IdenTrust™
part of HID Global

How to Install a Root Chain for Use with GSA ACES Certificates Using Microsoft® Internet Explorer 8 and Later

Before you can use your IdenTrust GSA ACES digital certificate, the Root Certificate Chain must be installed in your browser. This is a simple, two (2) step process:

1. Download the Root Certificate Chain file.
2. Import the Root Certificate Chain file in your browser.

Begin by **printing these instructions.** Then, click the appropriate Root Certificate Chain link for your certificate at the bottom of this page to begin the download process. Follow the instructions to navigate through each window.

Step 1: When you click the link above, the **"File Download"** window appears. Complete the following actions:	
Window Name	**Action**
1. **"File Download"**	1. Click the button for **"Save this file to disk"**. 2. Click **"OK"**.
2. **"Save As"**	1. Click the arrow to the right of the **"Save In:"** box and browse to your **"Windows Desktop"**. 2. Click **"Save"**. (The file will be saved on your Windows Desktop.)
The File Download is complete! Please continue on to **Step 2**.	

Step 2: Start the **"Certificate Import Wizard"** by completing the following:
Action
1. Locate the downloaded file on your Windows desktop. The icon looks like a paper certificate and the file has a **".p7b"** extension, which you can see if you hover over the file. (Please note that you may have to minimize or close other programs to get to the Windows desktop.)
2. Right-click the file.
3. A pop-up menu will appear. Click on **"Install Certificate"**. The **"Certificate Import Wizard"** will appear.

Step 3:	Step through the **"Certificate Import Wizard"** by performing the following:
Window Name	**Action**
1. Welcome to the **"Certificate Import Wizard"**	Click **"Next"**.
2. Certificate Store	1. By default, the button is checked for **"Automatically select the certificate store…"**. Keep the default selection. 2. Click **"Next"**.
3. Completing the **"Certificate Import Wizard"**.	Click **"Finish"**.
4. Root Certificate Store	When prompted **"Do you want to ADD the following certificate to the Root Store?"** Click **"Yes"**. You will receive a message saying **"The import was successful"**.
5. Internet Explorer browser	Open or maximize your browser and continue the application.

For ACES Certificates issued on or before November 6th, 2015:

- **Click here** to install the **ACES (CA X6)** Root Certificate Chain for Internet Explorer.
- **Click here** to install the **ACES SSL CA Certificate (ACES-X6-A4)** Root Certificate Chain.

For ACES Certificates issued on or after November 7th, 2015:

- **Click here** if you desire to use IdenTrust Public Sector Root CA 1 as a trust anchor: **ACES2IDTPub.p7b**.

Practice Note: Government relying applications should use the chain to Federal Common CA. End users needing to access IdenTrust systems for certificate management need to have the chain to IdenTrust Public Sector CA 1 installed. This chain is automatically pushed to end user systems on retrieval of individual ACES certificates.

Warning: To protect the identity of ACES certificate holders, only the certificate holder should be using the digital certificate. Allowing others to use your certificate through sharing your password or private key weakens the security of the system and presents a security danger to the certificate holder. Those certificate holders found to have shared this confidential information will be notified that their certificates can be revoked.