



ArcGIS and SSL Considerations

Bill Major and Craig Cleveland

2018 Esri DEVSummit Conference | Palm Springs, CA

Overview

ArcGIS Enterprise and SSL Considerations

1 - Fundamentals of Secure Communication

2 - Implementing SSL/TLS at the Web Tier

3 - Implementing SSL/TLS within ArcGIS Enterprise

4 - Troubleshooting Common SSL Problems

Fundamentals of Secure Communication

Encrypted & Trusted Communication



Fundamentals of Secure Communication

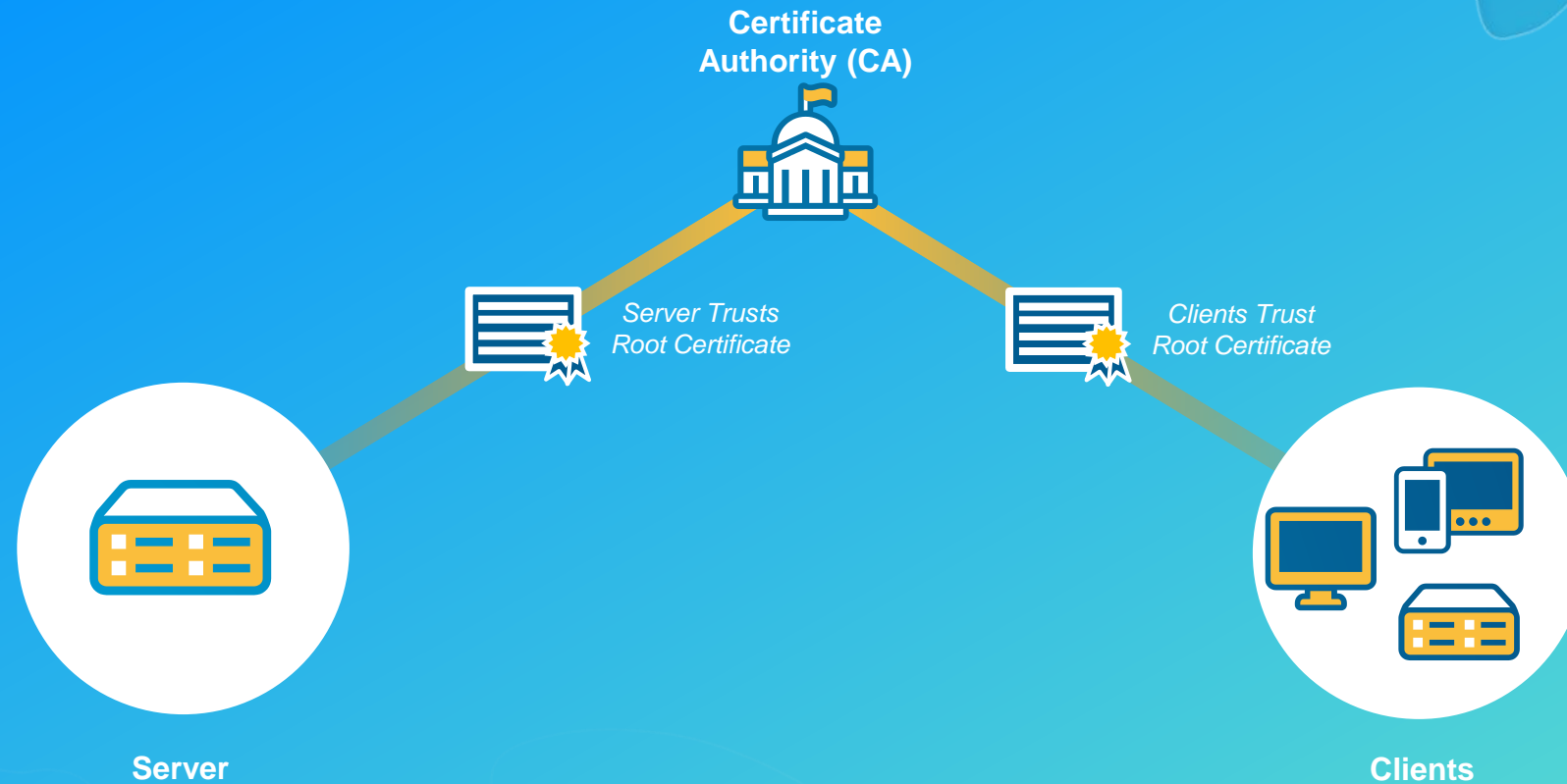
Server Certificates and Trust Stores



- **Secure Socket Layer (SSL)** - standard security technology for establishing an encrypted link between a web server and a browser
 - TLS v1.2
- **Certificate Authorities** establish trust by digitally signing server certificates for server identification and issuing user certificates for client identification (i.e. Public Key Infrastructure).
 - Open Internet SSL Checker: <https://www.sslshopper.com/ssl-checker.html>
- **Public key/private key pairing** for encrypted communication
- **Adjustments** needed to configure ArcGIS Enterprise to work properly in secure/closed environments

Fundamentals of Secure Communication

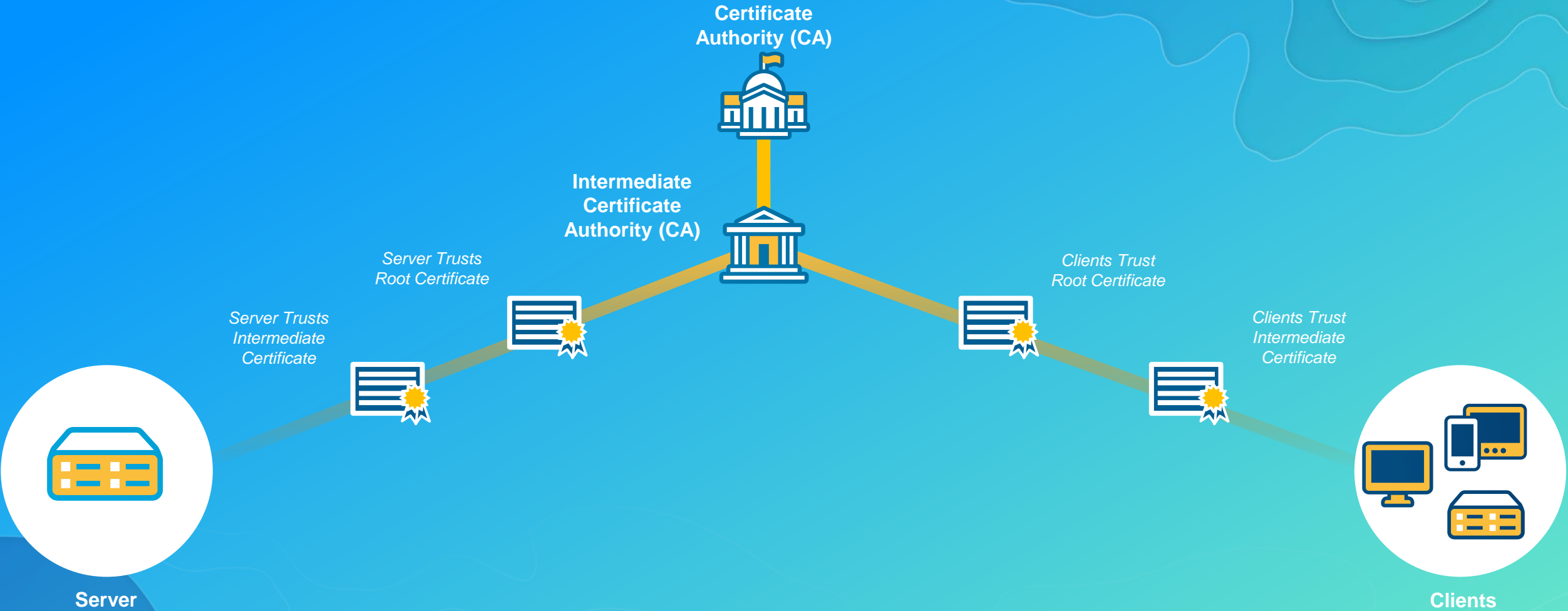
Certificate Authority (Root of Trust)



Trust, Encrypt, Communicate

Fundamentals of Secure Communication

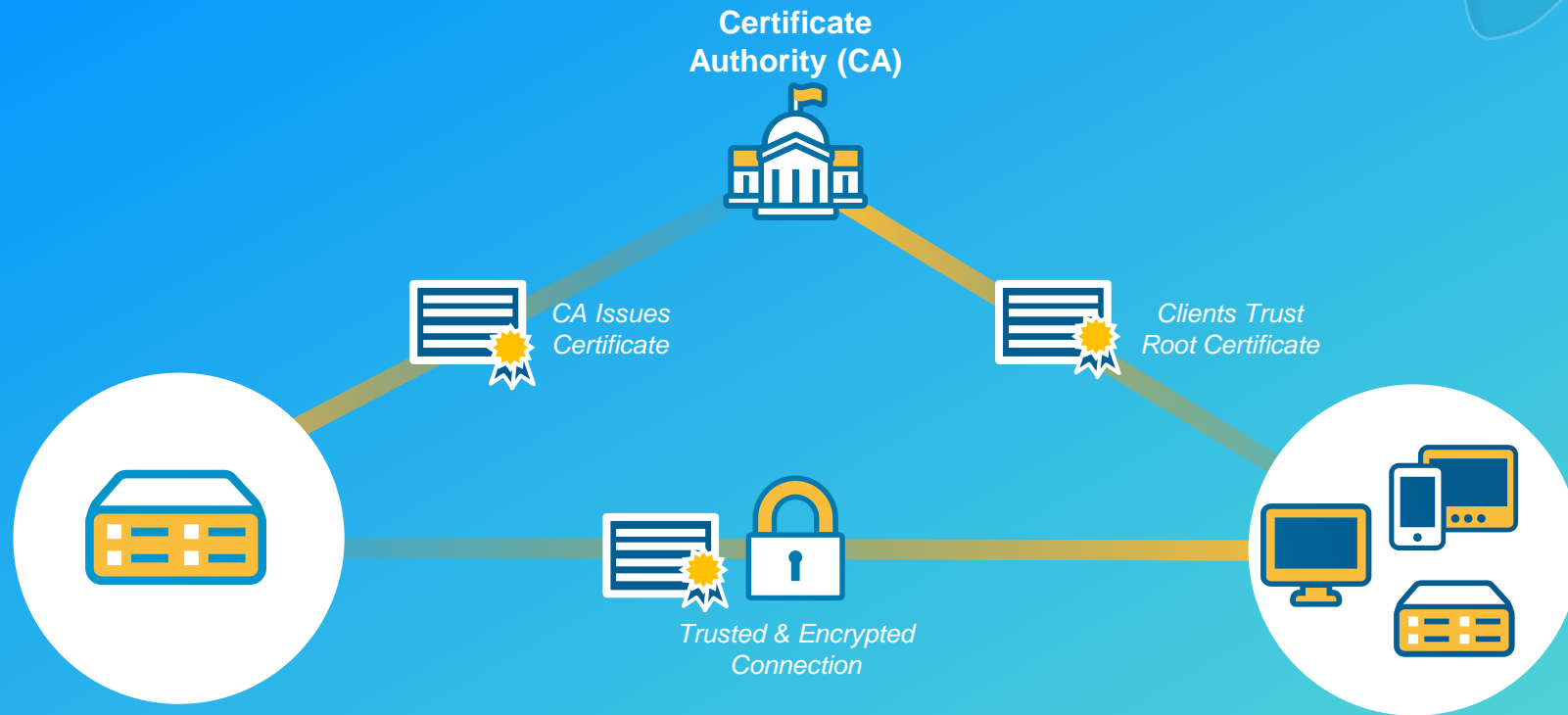
Intermediate Certificate Authority (Trust Chain)



Trust, Encrypt, Communicate

Fundamentals of Secure Communication

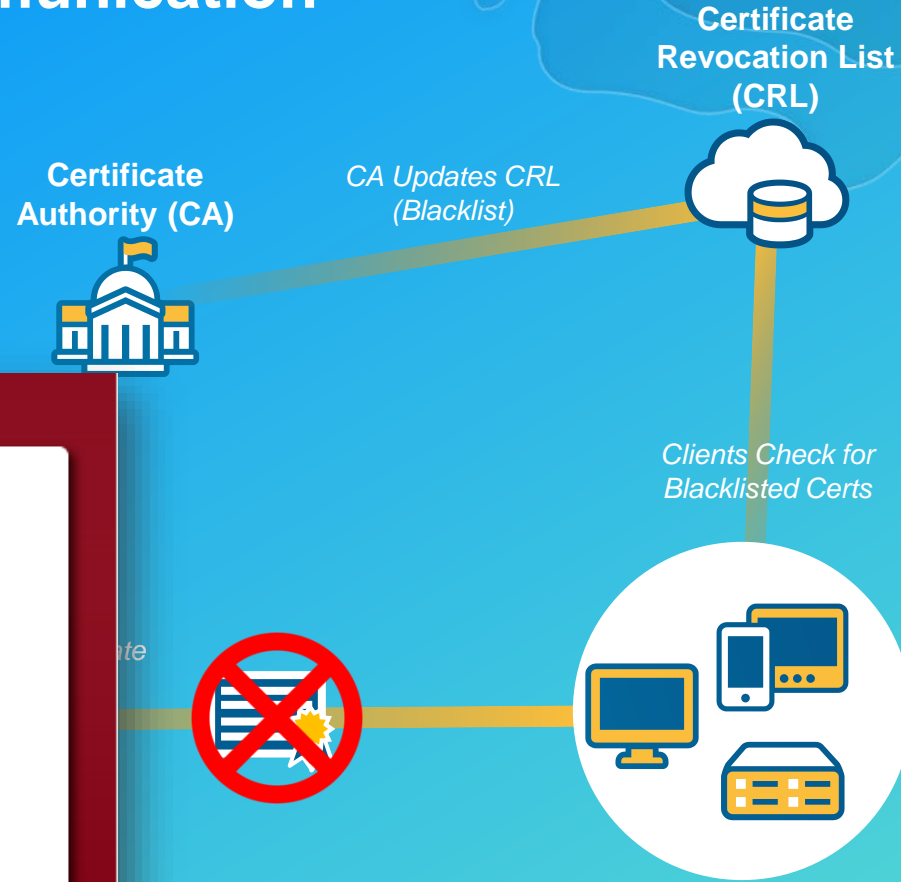
Establishing Trust for Encrypted Communication



Trust, Encrypt, Communicate

Fundamentals of Secure Communication

Certificate Revocation



The server's security certificate is revoked!

You attempted to reach [www.microsoft.com](#) but the certificate that the server presented has been revoked by its issuer. This means that the security credentials the server presented absolutely should not be trusted. You may be communicating with an attacker.

[Back to safety](#)

[▶ Help me understand](#)

What if a trusted server is compromised?

Fundamentals of Secure Communication

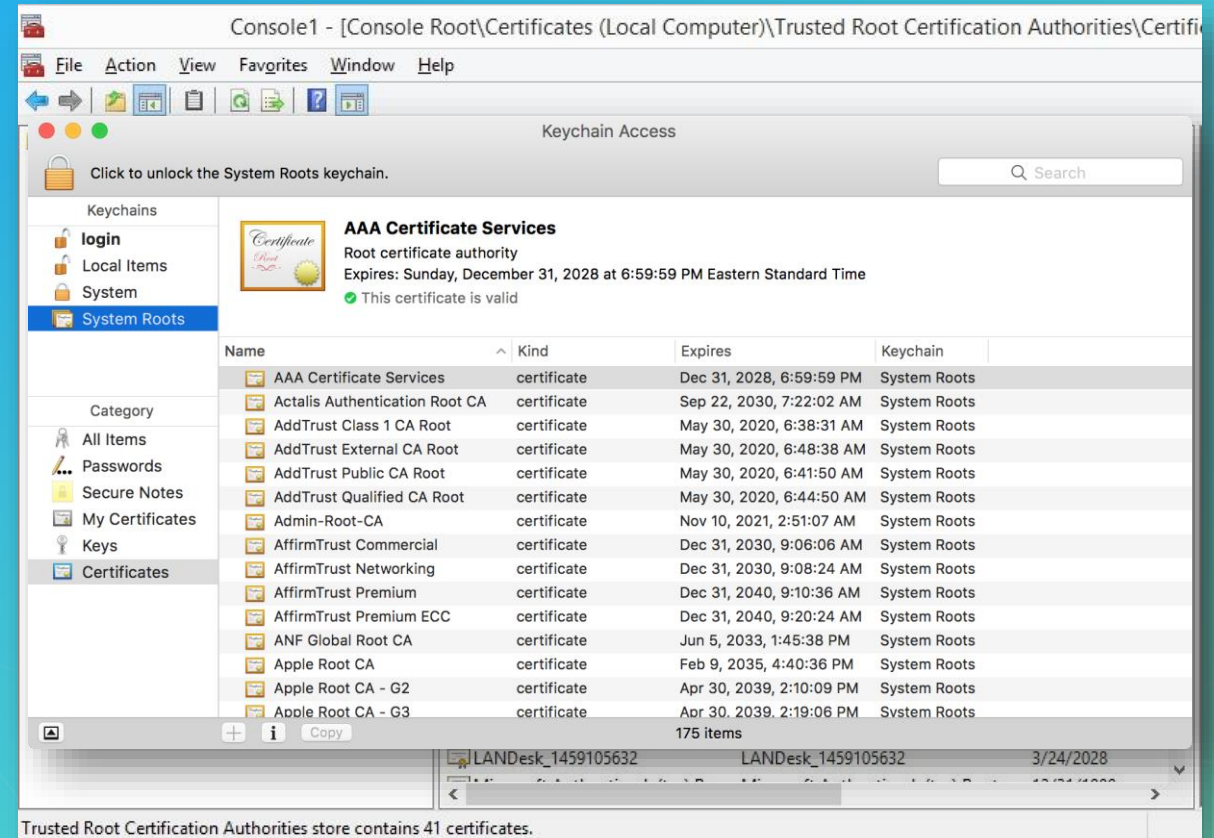
Trust Stores



- 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**



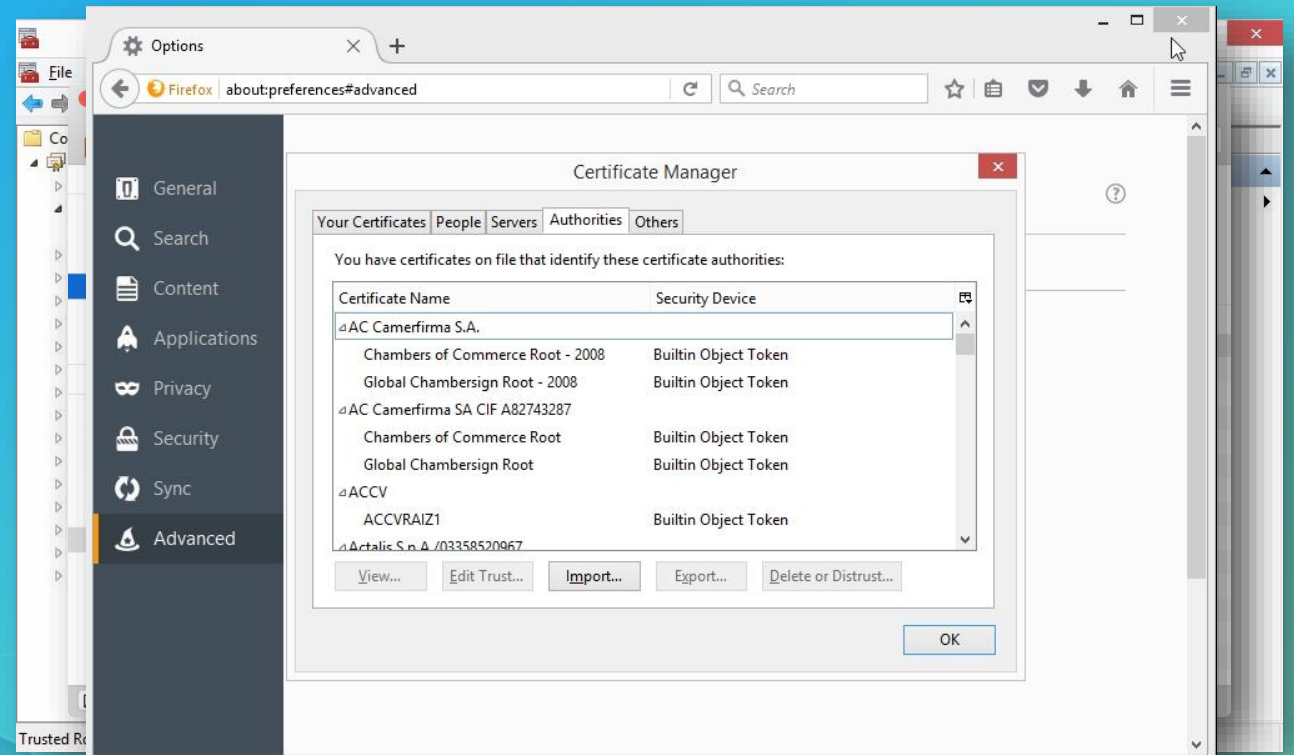
Fundamentals of Secure Communication

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!*



Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\]

File Action View Favorites Window Help

Console Root

- Certificates (Local Computer)
 - Personal
 - Trusted Root Certification Authorities
 - Certificates
 - Enterprise Trust
 - Intermediate Certification Authorities
 - Trusted Publishers
 - Untrusted Certificates
 - Third Party Root Certificates
 - Trusted Root Certification Authorities
 - Client Certificates
 - Removal Information
 - Certificate Revocation Lists
 - Smart Cards
 - Trusted Root Certification Authorities
 - Web Services
 - Windows

Issued To	Issued By	Expiration Date	In
AddTrust External CA Root	AddTrust External CA Root	5/30/20	Se
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/25	Se
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/28	Se
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/99	Ti
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/31	Se
DigiCert Global Root CA	DigiCert Global Root CA	11/9/31	Se
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/31	Se
DO NOT TRUST FiddlerRoot	DO NOT TRUST FiddlerRoot	11/7/22	Se

Firefox | Preferences | about:preferences#advanced

Your Certificates | People | Servers | Authorities | Others

You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
Equifax Secure Global eBusiness CA...	Builtin Object Token
Equifax Secure eBusiness CA-1	Builtin Object Token
▼ ESRI Enterprise Root	
ESRI Enterprise Root	Software Security Device
▼ Generalitat Valenciana	
Root CA Generalitat Valenciana	Builtin Object Token
▼ GeoTrust Inc.	
Apple IST CA 2 - G1	Software Security Device
GeoTrust Primary Certification Auth...	Builtin Object Token

View... Edit Trust... Import... Export... Delete or Distrust...

OK

View Certificates Security Devices

Trust Stores

Demonstration

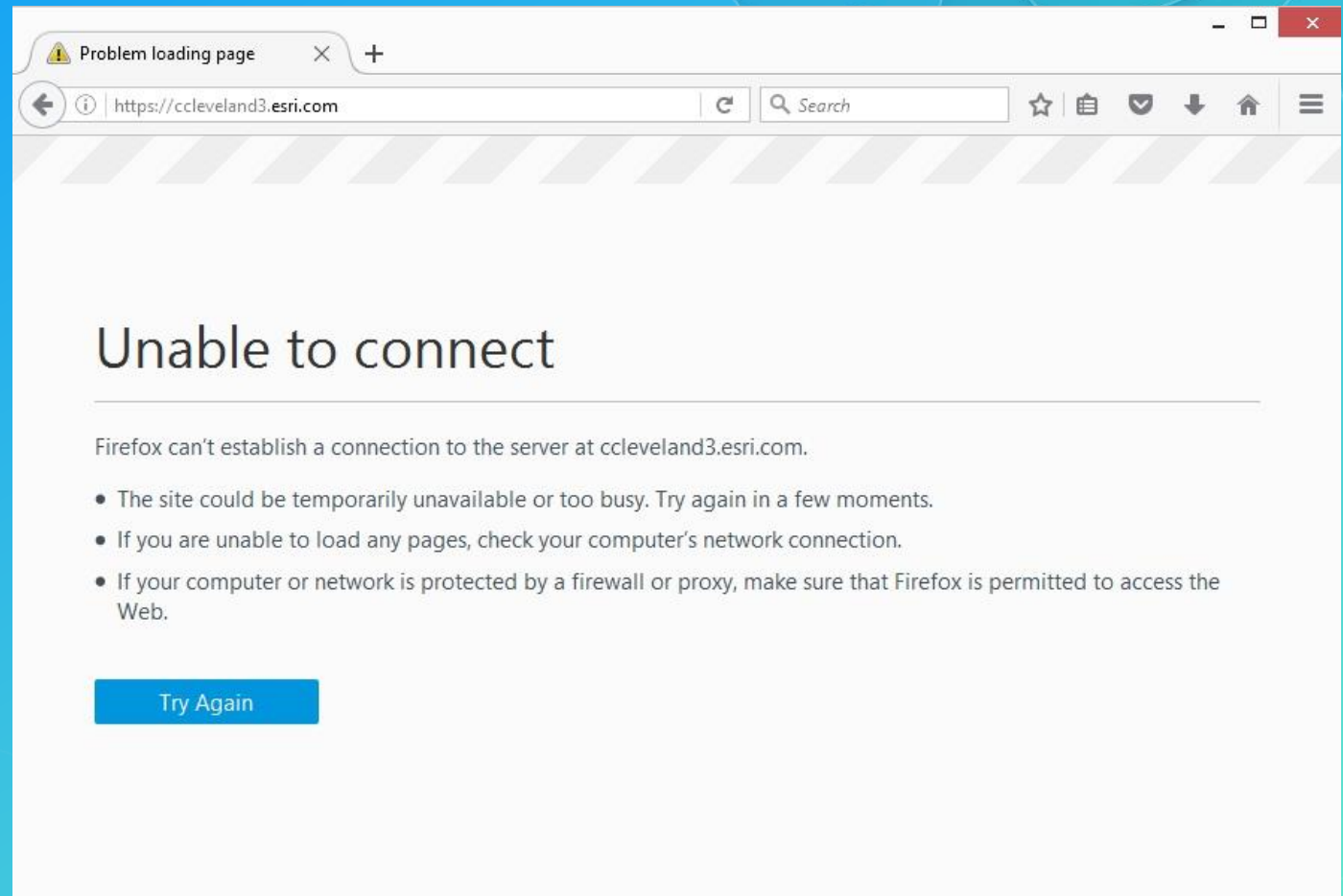
Implementing SSL/TLS at the Web Tier

The background features a gradient from dark blue on the left to light teal on the right. It is decorated with abstract, wavy, layered shapes in shades of teal and purple, resembling a topographic map or a stylized landscape. The text is positioned in the upper left quadrant.

Setting up SSL Certificates and Trusts

SSL-Enable Your Web Server

- **Some organizations mandate no HTTP(S) ports without using a properly signed server certificate.**
- **By default your web server only communicates via HTTP**
- **To enable SSL obtain a CA signed server certificate and configure your web server to use it**

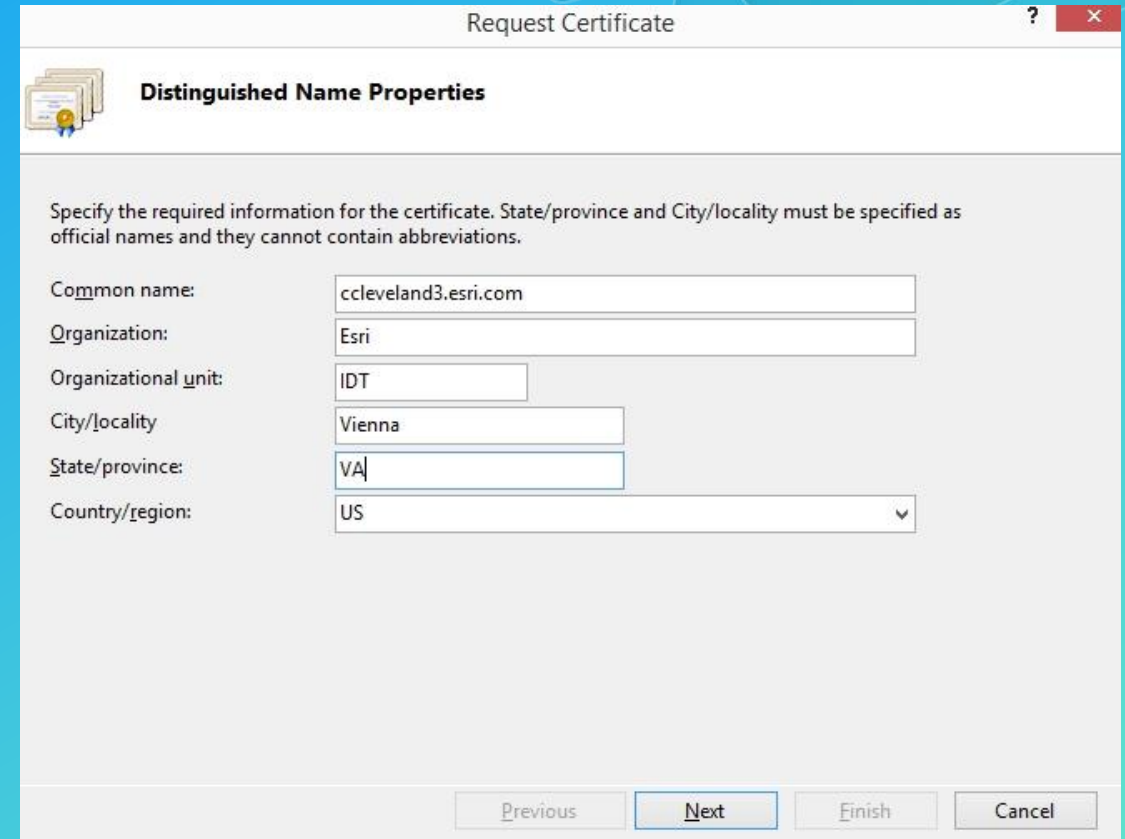


Setting up SSL Certificates and Trusts

SSL-Enable Your Web Server

1. Create certificate signing request

- *CSR's can be created in many ways – web servers, openssl, keytool, Portal & ArcGIS Server Admin pages*
- *The Common Name property of a CSR is the URL by which your web server will be accessed.*



The screenshot shows a Windows-style dialog box titled "Request Certificate" with a question mark icon and a close button. The main title is "Distinguished Name Properties" with a certificate icon. Below the title, there is a instruction: "Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations." The form contains several fields: "Common name:" with the value "ccleveland3.esri.com"; "Organization:" with the value "Esri"; "Organizational unit:" with the value "IDT"; "City/locality" with the value "Vienna"; "State/province:" with the value "VA"; and "Country/region:" with a dropdown menu showing "US". At the bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

Property	Value
Common name:	ccleveland3.esri.com
Organization:	Esri
Organizational unit:	IDT
City/locality	Vienna
State/province:	VA
Country/region:	US

Setting up SSL Certificates and Trusts

SSL-Enable Your Web Server

2. Present CSR to certificate authority

- *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).*

Microsoft Active Directory Certificate Services -- ESRI Enterprise Root

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or P in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	<pre>-----BEGIN NEW CERTIFICATE REQUEST----- MIIC3TCCAcaUCAQAwaDELMAkGA1UEBhMCMVVMxCz. EwhIYW1pbHRvbJENMAAsGA1UEChMERXNyYyTEMMA ExNjbGV2ZWxhbmQyLmVzcmkuY29tMIIBIjANBg CgKCAQEAgNmPA6F9fQ3xKRxOfwY/hncHb411hz +4iCg0dEIVn9FCwYNT/8veZzcKV80wgnD8Ncxf.</pre>
---	---

Certificate Template:

Web Server

Additional Attributes:

Attributes: san:dns=ccleveland3.esri.com

Submit >

Setting up SSL Certificates and Trusts

SSL-Enable Your Web Server


3. Download signed certificate

Microsoft Active Directory Certificate Services – ESRI Enterprise Root

Certificate Issued

The certificate you requested was issued to you.

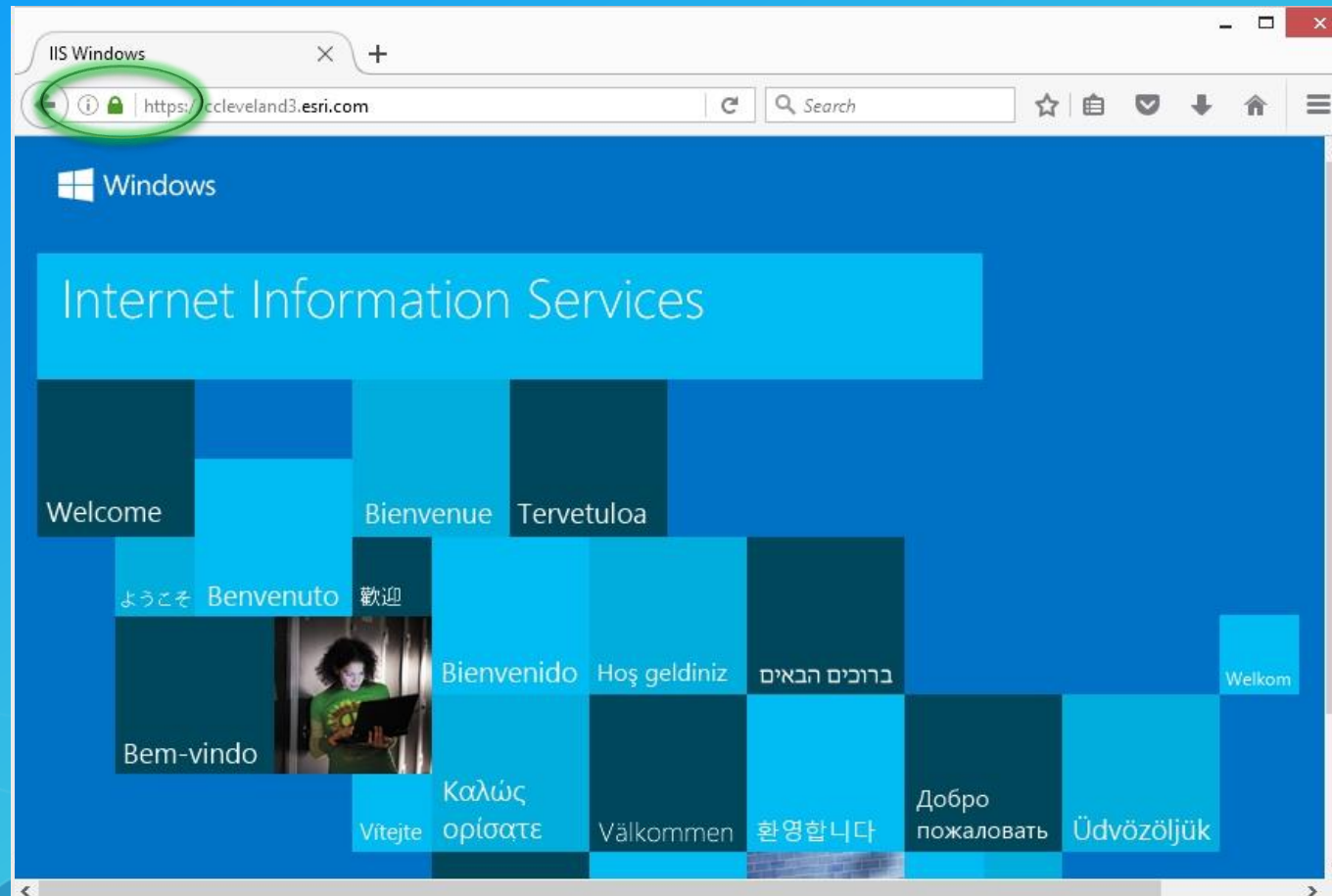
DER encoded or Base 64 encoded

 [Download certificate](#)
[Download certificate chain](#)

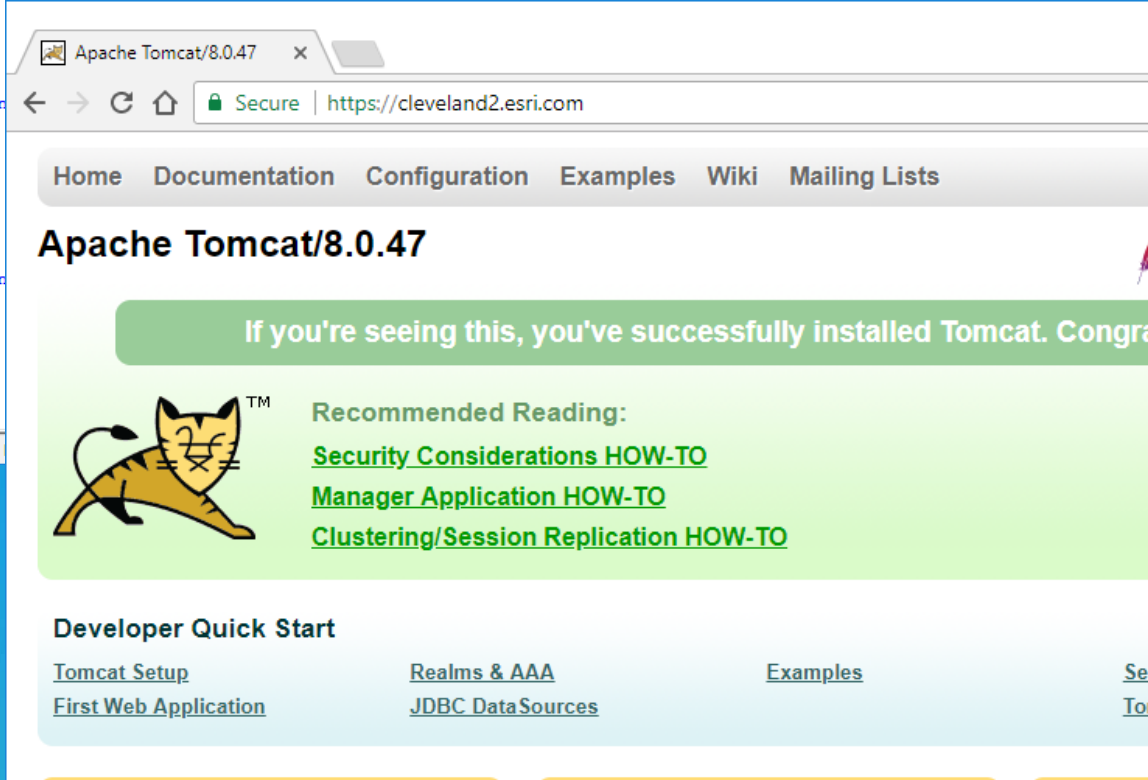
Setting up SSL Certificates and Trusts

SSL-Enable Your Web Server

4. Install and configure signed certificate on your web server




```
*C:\Program Files\Apache Software Foundation\Tomcat 8.0\conf\server.xml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
server.xml
70      connectionTimeout="20000"
71      redirectPort="8443" />
72      <!-- A "Connector" using the shared thread pool-->
73      <!--
74      <Connector executor="tomcatThreadPool"
75      port="80" protocol="HTTP/1.1"
76      connectionTimeout="20000"
77      redirectPort="8443" />
78      -->
79      <!-- Define a SSL/TLS HTTP/1.1 Connector on port 8443
80      This connector uses the NIO implementation that requires the JSSE
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
-->
```



SSL Enable Your Web Server

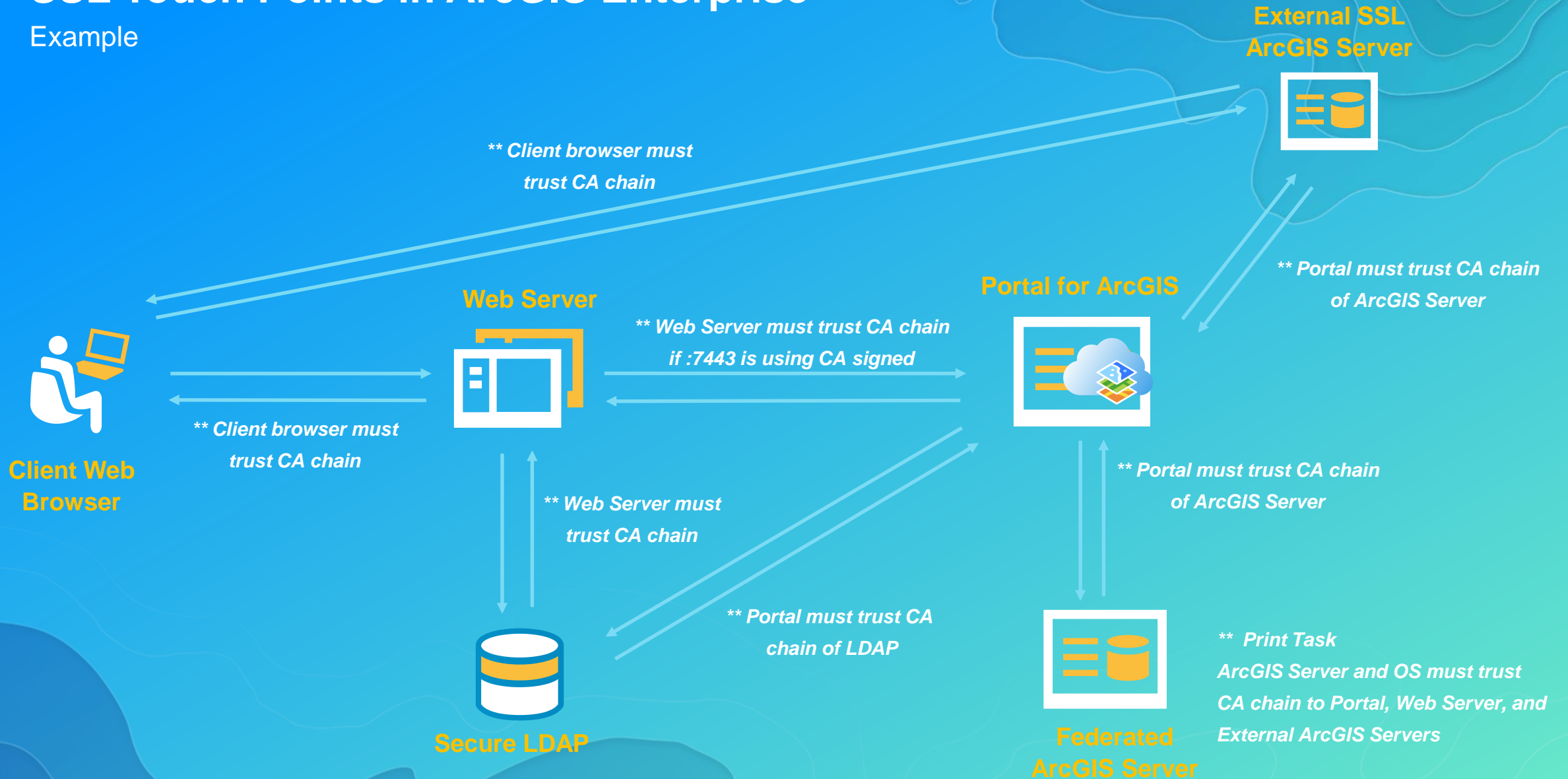
Demonstration

Implementing SSL/TLS within ArcGIS



SSL Touch Points in ArcGIS Enterprise

Example



Setting up SSL Certificates and Trusts

ArcGIS Enterprise - Server Certificates and Trust Stores



- **Portal for ArcGIS, ArcGIS Server, Data Store, GeoEvent and Web AppBuilder Developer Edition all install self-signed certificates to support communication on ports 7443, 6443, 2443, 6143 and 3344 respectively.**
 - *Each of these self-signed certificates can be replaced with CA signed certificates to have completely secure communication*
- **Consuming services from self-signed certificates is untrustworthy and easily compromised.**
 - *Remember Certificate Authorities establish trust!*
- **Additionally disable HTTP communication in Portal and ArcGIS Server**

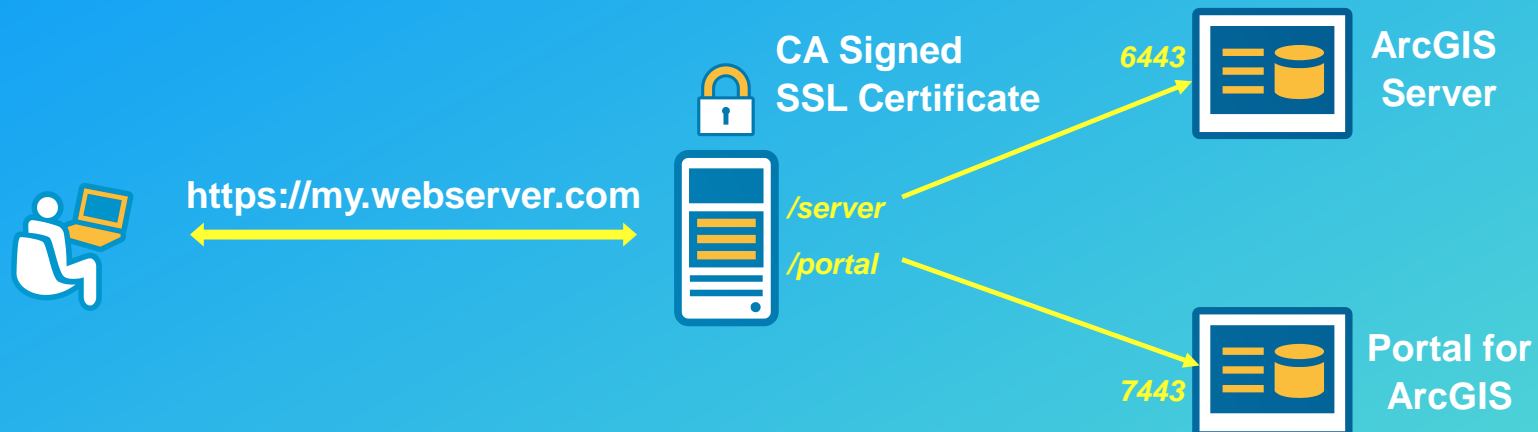
Setting up SSL Certificates and Trusts

Secure Communication Via Web Adaptor



- **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) to 443/80*



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

Setting up SSL Certificates and Trusts

Disable HTTP

- Additionally disable HTTP communication in Portal and ArcGIS Server to use only HTTPS communication
- From the ArcGIS Server admin, and the Portal My Organization settings disable all HTTP communication

The image shows two overlapping screenshots from the ArcGIS environment. The top screenshot is from the ArcGIS Server Administrator Directory, showing the 'Update Security Configuration' page. A warning message states: 'Warning: Changing Protocol will cause the web server to be restarted.' Below this, the 'Security Configuration' section has a 'Protocol:' dropdown menu set to 'HTTP and HTTPS', which is circled in red. The bottom screenshot is from the Portal for ArcGIS 'My Organization' settings, specifically the 'Security' tab. Under the 'Policies' section, the checkbox 'Allow access to the portal through HTTPS only.' is checked and circled in red. Other settings visible include 'Allow anonymous access to your portal.' and a 'Security' icon.

Setting up SSL Certificates and Trusts

Status Review

- *So far we've only covered installing and configuring CA signed certificates on the web tier, and disabling HTTP. Now the replacement of self-signed certificates needs to be completed at the app tier to have fully trusted, and secure communication.*

Updating internal ArcGIS Enterprise Certificates

Portal for ArcGIS

- The Portal Administrator directory provides tools to Import Intermediate or Root certificates and Existing Server Certificates, as well as the ability to generate a new Certificate Signing Request.
 - *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.

Portal Administrator Directory

[Home](#) > [Security](#) > [SSLCertificates](#)

SSL Certificates

- [portal](#)
- [samlcert](#)
- [dstrootca3](#)
- [portalaws](#)
- [letsencrypt](#)

Web Server SSL Certificate: portalAWS

Web Server SSL Protocols: TLSv1.2,TLSv1.1,TLSv1

Web Server SSL Cipher Suites: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA
```

Supported Operations: [Update](#) [Generate](#) [Import Root or Intermediate](#) [Import Existing Server Certificate](#)

Updating internal ArcGIS Enterprise Certificates

Portal for ArcGIS

- **When working in closed environments you must import root and intermediate certificates in addition to the existing server certificate!**
 - *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

Portal Administrator Directory

[Home](#) > [Security](#) > [SSLCertificates](#) > [Import Root or Intermediate Certificate](#)

Import Root or Intermediate Certificate

Warning

Unless selected otherwise, executing this operation will automatically restart the portal. This is necessary for the changes to take effect. This restart will take a couple minutes to complete and cause your portal resources to be temporarily unavailable. To verify that the restart has completed, log in to the Portal Administrator Directory again before continuing.

Alias:

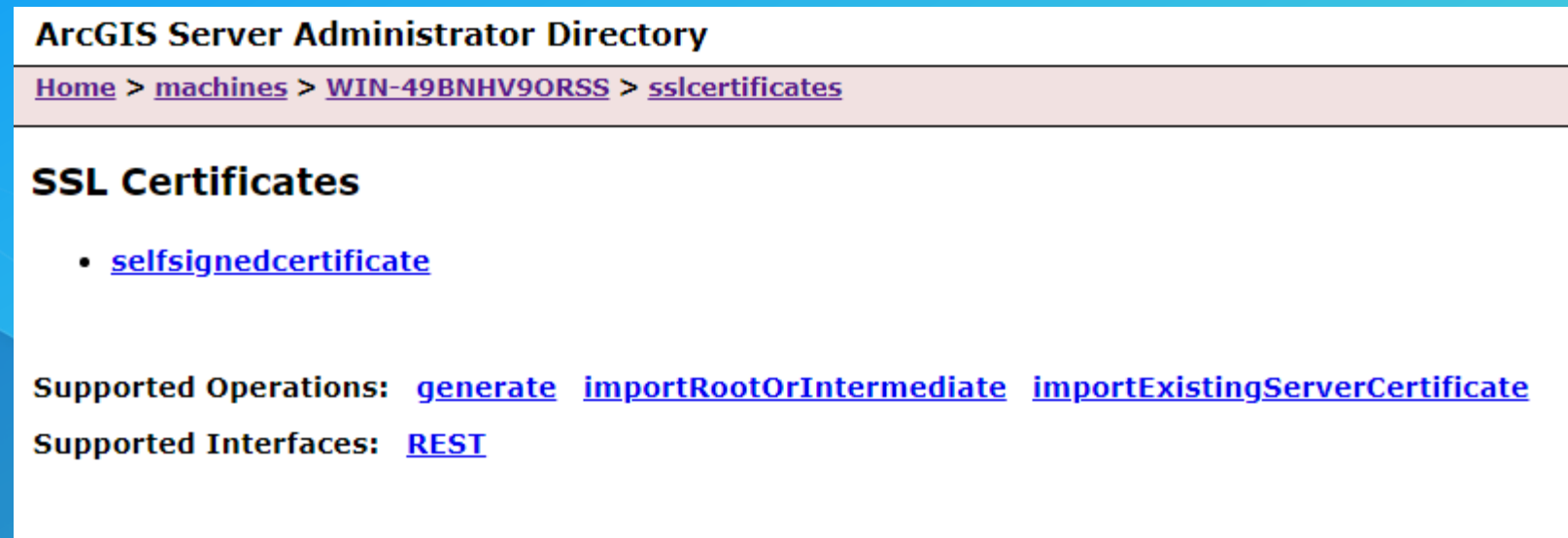
Do not restart the portal after import:

File: No file chosen

Updating internal ArcGIS Enterprise Certificates

ArcGIS Server

- ArcGIS Server Administrator Directory provides nearly identical tools to Portal, including the ability to Import Intermediate or Root certificates and Existing Server Certificates, as well as the ability to generate a new Certificate Signing Request.
- Accessed via Admin – machines – [machine name] – sslcertificates.



The screenshot displays the ArcGIS Server Administrator Directory interface. At the top, the title "ArcGIS Server Administrator Directory" is shown. Below it is a breadcrumb trail: "Home > machines > WIN-49BNHV9ORSS > sslcertificates". The main heading is "SSL Certificates". Underneath, there is a single bullet point: "selfsignedcertificate". At the bottom, the "Supported Operations" are listed as "generate", "importRootOrIntermediate", and "importExistingServerCertificate". The "Supported Interfaces" are listed as "REST".

Updating internal ArcGIS Enterprise Certificates

ArcGIS Server

- Import appropriate certificates, browse back to [machine name] and then Update.
- When working in closed environments you must import root and intermediate certificates in addition to the existing server certificate!
 - Hybrid environments using signed certificates from known CA's may not need this step (e.g. CA is DigiCert)
- *No ArcGIS Server service restart required...ArcGIS Server does this automatically.

ArcGIS Server Administrator Directory

[Home](#) > [machines](#) > [WIN-49BNHV9ORSS](#)

Machine - WIN-49BNHV9ORSS

Server Machine Properties

Name:	WIN-49BNHV9ORSS
Admin URL:	https://wdcintelgis.esri.com:6443
Platform:	Windows Server 2012 R2-amd64-
Server Start Time:	2018-01-29T21:04:40,763
Web server maximum heap size (in MB):	-1
Web server SSL Enabled :	true
Web server SSL Certificate:	SelfSignedCertificate
App server maximum heap size (in MB):	256
SOC maximum heap size (in MB):	64
Synchronize:	false

+ [Ports](#)

Resources: [status](#) [sslcertificates](#)

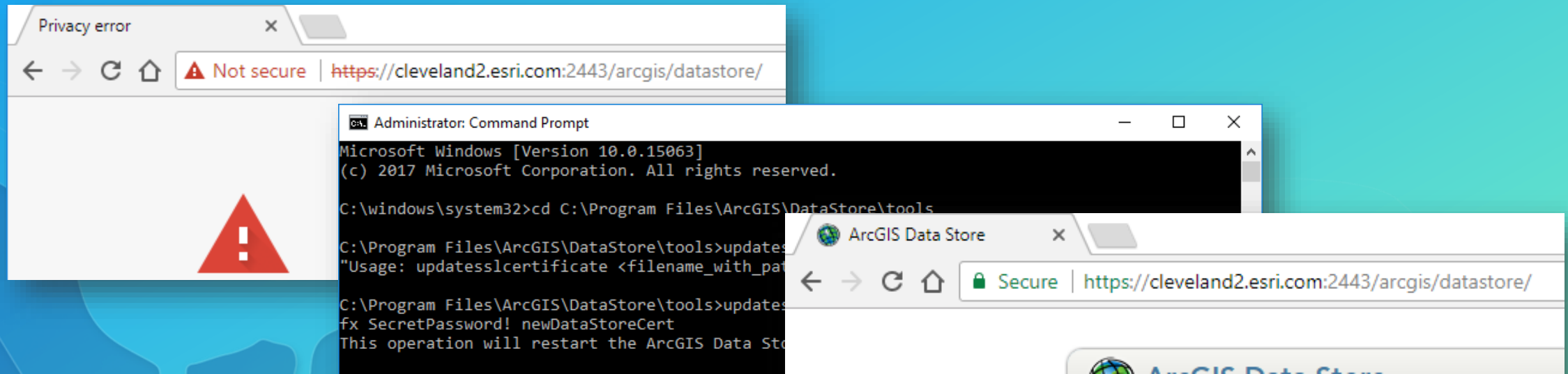
Supported Operations: [edit](#) [start](#) [stop](#) [unregister](#) [synchron](#)

Supported Interfaces: [REST](#)

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

Demonstration

Portal Administrator Directory Logged in as : Administrator | [Logout](#)
[Home](#) > [Security](#) > [SSLCertificates](#) [API Reference](#)

SSL Certificates

- [portal](#)
- [samIcert](#)

Web Server SSL Certificate: portal

Web Server SSL Protocols: TLSv1.2,TLSv1.1,TLSv1

Web Server SSL Cipher Suites: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,

ArcGIS Server Administrator Directory

Logged in: siteadmin [Administrator] | [Signout](#)

[Home](#) > [machines](#) > [CLEVELAND2.ESRI.COM](#) > [sslcertificates](#) [API Reference](#)

SSL Certificates

- [selfsignedcertificate](#)

Supported Operations: [generate](#) [importRootOrIntermediate](#) [importExistingServerCertificate](#)

Supported Interfaces: [REST](#)

Supported Op

Supported Int

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\windows\system32>cd C:\Program Files\ArcGIS\DataStore\tools

C:\Program Files\ArcGIS\DataStore\tools>updatesslcertificate.bat
"Usage: updatesslcertificate <filename_with_path> <password> <alias>"

C:\Program Files\ArcGIS\DataStore\tools>updatesslcertificate.bat C:\Temp\MySe
fx SecretPassword! newDataStoreCert
This operation will restart the ArcGIS Data Store web server.

Do you wish to continue (Yes or No)?Yes
```

Establishing Trust to external resources

Importing Root and Intermediate Certificates

- **In order to consume services from other SSL enabled web servers, proper trust must be created in ArcGIS Server and Portal.**
- **Importing Root and Intermediate certificates for external server certificates allows ArcGIS Server and Portal to trust the server SSL certificate being presented**
 - This trust establishes proper encryption channel
- **Example scenarios:**
 - Adding an HTTPS Map Service to Portal from an external organization.
 - Using ArcGIS Server Print Service to generate thumbnails for Portal for ArcGIS, 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

Portal Administrator Directory Logged in as : crai6422@AVWORLD | [Logout](#)

[Home](#) > [Security](#) > [SSLCertificates](#) [API Reference](#)

SSL Certificates

- [portal](#)
- [ccleveland3](#)
- [samcert](#)
- [esricaroot](#)

Web Server SSL Certificate: ccleveland3

Web Server SSL Protocols: TLSv1.2,TLSv1.1,TLSv1

Web Server SSL Cipher Suites:


Supported Operations: [Update](#) [Generate](#) [Import Root or Intermediate](#) [Import Existing Server Certificate](#)

Supported Interfaces: [REST](#)

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).



ArcGIS Server Administrator Directory Logged in: siteadmin [Administ

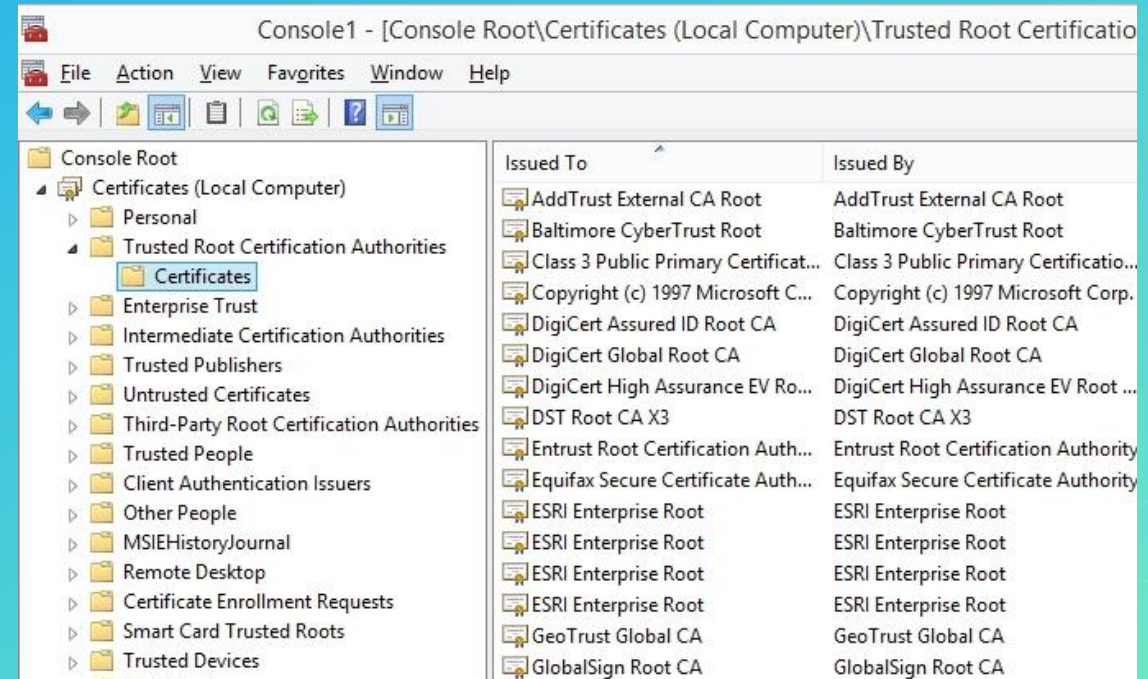
[Home](#) > [machines](#) > [CCLEVELAND3.ESRI.COM](#) > [sslcertificates](#)

SSL Certificates

- [esriroot](#)
- [ccleveland3](#)
- [selfsignedcertificate](#)

Supported Operations: [generate](#) [importRootOrIntermediate](#) [importExistingServerCertificate](#)

Supported Interfaces: [REST](#)



Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification

File Action View Favorites Window Help

Console Root

- Certificates (Local Computer)
 - Personal
 - Trusted Root Certification Authorities
 - Certificates
 - Enterprise Trust
 - Intermediate Certification Authorities
 - Trusted Publishers
 - Untrusted Certificates
 - Third-Party Root Certification Authorities
 - Trusted People
 - Client Authentication Issuers
 - Other People
 - MSIEHistoryJournal
 - Remote Desktop
 - Certificate Enrollment Requests
 - Smart Card Trusted Roots
 - Trusted Devices

Issued To	Issued By
AddTrust External CA Root	AddTrust External CA Root
Baltimore CyberTrust Root	Baltimore CyberTrust Root
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA
DigiCert Global Root CA	DigiCert Global Root CA
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...
DST Root CA X3	DST Root CA X3
Entrust Root Certification Auth...	Entrust Root Certification Authority
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority
ESRI Enterprise Root	ESRI Enterprise Root
ESRI Enterprise Root	ESRI Enterprise Root
ESRI Enterprise Root	ESRI Enterprise Root
ESRI Enterprise Root	ESRI Enterprise Root
ESRI Enterprise Root	ESRI Enterprise Root
GeoTrust Global CA	GeoTrust Global CA
GlobalSign Root CA	GlobalSign Root CA

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.

Portal Administrator Directory

[Home](#) > [Security](#) > [SSLCertificates](#)

SSL Certificates

- [portal](#)
- [ccleveland3](#)
- [samlcert](#)
- [esricaroot](#)

Web Server SSL Certificate: ccleveland3

Web Server SSL Protocols: TLSv1.2,TLSv1.1,TLSv1

Web Server SSL Cipher Suites:

ArcGIS Server Administrator Directory

[Home](#) > [security](#) > [config](#)

Security Configuration

Configuration Properties

Protocol:	HTTP And HTTPS
SSL Protocols:	
SSL Cipher Suites:	
Security for virtual directories enabled:	false
Authentication tier:	ARCGIS_PORTAL+
Authentication mode:	ARCGIS_PORTAL_TOKEN

Importing Certificates into Portal

Demonstration

Portal Administrator Directory Logged in as : Administrator | [Logout](#)

[Home](#) > [Security](#) > [SSL Certificates](#) [API Reference](#)

SSL Certificates

- [portal](#)
- [samcert](#)

Web Server SSL Certificate: portal

Web Server SSL Protocols: TLSv1.2,TLSv1.1,TLSv1

Web Server SSL Cipher Suites: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA

Supported Operations: [Update](#) [Generate](#) [Import Root or Intermediate](#) [Import Existing Server Certificate](#)

Supported Interfaces: [REST](#)

Common SSL Problems

The background features a teal-to-blue gradient with abstract, wavy, layered shapes in shades of purple and teal at the bottom. A faint topographic map overlay is visible in the upper right quadrant.

Missing SAN

Subject Alternative Name

- Recent releases of Chrome have enforced the need for a subject alternative name
- Must be included with your CSR

Privacy error x

Not secure | <https://portaldevsummit.esri.com>

Microsoft Active Directory Certificate Services -- ESRI Enterprise Root

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN NEW CERTIFICATE REQUEST-----  
MIIC4DCCAcgCAQAwazELMAkGA1UEBhMCVVMxCz.  
EwZlWlVubmExDTALBgNVBAoTBEVzcmkxDDAKBgl  
cG9ydGFsZGV2c3VtbWl0LmVzcmkuY29tMIIBIj.  
MIIBCgKCAQEAl19yL6Gxp47VnM4x8C0QBwd5XXI  
c2A6YXf+TKmwhk6Z7Mz/uDH0FFSK74uIGpca51
```

Certificate Template:

Web Server

Additional Attributes:

Attributes: san:dns=portaldevsummit.esri.co

Submit >

This page does not have an SSL certificate. This may be an attacker intercepting your connection.

Proceed to portaldevsummit.esri.com (unsafe).

How do you know you have an SSL Problem?

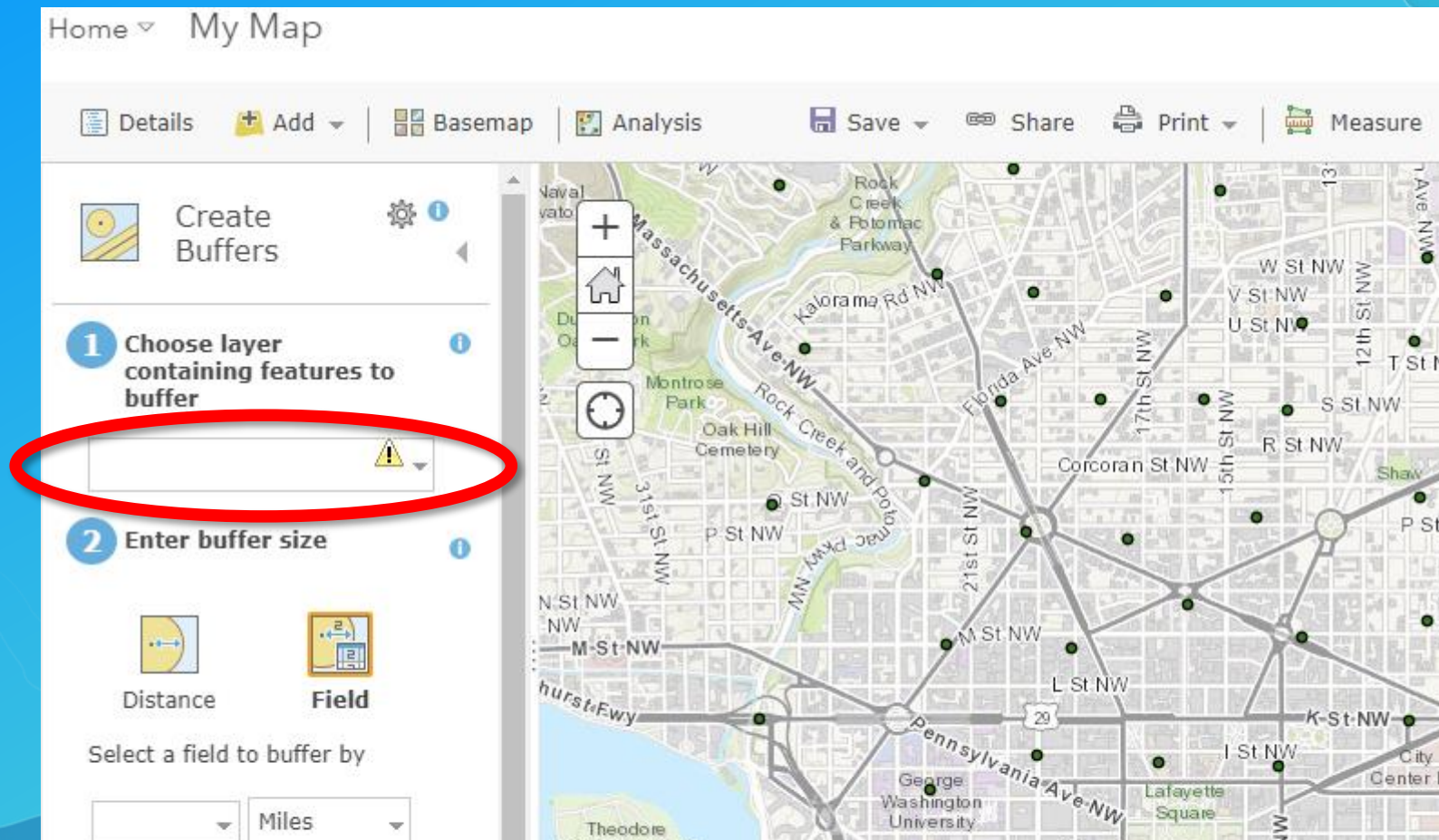
Log Analysis

SEVERE	URL 'https://techtxssl.esri.com:6443/arcgis/admin/services/Utilities/PrintingTools.GPServer/start' is not accessible: Error. java.security.cert.CertificateException: No subject alternative DNS name matching techtxssl.esri.com found..	2018-03-04T04:11:21,21	Sharing
SEVERE	URL 'https://techtxssl.esri.com:6443/arcgis/admin/services/Utilities/GeocodingTools.GPServer/start' is not accessible: Error. java.security.cert.CertificateException: No subject alternative DNS name matching techtxssl.esri.com found..	2018-03-04T04:11:20,990	Sharing
SEVERE	URL 'https://[REDACTED]/host/rest/services/Hosted/GII_Cert_Testing/FeatureServer/0?f=json' is not accessible: Error. sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target.	2018-03-04T05:15:10,69	Sharing
SEVERE	Invalid SSL certificate found. PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target	2018-03-04T05:15:10,68	Sharing

Unable to perform analysis

Missing trust chain in portaladmin

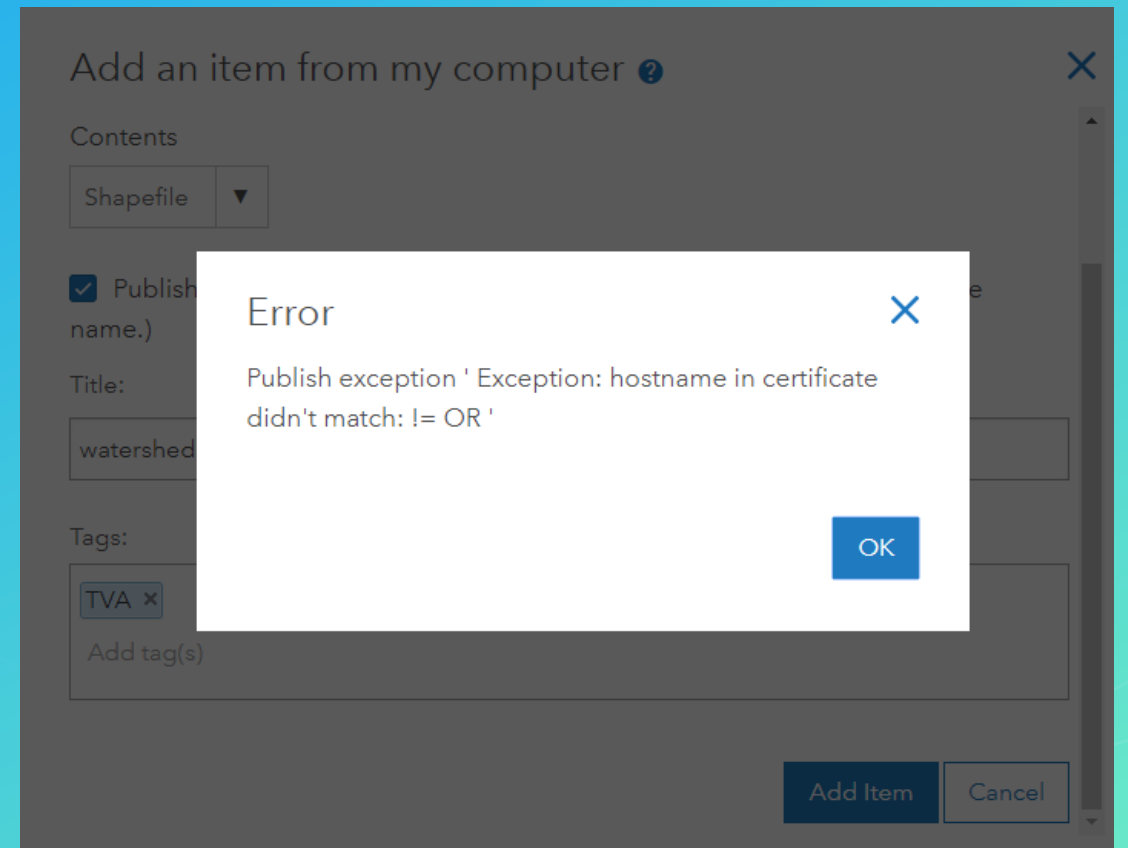
- Add trust chain to portaladmin endpoint



Federation issues when using DNS aliases

URL Name Mismatch

- ArcGIS Enterprise creates self-signed certificates
- Federation with a DNS alias will succeed but...
 - you will get errors later
- Make sure Admin URL used in Federation matches Certificate Name (or SAN)



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...*



esri

THE
SCIENCE
OF
WHERE