Agent is signed out from a session if agent logs into another extension.

Symptoms: When an agent logs in with the same credentials of another agent who is already logged in to a different extension, the first agent gets signed out with a message - "The User session got disconnected, because you signed into a different session". Agent 2 cannot sign in and gets the message you are already signed in extension 1.

Workaround:

1. Close and Re-launch IP Communicator on both desktop.
2. Close and Launch IP Communicator for both agent and sign in back to Cisco Finesse.

Defect ID: CSCup82687

Headline: Finesse.js doc does not include ClientServices.registerOnConnectHandler()

Symptoms: Finesse javascript library documentation is missing ClientServices.registerOnConnectHandler() and ClientServices.registerOnDisconnectHandler().

Conditions: Functions are not documented.

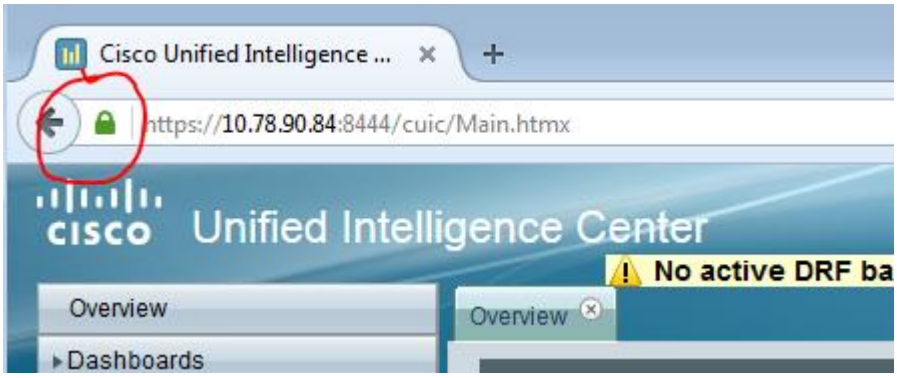
Workaround: Use ClientServices.registerOnConnectHandler() and ClientServices.registerOnDisconnectHandler() to trigger handler when BOSH is connected or disconnected.

Bug Search Tool

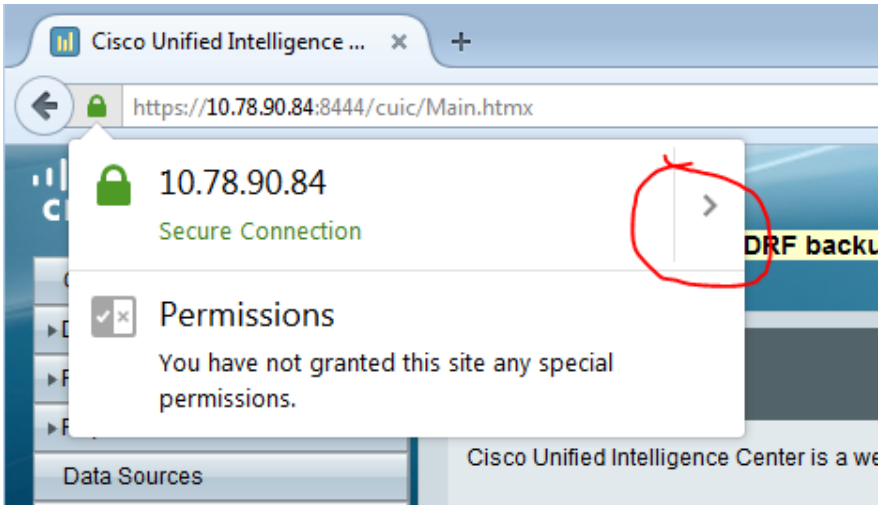
To access the Bug Search Tool, go to https://www.cisco.com/cisco/psn/bssprt/bss and log in with your Cisco.com user ID and password.

Procedure to Regenerate Certificates for SHA256 in Finesse

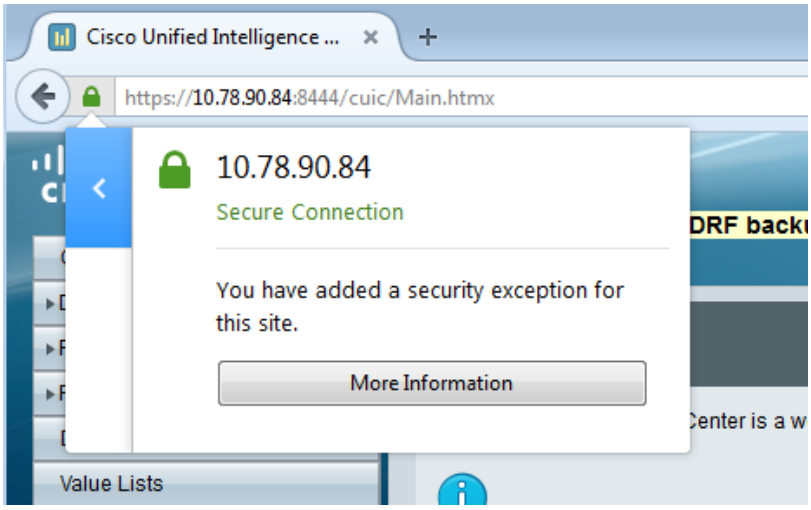
1. With the existing (SHA-1) Certificate, sign in to **https://<ip>:<port>/**page.
2. Verify the certificate from the following screen (click the LOCK icon).



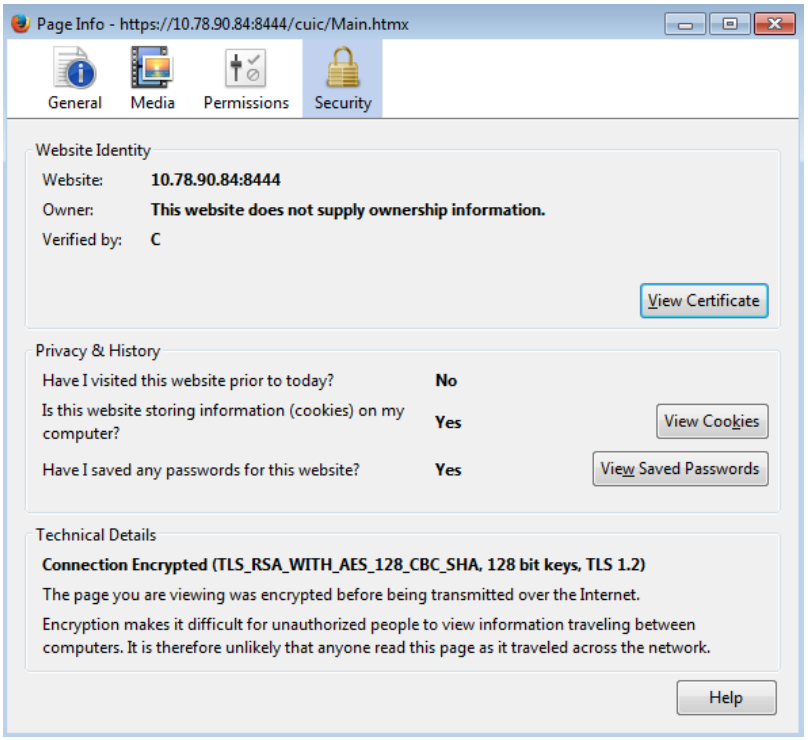
3. Select **Secure Connection**.



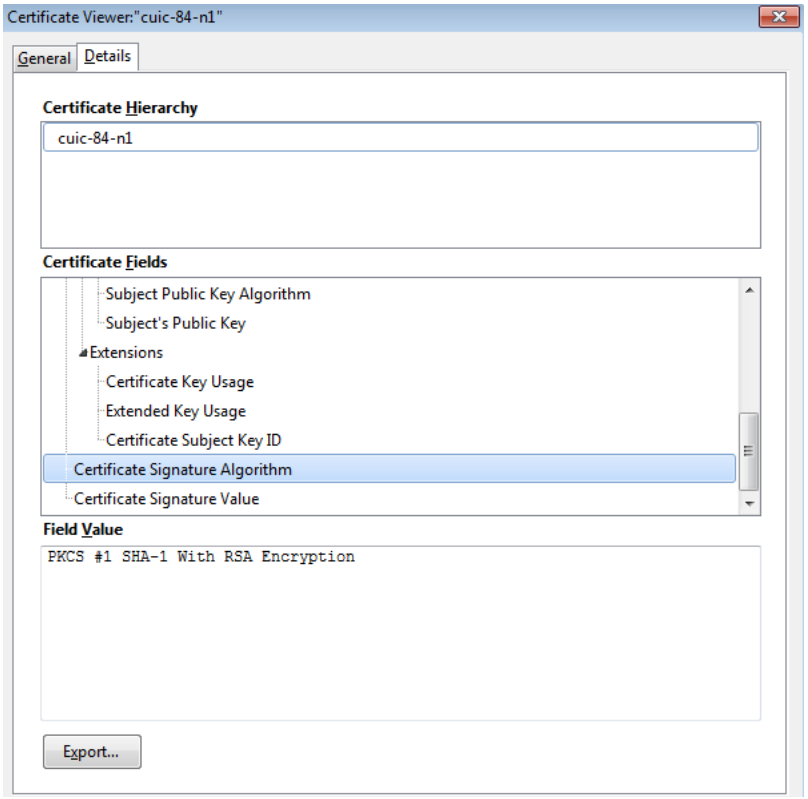
4. Select **More Information.**



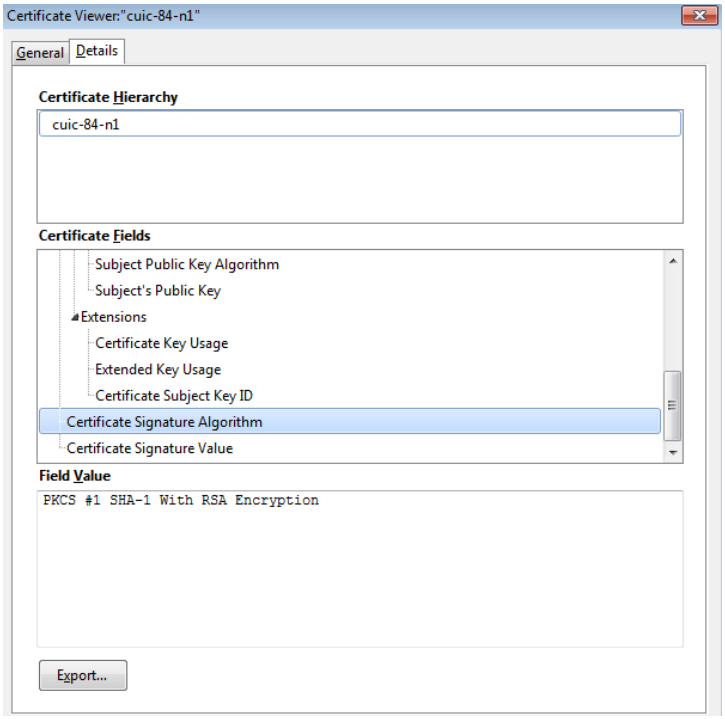
5. Select **Security** - > **View Certificate**.



6. Select **Details** -> **Certificate Fields** -> **Certificate Signature Algorithms**.

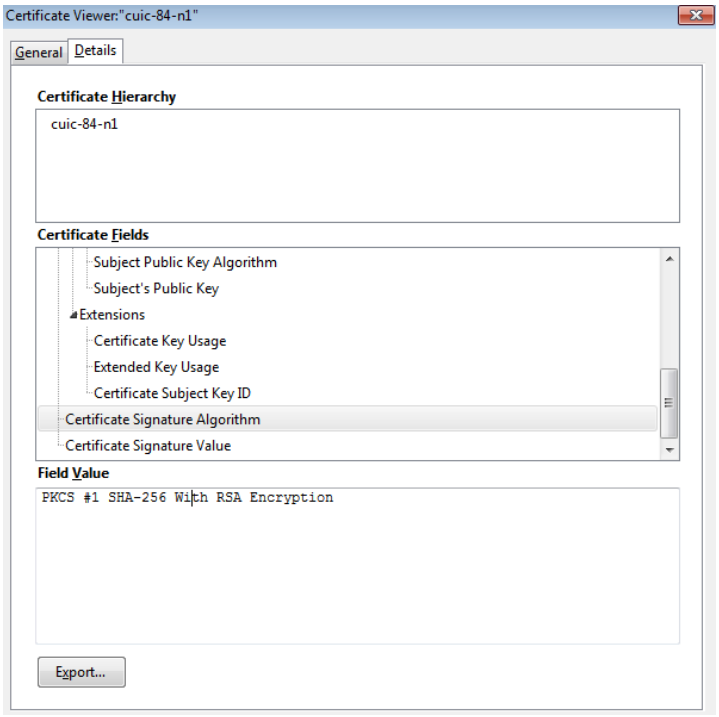


7. Verify that the Signature Algorithm shows **PKCS #1 SHA-1 With RSA Encryption.**



8. Generate the new certificate and follow steps from 1 to 6.

9. Select **Details** -> **Certificate Fields** -> **Certificate Signature Algorithms**.



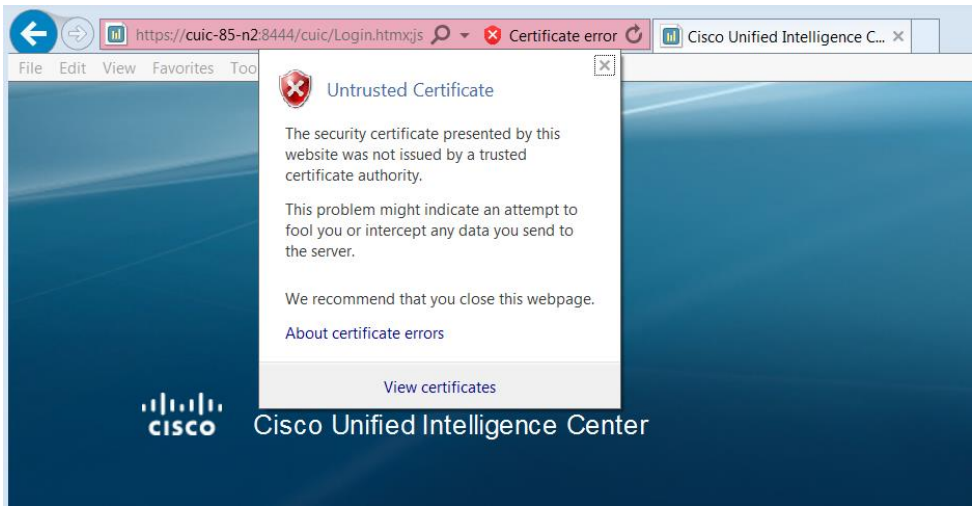
10. Verify that the Signature Algorithm shows **PKCS #1 SHA-256 With RSA Encryption.**

Internet Explorer

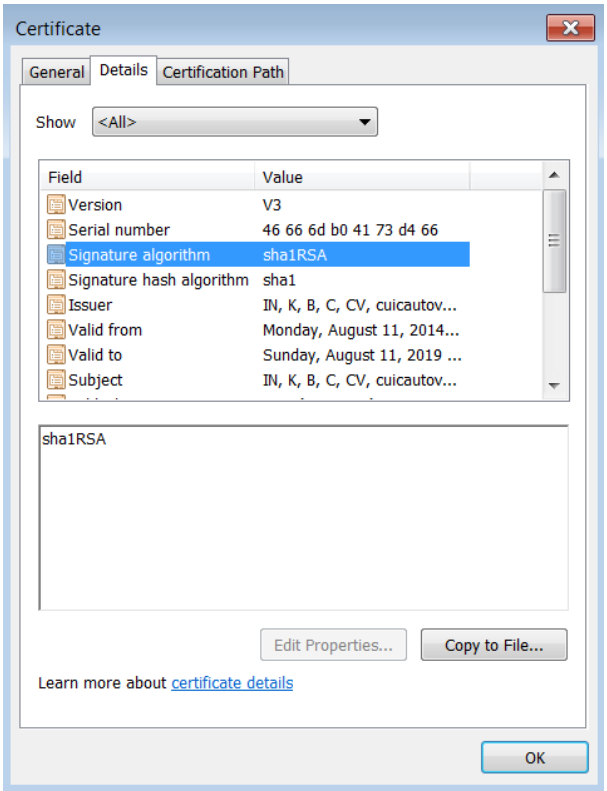
Prerequisites:

- Add IP and host name entry in to *C:\Windows\System32\drivers\etc\hosts file.*
- Use host name of the server instead of IP.

1. Sign in to https://<hostname>:<port>/page
2. To verify certificate, click **Certificate error** -> **View certificates**.



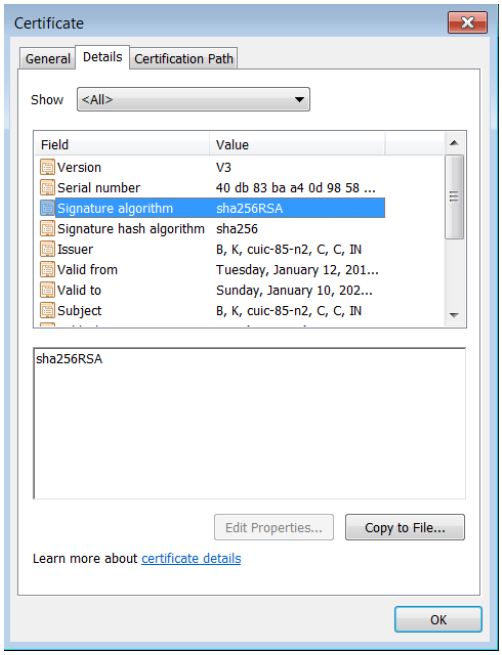
3. Select **Certificate** -> **Details** ->**Signature algorithm**.



4. Verify that the Signature algorithm shows **sha1RSA**.

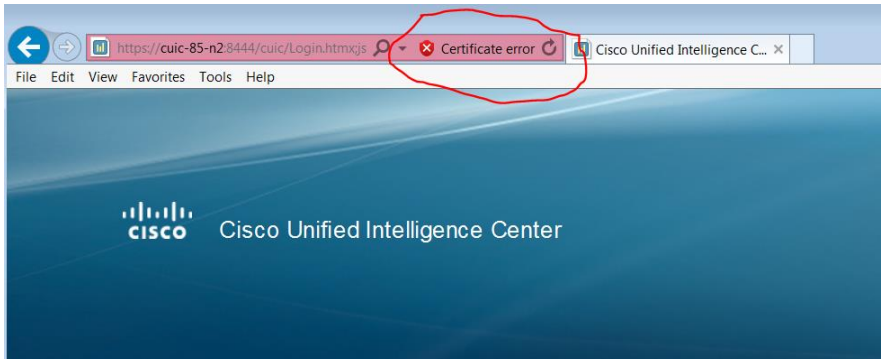
5. Generate the new certificate and follow steps from 1 to 3.

6. Select **Certificate** - > **Details** -> **Signature algorithm**.



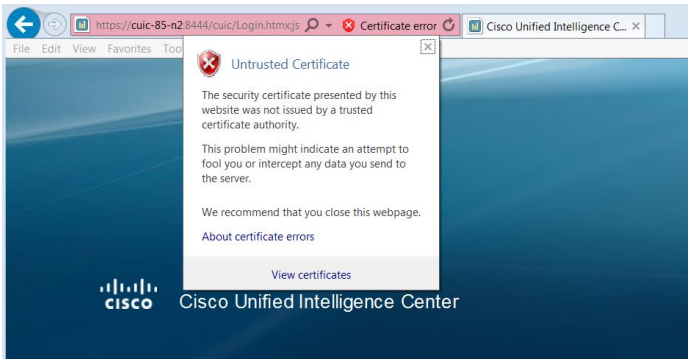
7. Verify that Signature Algorithm shows **sha256RSA**.

8. Verify even after generating new certificate SHA256, if the URL certificate status shows **Certificate Error**.

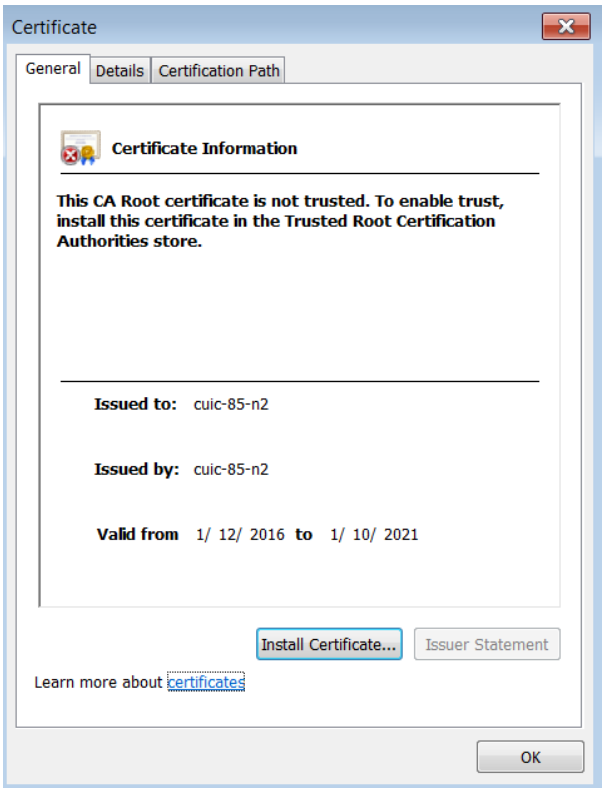


To fix this issue, import the Certificate:

a) Select **Certificate Error**-> **View Certificate**.

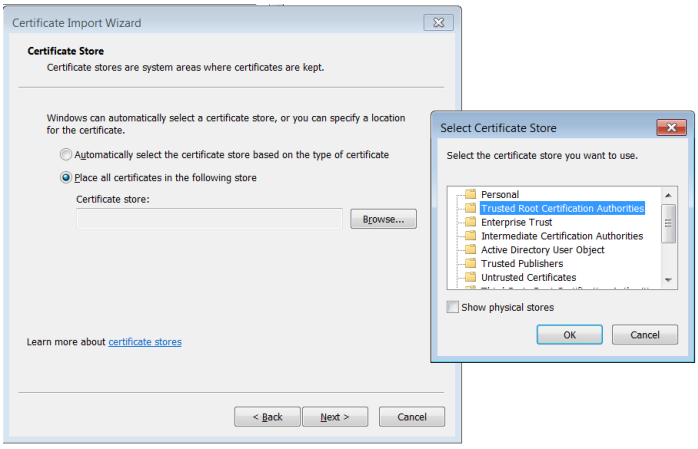


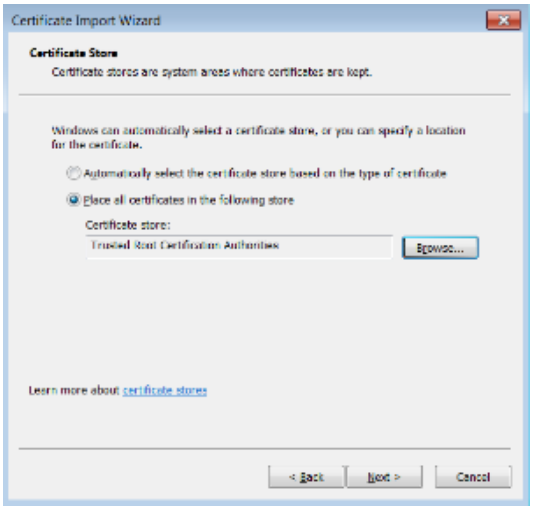
b) Select **Certificate** - > **Install Certificate.**



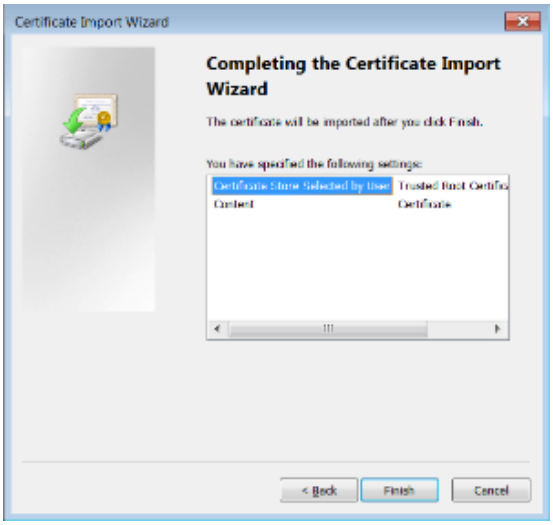
c) In Certificate Import Wizard -> **Next.**

d) Select the radio button **Place all certificate in the following store**, click **Browse** and select **Trusted Root Certificate Authorities.** Now click **OK** and **Next**.

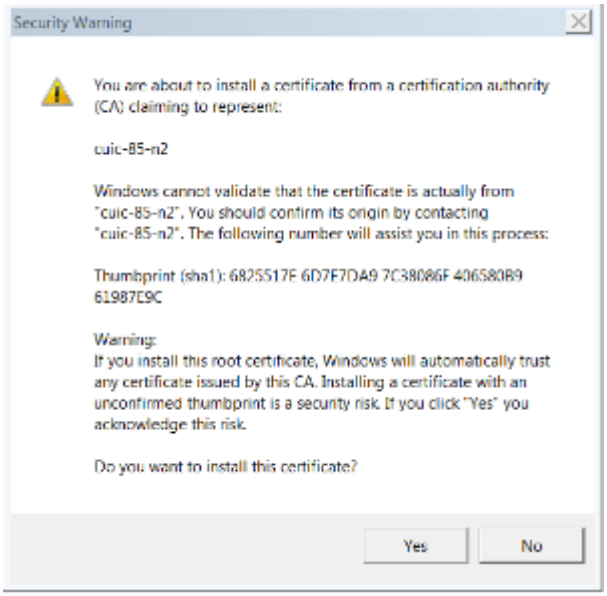




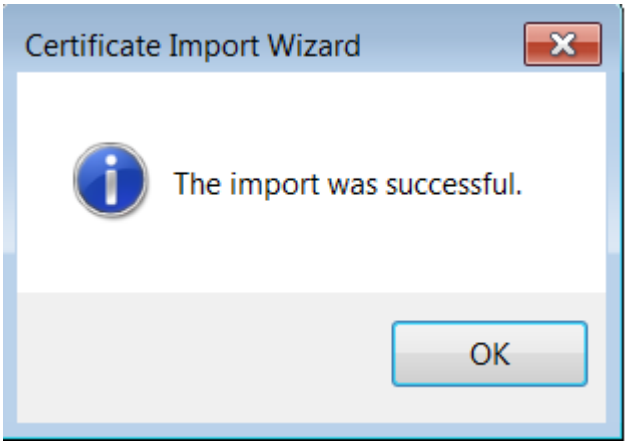
e) Select **Finish.**



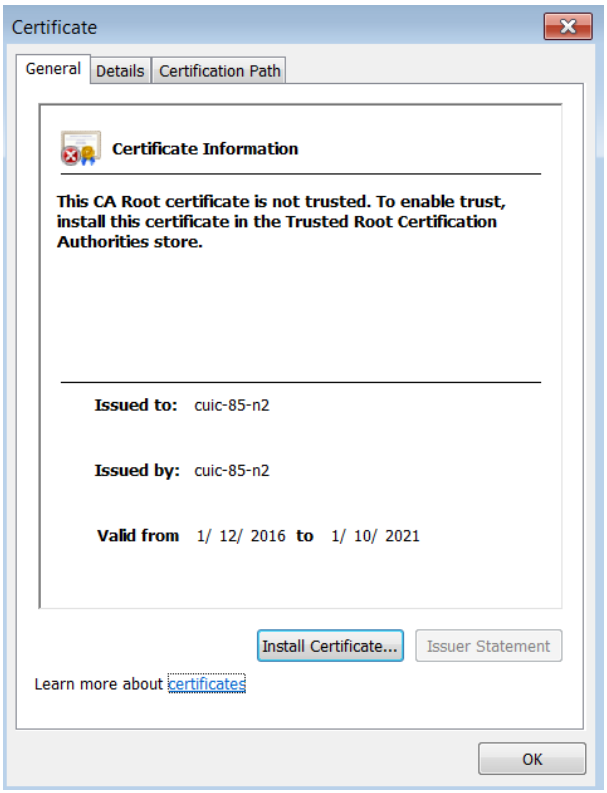
f) Select **Yes**.



g) Select **OK**.



h) Select **OK**.



i) Close the session and open a new browser. Verify if the **Certificate Error** issue is resolved. The screen should display a lock icon instead of an error.