Understand ECDSA certificates in an UCCX Solution

Contents

Introduction

This document describes how to configure the Cisco Unified Contact Center Express (UCCX) solution for the use of Elliptical Curve Digital Signature Algorithm (ECDSA) Certificates.

Prerequisites

Requirements

Before you proceed with the configuration steps that are described in this document, ensure that you have access to the Operating System (OS) Administration page for these applications:

- UCCX
- SocialMiner
- Cisco Unified Communications Manager (CUCM)
- UCCX Solution Certificate Configuration - http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html

An administrator must also have access to the certificate store on the agent and supervisor client PCs.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

As part of Common Criteria (CC) certification, Cisco Unified Communications Manager added ECDSA certificates in version 11.0. This affects all Voice Operating System (VOS) products such as UCCX, SocialMiner, MediaSense, etc from version 11.5.

More details about the **Elliptic Curve Digital Signature Algorithm** can be found here: https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767

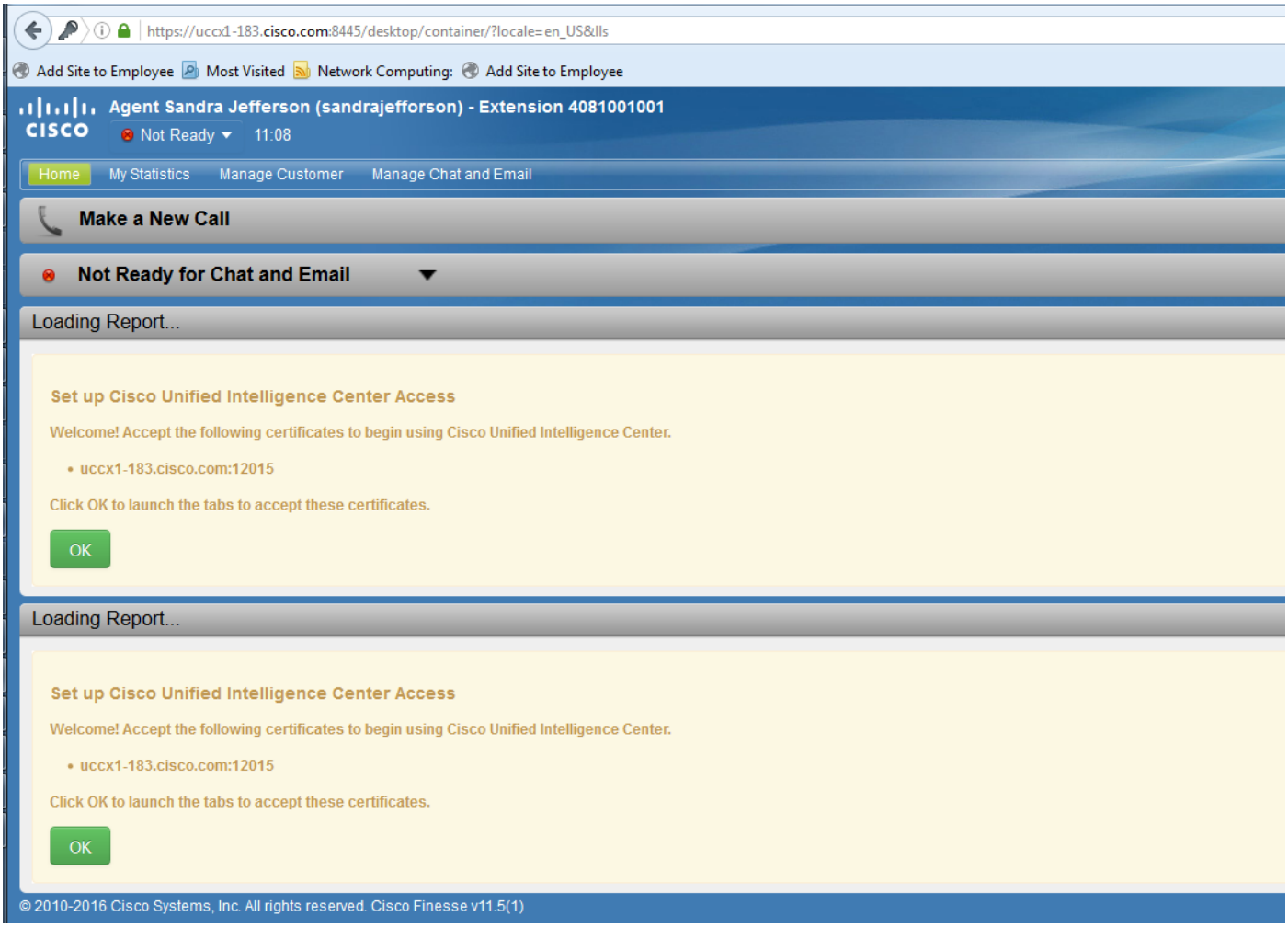
With respect to the UCCX solution, when you upgrade to 11.5, you are offered an additional certificate which was not present earlier. This is the Tomcat-ECDSA certificate.

This has also been documented in the pre-release communication: https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200651-UCCX-Version-11-5-Prerelease-Field-Commu.html?cachemode=refresh

Agent Experience

After an upgrade to 11.5, the agent might be asked to accept certificates on the Finesse desktop based on whether the certificate is self-signed or Certificate Authority (CA) signed.

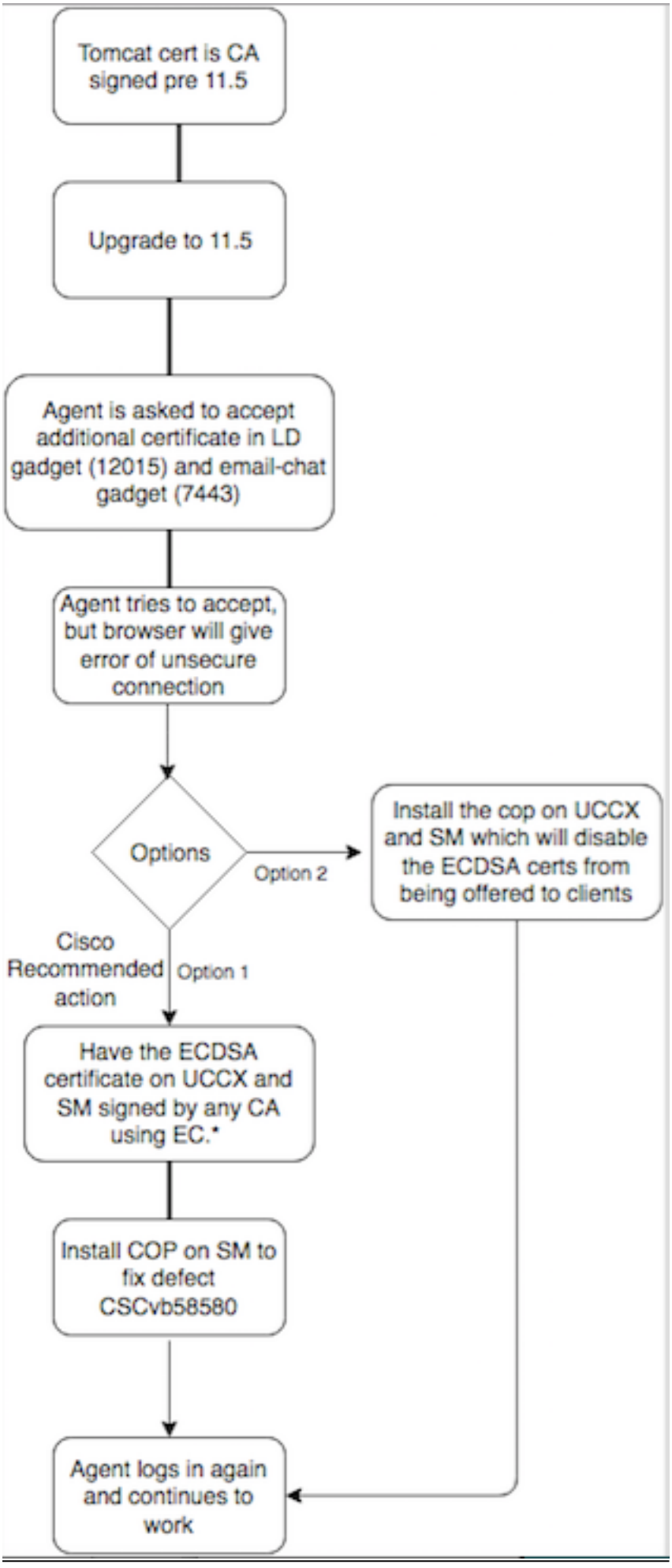
User experience post upgrade to 11.5



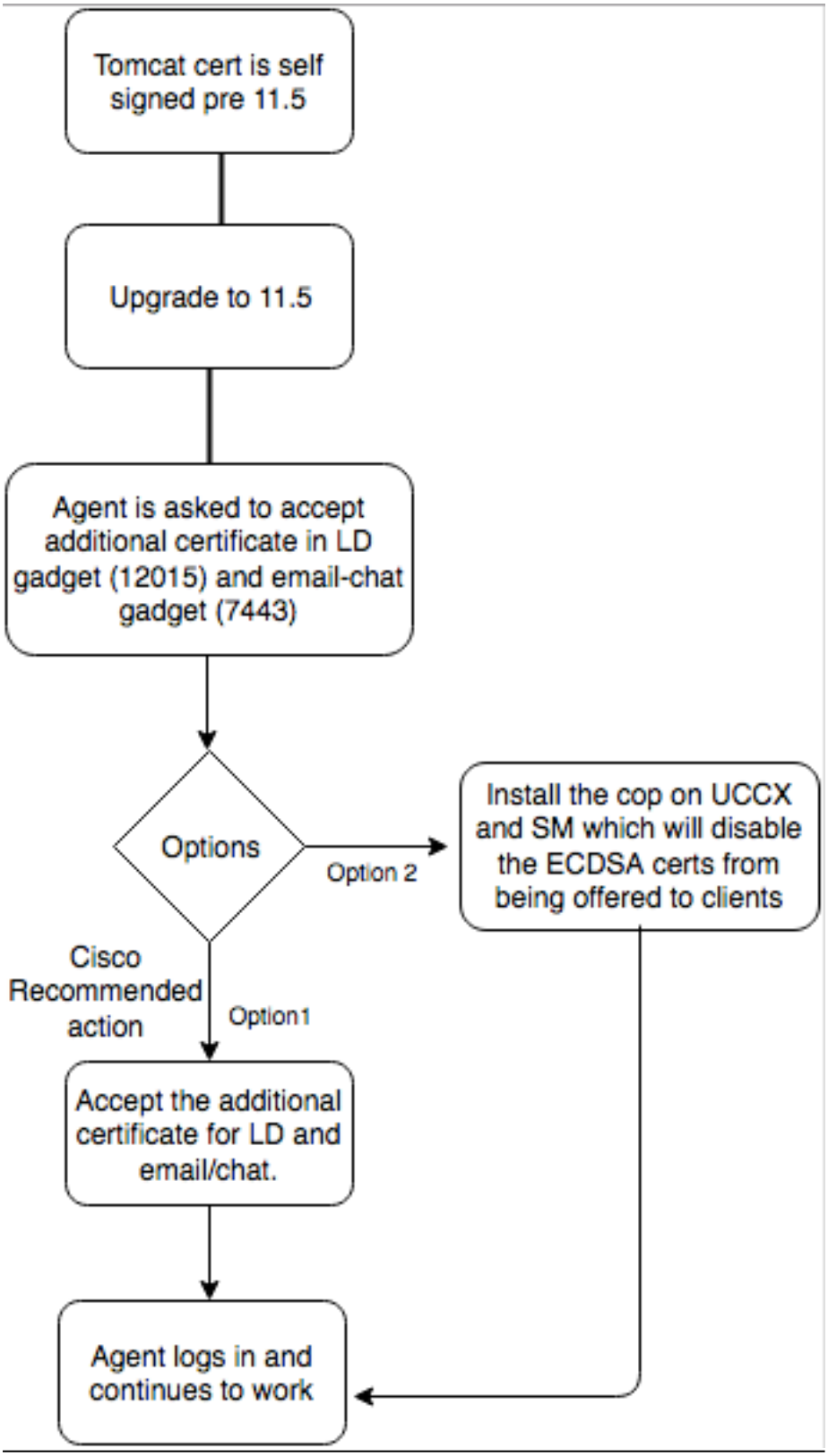
This is because the Finesse desktop is now offered an ECDSA certificate which was not offered earlier.

Procedure

CA signed certificates pre-upgrade


Tomcat cert is CA signed pre 11.5
Upgrade to 11.5
Agent is asked to accept additional certificate in LD gadget (12015) and email-chat gadget (7443)
Agent tries to accept, but browser will give error of unsecure connection
Options
Option 2
Install the cop on UCCX and SM which will disable the ECDSA certs from being offered to clients
Cisco Recommended action
Option 1
Have the ECDSA certificate on UCCX and SM signed by any CA using EC.*
Install COP on SM to fix defect CSCvb58580
Agent logs in again and continues to work

Self-Signed certificates pre-upgrade



Configure

The best practice recommended for this certificate

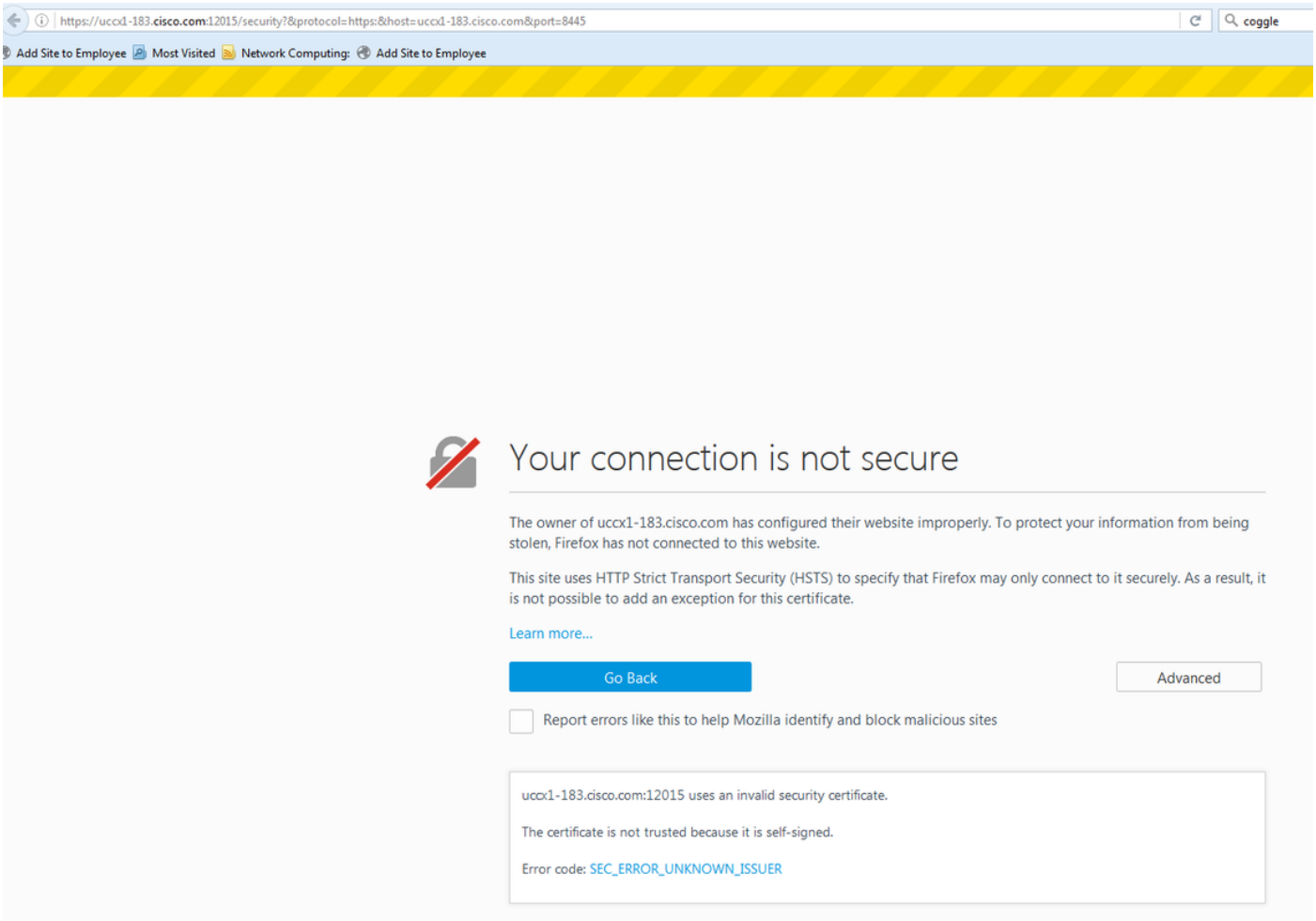
Signed Certificates for UCCX and SocialMiner

If you use CA signed certificates, this ECDSA certificate must be signed by a Certificate Authority (CA) along with other certificates

> **Note**: If CA signs this ECDSA certificate with RSA, this certifictate would not be presented to the client. For enhanced security, the ECDSA certificates offered to the client is the recommended best practice.

> **Note**: If the ECDSA certificate on SocialMiner is signed by a CA with RSA, it causes issues with email and chat. This is documented in defect CSCvb58580 and a cop file is available. This COP ensures that ECDSA certificates are not offered to clients. If you have a CA that is capable to sign ECDSA certificates with RSA only, do not use this certificate.Use the cop so that the ECDSA certificate is not offered and you have an RSA only environment.

If you use CA signed certificates and after upgrade you do not have the ECDSA certificate signed and uploaded, agents experience a message to accept the additional certificate. When they click on **OK,** they are redirected to the website. However, this fail because of security enforcement from the browser side since the ECDSA certificate is self signed and your other web certificates are CA signed. This communication is perceived as a securiry risk.



Complete these steps on each node of UCCX Publisher and Subscriber and SocialMiner, after an upgrade to UCCX and SocialMiner on version 11.5:

1. Navigate to the **OS Administration** page and choose **Security > Certificate Management**.

2. Click **Generate CSR**.

3. From the **Certificate List** drop-down list, choose **tomcat-ECDSA** as the certificate name and click **Generate CSR**.

4. Navigate to **Security > Certificate Management** and choose **Download CSR**.

5. From the pop-up window, choose **tomcat-ECDSA** from the drop-down list and click **Download CSR**.

Send the new CSR to the third-party CA or sign it with an internal CA who signs EC certificates. This would produce these signed certificates:

- Root Certificate for the CA (If you use the same CA for Application Certificates and EC certificates, you can skip this step)
- UCCX Publisher ECDSA Signed Certificate
- UCCX Subscriber ECDSA Signed Certificate
- SocialMiner ECDSA Signed Certificate

Note: If you upload the root and intermediate certificates on a publisher (UCCX), it would automatically be replicated to the subscriber. There is no need to upload the root or intermediate certificates onto the other, non-publisher servers in the configuration if all of the application certificates are signed via the same certificate chain. Also you can skip this upload of root certificate if the same CA signs the EC certificate and you have already done this when you configured the UCCX application certificates.

Complete these steps on each application server in order to upload the root certificate and EC certificate to the nodes:

1. Navigate to the **OS Administration** page and choose **Security > Certificate Management**.

2. Click **Upload Certificate**.

3. Upload the root certificate and choose **tomcat-trust** as the certificate type.

4. Click **Upload File**.

5. Click **Upload Certificate**.

6. Upload the application certificate and choose **tomcat-ECDSA** as the certificate type.

7. Click **Upload File**.

   Note: If a subordinate CA signs the certificate, upload the root certificate of the subordinate CA as the *tomcat-trust* certificate instead of the root certificate. If an intermediate certificate is issued, upload this certificate to the *tomcat-trust* store in addition to the application certificate. Also you can skip this upload of root certificate if the same CA signs the EC certificate and you have already done this when you configured UCCX application certificates.

8. Once complete, restart these applications:

Cisco SocialMinerCisco UCCX Publisher and Subscriber

Self-Signed Certificates for UCCX and SocialMiner

If the UCCX or SocialMiner use self-signed certificates, the agents need to be advised to accept the certificate warning they are offered in the chat-email gadget and Live Data gadgets.

In order to install self-signed certificates on the client machine, use a group policy or package manager, or install them individually in the browser of each agent PC.

For Internet Explorer, install the client-side self-signed certificates into the **Trusted Root Certification Authorities** store.

For Mozilla Firefox, complete these steps:

1. Navigate to **Tools > Options**.
2. Click the **Advanced** tab.
3. Click **View Certificates**.
4. Navigate to the **Servers** tab.
5. Click **Add Exception**.

1. **Note**: You can also add the security exception to install the certificate which is equivalent to the above process. This is a one time configuration on the client.

Frequently Asked Questions (FAQ)

We have CA signed certificates, and want to use ECDSA certificate which needs to be signed by an EC CA. While we wait for the CA signed certificate to be available, we need to have Live Data up. What can I do?

We do not want to sign this additional certificate or have agents accept this additional certificate. What can I do?

Although the recommendation is to have ECDSA certificates be presented to the browsers, there is an option to disable it. You can install a cop file on UCCX and SocialMiner which ensures that only the RSA certificates are presented to the client. The ECDSA certificate still remains in the keystore, but would not be offered to the clients.

If I use this cop to disable ECDSA certificates offered to the clients, can I enable it back?

Yes, there is a rollback cop provided. Once that is applied, you can get this certificate signed and uplaoded to the server(s).

Would all certificates be made ECDSA?

Currently not, but further security updates on the VOS platform in the future.

When do you install the UCCX COP?

- When you use self-signed certificates and do not want agents to accept additional certificates
- When you cannot get additional certificate signed by CA

When do you install the SM COP?

- When you use self-signed certificates and do not want agents to accept additional certificates
- When you cannot get additional certificate signed by CA
- When you have a CA which is capable to sign ECDSA certificates with RSA only

What are the certificates that are offered by different web server instances by default?

Certificate combination/Web server	Default Agent Experience after upgrade to 11.5 (without any cop)	UCCX Tomcat	UCCX Openfire (Cisco Unified CCX Notification Service)	UCCX SocketIO	SocialMiner Tomcat	SocialMiner Openfire
Self signed Tomcat, Self signed Tomcat-ECDSA	Agents would be asked to accept certificate in Live Data gadget and chat-email gadget	Self-signed	Self-signed	Self-signed	Self-signed	Self-signed
RSA CA signed Tomcat, RSA CA signed Tomcat-ECDSA	Agents can use Finesse and Live Data, but email-chat gadget won't load and SocialMiner webpage does not load.*	RSA	RSA	RSA	RSA	RSA (Need to install cop - CSCvb58580)
RSA CA signed Tomcat, EC CA signed Tomcat-ECDSA	Agents can use Finesse with both Live Data and chat-email*	RSA	RSA	ECDSA	RSA	ECDSA

RSA CA signed Tomcat, self signed Tomcat-ECDSA	Agents would be asked to accept additional certificate in Live Data and email-chat gadget. Accept certificate from Live Data gadget fails, accept certificate from email-chat gadget would be successful.*	RSA	RSA	Self-signed (Agents cannot accept due to browser enforced security measure. Refer to screenshot above. You must get the certificate signed by an EC CA or install the cop on UCCX to disable ECDSA certificates offered to the clients.)	RSA	Self-signed	

Related Information

- UCCX ECDSA COP - https://software.cisco.com/download/release.html?mdfid=286309734&softwareid=280840578&release=11.5(1)&flowid=80822
- SocialMiner ECDSA COP - https://software.cisco.com/download/release.html?mdfid=283613136&flowid=73189&release=11.5(1)&softwareid=283812550&sortparam=
- UCCX Certificate Information - http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html