# How to Extract the Bundle Certificate and Upload on Expressway Server

## Contents

Introduction Prerequisites Requirements Components Used Extract Bundle Certificate and upload on Expressway Server Upload Certificates on Expressway Server

### Introduction

This document describes the process to extract the Bundle certificate and upload on Expressway server.

# Prerequisites

#### Requirements

Cisco recommends that you have knowledge of these topics:

- Expressway Server
- Windows PC

#### **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, make sure that you understand the potential impact of any command.

## Extract Bundle Certificate and upload on Expressway Server

Step 1. Open the **BASE64** and you see a screen as shown in the image. Open the folder under **Logical Store Name**.

🚟 certmgr - [Certificates - Current Us	er]			$\times$
File     Action     View     Help       Image: Constraint of the second seco				
Certificates - Current User	Logical Store Name	CERTIFICATE C	HAIN.P7B	

Step 2. Open the chain and you see all the certificates in the certificate file (One Server certificate and three Root/intermediate certificate).

Issued To 🔺	Issued By	Expiration D	Intended Purpo	Friendly Name	Stat	Certificate T
Telstra AD Objects SHA1 C	Telstra Policy CA1	25/11/2019	<al></al>	<none></none>	R	Subordinate
🛱 Telstra Policy CA1	Telstra Root CA	25/11/2019	< <b>A</b>   >	<none></none>	R	Subordinate
🖼 Telstra Root CA	Telstra Root CA	16/11/2034	<a<b>I&gt;</a<b>	<none></none>	R	
🖏 tghnslev 11 expc. in. telstra. c	Telstra AD Objects SHA1 CA	11/12/2018	Server Authenti	<none></none>	R	Telstra Live

Step 3. Right click on the certificate you want to download, select All tasks > Export.

File Action View Help	ser\C:\USERS\ANMIRON\DESKTOP\/	ASIF\CERTSP\BASE64_HLEXPRES	
← ➡ Ž 🗊 🖻 🗟 [] ☐ Certificates - Current User		Issued By	Expiration Date
C:\USERS\ANMIRON\DESKT(	hlexpressc.hobbylobby.corp	HORRVI ORRV-ENTCA1 Open All Tasks Ope Copy Help	2/25/2018 3/28/2022 en 18 22 ort
Export a certificate	<		4

Step 4. The Certificate Export Wizard window appears.

<text><text><text><text></text></text></text></text>
< Back Next > Cancel

Step 5. Select Next, then Base-64 Encoded X.509 option, then Next.

Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible

Step 6. A new page appears, select **Browse**, then on the window that pops up, enter the file name for the Certificate, then select **Save**.

Certificate Export Wizard	Organize - New folder	i≣ •	0
File to Export Specify the name of the file you want to export File name:	Name Name No ite	Date modified Type Size Drag the cursor around the area want to capture.	
	File name: HEXXPRESSSC-ServerCent		•
<back next=""> Cancel</back>	Hide Folders	Save Cancel	

Step 7. That action returns you to the Browse page with the path under File Name, select Next.

Step 8. Select **Finish** on the next window and a small window will appear with the **The export was successful** message. The certificate is saved at the selected path.

Step 9. You have to repeat this process for each certificate in the chain.

#### **Upload Certificates on Expressway Server**

For the Root/Intermediate Certificates, Navigate to Expressway Web Page > Maintenance > Security Certificate > Trusted CA List > Browse. Now select the Certificate and then Append CA certificate. (This process is for each cert).

tatus Syster	n Configuration Users Maintenance			3	Help or Logo
rusted CA ce	rtificate	You are here	: Maintenance • Sec	curity • Trus	ted CA certifical
Туре	Issuer	Subject	Expiration date	Validity	View
Certificate	O=Temporary CA 51c787dd-d64d-4e58-90ec-f89cfe2eadec, OU=Temporary CA 51c787dd-d64d-4e58-90ec-f89cfe2eadec, CN=Temporary CA 51c787dd-d64d-4e58-90ec- f89cfe2eadec	Matches Issuer	Sep 26 2021	Valid	View (decoded)
Certificate	CN=junaranj-WIN2012AD-DNS-CA-1	Matches Issuer	Jun 22 2036	Valid	View (decoded)
Show all (decoded)	Show all (PEM file) Dolete Select all Unselect all				

In order to upload the server certificate, Navigate on the **Expressway web page > Maintenance** > **Security Certificates > Server Certificates.** 

Status System Configuration Users I	Maintenance	? Help. @ Logout
Server certificate	You are here: Maintenance * Secur	rity · Server certificate
Server certificate data		· · · · · · · · · · · · · · · · · · ·
Server certificate	Show (decoded) Show (PEM file)	
Currently loaded certificate expires on	Dec 20 2018	
Reset to default server certificate		
Certificate signing request (CSR)		
Certificate request	There is no certificate signing request in progress	
Generate CSR		
Upload new certificate		
Select the server private key file	Browse No file selected.	
Select the conver certificate file	Browse Ne file selected	

**Note**: Once you upload the server certificate, a message indicates a restart is required for the change to take effect.