ArcGIS Enterprise:
Security
Gerhard Trichtl
Markus Schlager
ESRI EUROPEAN DEVELOPER SUMMIT
Focus of this session

Security best practices for ArcGIS Enterprise

- ArcGIS Server
- Portal for ArcGIS
- Everything around SSL
- Advanced Options

Strongly Recommended:
Knowledge of ArcGIS Server and Portal for ArcGIS
Security?
Markus Schlager
History of Data Breaches

Interactive version: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Credit: Microsoft, 2018
Global Data Volume

Annual Size of the Global DataspHERE

Source: Data Age 2025, sponsored by Seagate with data from IDC Global DataSphere, Nov 2018
Defense In Depth Paradigm

- Security plans have many “layers” – multiple levels of security
- Each feature discussed is considered a “layer”

“The intention is to create a reliable system using the multiple layers, rather than making any one layer perfectly reliable.”

Non-technical layers

- Physical Security
- Social Engineering
- Phishing

Source: https://xkcd.com/1694/
Authentication/Authorization

Gerhard Trichtl
No focus on ArcGIS Sharing Model

Talk to us at the ArcGIS Enterprise booth!
Authentication vs. Authorization

- Authentication – Who I’m
- Authorization – Where did I have access
Authentication Methods

- Username and Passwort (ensure those are transfered via https)
- WebTier-Authentication with SSO
- Multifactor Authentication – having several steps to authentication – higher security
ArcGIS Online with MFA
Make your ArcGIS Online Organization Ready for MFA

- Organization - Security

Multifactor Authentication

Multifactor authentication provides all members with ArcGIS accounts in your organization with an extra level of security by requesting an additional verification code at the time of login.

- Allow members to choose whether to set up multifactor authentication for their individual accounts.

Add at least two administrators from the list at left to the Designated Administrators list at the right to enable multifactor authentication. Designated Administrators receive requests to troubleshoot members’ multifactor authentication issues. Click Save on this page to confirm this action.

Click a name to add.

Administrator

Click a name to remove.

Designated Administrators
Within your profile activate MFA

- Edit your Profile and enable Multifactor Authentication
Configure Multifactor Authentication

Follow these steps to add an extra level of security to your account. Once you’re finished, you’ll be asked for additional security information each time you sign in to your account from any computer or device.

Install a supported authenticator app on your device

- Google
  - Google Authenticator
- iOS
  - Google Authenticator
- Windows
  - Authenticator

Use the app to scan this QR code

Can’t scan the code?

Cancel  Back  Next
Everything around SSL

Markus Schlager
Common Problems

Browser Behavior
Common Problems

Unable to perform analysis
Fundamentals of Secure Communication

• **SSL = Secure Socket Layer**
  - Standard security technology
  - Establish an *encrypted link* between a *web server* and a *client*
  - Current most common SSL version → TLS v1.2

• **CA = Certificate Authority**
  - Certificates prove the identity of a client or a server
  - CAs establish trust by digitally *signing certificates* for servers or clients

• Public key/private key pairing for encrypted communication → **Public Key Infrastructure**
Fundamentals of Secure Communication
Certificate Authority (Root of Trust)

Trust, Encrypt, Communicate
Fundamentals of Secure Communication

Intermediate Certificate Authority (Signing Chain)

Root Certificate Authority (CA)

Intermediate Certificate Authority (CA)

Server Trusts Root CA Certificate

Server

Certiﬁcate

Server Trusts Intermediate Certificate

Clients Trust Root CA Certificate

Clients

Certiﬁcate

Trust, Encrypt, Communicate
Fundamentals of Secure Communication

Establishing Trust for Encrypted Communication

Certificate Authority (CA)

CA Issues Certificate

Clients Trust Root Certificate

Trusted & Encrypted Connection

Server

Clients

Trust, Encrypt, Communicate
Fundamentals of Secure Communication

Certificate Revocation

What if a trusted server is compromised?

The server's security certificate is revoked!

You attempted to reach [redacted] using [redacted] 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
Fundamentals of Secure Communication

Trust Stores and your OS

• 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 your Browser

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

- Firefox has its own trust store
  - Managed separately!
Fundamentals of Secure Communication

Trust Stores and your Web Server

• If you use Web Adaptor, you also use a Web Server
  - IIS
  - Apache Tomcat

• Portal and ArcGIS Server have a built-in Web Server

• Usually some configuration is needed for HTTPS in your Web Server
Setting up SSL Certificates and Trusts

1. Create certificate signing request (CSR)
   - CSRs can be created in many ways: Web Server, 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
   - IIS and ArcGIS Enterprise automatically create a keystore
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).
Common Problems

Browser Behavior

Your connection is not private

Attacks might be trying to steal your information from devsummitssl.dev.geocloud.com (for example, passwords, messages, or credit cards).

Learn more

This server could not prove that it is devsummitssl.dev.geocloud.com. Its security certificate does not specify Subject Alternative Names. This may be caused by a misconfiguration or an attacker intercepting your connection.
Setting up SSL Certificates and Trusts

SSL-Enable Your Web Server

3. Download signed certificate

![Certificate Issue Dialog]

The certificate you requested was issued to you.

- DER encoded
- 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
SSL Touch Points in ArcGIS Enterprise

Example

**Client browser must trust CA chain**

**Web Server**

**Client Web Browser**

**Web Server must trust CA chain**

if :7443 is using CA signed

**Portal must trust CA chain of ArcGIS Server**

**Portal must trust CA chain of ArcGIS Server**

**Portal must trust CA chain**

of LDAP

**Print Task**

ArcGIS Server and OS must trust CA chain to portal, Web Server, and External ArcGIS Servers
Secure communication via ArcGIS Web Adaptor

- Internal self-signed certificates
- 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
Internal Ports and Self-Signed Certificates

• Since 10.7 - Portal for ArcGIS and ArcGIS Server are “HTTPS Only” by default!

• Self-signed certificates are installed during the setup to support communication:
  - Portal for ArcGIS – port 7443
  - ArcGIS Server – port 6443
  - ArcGIS Data Store – port 2443
  - Other components: GeoEvent (6143), Web AppBuilder Developer Edition (3344), Notebook Server (11443), etc.

• Each of these self-signed certificates can be replaced with CA signed certificates to have completely secure communication
  - Remember Certificate Authorities establish trust!
Updating internal ArcGIS Enterprise Certificates

Portal for ArcGIS

- Accessed via Portaladmin > Security > SSLCertificates
- Used for:
  - Updating internal ArcGIS Enterprise certificates
  - Establishing trust chains with external servers
- Tools to:
  - Generate a new Certificate Signing Request.
  - Import Existing Server Certificates
  - Import Root or Intermediate certificates
- Import appropriate certificates and then Update
Updating internal ArcGIS Enterprise Certificates
Portal for ArcGIS

- In closed environments with internal CAs 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)

- Since 10.6 – option **not** to restart the portal service directly after importing root or intermediate certificates
Updating internal ArcGIS Enterprise Certificates

ArcGIS Server

- Similar to Portal for ArcGIS
- Accessed via Serveradmin > Machines > [Machine Name] > SSLCertificates
- Tools to:
  - Generate a new Certificate Signing Request.
  - Import Existing Server Certificates
  - Import Root or Intermediate certificates
Updating internal ArcGIS Enterprise Certificates
ArcGIS Server

- Import appropriate certificates, browse back to [machine name] and then Edit

- In closed environments with internal CAs 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
Updating internal ArcGIS Enterprise Certificates

ArcGIS Data Store

- ArcGIS Data Store ships with a number of batch files for managing its properties
  - Accessed at C:\Program Files\ArcGIS\DataStore\tools
  - updatesslcertificate.bat

- 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
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 for ArcGIS

- Importing Root and Intermediate certificates for external server certificates create this trust to 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

- Use Portal Administrator directory to import Root and Intermediate certificates

- Let Portal for ArcGIS restart after the last certificate
Common Problems

Unable to perform analysis
Establishing Trust to external resources

ArcGIS Server

- Use the Server Administrator Directory to import Root and Intermediate certificates

- On the Server-machine, also import Root and Intermediate certificates into the OS Trust Store (needed for GP Services)
Additional SSL Considerations
Restrict SSL protocols and cipher suites

- Within ArcGIS Enterprise you can specify
  - which SSL protocols and encryption algorithms to use
  - Toggle HSTS
Import SSL Certificates in AGOL?
Trust in AGOL for custom CAs

- Adding ArcGIS Server service URLs as items coming from custom CA SSL end points in AGOL can cause problems
- AGOL supports registering SSL certificates with your Organization
- Only REST API calls supported; no UI experience at the moment

- 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)
„Security“ around Products
ArcGIS Enterprise: Behind the scenes

- Includes 3 components: Portal for ArcGIS – ArcGIS Server – ArcGIS Data Store
“Security” around Products

- **ArcGIS Server**
  - Enable and use HTTPS
  - Disable services directory
  - Restrict cross domain requests
  - Restrict System folder permissions
  - Disable PSA account
  - Scan Server script

- **Portal for ArcGIS**

- **Additional Information**
Review: ArcGIS Server Administrator Directory

https://localhost:6443/arcgis/admin

- Web App, provides interface into an ArcGIS Server site
- Many security settings enabled via this interface
Enable and Use HTTPS

- HTTPS – *Hypertext Transfer Protocol Secure*
- Initial step in creating a secure environment should always be to encrypt traffic
- Protects against a simple network sniffer
- Enabled by default in 10.4+
- Recommended to restrict to HTTPS only if possible
- ArcGIS Server Admin Directory
  - Security > config > update

Update Security Configuration

![Update Security Configuration](image)

Warning

Once this operation completes, ArcGIS Server may be restarted. During this time, your ArcGIS Server resources will be temporarily in the ArcGIS Server Administrator Directory.

Protocol: HTTPS Only

SSL Protocols: TLSv1.2

SSL Cipher Suites:

HTTP Strict Transport Security (HSTS) enabled: [ ]
Disable the Services Directory

- ArcGIS REST Services Directory exposes web services api in HTML format
  - [https://server.mydomain.com/arcgis/rest](https://server.mydomain.com/arcgis/rest)
- Recommended NOT to expose REST services directory on Production Servers

**Before**

<table>
<thead>
<tr>
<th>ArcGIS REST Services Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home &gt; services</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Folder: /</td>
</tr>
<tr>
<td>Current Version: 10.71</td>
</tr>
<tr>
<td>View Footprints In: <a href="https://server.mydomain.com/arcgis/rest">ArcGIS Online Map Viewer</a></td>
</tr>
<tr>
<td>Folders:</td>
</tr>
<tr>
<td>- Hosted</td>
</tr>
<tr>
<td>- System</td>
</tr>
<tr>
<td>- Utilities</td>
</tr>
<tr>
<td>Services:</td>
</tr>
<tr>
<td>- <a href="https://server.mydomain.com/arcgis/rest">SampleWorldCities</a> (MapServer)</td>
</tr>
</tbody>
</table>

**After**

<table>
<thead>
<tr>
<th>ArcGIS REST Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
</tr>
</tbody>
</table>

**Error:** Services Directory has been disabled.  
**Code:** 403
How to Disable the Services Directory

- **Server Administrator Directory**
  - System > Handlers > Rest > Servicesdirectory > edit
  - Uncheck *Services Directory Enabled* option

- **Help topic:** Disable the Services Directory

---

**ArcGIS Server Administrator Directory**

**Services Directory**

- Services Directory: Enabled
- AllowedOrigins: *
- Javascript API URL: https://js.arcgis.com/4.10/
- Javascript API CSS URL: https://js.arcgis.com/4.10/esri/css/main.css
- ArcGIS.com Map Text: ArcGIS Online Map Viewer
- ArcGIS.com URL: http://www.arcgis.com/home/webmap/viewer.html

**Edit Services Directory**

- Services Directory Enabled: **✓**
Restrict Cross-Domain (CORS) Requests

enterprise.arcgis.com > Search “cross-domain requests”

- **For JavaScript** applications, a common method used to make cross domain requests is called a CORS request (cross origin resource sharing)
- Required when making POST requests to Feature or GP services on a different server
How to Restrict Cross-Domain Requests

• By default, ArcGIS Server allows all cross-domain requests
• These can be restricted in the Server Administrator Directory
  - system > handlers > rest > servicesdirectory > edit
  - AllowedOrigins - specify a comma-separated list of domain names that are allowed to make CORS requests to access your web services
• Does NOT restrict overall access to the web services

<table>
<thead>
<tr>
<th>ArcGIS Server Administrator Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Home</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Services Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services Directory: Disabled.</td>
</tr>
<tr>
<td>Javascript API URL:</td>
</tr>
<tr>
<td>Javascript API CSS URL:</td>
</tr>
</tbody>
</table>
Restrict System Folder Permissions in Manager

- Verify System folder permissions are limited to Administrators and Publishers only
  - Prevents potential Denial of Service due to resource consumption, service deletion, etc.
  - Usually changed from default when troubleshooting
Disable Primary Site Administrator (PSA) Account

- Recommend disable the PSA account to remove an alternate method of administering ArcGIS Server outside of your enterprise users
- Access the Server Administrator Directory
  - Security > PSA > disable

ArcGIS Server Administrator Directory

Primary Site Administrator Account
Manage the primary site administrator account.
Disabled: false

Supported Operations: update, enable, disable
Supported Interfaces: REST
Scan GIS Server for Security Checks

- serverScan.py is a script in the Server installation directory
  - Located: \<install directory>\ArcGIS\Server\tools\admin
- Script checks for security settings → generates a report that makes recommendations to improve security

<table>
<thead>
<tr>
<th>Id</th>
<th>Severity</th>
<th>Property Tested</th>
<th>Scan Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS02</td>
<td>Critical</td>
<td>Standardized queries</td>
<td>Enforcing standardized queries is disabled. To provide protection against SQL injection attacks, it is critical that this option be enabled. <a href="#">More information</a></td>
</tr>
<tr>
<td>SS09</td>
<td>Important</td>
<td>Dynamic workspace</td>
<td>Map service: SampleWorldCities. One or more dynamic workspaces are registered with this map service. To prevent a malicious party from obtaining the workspace ID and potentially gaining access, these dynamic workspaces should be removed. <a href="#">More information</a></td>
</tr>
<tr>
<td>SS07</td>
<td>Important</td>
<td>Rest services directory</td>
<td>The Rest services directory is accessible through a web browser. Unless being actively used to search for and find services by users, this should be disabled to reduce the chance that your services can be browsed, found in a web search, or queried through HTML forms. This also provides further protection against cross-site scripting (XSS) attacks. <a href="#">More information</a></td>
</tr>
<tr>
<td>SS12</td>
<td>Recommended</td>
<td>Feature service operations</td>
<td>Feature service: Hosted/Airports. This feature service has the update and/or delete operations enabled and is open to anonymous access. This allows the feature service data to be changed and/or deleted without authentication. <a href="#">More information</a></td>
</tr>
<tr>
<td>SS11</td>
<td>Recommended</td>
<td>PSA account status</td>
<td>The primary site administrator account is enabled. It is recommended that you disable this account to ensure that there is not another way to administer ArcGIS Server other than the group or role that has been specified in your configuration. <a href="#">More information</a></td>
</tr>
</tbody>
</table>
### Potential security items to review

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Property</th>
<th>Scan Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS08</td>
<td>Important</td>
<td>Cross-domain requests</td>
<td>Cross-domain requests are unrestricted. To reduce the possibility of an unknown application sending malicious commands to your web services, it is recommended to restrict the use of your services to applications hosted only in domains that you trust. <a href="#">More information</a></td>
</tr>
<tr>
<td>SS07</td>
<td>Important</td>
<td>Rest services directory</td>
<td>The Rest services directory is accessible through a web browser. Unless being actively used to search for and find services by users, this should be disabled to reduce the chance that your services can be browsed, found in a web search, or queried through HTML forms. This also provides further protection against cross-site scripting (XSS) attacks. <a href="#">More information</a></td>
</tr>
<tr>
<td>SS11</td>
<td>Recommended</td>
<td>PSA</td>
<td>The primary site administrator account is enabled. It is</td>
</tr>
</tbody>
</table>
ServerScan.py

ArcGIS Server Security Scan Report - 11/02/19

REDLANDS (10.8)

Potential security items to review

<table>
<thead>
<tr>
<th>Id</th>
<th>Severity</th>
<th>Property Tested</th>
<th>Scan Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS08</td>
<td>Important</td>
<td>Cross-domain requests</td>
<td>Cross-domain requests are unrestricted. To reduce the possibility of an unknown application sending malicious commands to your web services, it is recommended to restrict the use of your services to applications hosted only in domains that you trust. <a href="#">More information</a></td>
</tr>
<tr>
<td>SS07</td>
<td>Important</td>
<td>Rest services directory</td>
<td>The Rest services directory is accessible through a web browser. Unless being actively used to search for and find services by users, this should be disabled to reduce the chance that your services can be browsed, found in a web search, or queried through HTML forms. This also provides further protection against cross-site scripting (XSS) attacks. <a href="#">More information</a></td>
</tr>
<tr>
<td>SS11</td>
<td>Recommended</td>
<td>PSA account status</td>
<td>The primary site administrator account is enabled. It is recommended that you disable this account to ensure that there is not another way to administer ArcGIS Server other than the group or role that has been specified in your configuration. <a href="#">More information</a></td>
</tr>
</tbody>
</table>
“Security” around Products

- **ArcGIS Server**
- **Portal for ArcGIS**
  - Enforce HTTPS Communication only
  - Disable ArcGIS Portal Directory (aka Sharing API)
  - Restrict proxies
  - Disable the ‘Create An Account’ button on the sign-in page
  - Restrict cross-domain (CORS) requests
  - Trusted servers list
  - Scan Portal script
- **Additional Information**
Enable HTTPS Communication

- Enforce HTTPS so that all communication in your portal is sent using HTTPS
- Configure your portal and the web server hosting ArcGIS Web Adaptor to only allow communication through HTTPS
- Default since 10.7
Disable ArcGIS Portal Directory (Production Servers)

Ex. https://portal.mydomain.com/arcgis/sharing/rest

- Provides an HTML-based representation of all of Portal items
  - services, web maps, and content
- Recommend disable this to reduce the chance that your items can be browsed, found in a web search, or queried through HTML forms
How to Disable ArcGIS Portal Directory

- Access the Portal Administrator Directory
  - Security > Config > Update Security Configuration
  - Set “disableServicesDirectory” = true
Restrict Machines Accessible by Portal

- Portal ships with a built-in proxy server that is used in some scenarios to access resources on different machines
  - Storing credentials (Single Sign On)
  - OGC Services
  - Non-CORS Systems
Restrict Machines Accessible by Portal

- Portal ships with a built-in proxy server that is used in some scenarios to access resources on different machines
- By default the portal's proxy is open
  - Your Portal can be used to launch attacks against internal and external targets
How to Restrict Proxies

• Access the Portal Administrator Directory
  - Security > Config > Update Security Configuration
  - Add “allowedProxyHosts” property and specify the list of approved hostnames
Disable ‘Create An Account’ on Sign In Page

- Disable the ability to create a new built-in Portal account
- My Organization > Edit settings > Security
Restrict Cross-Domain (CORS) Requests

- Limits external JavaScript applications making CORS requests to Portal items
- Does NOT restrict overall access to Portal items
Trusted Servers

- A list of servers to where web-tier credentials will be included when a web map or app makes a CORS request to a secured resource
Trusted Servers

- Proxy request from Portal cannot be used to access GIS services secured with web-tier authentication
- A cross-domain request from the browser with credentials is required
Allow Portal Access

- Needed to access layer from other Portals that use SAML authentication
SAML Access to any ArcGIS Enterprise
Bring secured services together from anywhere!
Scan Portal for Security Checks

- portalScan.py is a script in the Portal installation directory
  - Location: `<install_directory>\ArcGIS\Portal\tools\security`
- When you run the script, it checks for security settings → generates a report that makes recommendations to improve security

<table>
<thead>
<tr>
<th>Id</th>
<th>Severity</th>
<th>Property Tested</th>
<th>Scan Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS01</td>
<td>Critical</td>
<td>Proxy restrictions</td>
<td>The portal proxy capability is unrestricted. This should be limited to trusted web addresses. More information</td>
</tr>
<tr>
<td>PS03</td>
<td>Important</td>
<td>Portal services</td>
<td>The portal services directory is accessible through a web browser. This should be disabled to reduce the chances that your portal items, services, web maps, groups, and other resources can be browsed, found in a web search, or queried through HTML forms. More information</td>
</tr>
<tr>
<td>PS04</td>
<td>Important</td>
<td>Web communication</td>
<td>To prevent the interception of any communication within the portal, it is recommended that you configure your portal and the web server hosting the Web Adaptor to enforce HTTPS. More information</td>
</tr>
<tr>
<td>PS06</td>
<td>Recommended</td>
<td>Anonymous access</td>
<td>To prevent any user from accessing the Home application without first providing credentials to the portal, it is recommended that you configure your portal to disable anonymous access. More information</td>
</tr>
<tr>
<td>PS05</td>
<td>Recommended</td>
<td>Built-in account</td>
<td>By default, users can click the Create An Account button on the portal sign-up page to create a built-in portal account. If you are using enterprise accounts or you want to create all accounts manually, this option should be disabled. More information</td>
</tr>
<tr>
<td>PS09</td>
<td>Recommended</td>
<td>Cross-domain requests</td>
<td>Cross-domain (CORS) requests are unrestricted. To reduce the possibility of an unknown application accessing a shared portal item, it is recommended to restrict cross-domain requests to applications hosted only in domains that you trust. More information</td>
</tr>
</tbody>
</table>
“Security” around Products

- **ArcGIS Server**
- **Portal for ArcGIS**
  - Enforce HTTPS Communication only
  - Disable ArcGIS Portal Directory (aka Sharing API)
  - Restrict proxies
  - Disable the ‘Create An Account’ button on the sign-in page
  - Restrict cross-domain (CORS) requests
  - Trusted servers list
  - Scan Portal script
- **Additional Information**
Additional Infos
Check for Updates / Patch Notification

ArcGIS Enterprise Patch Notification

Installed Components

- Portal for ArcGIS 10.5.1

Available Updates

- Portal for ArcGIS
- Portal for ArcGIS 10.5.1 Custom Basemap Extent Patch
  - Products: Portal for ArcGIS
  - Release Date: 08/03/2017
- Portal for ArcGIS Security 2018 Update 1 Patch
  - Products: Portal for ArcGIS
  - Release Date: 02/14/2018
- ArcGIS Security Update for Flexera CVE-2016-10395 patch
  - Products: ArcGIS Server, Portal for ArcGIS
  - Release Date: 08/02/2017

Installed Patches

- Portal for ArcGIS
  - (none)

To browse a full list of Esri patches and service packs, visit the Esri Support site:

https://support.esri.com/Downloads
Security Findings?
Esri PSIRT!

- [https://trust.arcgis.com](https://trust.arcgis.com)

- Vulnerability - report a vulnerability found in our site or application.

- Suspicious E-mail from Esri - if you believe you were targeted by a possible phishing attack from an Esri e-mail address, or have received other suspicious e-mail correspondence from Esri.

- Privacy Issue - if you have a privacy concern related to our application or organization.

- Other - for all other security, privacy or compliance related concerns.
Questions?
Please Take Our Survey on the App

Download the Esri Events app and find your event

Select the session you attended

Scroll down to find the feedback section

Complete answers and select “Submit”