Create Umbrella Custom Root Certificate with AD Certificate Services

Contents

Introduction

This document describes instructions for creating a custom root certificate using Microsoft Windows Active Directory (AD) Certificate Services.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- A version of Microsoft Windows Server which is currently supported by Microsoft
- Active Directory Certificate Services installed on the Windows Server
- An account with the Active Directory Certificate Services and Web Service/Web Enrolment Service roles
- Certificate Services configured to issue certificates with UTF-8 encoding ("UTF8STRING")

Components Used

The information in this document is based on Cisco Umbrella.

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.

Overview

This article contains instructions for creating a custom root certificate (which is used in place of the standard Cisco Umbrella Root CA certificate) using Microsoft Windows Active Directory Certificate Services, and then using that root certificate to sign a Certificate Signing Request (CSR) from Umbrella's Customer CA-

signed CA certificate feature.

Certificate String Encoding

If your Certificate Services is configured to use the default encoding ("PRINTABLESTRING") then the certificate chain produced cannot be trusted by certain web clients, most notably Firefox.

The Cisco Umbrella Secure Web Gateway proxy uses a certificate chain which encodes strings with UTF8STRING encoding. If your issuing certificate (for example, your root certificate) which signs the CSR to create the **Cisco Umbrella Customers CA** intermediate certificate is encoded with PRINTABLESTRING, then the encoding of the Cisco Umbrella Customers CA certificate's **Subject** field is PRINTABLESTRING. This encoding cannot match the UTF8STRING encoding of the **Issuer** field in the Cisco Umbrella R1 CA intermediate certificate, which is next in the certificate chain.

RFC 5280 Section 4.1.2.6 requires that a certificate chain maintain the same string encoding between the **Issuer** field of an issued certificate and the **Subject** field in the issuing certificate:

"When the subject of the certificate is a CA, the subject field MUST be encoded in the same way as it is encoded in the issuer field (Section 4.1.2.4) in all certificates issued by the subject CA."

Many browsers do not enforce this requirement, but some (most notably Firefox) do. As a result, web clients such as Firefox can generate an untrusted site error and not load websites when using Secure Web Gateway (SWG) with the Customer CA-signed CA certificate feature.

To work around this issue, use a browser such as Chrome which does not enforce RFC 5280's requirement.

Step 1: Preparing AD Certificate Services Template

1. Open the Active Directory Certification Authority MMC by navigating to **Start > Run > MMC.**

2. Select **File > Add/Remove Snap-in** and add the **Certificate Templates** and **Certification Authority** snap-ins. Select **OK**.

3. Expand **Certificate Templates** and right-click on **Subordinate Certification Authority.** Click on **Duplicate Template**.

You can now create a custom certificate template to comply with the requirements listed in the Umbrella documentation.

These are the requirements that are detailed at the time of this article's creation:

- **General** tab
  - Give the template a name which has meaning to you.
  - Set the **Validity Period** for 35 Months (3 years less a month).
  - Set the **Renewal Period** to 20 Days.
- **Extensions** tab
  - Double-click on **Basic Constraints**.
    - Ensure that **Make this extension critical** is selected.
  - Under **Key Usage**:
    - Ensure that **Certificate Signing** & **CRL Signing** are selected.
    - Deselect **Digital Signature**.
    - Ensure **Make this extension critical** is ticked here too.
- Select **Apply** and **OK**

Step 2: Issue the Template

1. Back in the MMC that you set up in step 2 of the previous process, expand the **Certificate Authority** section.

2. In the newly expanded section, right-click on the **Certificate Templates** folder and select **New > Certificate Template to Issue**.

3. In the new window, select the name of the certificate template that you created in the last section and select **OK**.

The CA is now ready to facilitate the request.

Step 3: Downloading and Signing the CSR

1. Log into your **Umbrella Dashboard** (https://dashboard.umbrella.com).

2. Navigate to **Deployments > Configuration > Root Certificate**.

3. Select the **Add (+)** Icon in the corner and name your CA in the new window.

4. Download the **Certificate Signing Request (CSR)**.

5. In a new browser tab, navigate to web services for **Active Directory Certificate Services**. (If you are using local machine, this would be 127.0.0.1/certsrv/ or similar.)

6. In the new page, select **Request a Certificate**.

7. Select **Advanced Certificate Request**.

8. Under **Saved Request,** copy and paste the contents of the CSR that you downloaded in step 4 (you must open it with a text editor).

9. Under **Certificate Template** select the name of the certificate template that you created in the "Preparing AD Certificate Services Template section" and select **Submit**.

10. Be sure to select **Base64 Encoded** and select **Download Certificate** and make note of the .cer file location.

Step 4: Upload the Signed CSR (and Public Root Cert)

1. On your **Umbrella Dashboard**, navigate to **Deployment > Configuration > Root Certificate**.

2. Select the root certificate that you created in Step 3 of the previous section.

3. Select **Upload CA** at the bottom right corner of the line*.

4. Select top **Browse** button (**Certificate Authority (Signed CSR)**).

5. Browse to the location of the .cer file that you created in the previous section and select **Save**.

6. Select **Next** and select the groups of computers/users that you would like the certificate to be used with (instead of the Cisco Root Certificate) and select **Save**.

*You can also upload the CA certificate optionally. This can be retrieved from the web interface of your certification authority server (http://127.0.0.1/certsrv/) and then selecting **Download a CA Certificate, Certificate Chain, or CRL.** Complete the onscreen prompts to "Download the CA certificate" in Base 64.