Cisco Finesse Release 10.5(1) ES09

Contents

Cisco Finesse Release 10.5(1) ES09

File Name	MD5 Checksum
ccd-finesse.1051.ES09.10000.cop.sgn	95:75:ae:4e:67:6e:e8:e6:5f:d6:61:ef:a3:84:61:82
ccd-finesse.1051.ES.Rollback.cop.sgn	6f:d5:55:c5:8b:55:f6:9c:f9:29:26:86:44:dc:61:9a

Cisco Finesse Release 10.5(1) ES9 is cumulative. It contains all fixes from Cisco Finesse Release 10.5(1) ES1 to 10.5(1) ES8.

Valid Upgrade Paths

Cisco Finesse Release 10.5(1) ES9 is delivered as a Cisco Option Package (COP) file. If using any other 10.5 ES versions, you must upgrade to 10.5(1) ES8 or rollback to 10.5(1) and then install ES9.

The supported upgrade paths for 10.5(1)-ES09 are:

- 10.5(1)
- 10.5(1) ES8

Installing Finesse Release 10.5(1) ES9

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 happen. Installing this patch or performing a rollback stops and restarts certain Finesse services. To avoid interruption to agents, perform the installation or rollback during a maintenance window.

1. Download **ccd-finesse.1051.ES09.10000.cop.sgn** to an SFTP server that can be accessed by the Finesse system.
2. Use SSH to log in to your 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 you can ignore this message. No reboot is required.
6. To verify 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.ES09.10000.cop

7. Check that the installation was successful by signing in to Finesse ((http://IP-Address or hostname of Finesse server/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 the Finesse system.
2. Use **SSH** to log in to your 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 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 Finesse Rollback COP file restores your system to the base 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) ES9

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

Symptoms: 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 Finesse agent screen after blind transfer to IP-IVR RP.

Symptoms: When transferring a call from one 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: Finesse displays ConnectionDeviceID instead of ANI during a transfer.

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

As 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 CCE, PQ's do not show in the agent's queue statistic gadget.

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

Workaround: Try logging in again.

Defect ID: CSCvb54353

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

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

Workaround: None

Defect ID: CSCva72280

Headline: 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: Finesse returns wrong line state.

Symptoms: Typically when VOIP inbound calls from Skype, Viber or other internet service providers are received, Finesse intermittently returns the wrong LINE state. This could be because Finesse reports that customer leg is in (INITIATING/ALERTING); while IVR APP is designed to drop the call if customer leg is not ACTIVE.

Workaround: None

Defect ID: CSCvd00580

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

Symptoms: When the REST proxy authentication is enabled, 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 conferenced call, where if one agent ends the call, the second agent loses control and is unable to end the call.

Workaround: None

Resolved Caveats in Cisco Finesse Release 10.5(1) ES8

Defect ID: CSCux28810

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

Symptoms: All agents show a red banner intermittently that says disconnected from Finesse Server. Agents will not be to login to Finesse during this time.

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

Defect ID: CSCuz11421

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

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

Workaround: The Agent has to click in any area on the browser window to release the 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: 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 (Ex: 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 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 Finesse API for Gadgets integration. An attacker could exploit this vulnerability by submitting a HTTP request to the Finesse server.

Workaround: None

Note: This fix ensures that gadgets that invoke 3rd party REST APIs proxied via Finesse shindig are authenticated by Shindig. After installation of 10.5(1) ES08, the REST proxy authentication is enabled by default. Finesse provides a new utils commands which can be used to disable / 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 finesse failover. An agent who has logged out is shown as logged 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**

Now, restart Cisco Finesse Tomcat service on both Finesse nodes.

Defect ID: CSCuz38289

Headline: Finesse agent is unable to change state after idling for 30 minutes.

Workaround: Disable RestProxy Authentication to revert back to old behavior. Rollback ES3 COP file or login 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) ES7.

Workaround: Remove 10.5(1)ES7 or revert default openfire password in the backend.

Resolved Caveats in Cisco Finesse Release 10.5(1) ES7

Defect ID: CSCuw86228

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

Symptoms: PhonePad.xd.js has event handlers for the dial-pad mouse/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: Finesse Supervisor cannot see an agent's status update after PG failover.

Symptoms: Agent state is out of sync after finesse failover. An agent who has logged out is shown as logged 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 finesse notification service runs out of memory.

Workaround: None

Resolved Caveats in Cisco Finesse Release 10.5(1) ES6

Defect ID: CSCuy52732

Headline: sha256 support on 10.0 and 10.5 versions.

Note: Procedure for certificate regeneration

Resolved Caveats in Cisco Finesse Release 10.5(1) ES5

Defect ID: CSCux13711

Headline: PCCE 10.5.2 validation fails with Finesse 10.5_ES4.

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

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

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) ES4

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 Finesse.

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

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

Workaround: Restart Finesse Notification and Tomcat Service.

Defect ID: CSCuv76434

Headline: Finesse Logjam Vulnerability.

Symptoms: 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 Finesse in a UCCE environment or UCCX with co-resident Finesse.

Workaround: No workarounds currently exist to change Finesse to be protected from Logjam exploitation, but users of Firefox can perform the following workaround to regain access to 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) ES3

Defect ID: CSCus78964

Headline: CCX/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 Finesse 10.5.1 ES2, when the Supervisor has focus 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: Finesse clients take 3 minutes to detect server NIC is disabled\offline.

Symptoms: Agent\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 logs into Finesse and is in READY\NOT READY state. Using vSphere client, go into 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 Finesse server is not responding before then attempting to connect to the B side server.

Workaround: None

Changes in Cisco Finesse Release 10.5(1) ES2

NTLMv2 Support for Finesse Authentication to AWDB

With Finesse Release 10.5(1) ES2, Finesse is now configured to use only NTLMv2 for authentication to the AWDB. Finesse no longer supports NTLMv1 authentication. As all releases of Unified CCE supported by Finesse 10.5(1) support NTLMv2, no additional configuration is required to support this feature.

Resolved Caveats in Cisco Finesse Release 10.5(1) ES2

Defect ID: CSCuq94553

Headline: 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*: <a href="javascript: void(0);" id="clear">clear</a>*

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

Workaround: None - but sorting again would put them in the right order.

Defect ID: CSCur35372

Headline: Finesse Tomcat crashes with OOM.

Symptoms: Finesse Tomcat service crashes and agents cannot login.

Conditions: This issue occurs after some undetermined period of running and depends on types of gadgets being hosted in 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: Finesse 10.5 Failover Tool stuck while loading.

Symptoms: Finesse Desktop Failover Tool gets stuck while loading when following the **Ensure Failover Functions Correctly** section of the Finesse 10.5 installation guide.

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

Conditions:

1. 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/supervisor desktop.

Defect ID: CSCur53045

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

Symptoms: Within the context of outbound, if BABuddyName is given internationalized characters, they might not get rendered correctly on the 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) ES1

Cisco Finesse Release 10.5(1) ES1 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 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) ES1

Defect ID: CSCuo34735

Headline: EIM/WIM 9.0(2) Gadget and Finesse Version 10 incompatible.

Symptoms: The gadget is provided with EIM/WIM 9.0(2) for use within Finesse Release 10. Within Finesse via EIM/WIM gadget, the EIM/WIM UI fails to produce Username / Password entry options within Finesse version 10, the logo and butterfly are displayed but there are no input areas. However, Finesse Release 9 with EIM/WIM gadget installed running IE9 in Compatibility Mode works properly and displays input fields.

Conditions: The condition that has changed in Finesse Release 10 this release is unable to be used with IE in compatibility mode and requires Non-Compatibility mode which causes gadget to not function. Therefore the two are incompatible. Despite the fact that the compatibility matrix displays Finesse 10 compatible with EIM/WIM 9.0(2).

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

Defect ID: CSCup21532

Headline: Warning exception repeated in Tomcat Catalina logs.

Symptoms: The following message repeats itself and fills Finesse's 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 Finesse 10.5 release. The jar upgrade was to fix CDET CSCuo27571. So any Finesse deployment running Finesse version 10.5 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 login to the desktop after restarting Cisco Finesse Tomcat.

1. Login 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 re-login 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: 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: Finesse wrap-up API does not handle single extended ASCII code character.

Symptoms: Currently 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.

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 logged 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 logged out with a message - "The User session got disconnected, because you signed into a different session".

Agent 2 cannot log in and gets the message you are already logged on extension 1.

Workaround:

1. Close and Re-launch IP Communicator on both desktop.
2. Close and Launch IP Communicator for both agent and log back into Finesse.

Defect ID: CSCup82687

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

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

Conditions: Functions are not documented.

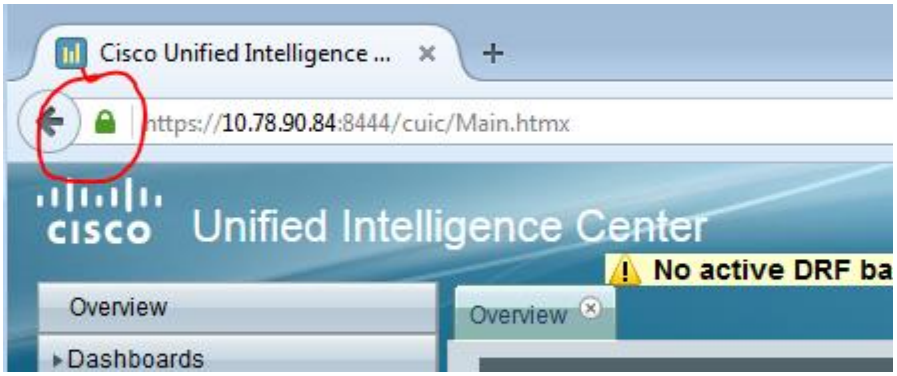
Workaround: Use ClientServices.registerOnConnectHandler() and ClientServices.registerOnDisconnectHandler() to trigger handler when BOSH is connected or disconnected.

Bug Search Tool

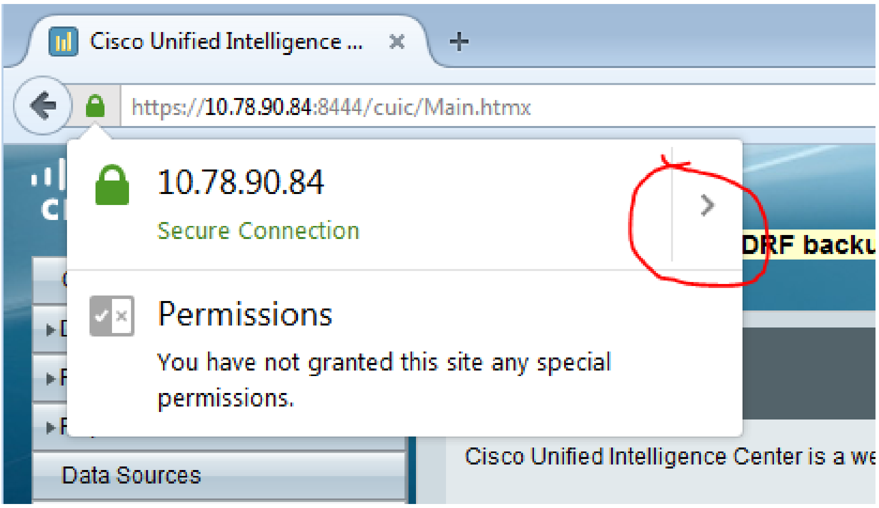
To access the Bug Search Tool, go to https://www.cisco.com/cisco/psn/bssprt/bss and log in with your Cisco.com user ID and password.

Procedure to Regenerate Certificates for SHA256 in Finesse:

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


Cisco Unified Intelligence ...
https://10.78.90.84:8444/cuic/Main.htmx
cisco
Unified Intelligence Center
No active DRF ba
Overview
Dashboards
Overview

3. Select **Secure Connection.**


Cisco Unified Intelligence ...
https://10.78.90.84:8444/cuic/Main.htmx
DRF backu
Data Sources

10.78.90.84

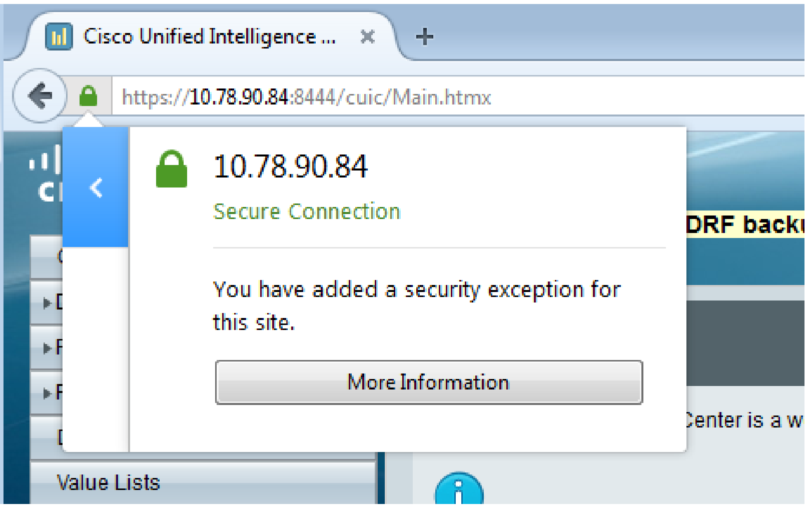
Secure Connection

Permissions

You have not granted this site any special permissions.

Cisco Unified Intelligence Center is a we

4. Select **More Information.**


Cisco Unified Intelligence ...
https://10.78.90.84:8444/cuic/Main.htmx
DRF backu
More Information
Value Lists

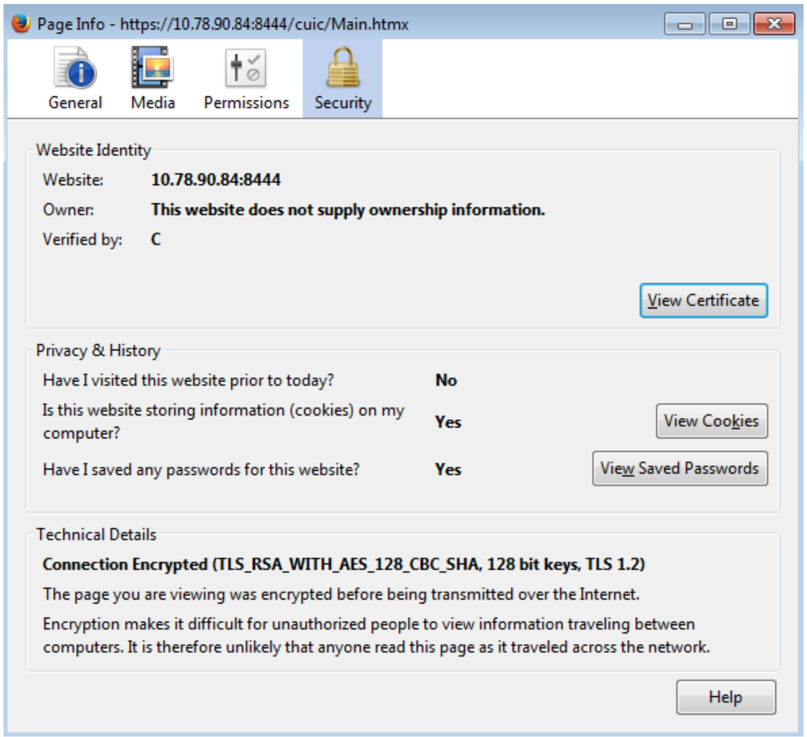
10.78.90.84

Secure Connection

You have added a security exception for this site.

Center is a w

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



Page Info - https://10.78.90.84:8444/cuic/Main.htmx

Website Identity

Website: **10.78.90.84:8444**

Owner: **This website does not supply ownership information.**

Verified by: **C**

Privacy & History

Have I visited this website prior to today? **No**

Is this website storing information (cookies) on my computer? **Yes**

Have I saved any passwords for this website? **Yes**

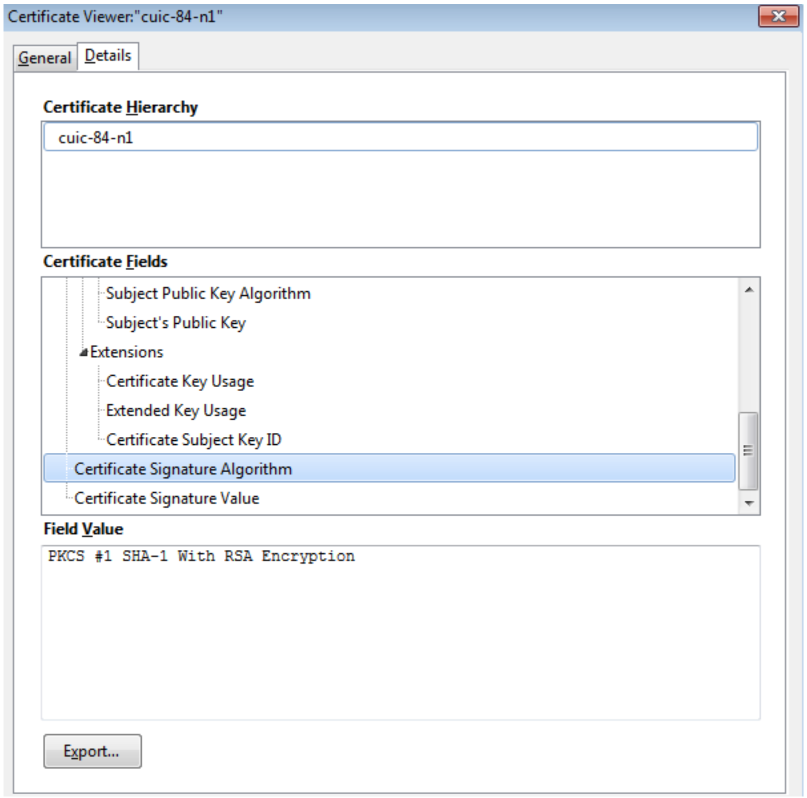
Technical Details

Connection Encrypted (TLS_RSA_WITH_AES_128_CBC_SHA, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

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



Certificate Viewer:"cuic-84-n1"

Certificate Hierarchy

cuic-84-n1

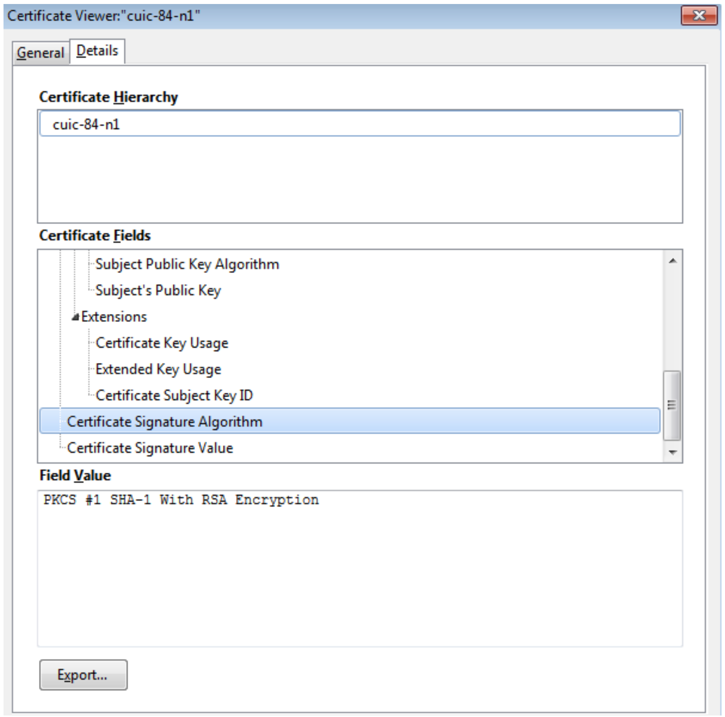
Certificate Fields

Subject Public Key Algorithm
Subject's Public Key
Extensions
Certificate Key Usage
Extended Key Usage
Certificate Subject Key ID
Certificate Signature Algorithm
Certificate Signature Value

Field Value

```
PKCS #1 SHA-1 With RSA Encryption
```

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


Certificate Viewer:"cuic-84-n1"
General
Details
Certificate Hierarchy
Certificate Fields
Subject Public Key Algorithm
Subject's Public Key
Extensions
Certificate Key Usage
Extended Key Usage
Certificate Subject Key ID
Certificate Signature Algorithm
Certificate Signature Value
Field Value
Export...

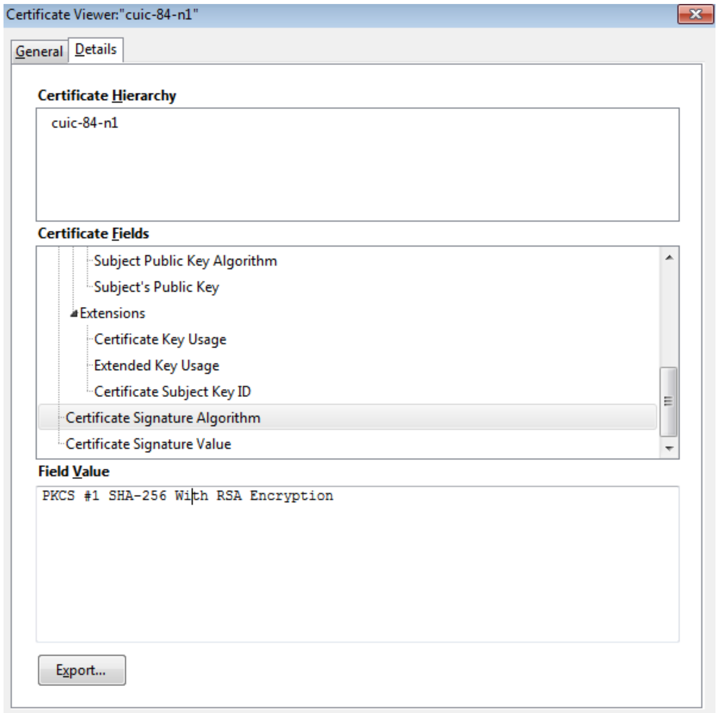
Certificate Hierarchy: cuic-84-n1

Field Value:

```
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.**


Certificate Viewer:"cuic-84-n1"
General
Details
Certificate Hierarchy
Certificate Fields
Subject Public Key Algorithm
Subject's Public Key
Extensions
Certificate Key Usage
Extended Key Usage
Certificate Subject Key ID
Certificate Signature Algorithm
Certificate Signature Value
Field Value
Export...

Certificate Hierarchy: cuic-84-n1

Field Value:

```
PKCS #1 SHA-256 With RSA Encryption
```

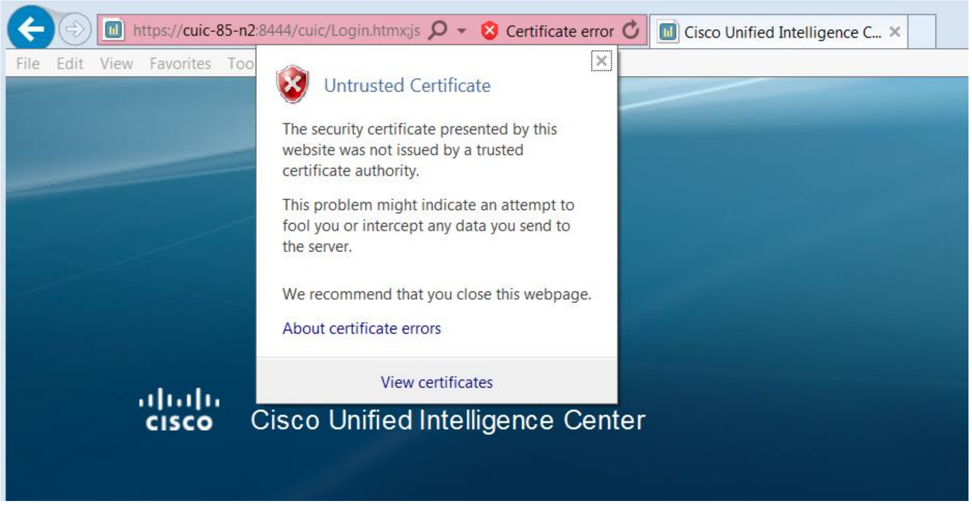
10. Verify that the Signature Algorithm shows **PKCS #1 SHA-256 With RSA Encryption.**

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



Untrusted Certificate

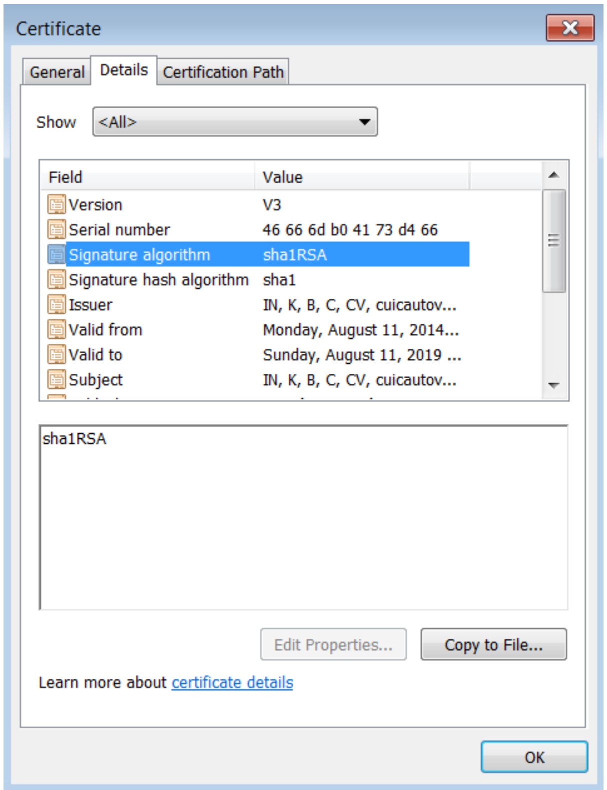
The security certificate presented by this website was not issued by a trusted certificate authority.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

https://cuic-85-n2:8444/cuic/Login.htmx;js
Certificate error
Cisco Unified Intelligence C...
File
Edit
View
Favorites
Too
About certificate errors
View certificates
Cisco Unified Intelligence Center

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



Show <All>

Field	Value
Version	V3
Serial number	46 66 6d b0 41 73 d4 66
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	IN, K, B, C, CV, cuicautov...
Valid from	Monday, August 11, 2014...
Valid to	Sunday, August 11, 2019 ...
Subject	IN, K, B, C, CV, cuicautov...

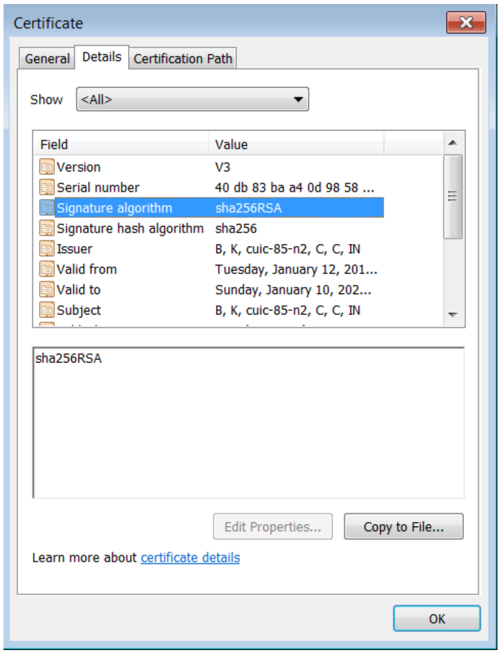
sha1RSA

Learn more about certificate details

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.



Show <All>

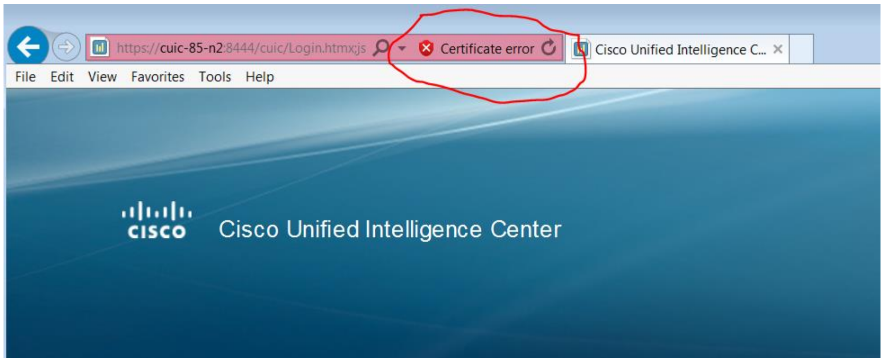
Field	Value
Version	V3
Serial number	40 db 83 ba a4 0d 98 58 ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	B, K, cuic-85-n2, C, C, IN
Valid from	Tuesday, January 12, 201...
Valid to	Sunday, January 10, 202...
Subject	B, K, cuic-85-n2, C, C, IN

sha256RSA

Learn more about certificate details

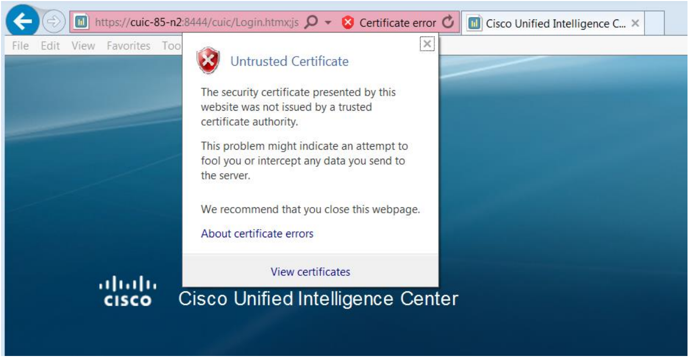
7. Verify that Signature Algorithm shows **sha256RSA.**

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


https://cuic-85-n2:8444/cuic/Login.htmx;js
Certificate error
Cisco Unified Intelligence C...
File Edit View Favorites Tools Help
cisco
Cisco Unified Intelligence Center

To fix this issue, import the Certificate:

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


https://cuic-85-n2:8444/cuic/Login.htmx;js
Certificate error
Cisco Unified Intelligence C...
File Edit View Favorites Too
cisco
Cisco Unified Intelligence Center

Untrusted Certificate

The security certificate presented by this website was not issued by a trusted certificate authority.

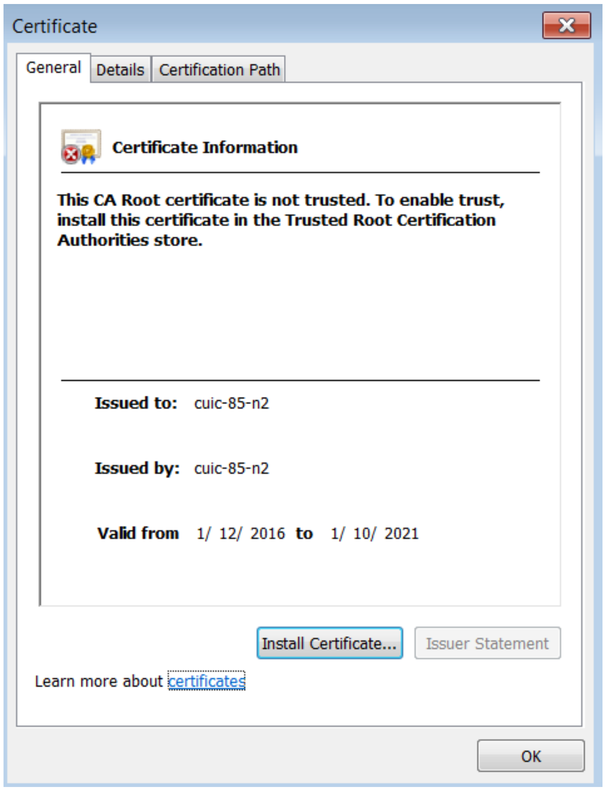
This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

View certificates

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



Certificate Information

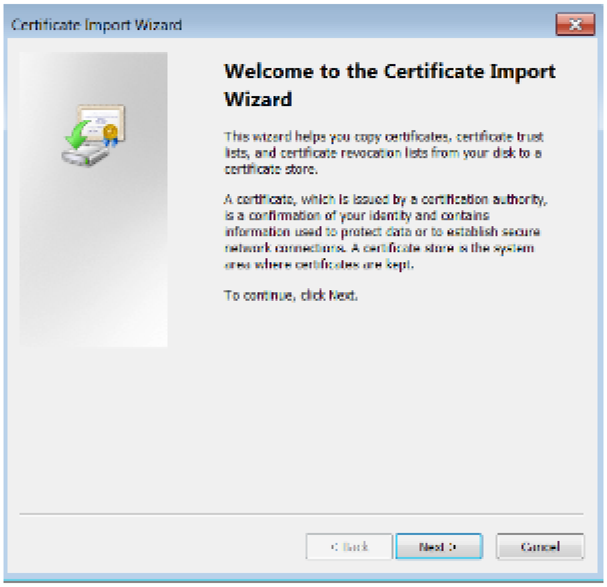
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: cuic-85-n2

Issued by: cuic-85-n2

Valid from 1/ 12/ 2016 **to** 1/ 10/ 2021

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



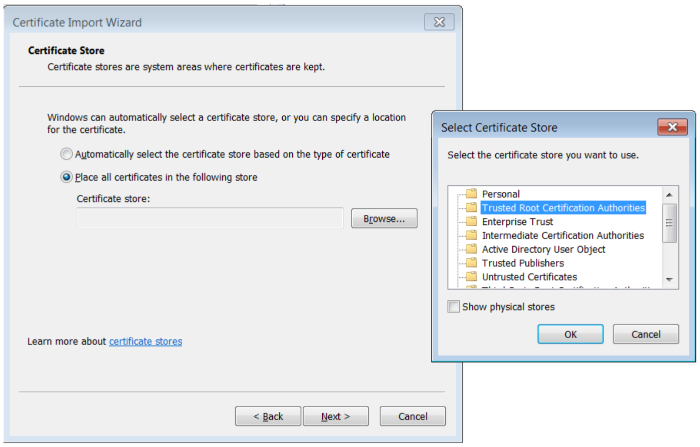
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click 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.**



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

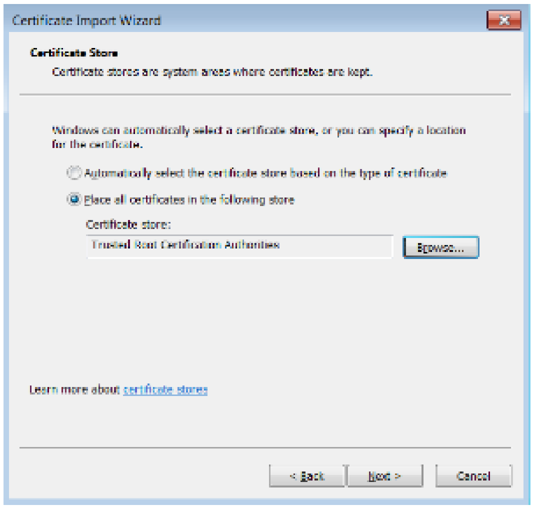
Learn more about certificate stores

Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

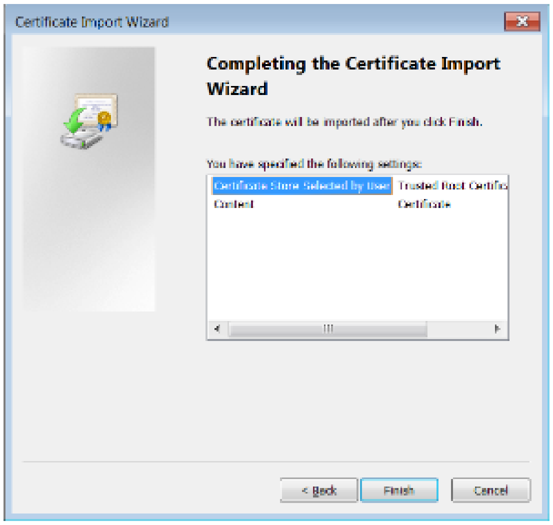
● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Learn more about certificate stores

e) Select **Finish.**



Certificate Import Wizard

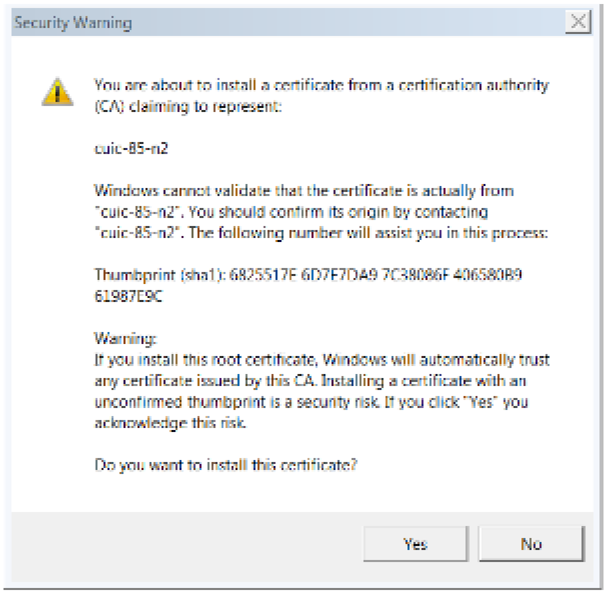
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certific
Content	Certificate

f) Select **Yes.**



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

cuic-85-n2

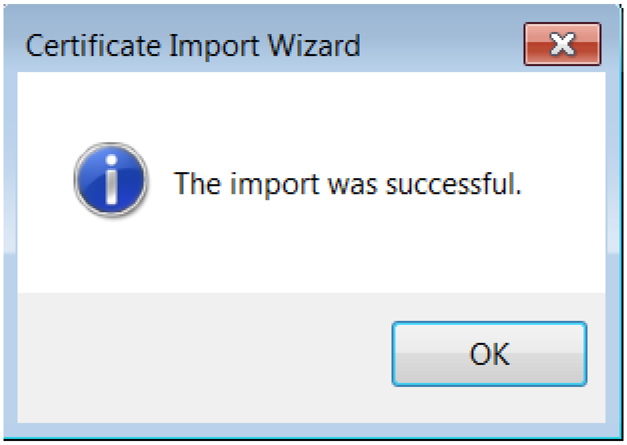
Windows cannot validate that the certificate is actually from "cuic-85-n2". You should confirm its origin by contacting "cuic-85-n2". The following number will assist you in this process:

Thumbprint (sha1): 6825517E 6D7E7DA9 7C38086F 406580B9 61987E9C

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

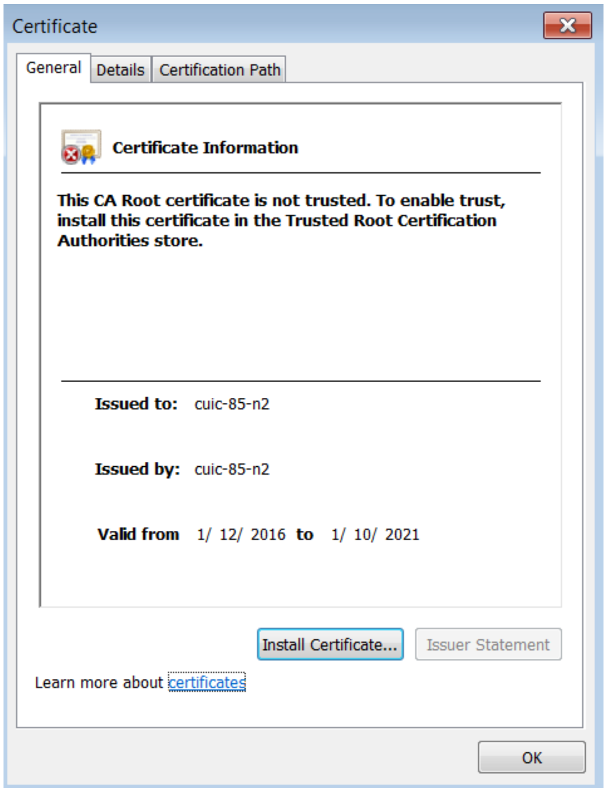
g) Select **OK**.



Certificate Import Wizard

The import was successful.

h) Select **OK.**



Certificate Information

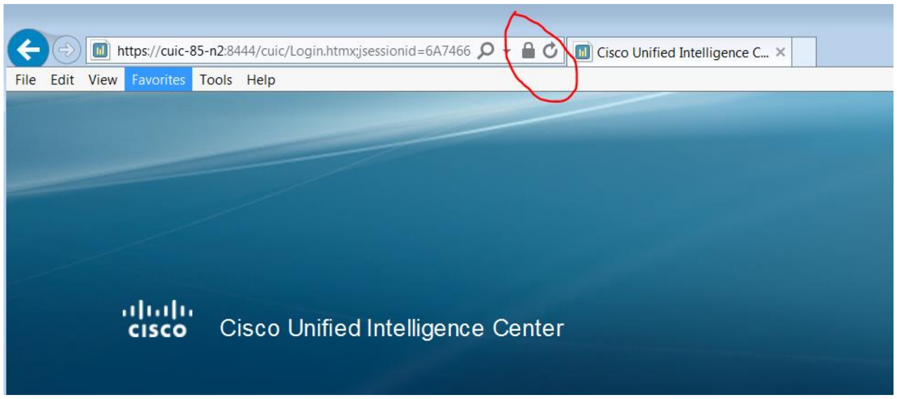
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: cuic-85-n2

Issued by: cuic-85-n2

Valid from 1/ 12/ 2016 to 1/ 10/ 2021

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.


https://cuic-85-n2:8444/cuic/Login.htmx;jsessionid=6A7466
Cisco Unified Intelligence C...
File
Edit
View
Favorites
Tools
Help
cisco
Cisco Unified Intelligence Center