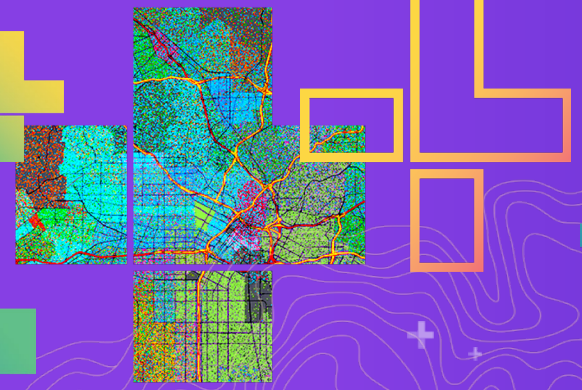
ArcGIS Enterprise and SSL Considerations

Bill Major & Craig Cleveland

2020 ESRI DEVELOPER SUMMIT | Palm Springs, CA



Overview

ArcGIS Enterprise and SSL Considerations

1 – Common SSL Problems

2 – Fundamentals of Secure Communication

3 – Implementing SSL at the Web Tier

4 – Implementing SSL within ArcGIS Enterprise

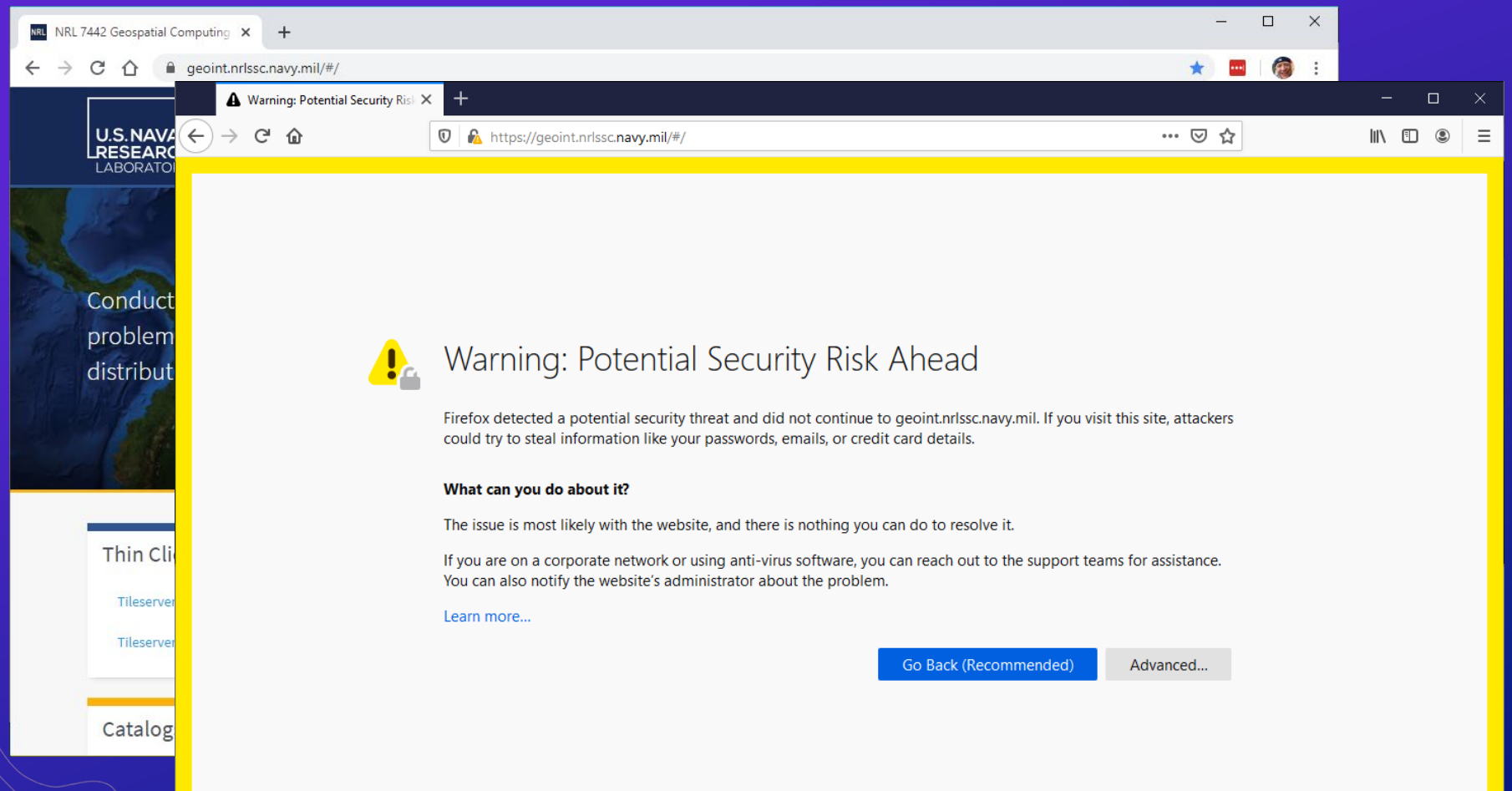
Common SSL Problems

What problems do you regularly see?

Common SSL Problems

Browser issues

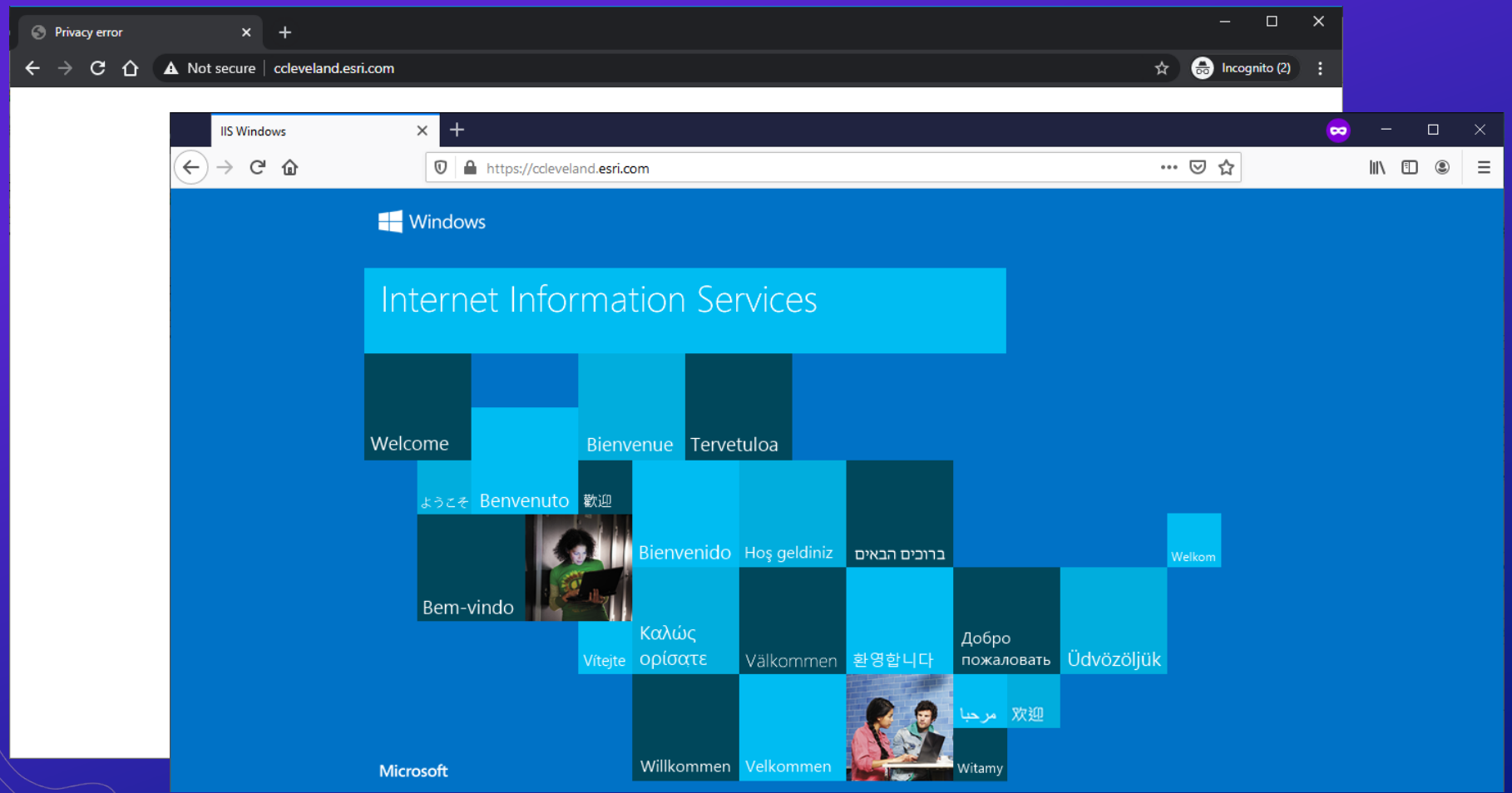
- **Site loads fine in Chrome..but Firefox throws warnings.**



Common SSL Problems

Browser issues

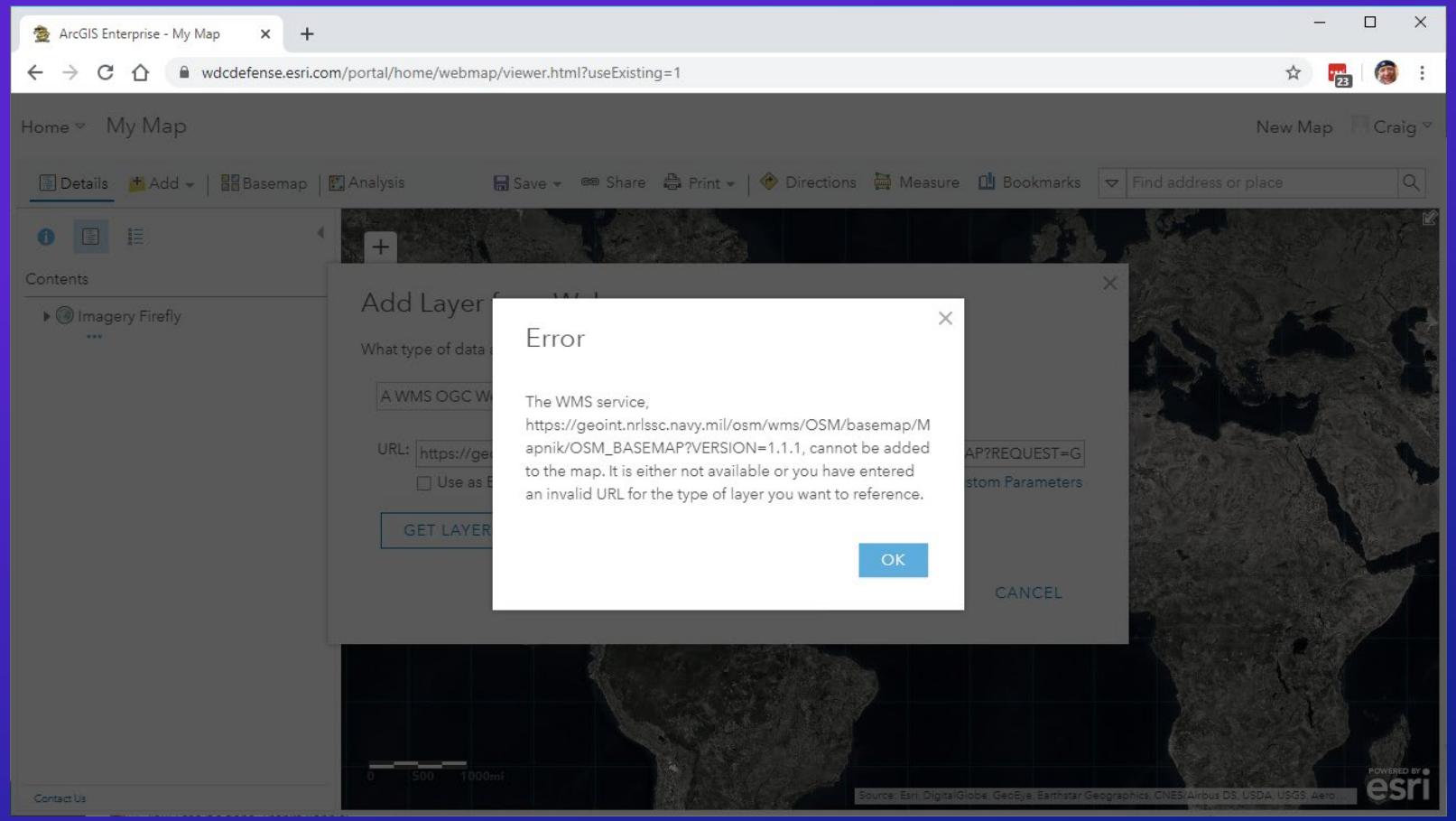
- **Chrome throws warnings..but the site loads fine in Firefox.**



Common SSL Problems

Unable to add layers to Map Viewer

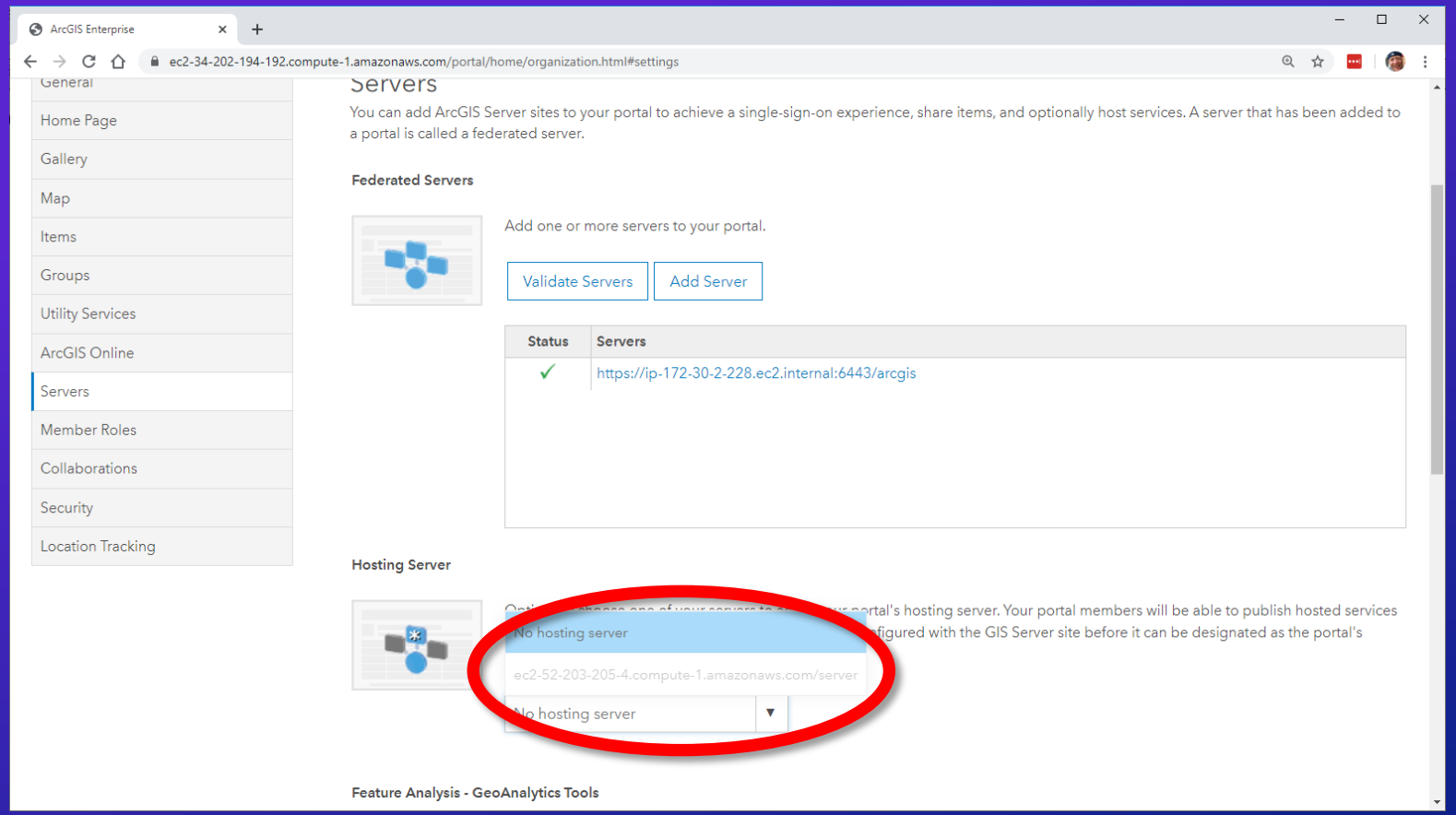
- **Adding a layer to the Map Viewer…errors out.**



Common SSL Problems

Unable to define hosting server

- **Federation goes fine…but unable to define the hosting server.**



Common SSL Problems

Solutions!!!

- **Look for the lock symbol in the upper right hand corner of slides for solutions to these common SSL problems**

Fundamentals of Secure Communication

Encrypted & Trusted Communication

Fundamentals of secure communication

The basics

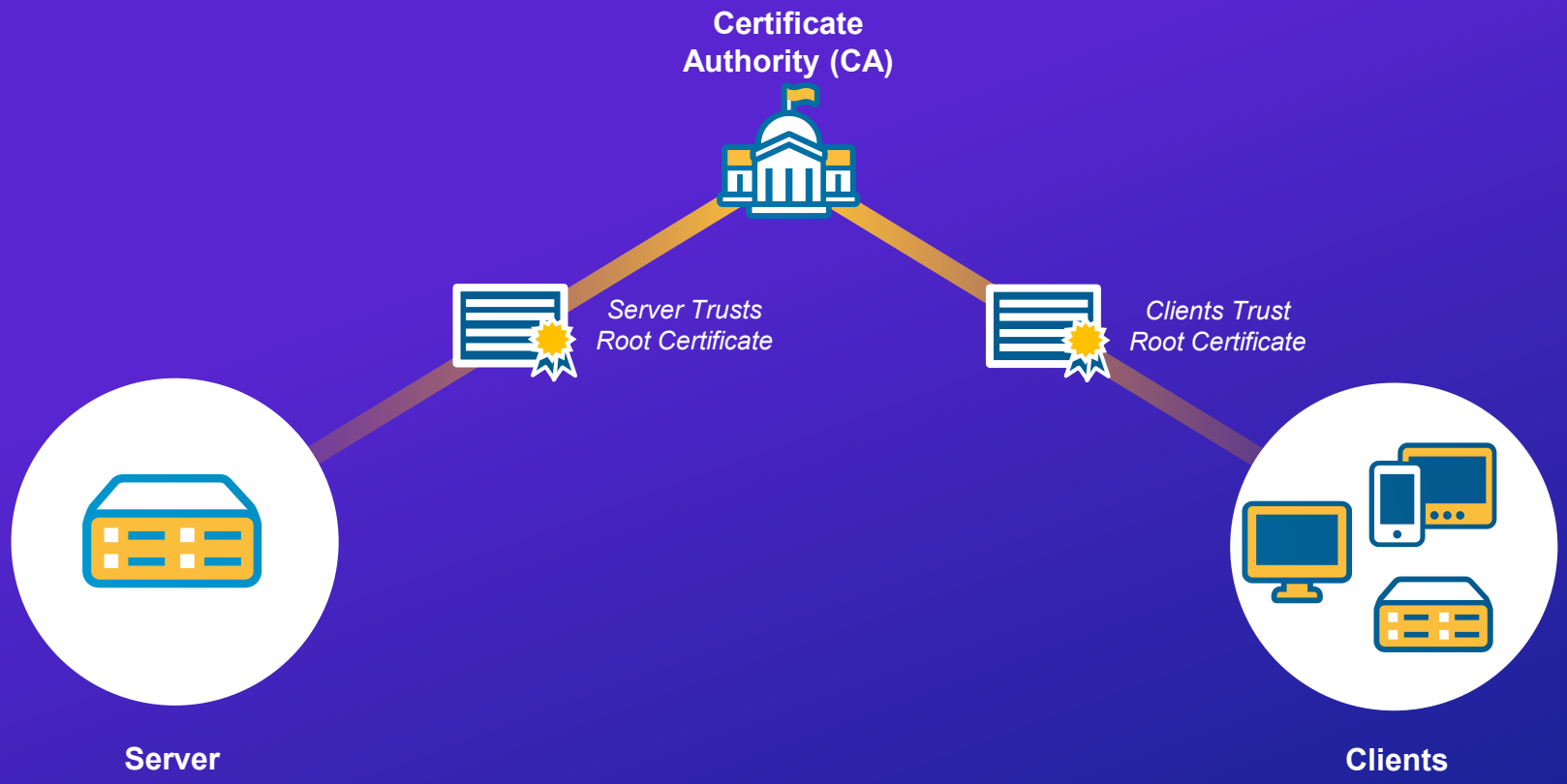
- **Secure Socket Layer (SSL) - standard security technology for establishing an encrypted link between a web server and a browser**
  - **Transport Security Layer (TLS) - v1.2/1.3**

- **Certificate Authorities (CA) establish trust by digitally signing server certificates for server identification and issuing user certificates for client identification (i.e. public key infrastructure).**

- **Public key/private key pairing for encrypted communication**

Fundamentals of secure communication

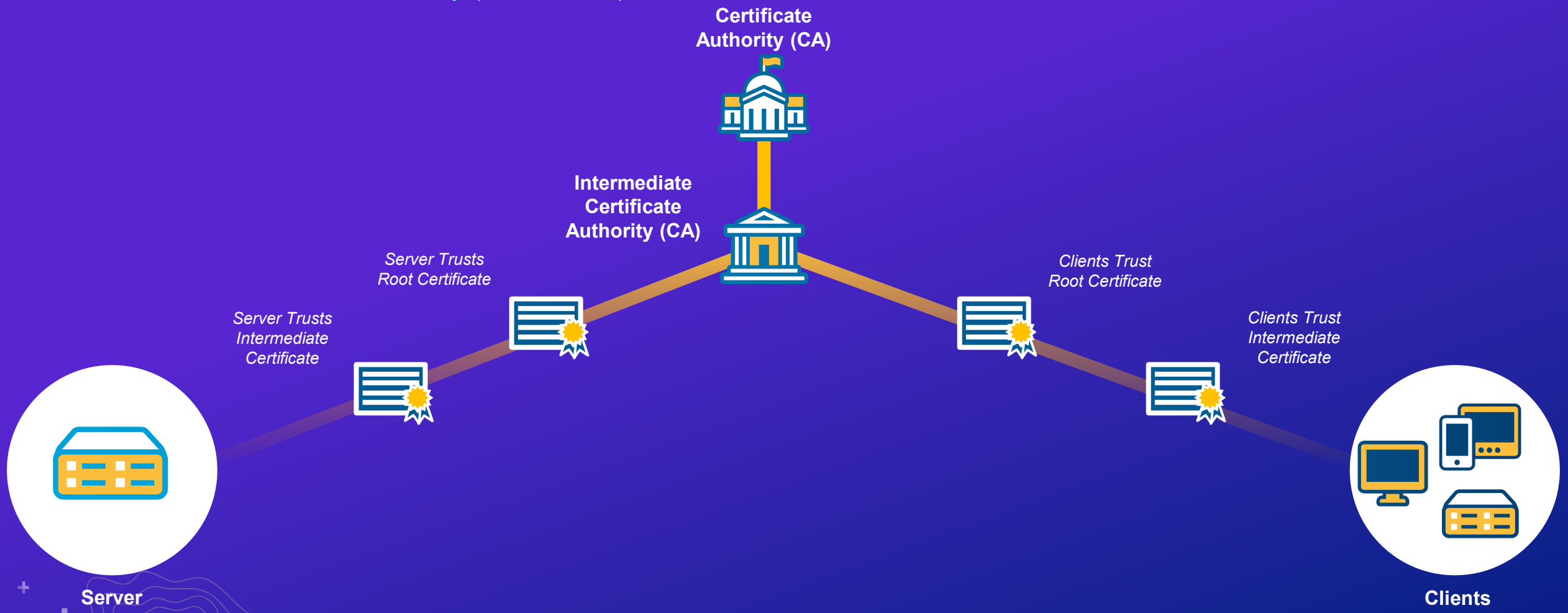
Certificate Authority (Root of Trust)



Trust, Encrypt, Communicate

Fundamentals of secure communication

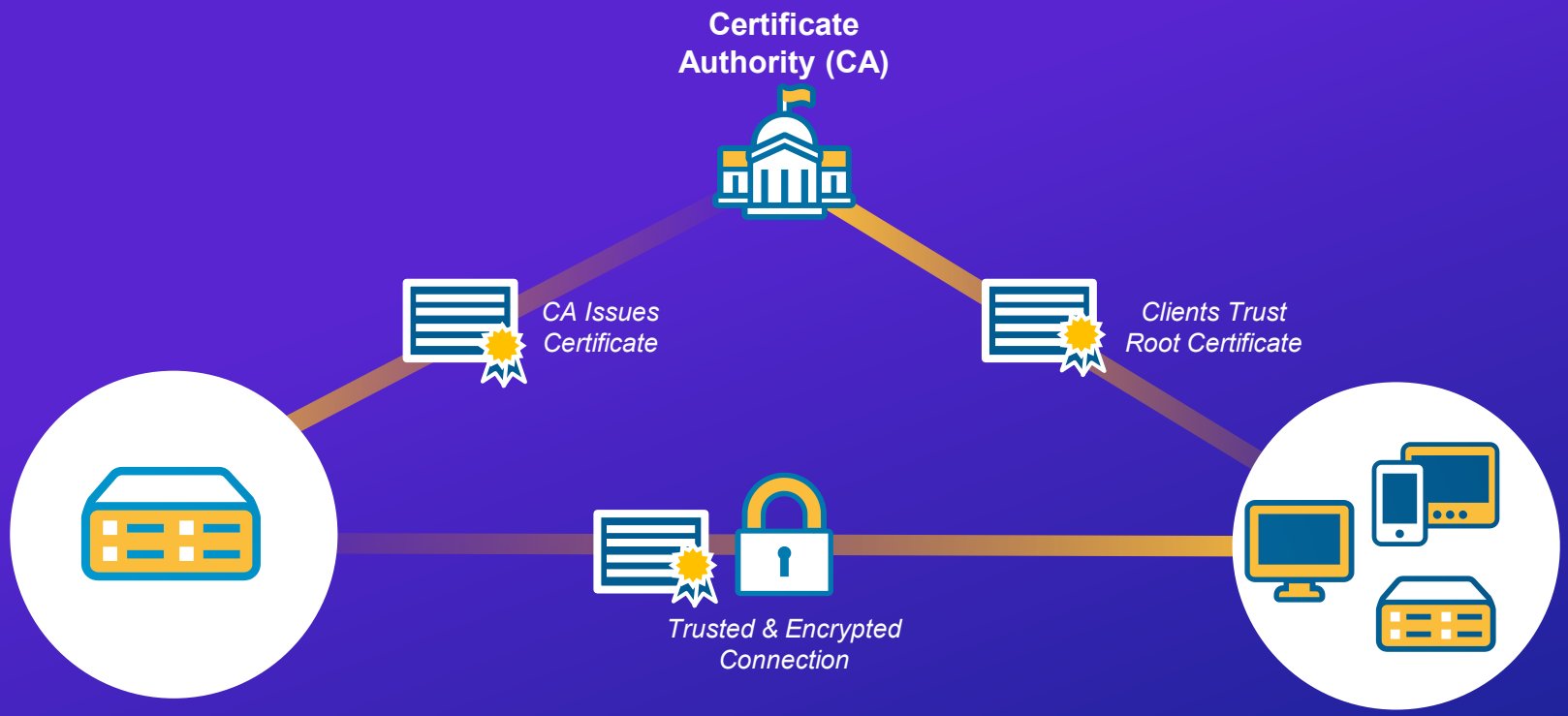
Intermediate Certificate Authority (Trust Chain)



Trust, Encrypt, Communicate

Fundamentals of secure communication

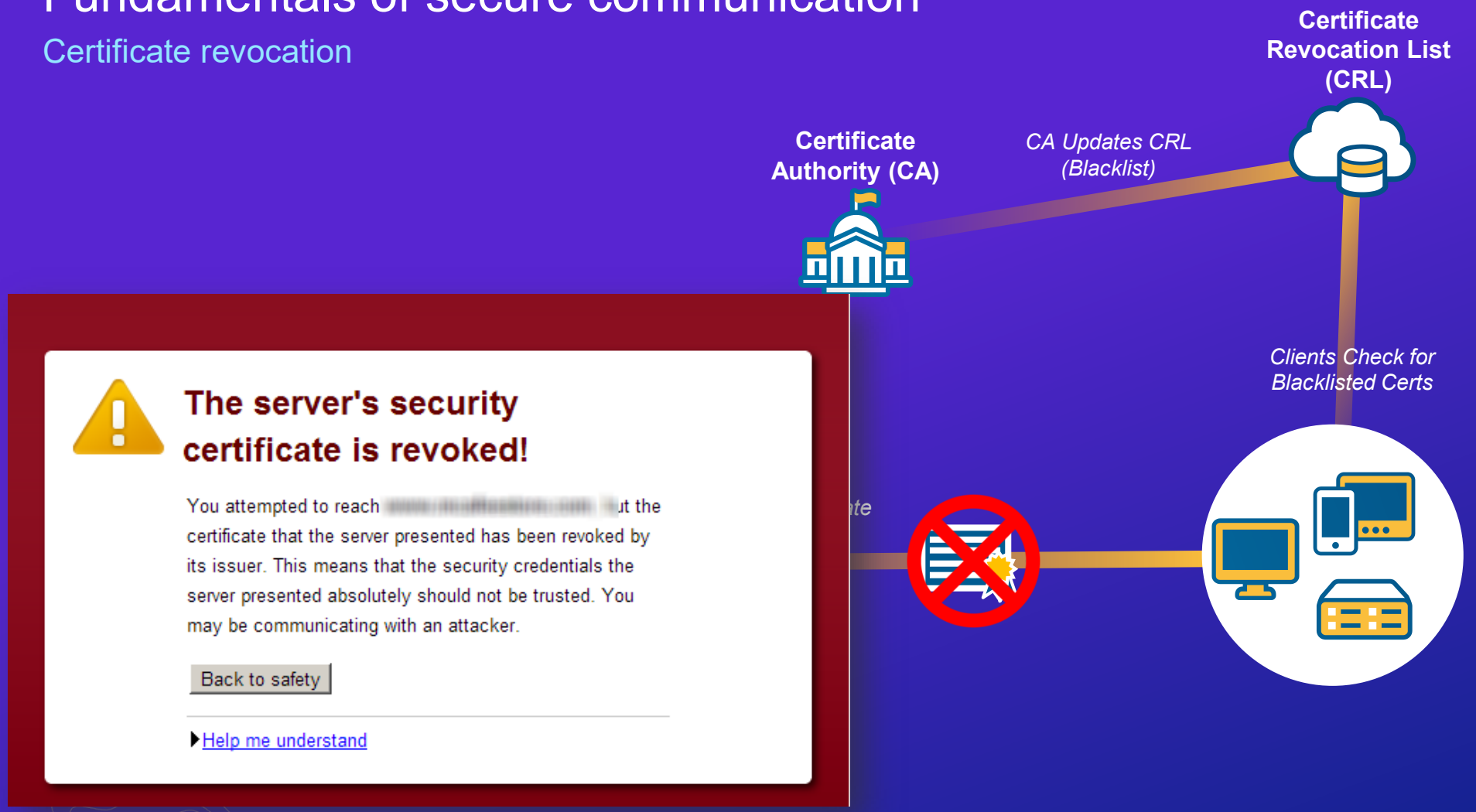
Establishing Trust for Encrypted Communication



Trust, Encrypt, Communicate

Fundamentals of secure communication

Certificate revocation



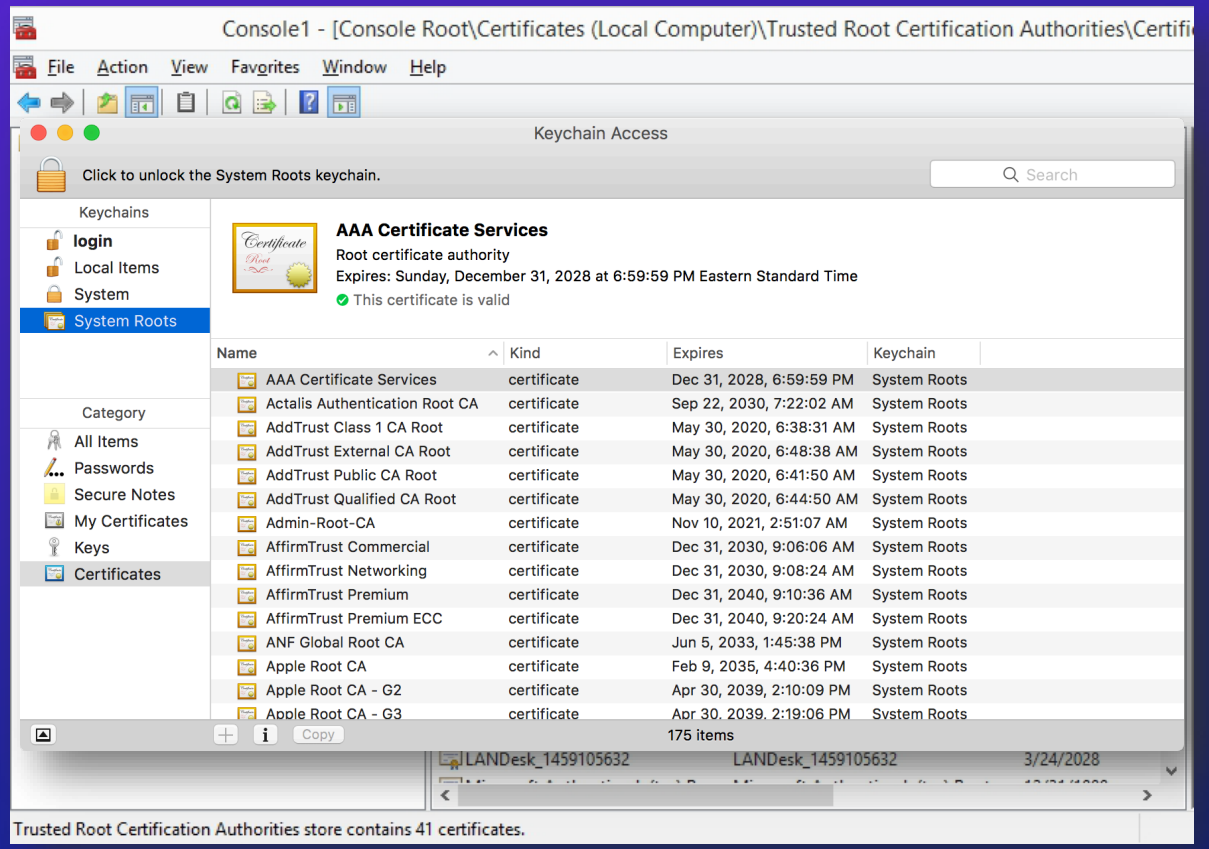
What if a trusted server is compromised?

Fundamentals of secure communication

Trust stores

- **To access the Windows trust store use the Microsoft Management Console**
  - ***Start – MMC – File – Add/Remove Snap-in – Certificates***

- **To access the Mac trust store use Keychain Access**

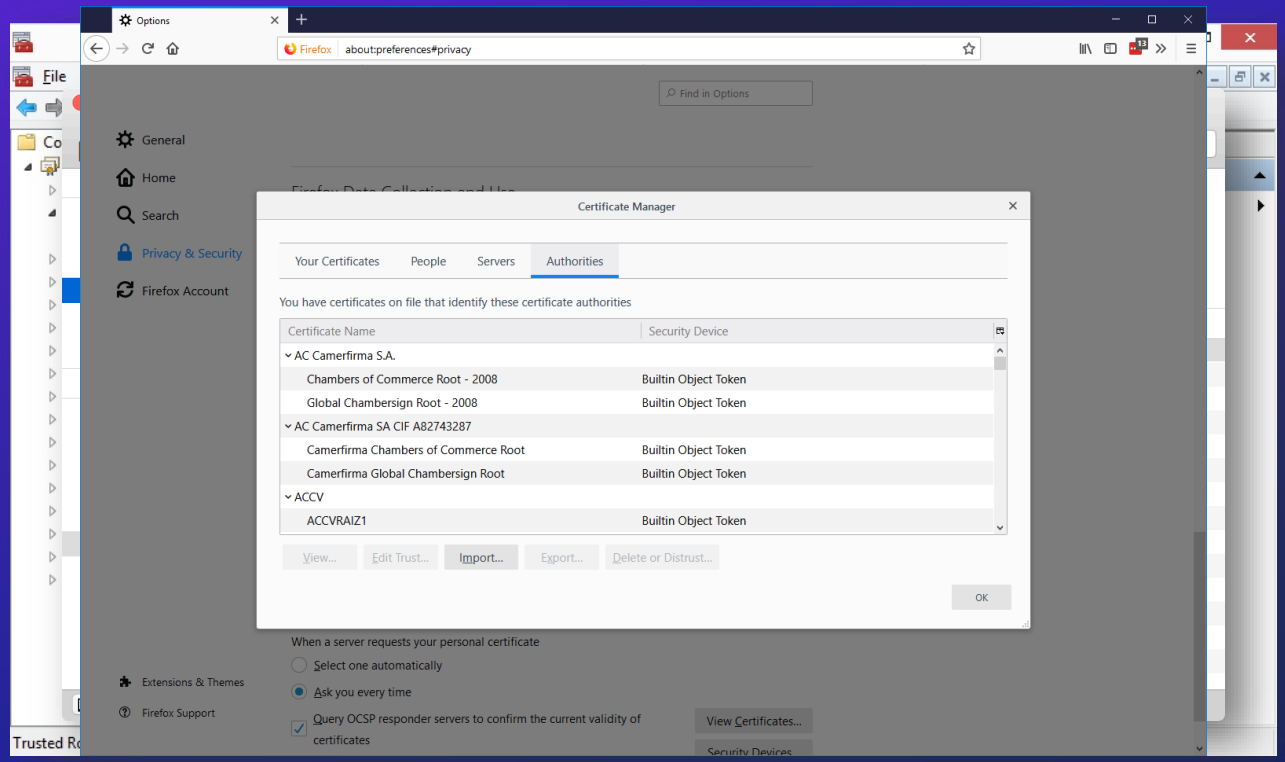


Fundamentals of secure communication

Trust stores and browsers

- **Internet Explorer and Chrome use the Windows trust store**
  - ***Keychain Access for Macs (Chrome Only)***

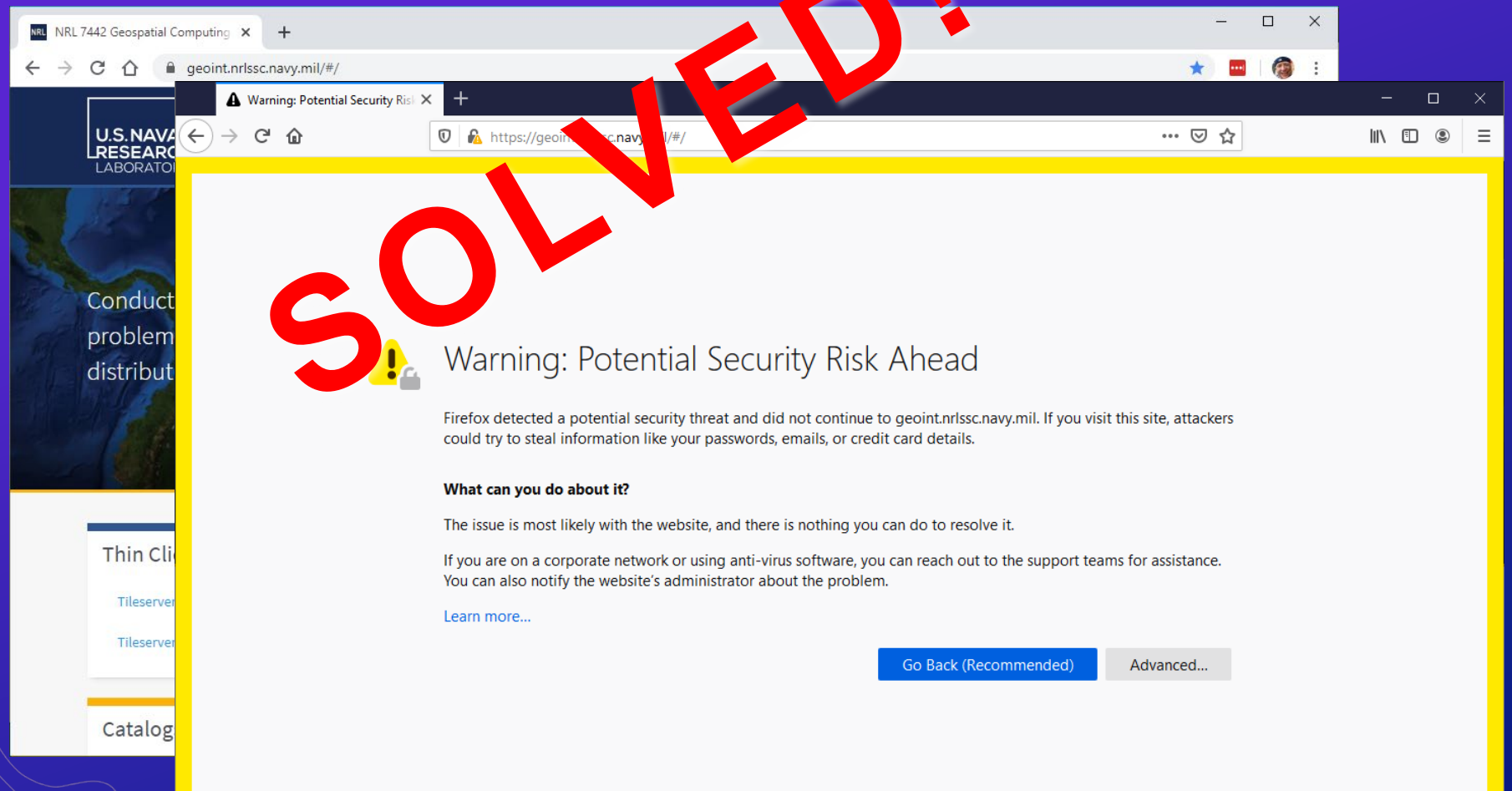
- **Firefox has its own trust store**
  - ***Managed separately!***



Common SSL Problems

Browser issues

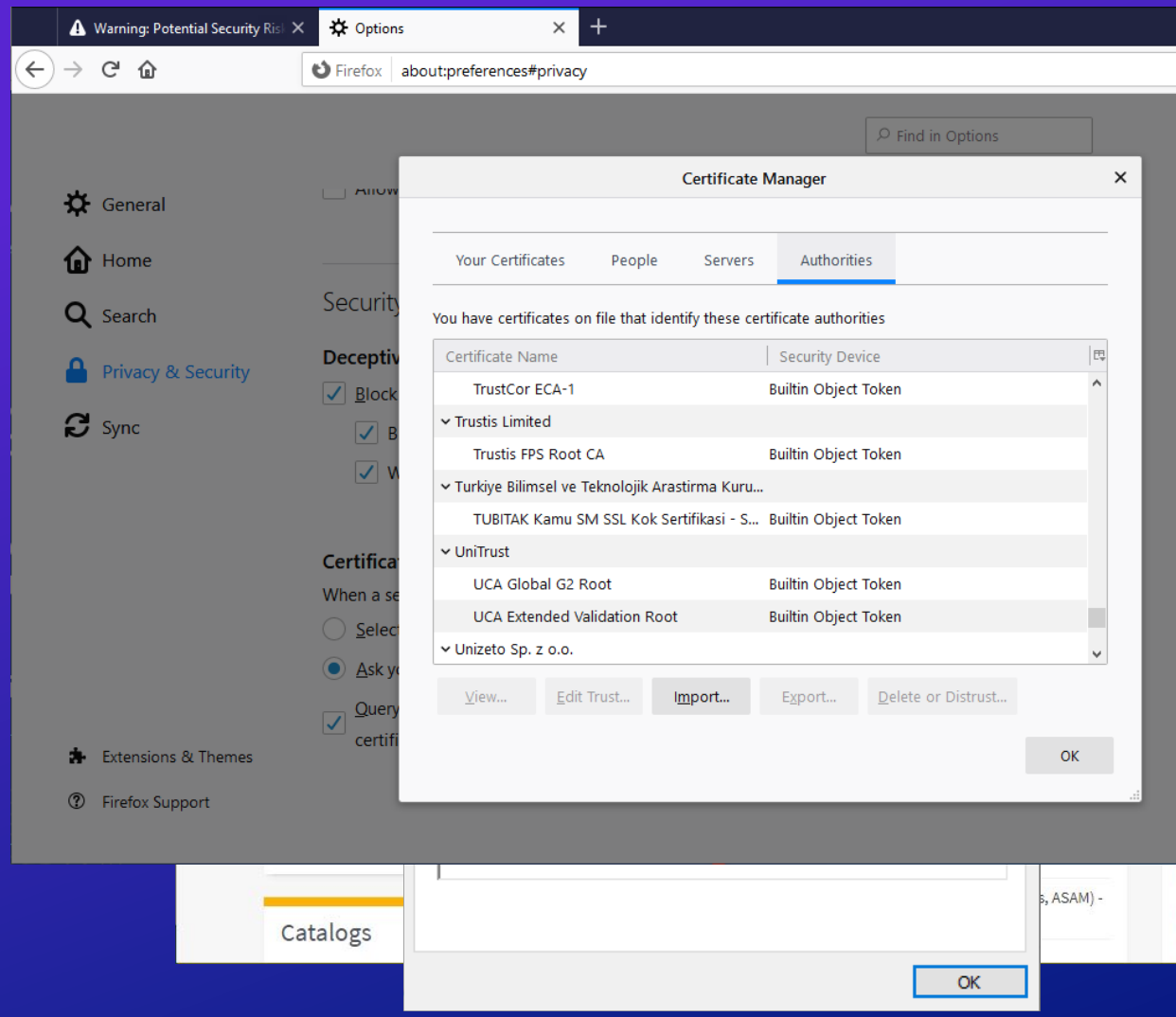
- **Site loads fine in Chrome..but Firefox throws warnings.**

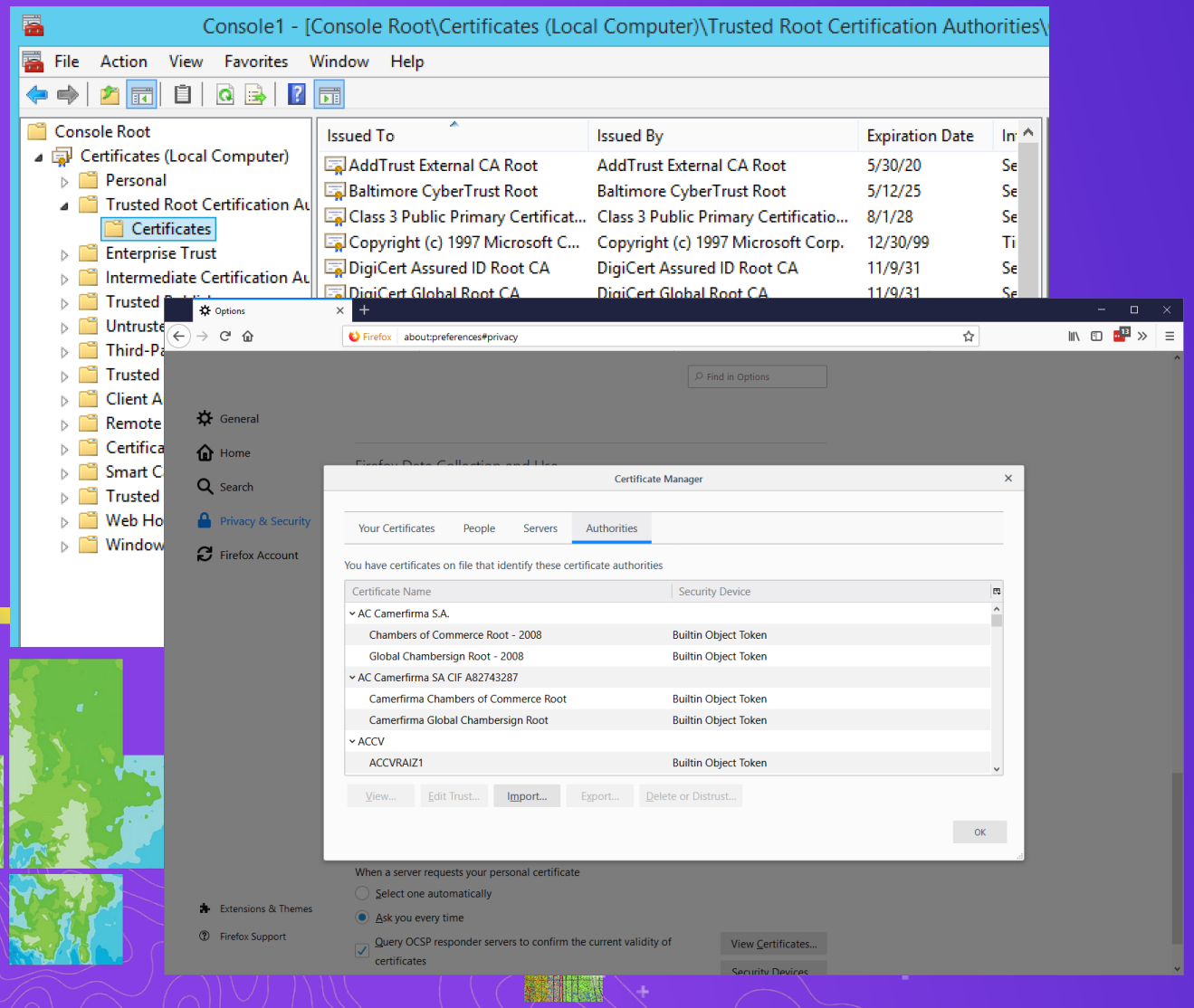


Browser issue – *solved!*

Cause - missing trust chain

- **Firefox uses its own trust store and doesn't always have the same trust chains as your operating system (i.e. what is used by Chrome)**
- **Must import trust chain into Firefox trust store to establish trust**
- **Troubleshooting Tips & Tricks**
  - Works in Chrome (or IE), but not Firefox
  - Inspect the server certificate and its certification path to see if it looks "unique".
    Tip: it's easier to do in Chrome.
  - Export trust chain from Chrome and import into Firefox.





Trust Stores

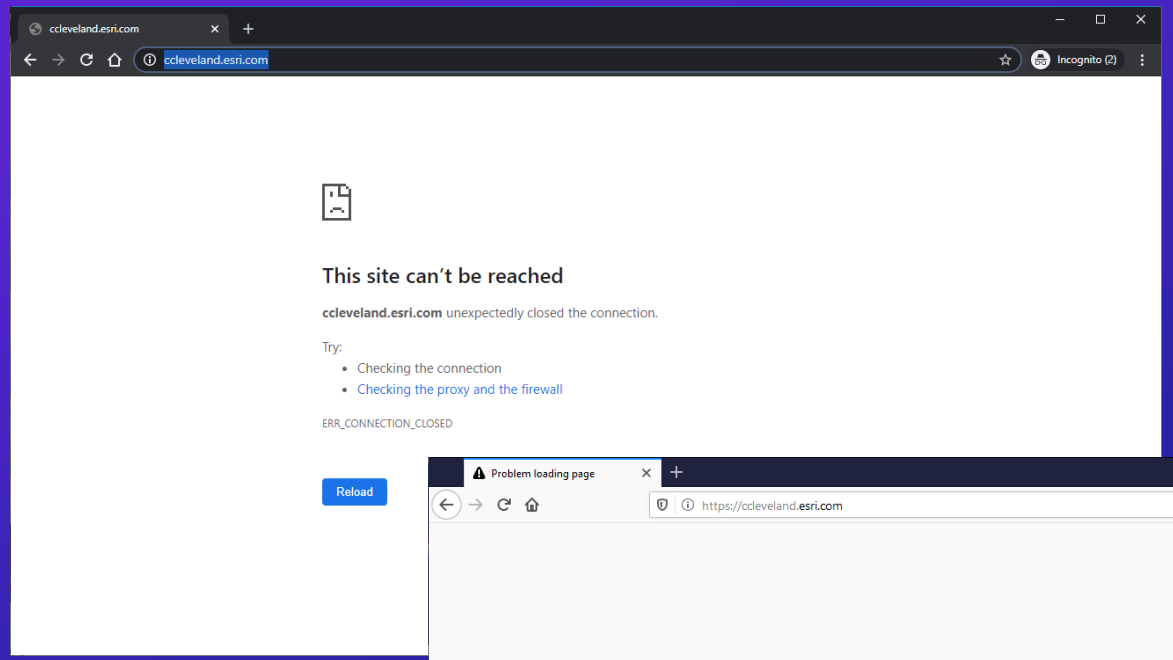
Demonstration

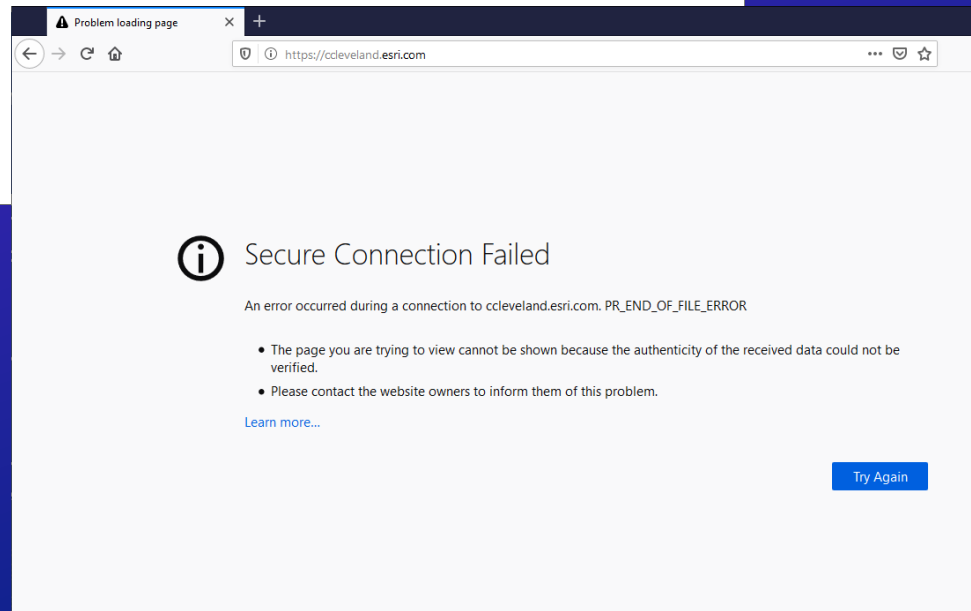
Implementing SSL at the Web Tier

Setting up SSL Certificates and Trusts

Enable HTTPS on your web server

- **Some organizations mandate no HTTP, or no HTTPS without using a properly signed server certificate.**
- **By default your web server only communicates via HTTP**
- **To enable HTTPS obtain a CA signed server certificate and configure your web server to use it**





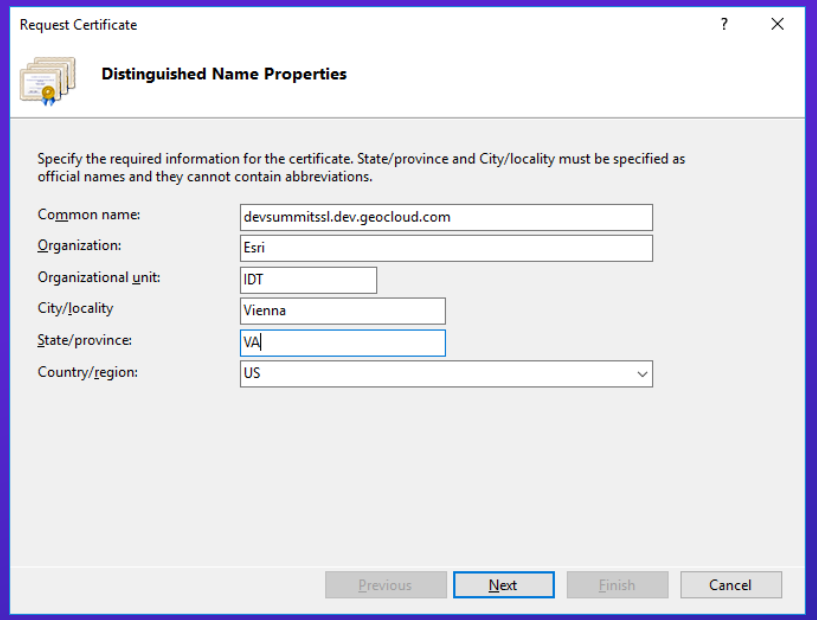
Setting up SSL Certificates and Trusts

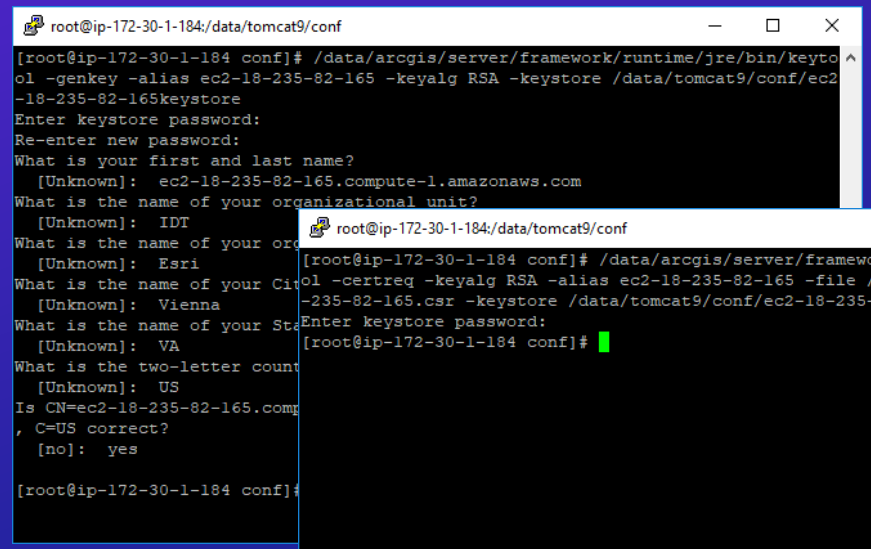
Enable HTTPS on your web server

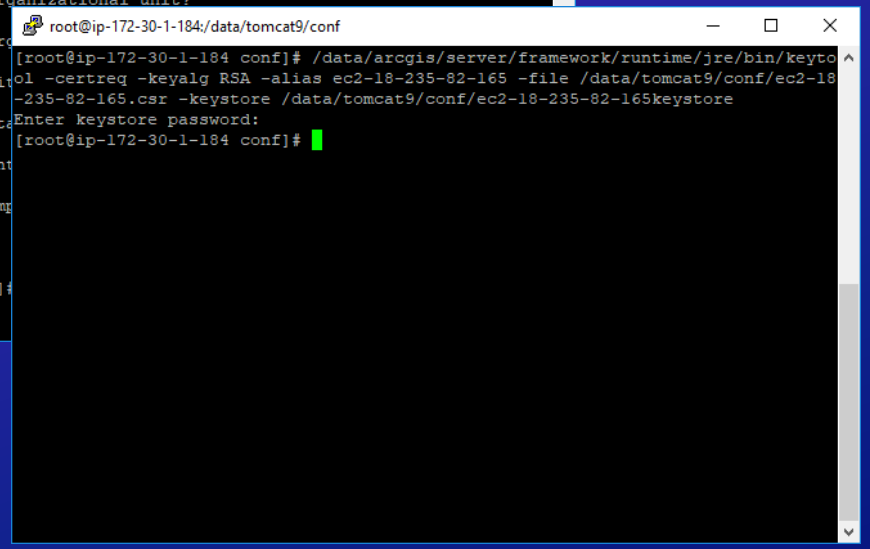
1. **Create certificate signing request (CSR)**

   - *CSR's can be created in many ways – web servers, openssl, keytool, Portal & ArcGIS Server Admin pages*

   - *Note: the Common Name (cn) property of a CSR is the URL by which your web server will be accessed.*





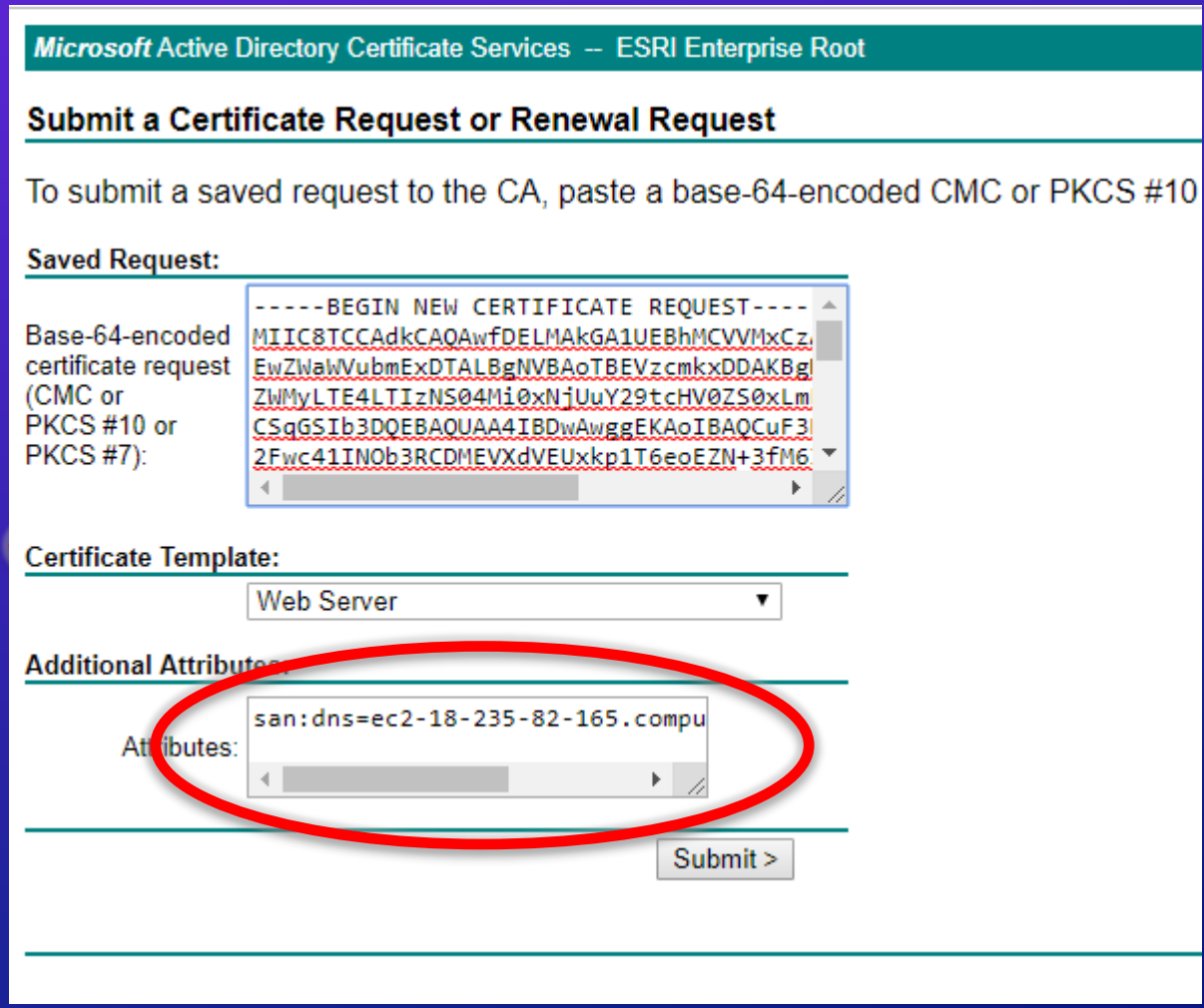


Setting up SSL Certificates and Trusts

Enable HTTPS on your web server

2. **Present CSR to certificate authority (CA)**

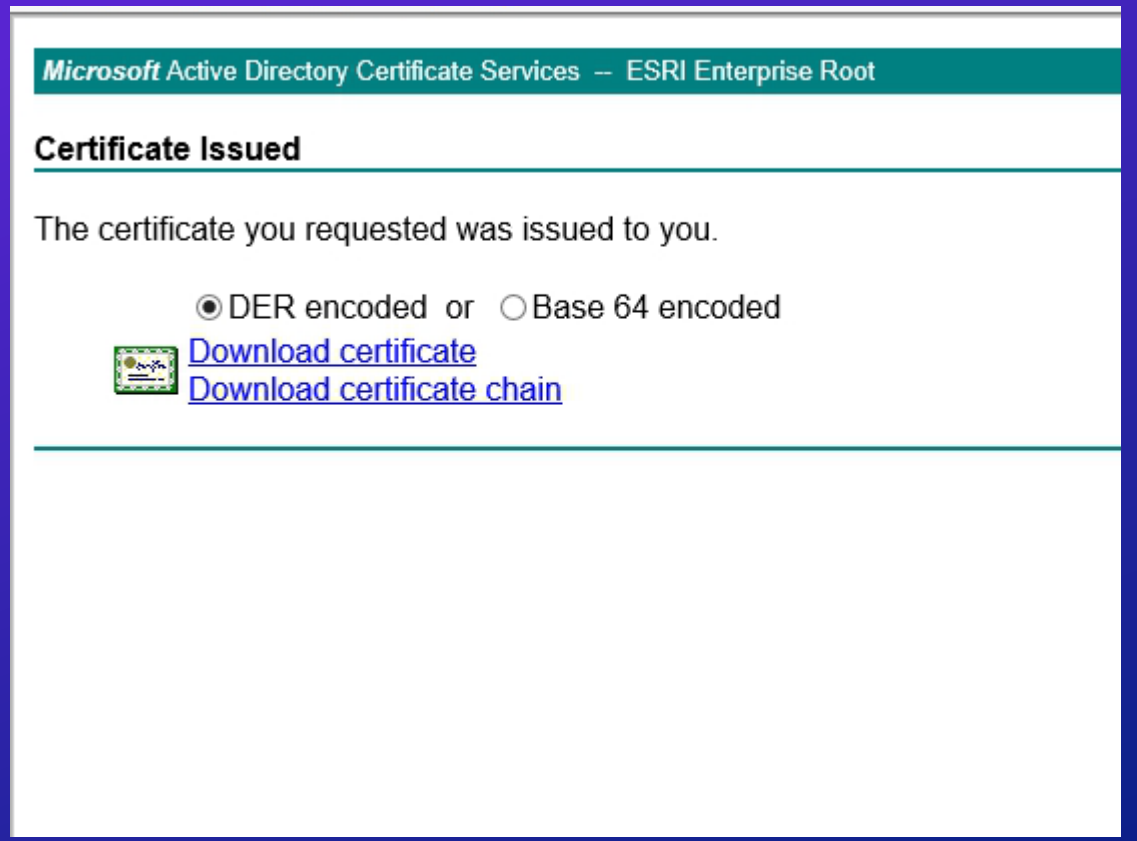
   - *Depending on deployment locale your CA may be public or local (e.g. DigiCert vs. Internal Organization CA)*
   - *Be sure to specify a subject alternative name (SAN) when presenting your CSR to your CA (e.g. san:dns=myserver.esri.com). Now required by most major browsers (e.g. Chrome)!*



Setting up SSL Certificates and Trusts

Enable HTTPS on your web server

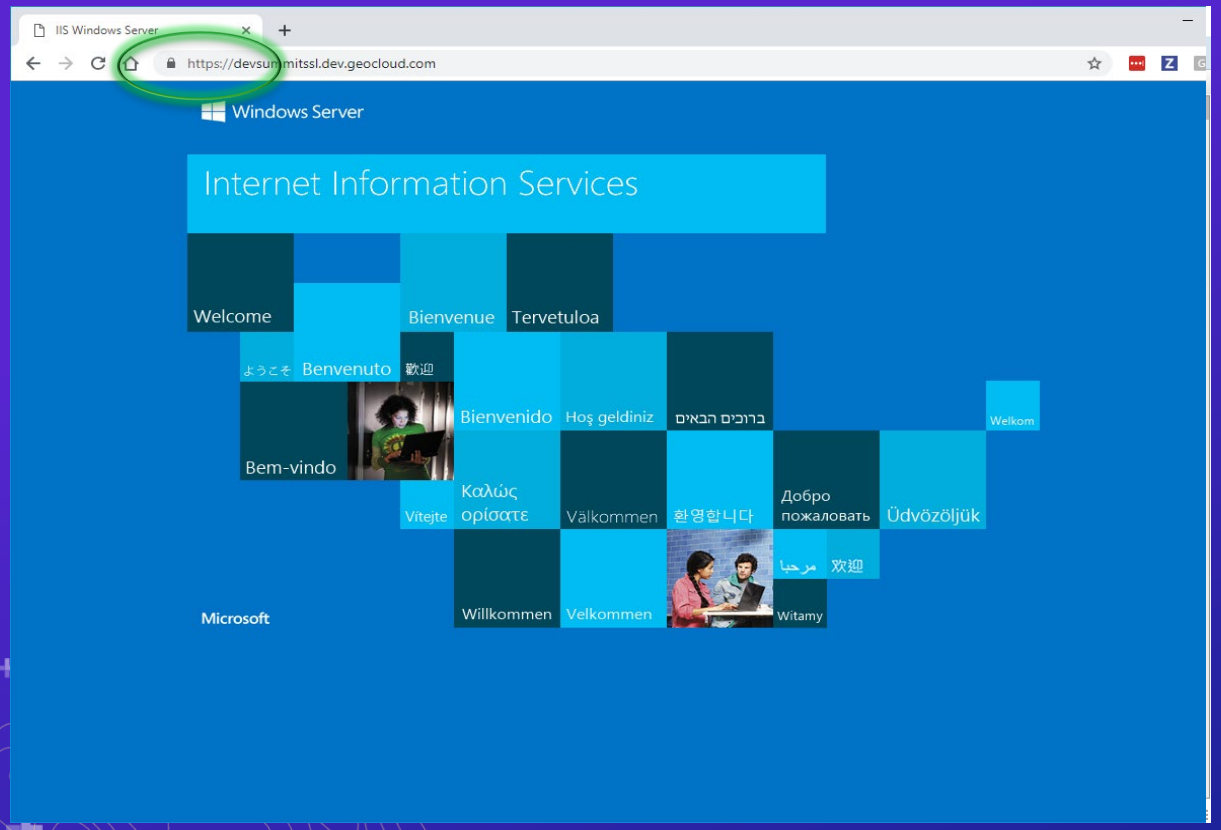
3. **Download signed certificate**

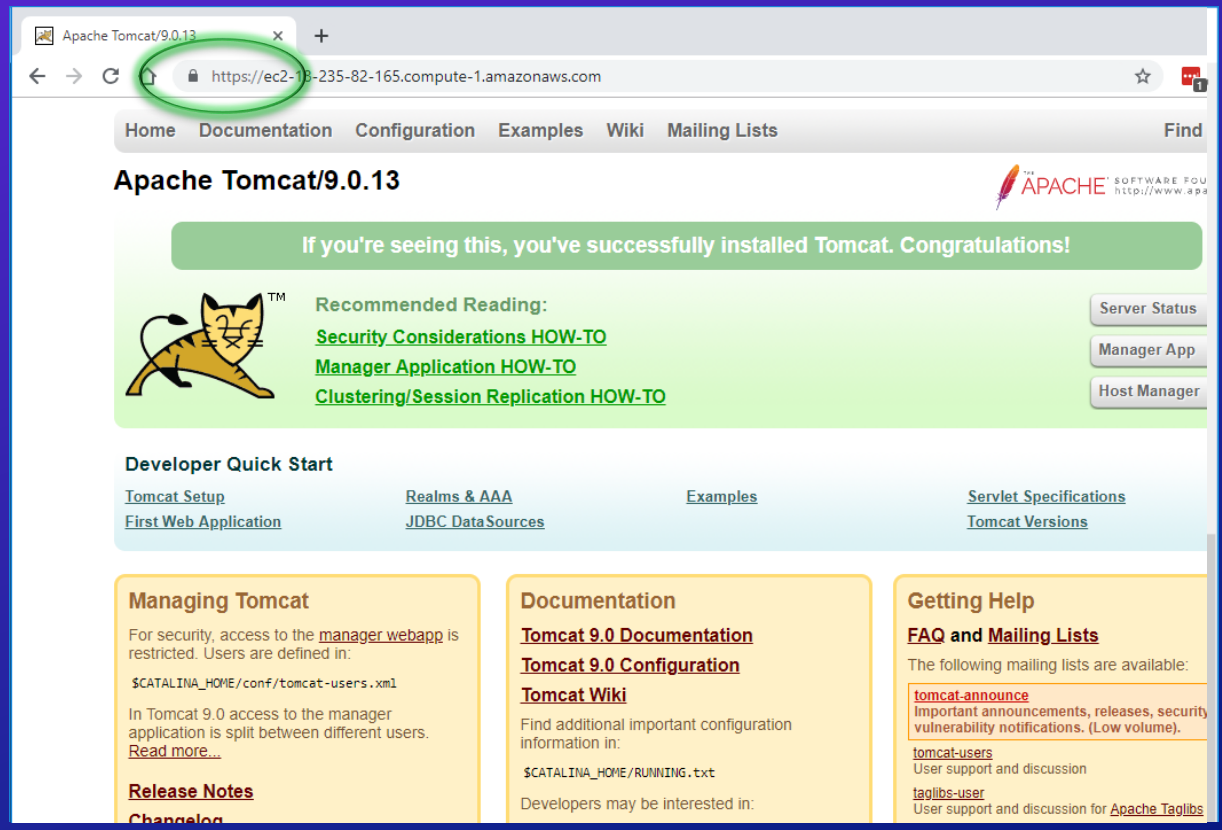


Setting up SSL Certificates and Trusts

Enable HTTPS on your web server

4. Install and configure signed certificate on your web server

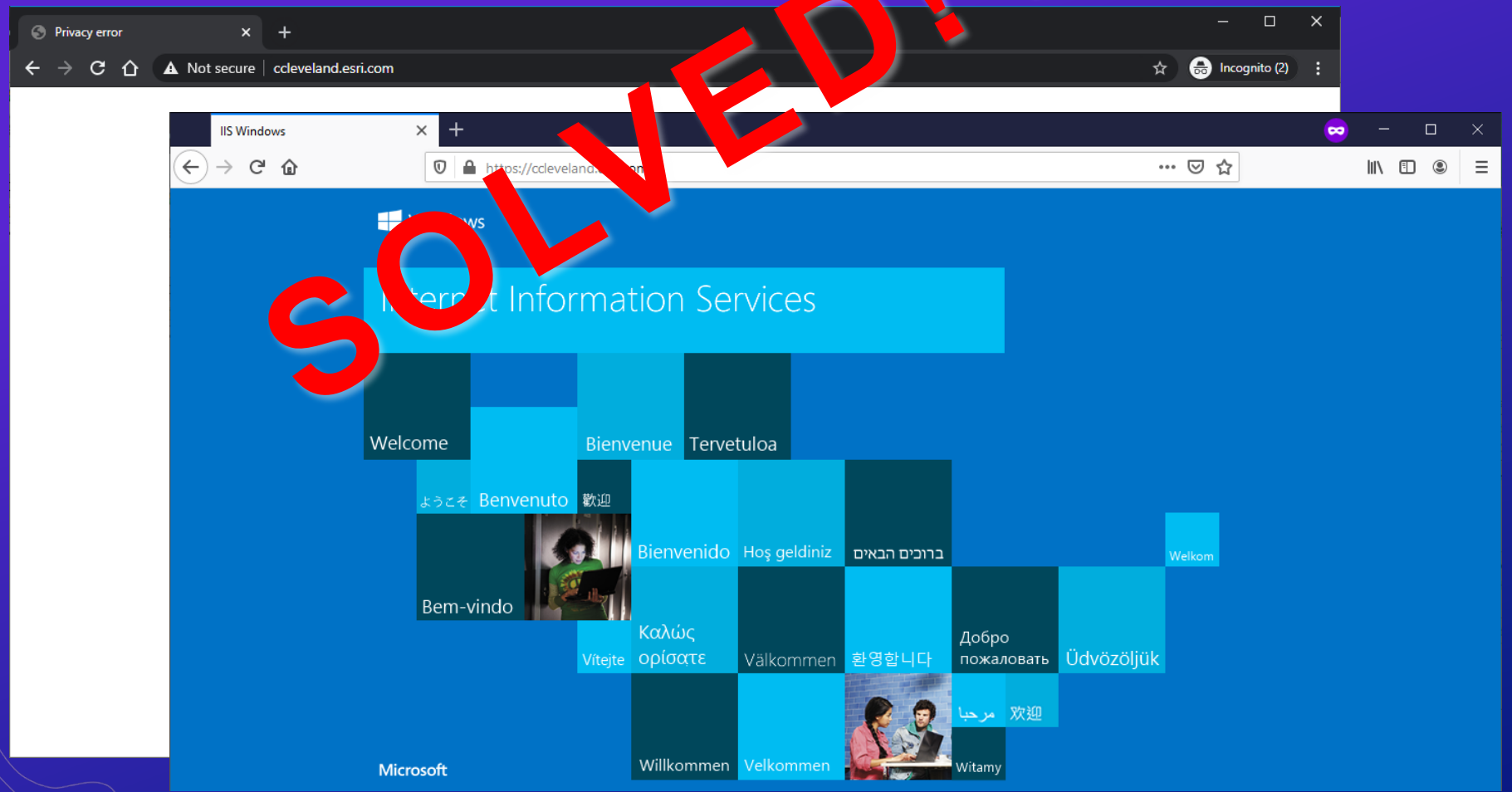




Common SSL Problems

Browser issues

- **Chrome throws warnings..but the site loads fine in Firefox**

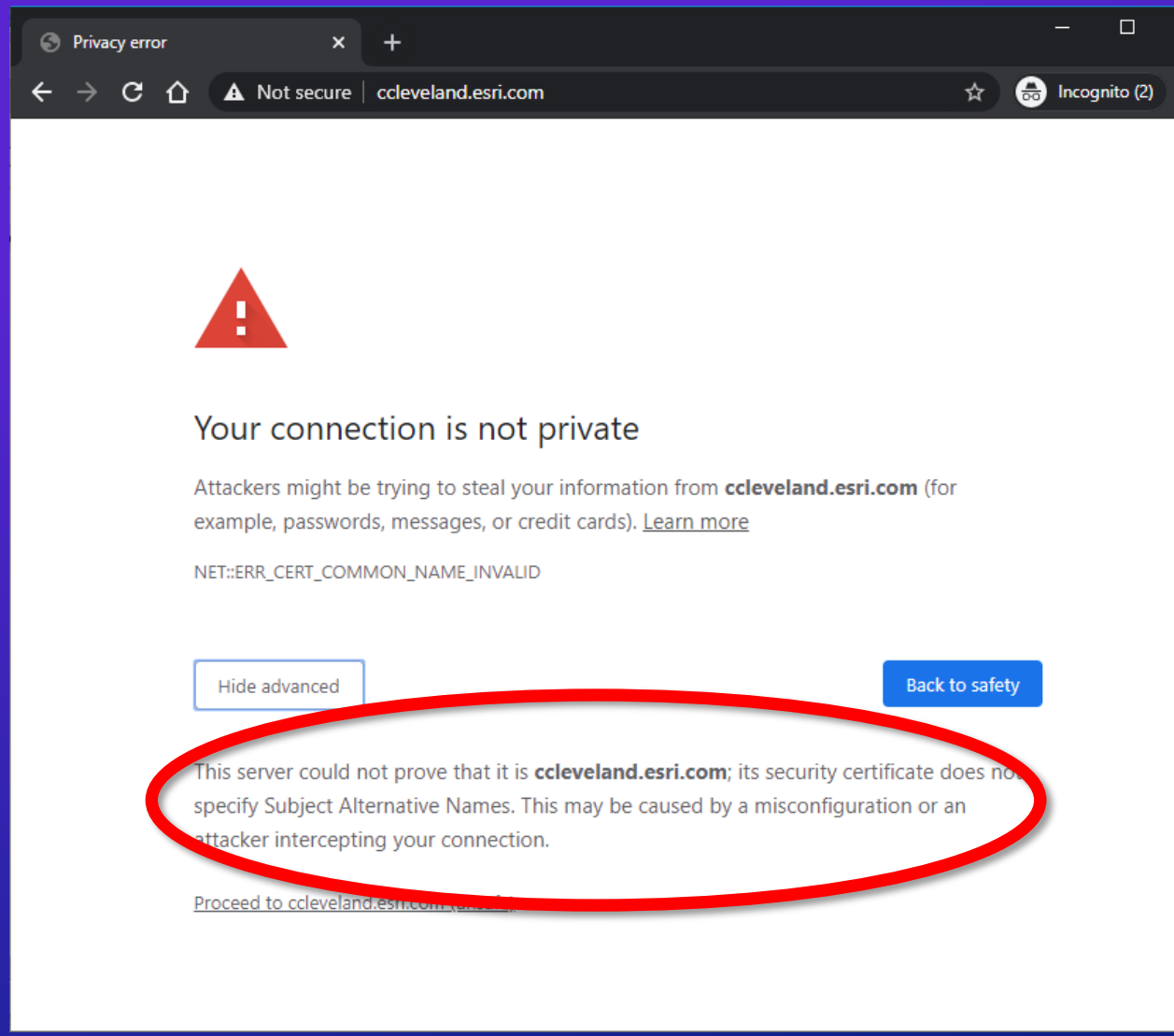


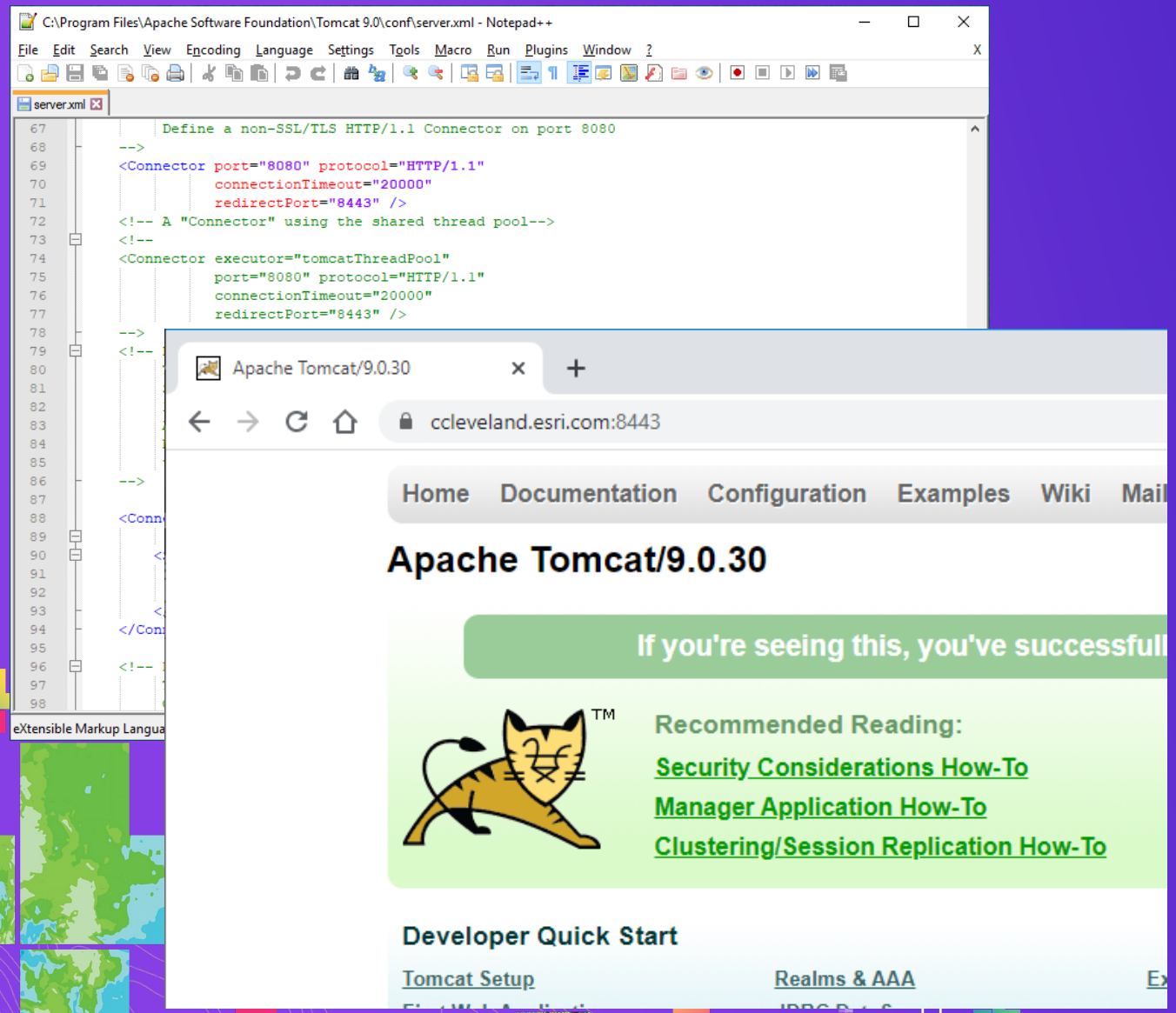
SOLVED!!!

Browser issue – *solved!*

Cause - missing Subject Alternative Name (SAN)

- **Recent releases of Chrome have enforced the need for a subject alternative name (SAN)**
- **Must be included with your CSR**
- **Troubleshooting Tips & Tricks**
  - Expose the “Advanced” options when you receive warnings
  - Works in Firefox (or IE), but not Chrome





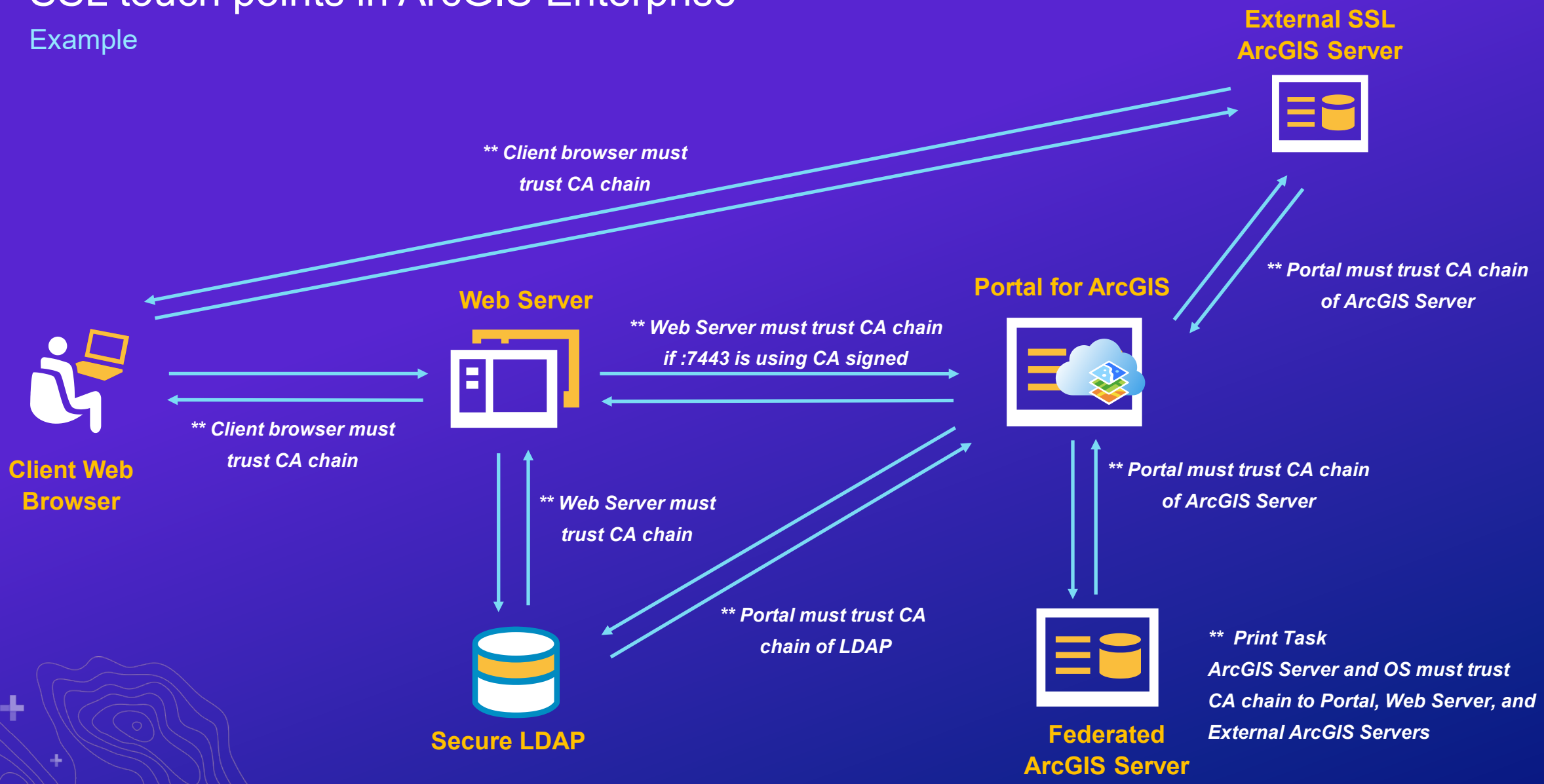
Enable HTTPS on your web server

Demonstration

Implementing SSL within ArcGIS Enterprise

SSL touch points in ArcGIS Enterprise

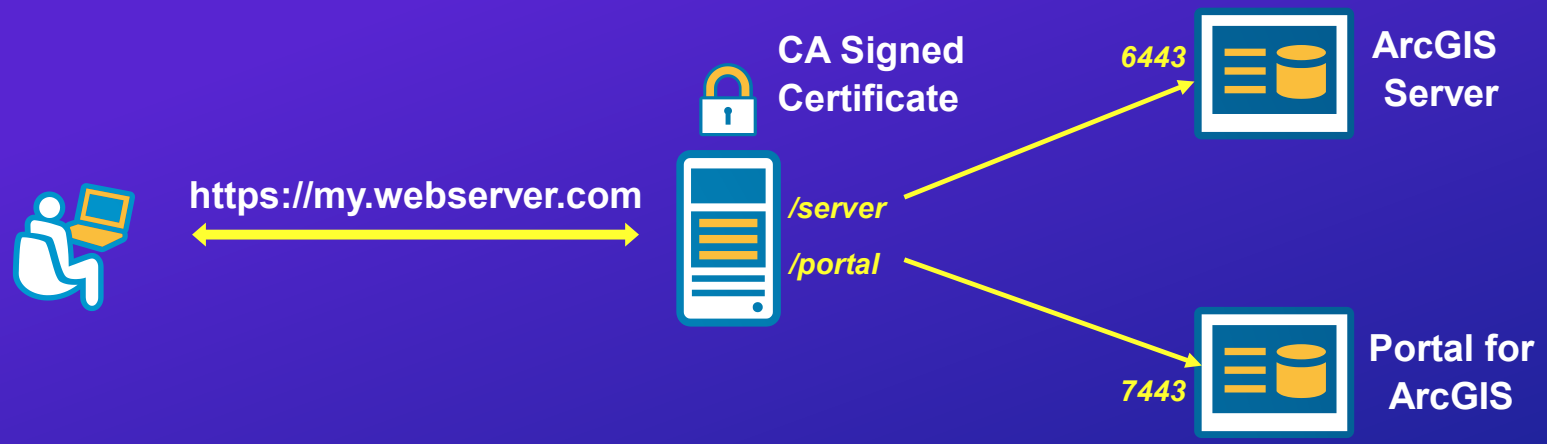
Example



Secure communication via ArcGIS Web Adaptor

Taking advantage of CA signed certificates on your web server

- **The first step to implementing secure communication is installing and configuring the Web Adaptor**
  - *Moves traffic from 6443/6080 (ArcGIS Server) and 7443/7080 (Portal for ArcGIS) to 443/80*



- **Moving traffic to default ports allows clients to take advantage of CA signed server certificates at the web tier**

Implementing SSL within ArcGIS Enterprise

Status Review

So far we've only covered installing and configuring CA signed certificates on the web tier, moving our user traffic to that tier, and therefore utilizing CA signed certificates. IF we want/need fully trusted and secure communication we now need to replace the self-signed certificates at the application tier.

ArcGIS Enterprise internal certificates

Certificates at the application tier

- **Portal for ArcGIS, ArcGIS Server, and Data Store all install self-signed certificates to support communication on ports 7443, 6443 and 2443 respectively.**
  - *Other components follow a similar paradigm – GeoEvent (6143), Notebook Server (11443), Mission Server (20443), Web AppBuilder Developer Edition (3344), etc.*

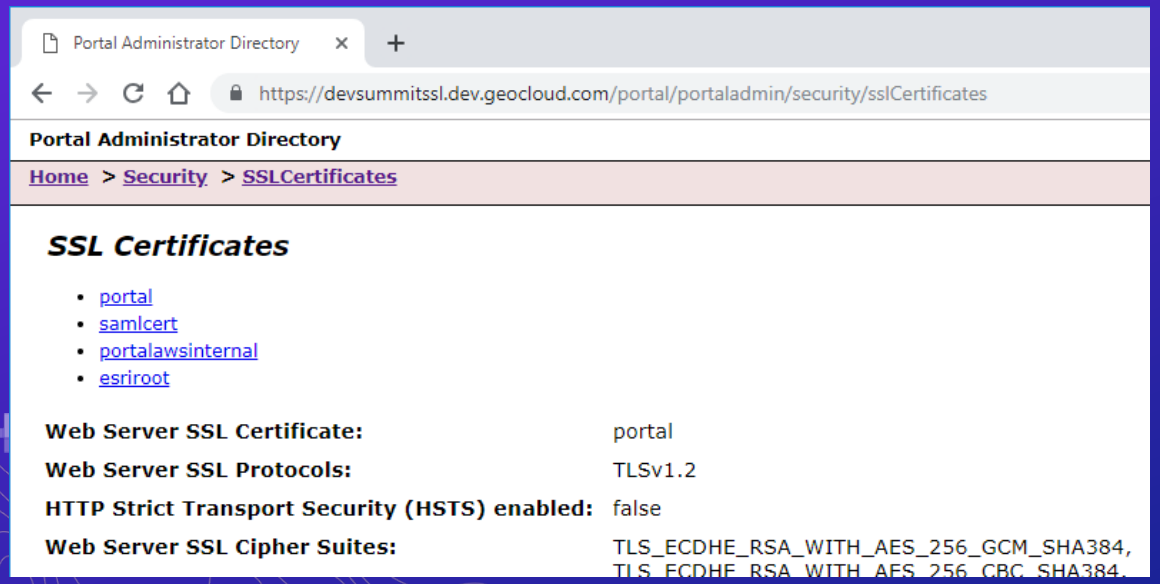
- **Each of these self-signed certificates can be replaced with CA signed certificates to have completely secure communication**
  - *Remember Certificate Authorities establish trust!*

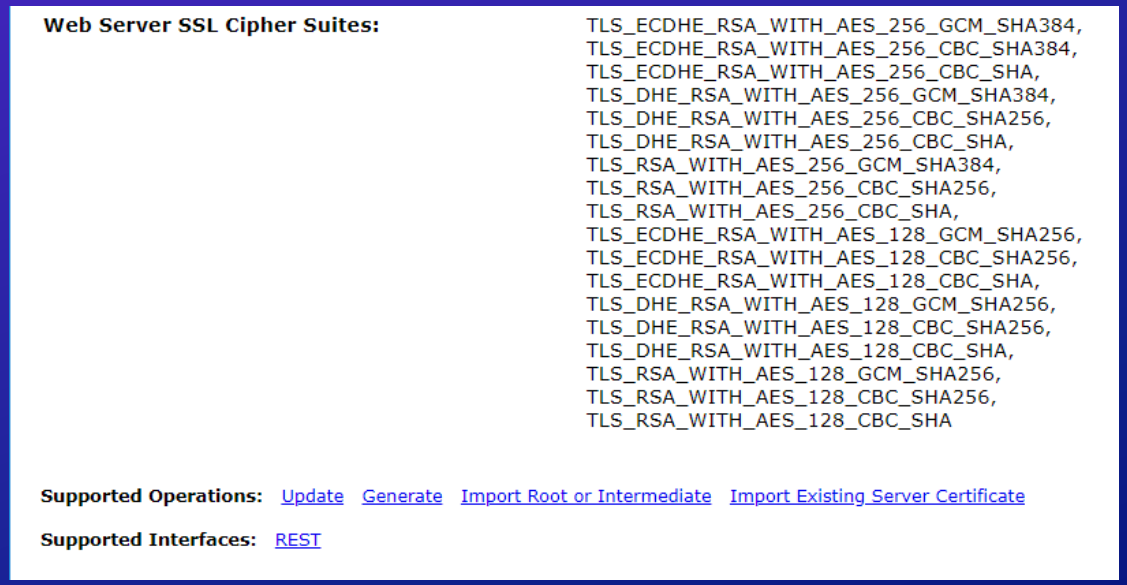
- ***New at 10.7 - Portal for ArcGIS and ArcGIS Server are HTTPS *only* by default!**

Updating internal ArcGIS Enterprise certificates

Portal for ArcGIS

- **The Portal Administrator directory provides tools to import root or intermediate certificates, existing server certificates, as well as the ability to generate a new Certificate Signing Request (CSR).**
  - *Used for updating internal ArcGIS Enterprise certificates, as well as establishing trust chains with external servers*
  - *Accessed via Portaladmin – Security – SSLCertificates. Import appropriate certificates and then Update.*



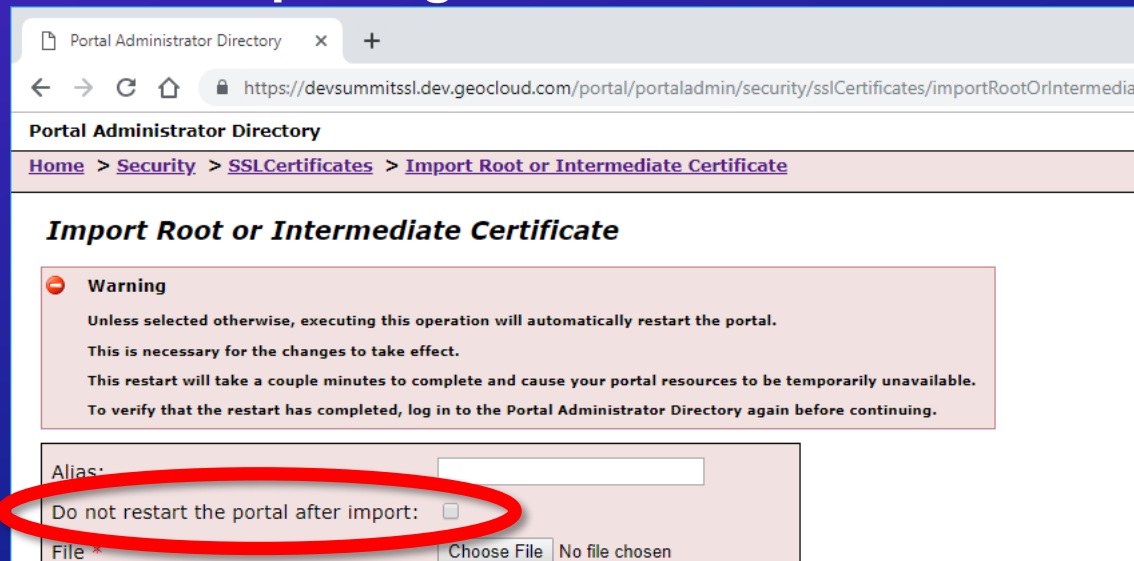


Updating internal ArcGIS Enterprise certificates

Portal for ArcGIS

- **If working in closed environment and replacing Portal for ArcGIS's self signed certificates (i.e. on 7443) be sure to import root and intermediate certificates as needed to establish your trust chain!**
  - *Hybrid environments using signed certificates from known CA's may not need this step (e.g. CA is DigiCert)*

- **New at 10.6 – option to *not* restart Portal service after importing certificates**
  - *At 10.5/1.5.1 Portal service restarted automatically*
  - *At 10.4.1 and prior Portal service needed to be restarted manually*



Updating internal ArcGIS Enterprise certificates

ArcGIS Server

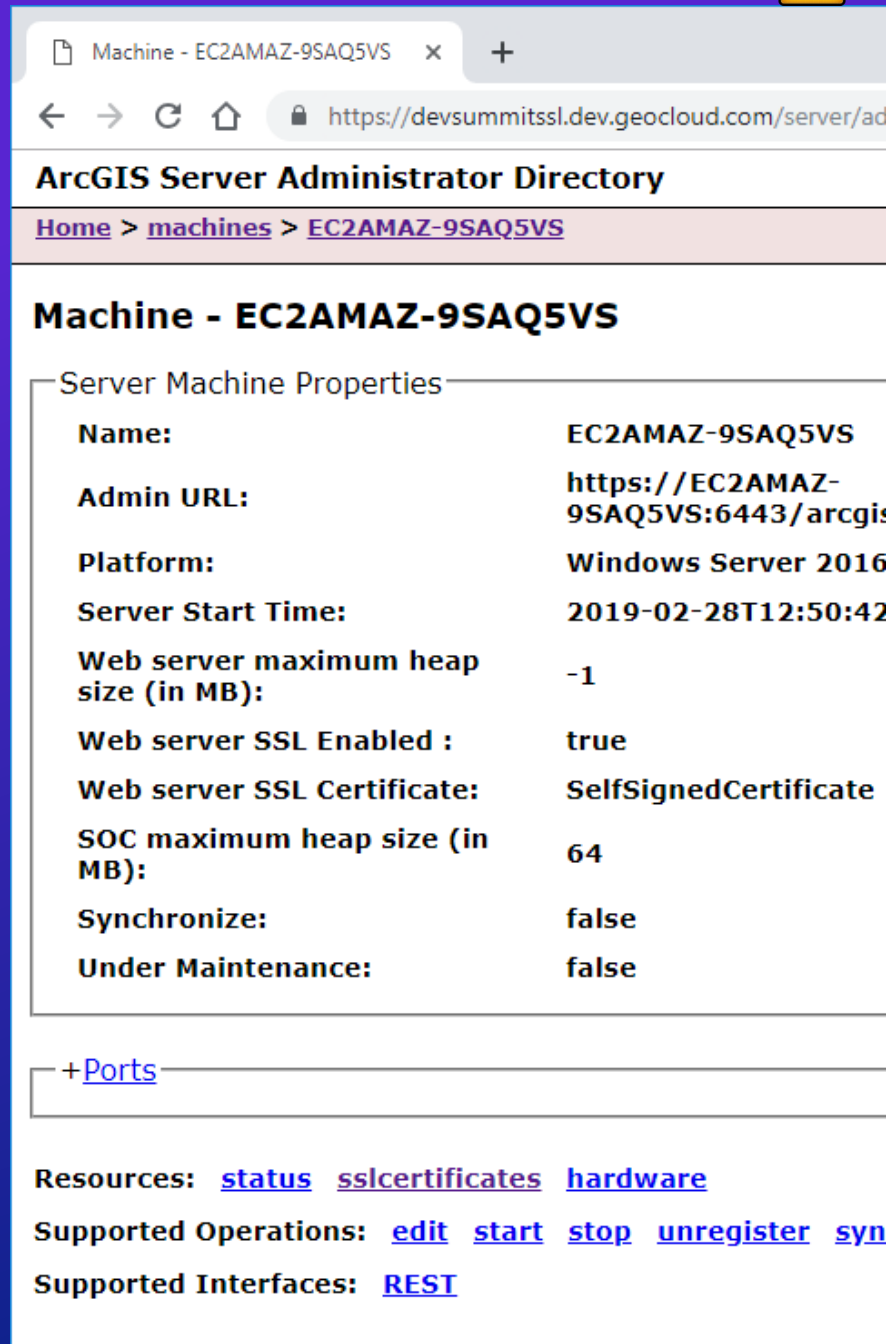
- **ArcGIS Server Administrator Directory provides nearly identical tools to Portal for ArcGIS, including the ability to import root or intermediate certificates, existing server certificates, as well as the ability to generate a new Certificate Signing Request (CSR).**

- **Accessed via Admin – machines – [machine name] – sslcertificates.**

Updating internal ArcGIS Enterprise certificates

ArcGIS Server

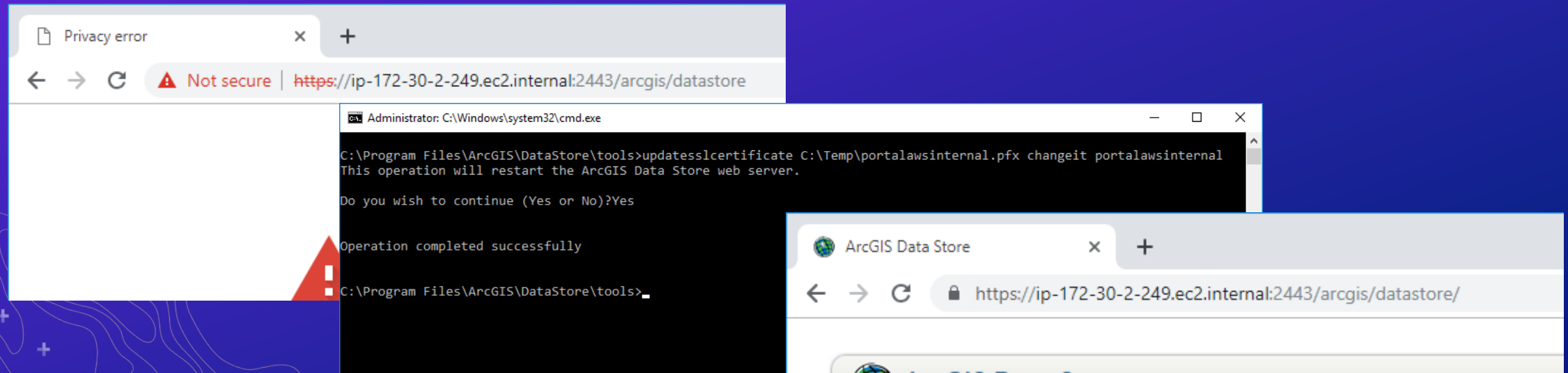
- **Import/generate appropriate certificates, browse back to [machine name] and then Update.**
- **If working in closed environment and replacing self signed certificates (i.e. on 6443) be sure to import root and intermediate certificates as needed to establish your trust chain!**
  - *Hybrid environments using signed certificates from known CA's may not need this step (e.g. CA is DigiCert)*
- **Unlike Portal for ArcGIS, the ArcGIS Server service will restart automatically.**



Updating internal ArcGIS Enterprise certificates

Data Store for ArcGIS

- **Data Store for ArcGIS ships with a number of batch files for managing its properties, and one of those is updatesslcertificate.bat.**
  - *Accessed at C:\Program Files\ArcGIS\DataStore\tools*
- **The certificate file must be in PKCS12 format with a file extension of .pfx or .p12**
- **Prompted for Data Store restart at completion of process**

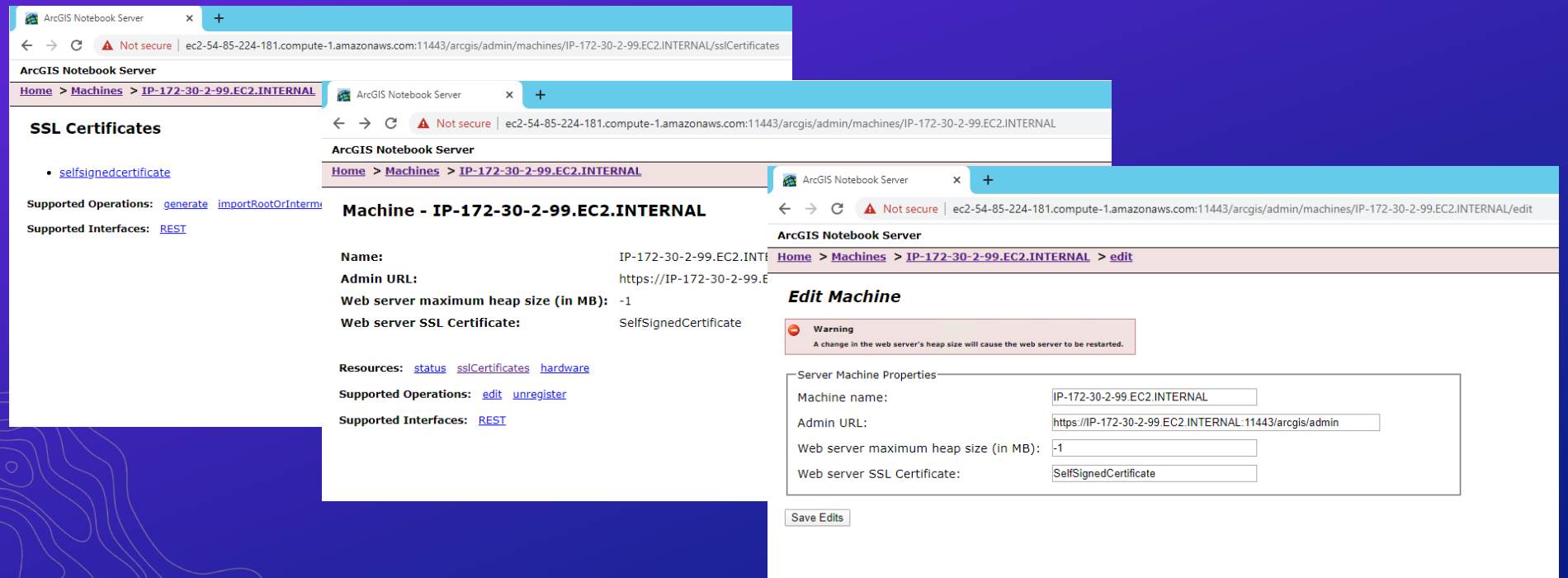


Updating internal ArcGIS Enterprise certificates

Notebook Server & Mission Server

- **Both Notebook Server and Mission Server use an identical process to ArcGIS Server to update their internal web server certificates (ports 11443 and 20443 respectively)**

- **Accessed via Admin – machines – [machine name] – sslcertificates.**



Updating internal ArcGIS Enterprise certificates

GeoEvent Server

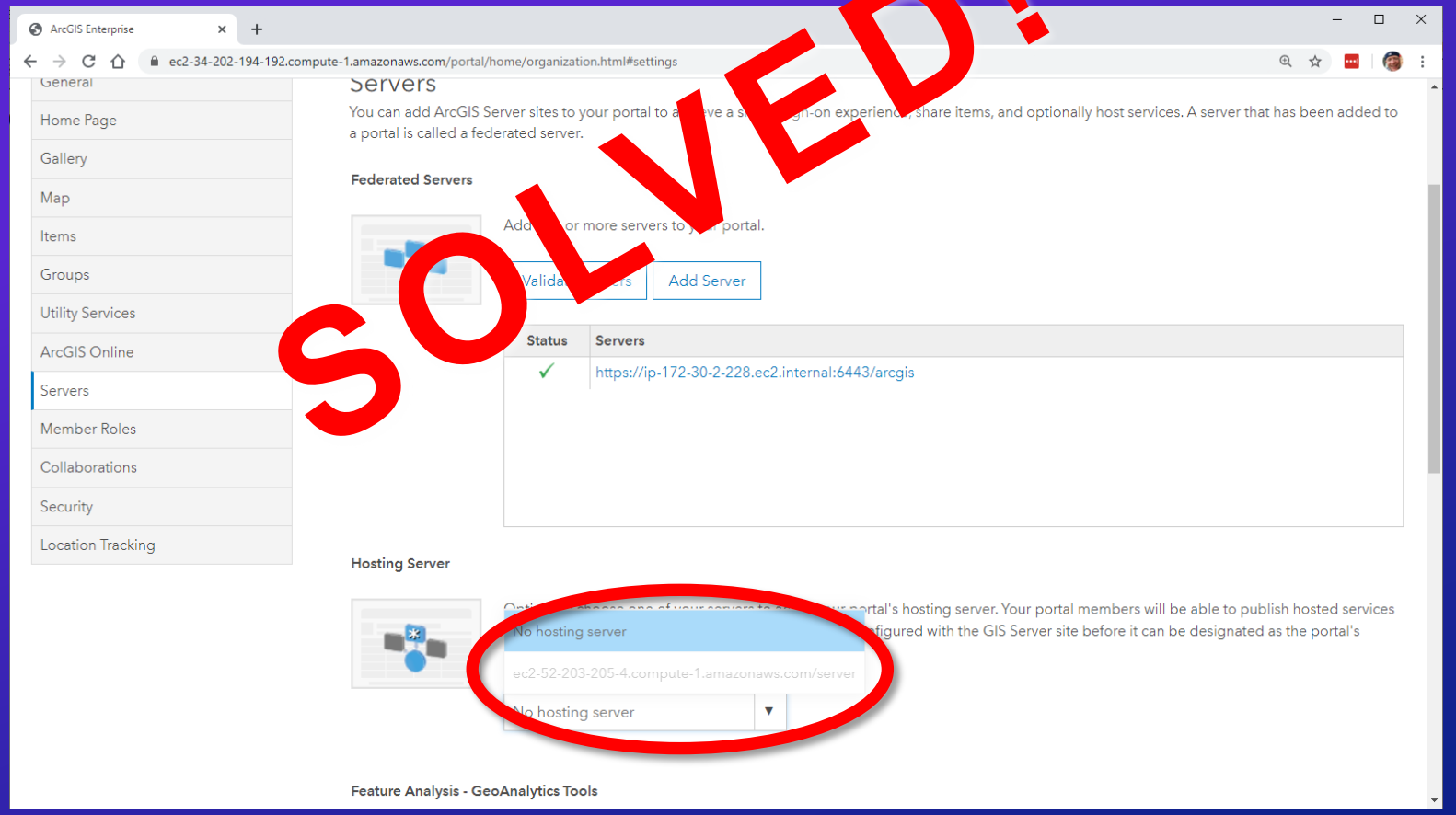
- **GeoEvent Server uses it's co-located/adjacent/[insert correct adjective here] ArcGIS Server trust store**

- **After ArcGIS Server certificates are updated the GeoEvent Server service must be restarted to reflect these changes.**
  - *Note: it's often required to bounce GeoEvent service 2 or 3 times to recognize new certs*

Common SSL Problems

Unable to define hosting server

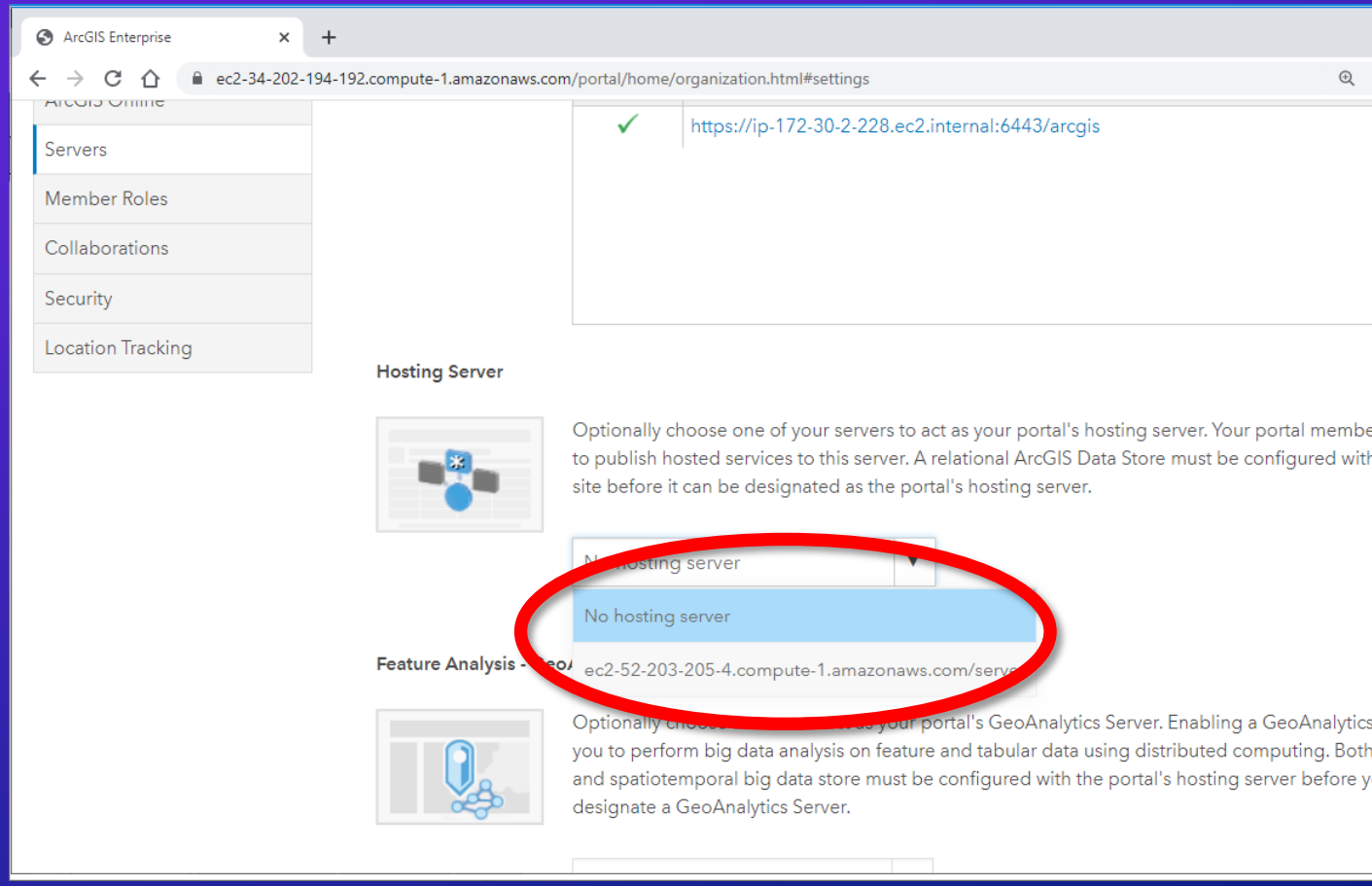
- **Federation goes fine…but unable to define the hosting server.**

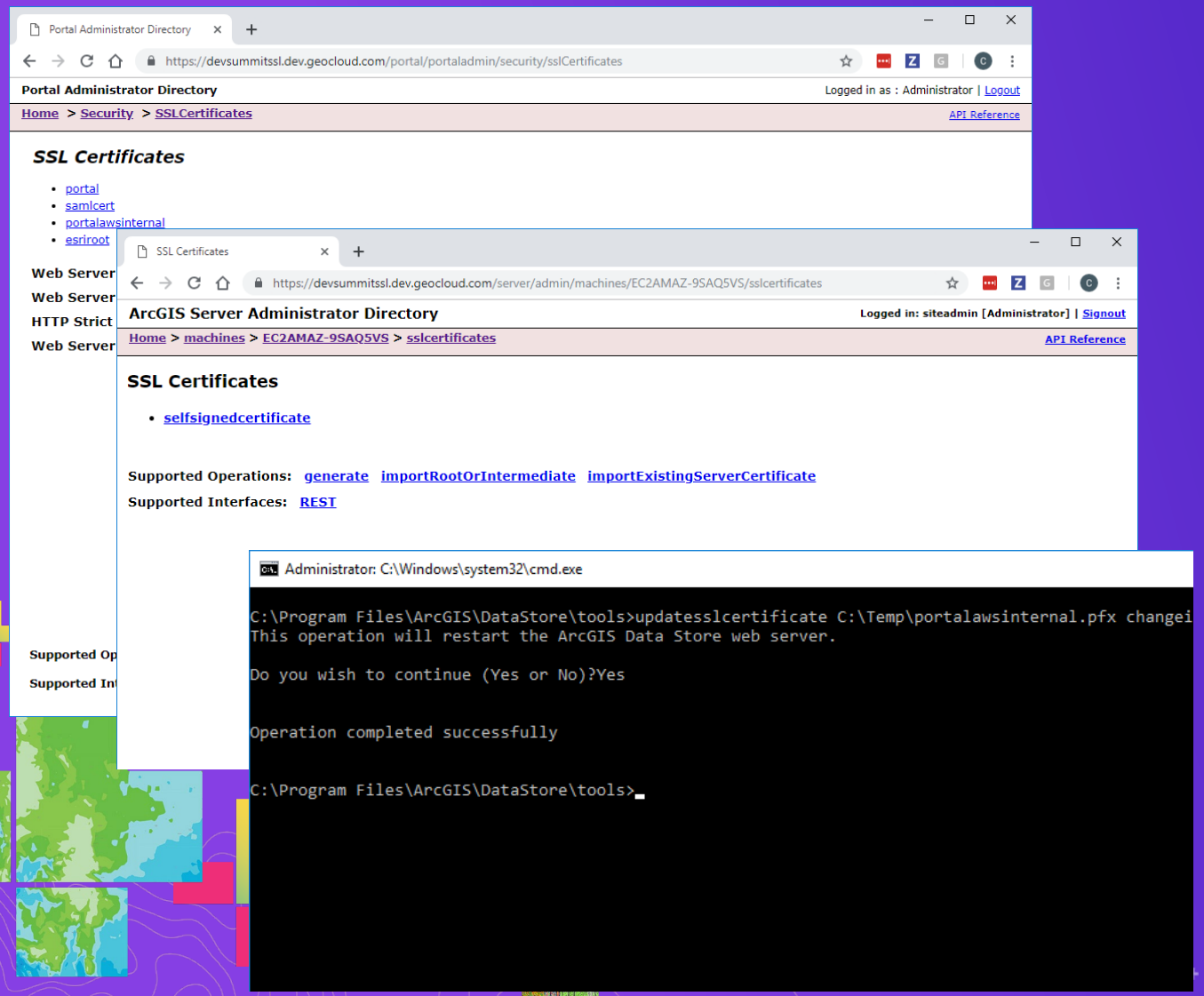


Unable to define hosting server – *solved!*

Cause – certificate mismatch

- **Internal ArcGIS Server certificate is configured for the machine name, but the administrative URL referenced with federation is for the internal DNS**
- **Recreate self signed certificate to use internal DNS**
- **Troubleshooting Tips & Tricks**
  - Federation goes fine, but can't define the hosting server
  - Use the Portal for ArcGIS logs





Updating internal ArcGIS Enterprise certificates

Demonstration

Establishing trust to external resources

Importing Root and Intermediate Certificates

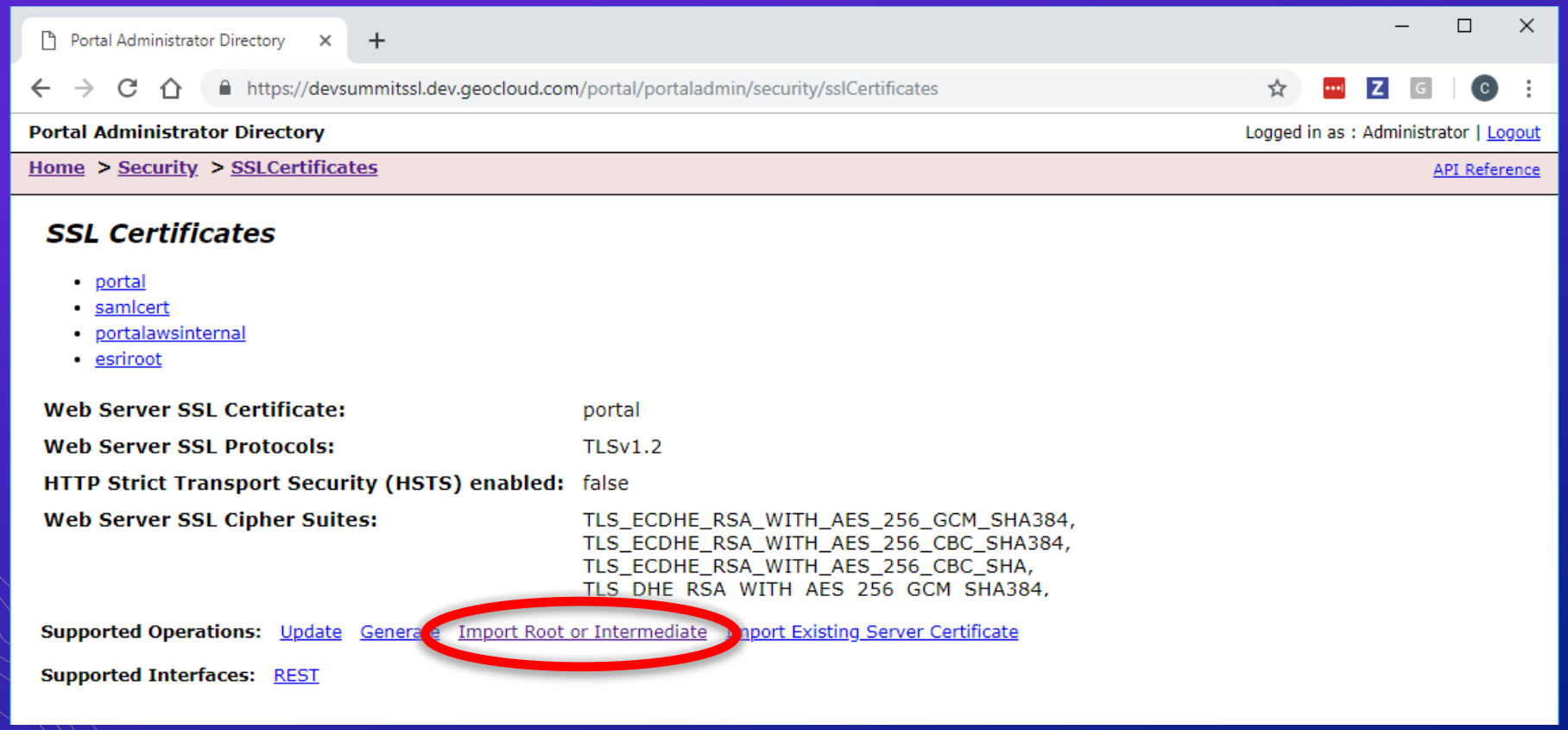
- **In order to consume services from other secure web servers proper trust must be created with ArcGIS Enterprise. This is done by importing trust chains (i.e. root and intermediate certificates) into appropriate admin endpoints.**
  - This trust establishes proper encryption channel
  - *Note: this does not apply to server certificates signed by well known certificate authorities (e.g. Symantec, GoDaddy, etc.).*

- **Example scenarios:**
  - Adding an HTTPS map service to the Portal for ArcGIS map viewer from an external organization.
  - Using ArcGIS Server Print Service to generate thumbnails for web maps using HTTPS Map Services.

Establishing trust to external resources

Portal for ArcGIS

- **In Portal for ArcGIS use the Portal Administrator directory to import root and intermediate certificates**

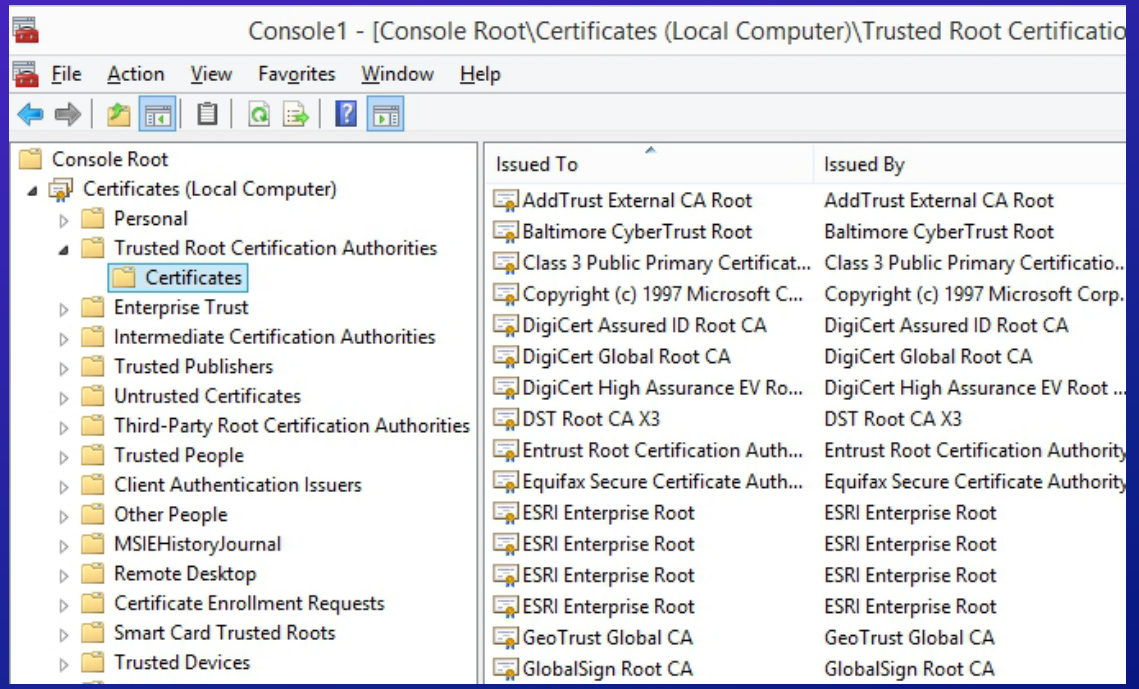


Establishing trust to external resources

ArcGIS Server

- **In ArcGIS Server use the Administrator Directory import root and intermediate certificates**

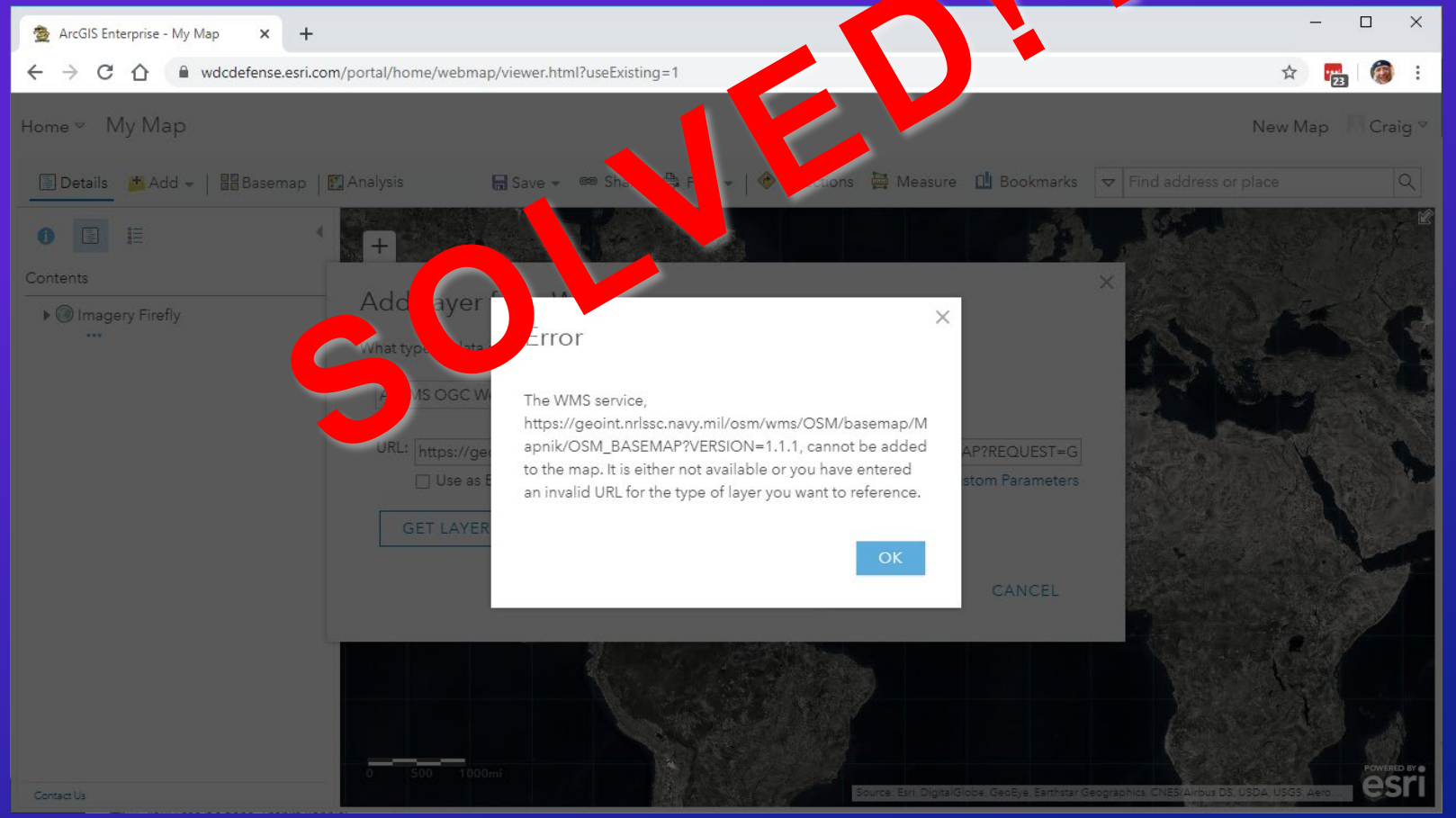
- **On the Server, import root and intermediate certificates into the OS Trust Store (needed for GP Services).**



Common SSL Problems

Unable to add layers to Map Viewer

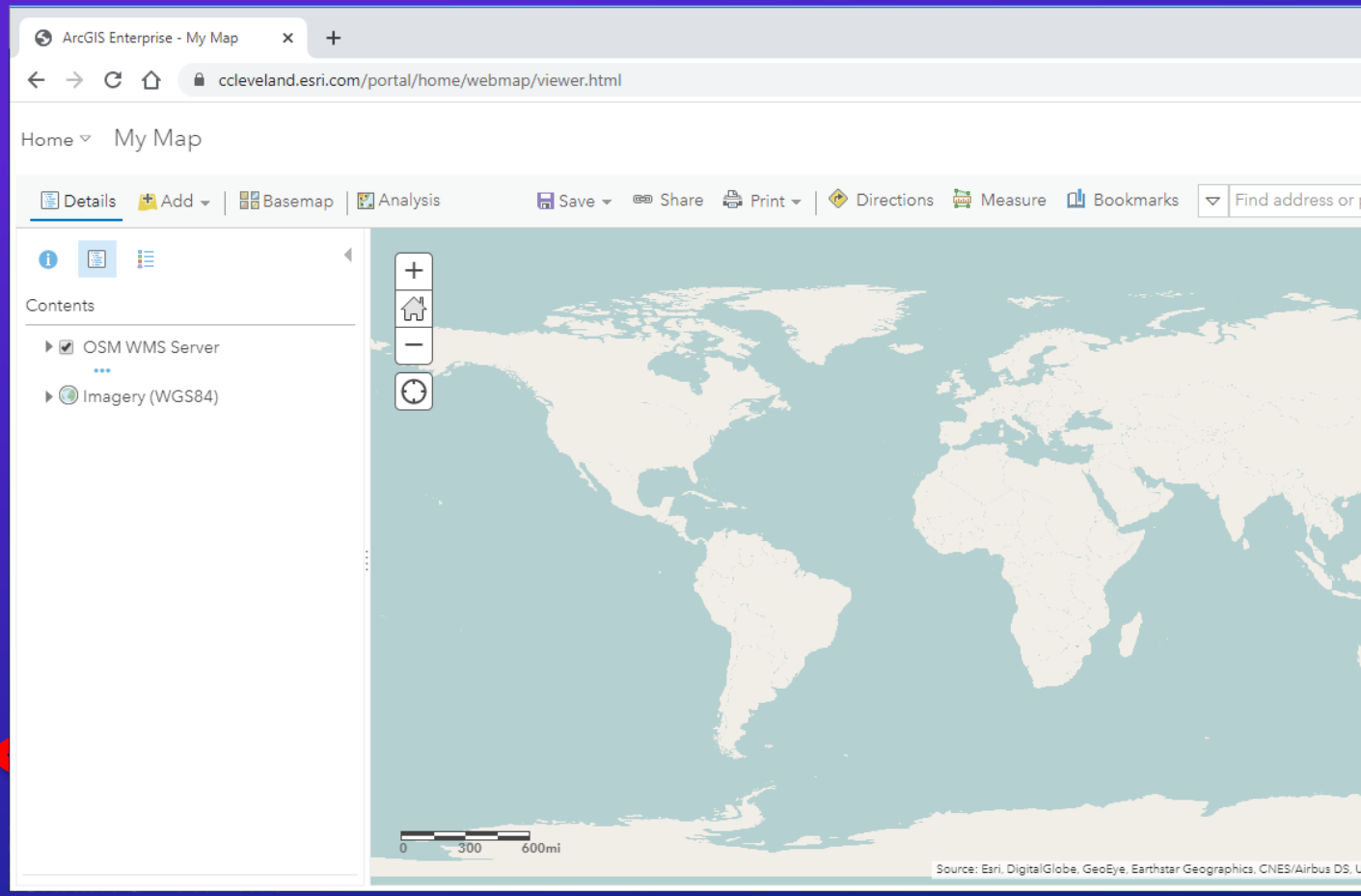
- **Adding a layer to the Map Viewer…errors out.**

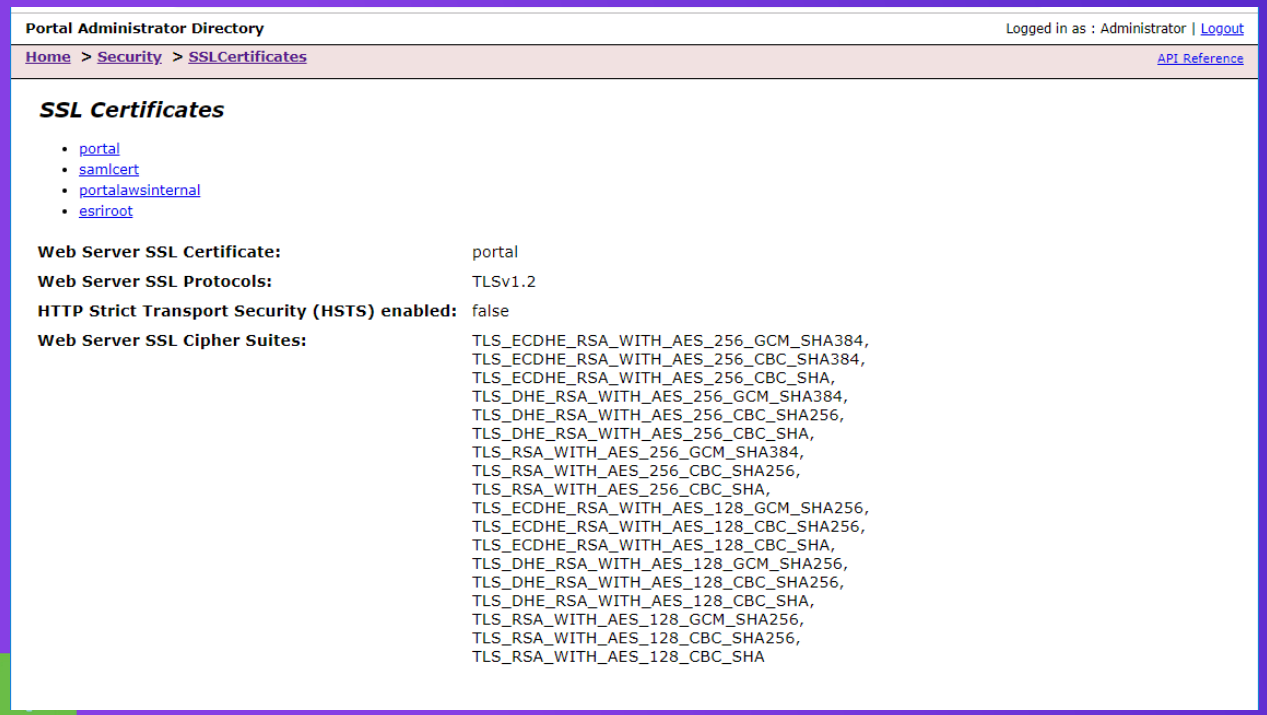


Unable to add layers to Map Viewer – *solved!*

Cause - missing trust chain in Portal

- **Web Server is protected by a DOD trust chain not known to Portal for ArcGIS**
- **Import trust chain into Portal for ArcGIS to establish trust and allow layers to render**
- **Troubleshooting Tips & Tricks**
  - Use the Portal for ArcGIS logs to find clues about SSL errors
  - Inspect browser console for SSL errors





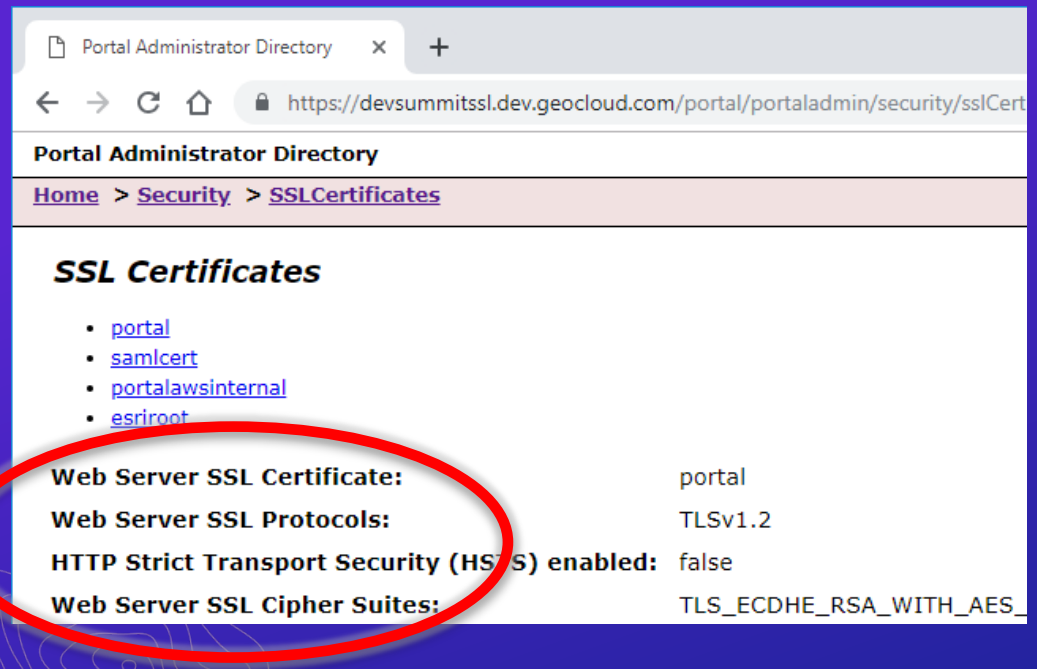
Importing certificates into Portal for ArcGIS

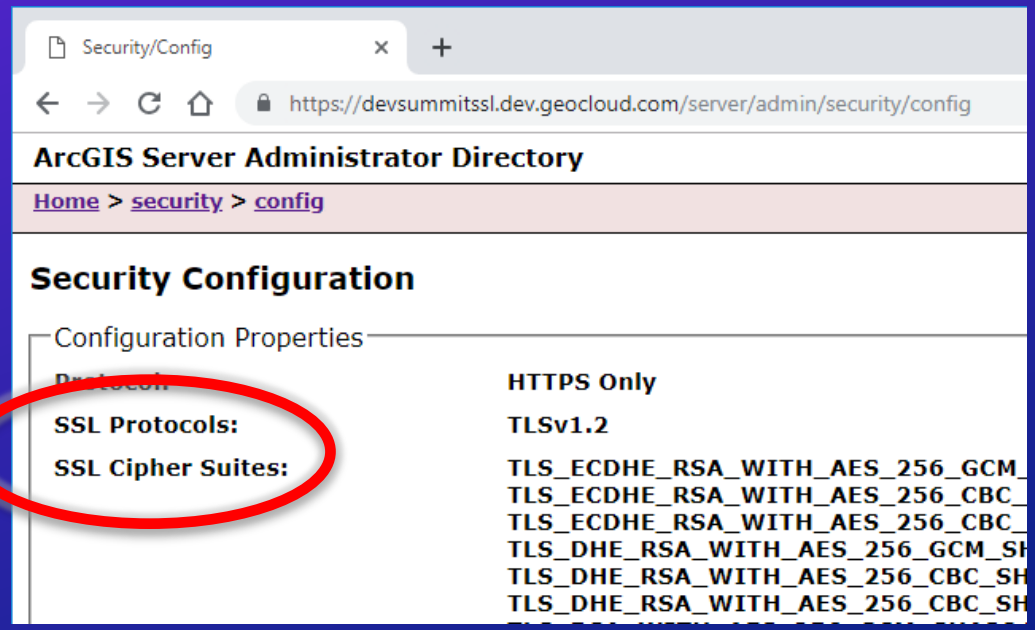
Demonstration

Additional considerations

Restrict SSL protocols and cipher suites

- **Within the respective ArcGIS Enterprise components you can specify which SSL protocols and encryption algorithms to use to secure communication.**





Import certificates into ArcGIS Online

Trust in ArcGIS Online for custom CAs

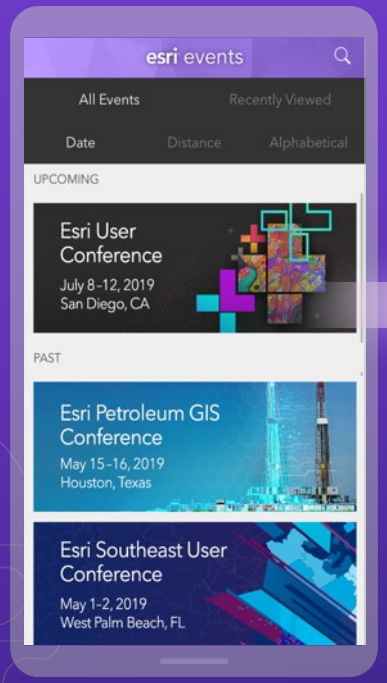
- **Focused on handling secured ArcGIS Server service and app proxies**
- **Only REST API calls supported; no UI experience currently**
- **List Certificates** https://<portal-url>/certificates
  - https://developers.arcgis.com/rest/users-groups-and-items/certificates.htm
- **Register Certificate** https://<portal-url>/certificates/register(POST only)
  - https://developers.arcgis.com/rest/users-groups-and-items/register-certificate.htm

Key Takeaways

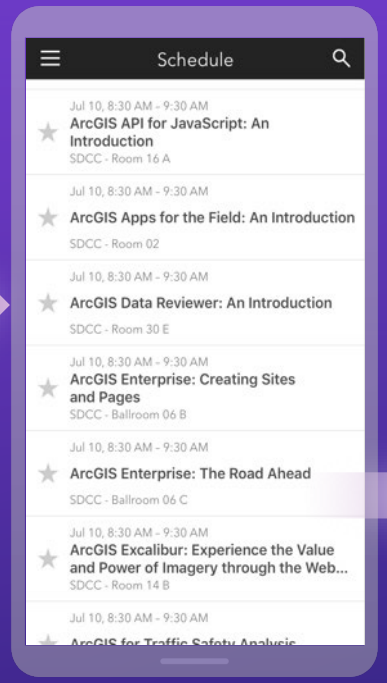
- **SSL is about secure and encrypted communication**
- **SSL begins at the web tier, and extends to each ArcGIS Enterprise component which provides support for SSL**
  - *Web tier is easy, application tier takes some more work…*
- **Portal and ArcGIS Server logs are key in troubleshooting SSL issues**

Please Share Your Feedback in the App

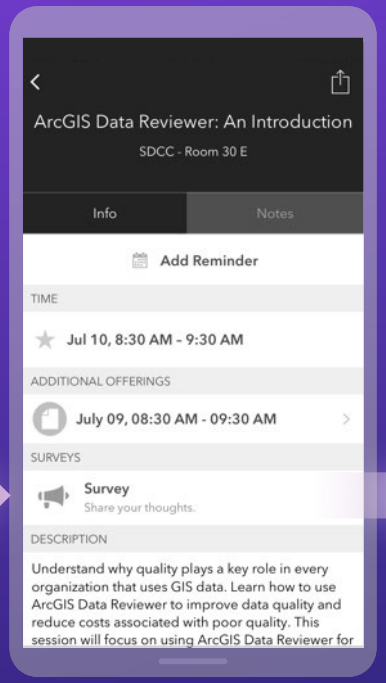
Download the Esri Events app and find your event



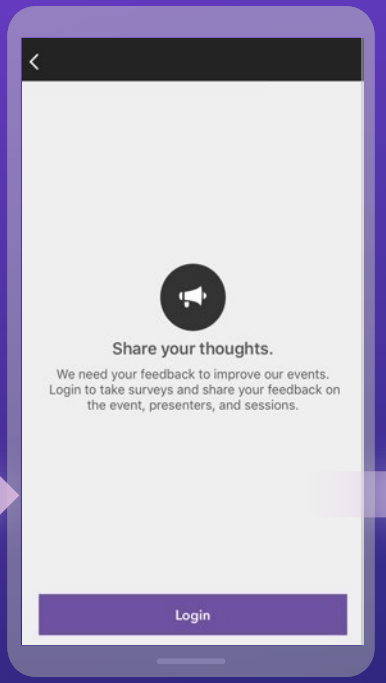
Select the session you attended



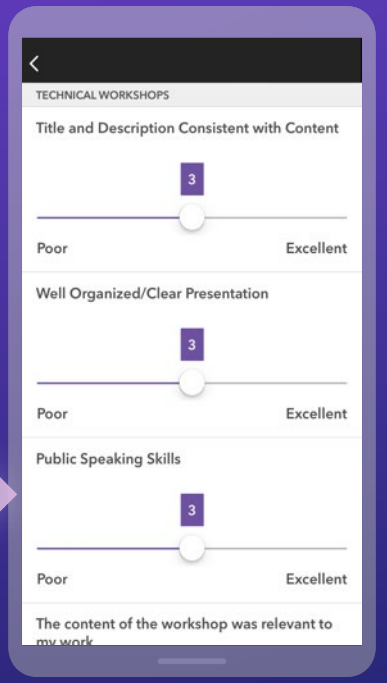
Scroll down to "Survey"



Log in to access the survey



Complete the survey and select "Submit"



esri
THE
SCIENCE
OF
WHERE