Generate SHA-256 Self-Signed Certificates for Cisco UCCE Web Services

Contents

Introduction

This document describes a process of generating self-signed certificates using SHA-256 certificate signature algorithm for Cisco Unified Contact Center Enterprise (UCCE) web services like Web Setup or CCE Administration.

Problem

Cisco UCCE has several web services hosted by Microsoft Internet Information Services (IIS) server. Microsoft IIS in UCCE deployment by default is using self-signed certificates with SHA-1 certificate signature algorithm.

SHA-1 algorithm is considered unsecure by most of the browsers, therefore at some point critical tools like CCE Administration used by supervisors for agent reskilling may become unavailable.

Solution

The solution to that problem is to generate SHA-256 certificates for IIS server to use.

> **Warning**: It is recommended to use Certificate Authority signed certificates. So generating self-signed certificates described here should be considered as a temporary workaround to restore the service quickly.

> **Note**: In case ICM Internet Script Editor application is used for remote script management there is a need to use SSL Encryption Utility to generate certificate for it.

Solution for WebSetup and CCE Administration

1. Start Windows PowerShell tool on UCCE server.

2. In PowerShell type the command

```
New-SelfSignedCertificate -DnsName "pgb.allevich.local" -CertStoreLocation
"cert:\LocalMachine\My"
```

Where the parameter after **DnsName** will specify certificate common name (CN). Replace the parameter after DnsName to the correct one for the server. The certificate will be generated with a validity of one year.

> **Note**: Common name in the certificate has to match Fully Qualified Domain Name (FQDN) of the server.

3. Open Microsoft Management Console (MMC) tool. Select **File** -> **Add/Remove Snap-In...** -> select **Certificates**, choose **Computer account** and **add** it to the selected snap-ins. Press ok, then navigate to **Console Root** -> **Certificates (Local Computer)** -> **Personal** -> **Certificates**.

Ensure that the newly created certificate is present here. The certificate will not have friendly name configured, so it can be recognized based on its CN and expiration date.

Friendly name can be assigned to the certificate by selecting the certificate **properties** and filling **Friendly name** textbox with the appropriate name.

4. Start Internet Information Services (IIS) Manager. Select IIS Default Web Site and on the right pane choose **Bindings**. Select **HTTPS** -> **Edit** and from the SSL certificate list select self-signed SHA-256 generated certificate.

5. Restart "World Wide Web Publishing Service" service.

Solution for Diagnostic Framework Portico

1. Repeat the steps 1-3.

A new self-signed certificate will be generated. For Portico tool there is another way of binding the certificate.

2. Remove the current certificate binding for Portico tool.

```
cd c:\icm\serviceability\diagnostics\bin

DiagFwCertMgr /task:UnbindCert
```

3. Bind the self-signed certificate generated for Portico.

Open the self-signed certificate generated for Portico tool and select **Details** tab. Copy the Thumbprint value to the text editor.

> **Note**: In some text editors the thumbprint is automatically prepended with a question mark. Remove it.

Remove all space characters from the thumbprint and use it in the following command.

```
DiagFwCertMgr /task:BindCertFromStore /certhash:<thumbprint-value>
```

4. Ensure that the certificate binding was successful using this command.

```
DiagFwCertMgr /task:ValidateCertBinding
```

Similar message should be displayed in the output.
"The certificate binding is VALID"

5. Restart the Diagnostic Framework service.

```
sc stop "diagfwsvc" sc start "diagfwsvc"
```

Verification

Clear the browser cache and history. Access CCE Administration service web page and you should get a self-signed certificate warning.

View the certificate details and ensure that the certificate has SHA-256 certificate signature algorithm.

Related Articles

Generate CA Signed Certificate for UCCE Diagnostic Portico Tool

Generate CA Signed Certificate for UCCE Web Setup

Generate CA Signed Certificate for VOS Based Server Using CLI

Generate CA Signed Certificate for CVP OAMP Server