2013 Esri Europe, Middle East, and Africa User Conference

October 23-25 | Munich, Germany

esri Deutschland

Security mit ArcGIS Online

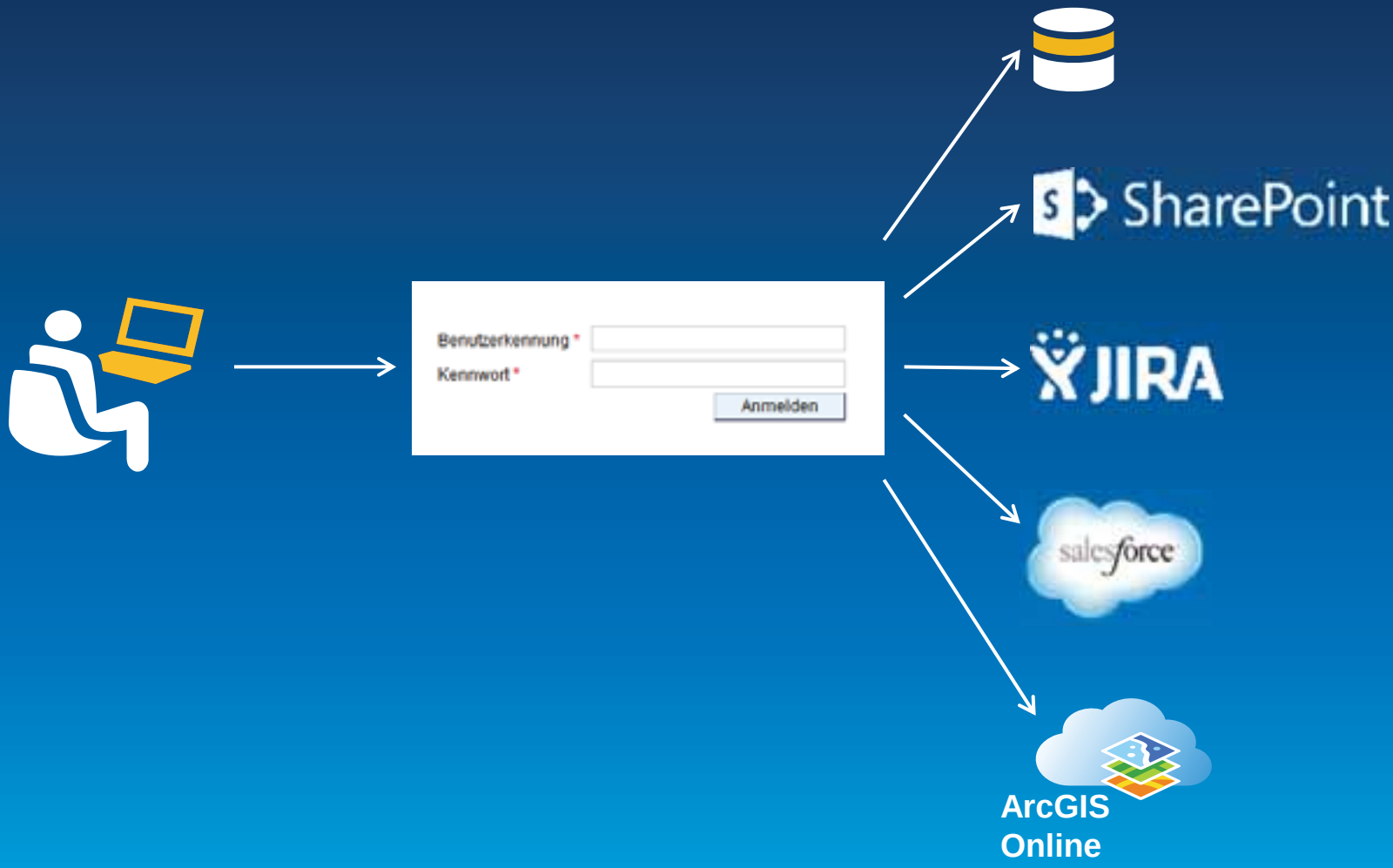
Dr. Gerd van de Sand

Intro

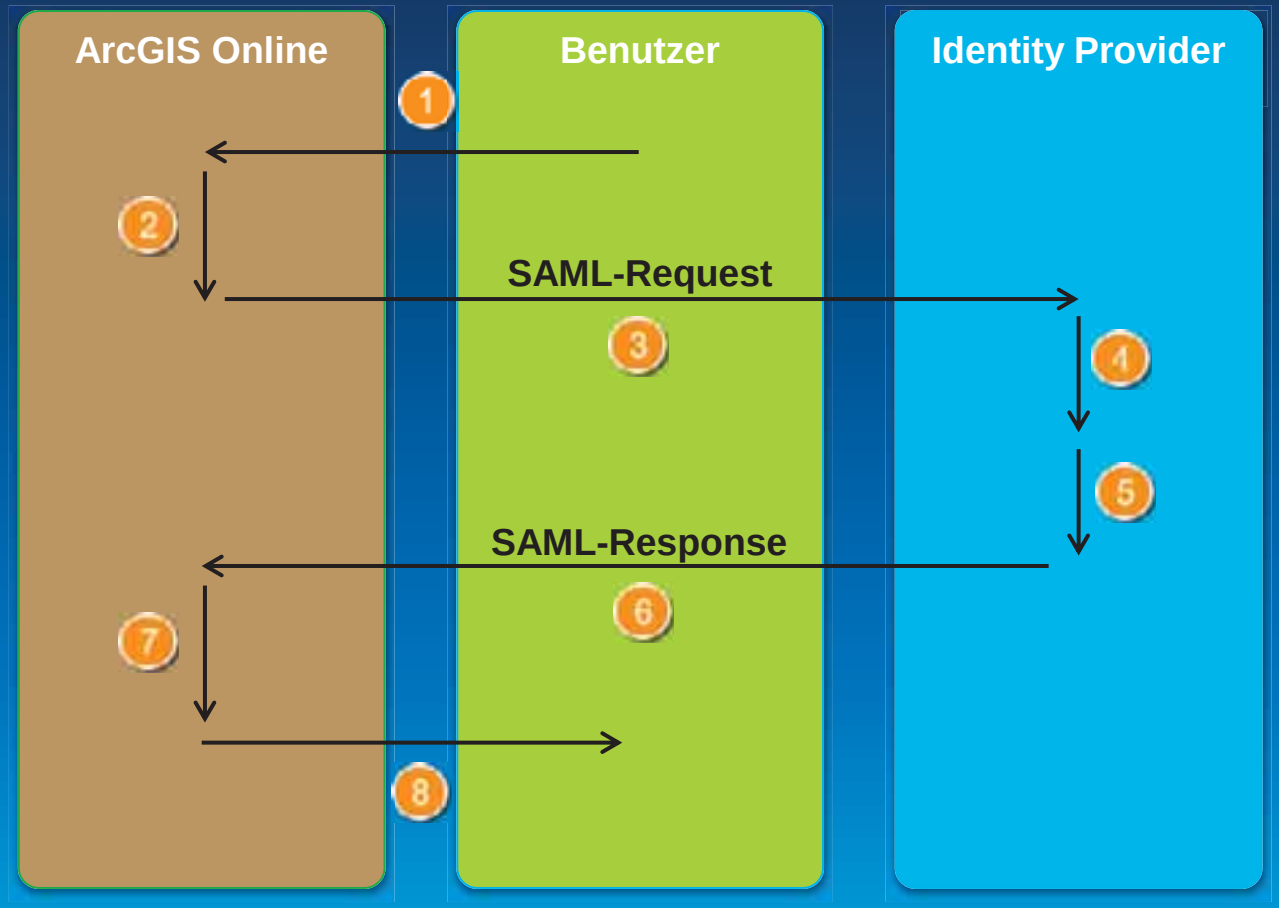
- “Enterprise logins are now supported via SAML 2.0 providing federated identity management.”
- “Developers can utilize OAuth 2-based APIs to manage user and app logins.”

Single Sign On mit SAML

Was versteht man unter “Single Sign On”?



Wie funktioniert SAML?



1. Benutzer greift auf AGOL zu
2. AGOL erzeugt SAML-Request
3. AGOL schickt SAML-Request an IP
4. IP parst und authentifiziert SAML
5. IP erzeugt SAML-Response
6. IP antwortet mit SAML-Response
7. AGOL verifiziert SAML-Response
8. Benutzer ist bei AGOL angemeldet

Identity Provider für ArcGIS Online

ArcGIS.com-Hilfe

Ressource Center

- Arbeiten mit Webkarten
- Hinzufügen von Inhalt
- Freigeben von Inhalten
- Zugreifen auf Inhalte
- Arbeiten mit Gruppen
- Verwalten Ihres Kontos
- Verwalten einer Organisation
  - Verwalten einer Organisation
  - Verwalten einer Subscription
  - Konfigurieren der Website
    - Konfigurieren der Website
    - Konfigurieren allgemeiner Einstellungen für die Website
    - Konfigurieren der Startseite
    - Konfigurieren der Galerie
    - Konfigurieren von Map Viewer
    - Konfigurieren von Elementdetails
    - Konfigurieren von Gruppen
    - Konfigurieren von Utility Services
    - Konfigurieren von Sicherheitseinstellungen
      - Konfigurieren von Sicherheitseinstellungen
      - Standardrolle SQL-Funktionen in ArcGIS Online
      - Einrichten von Enterprise-Anmeldenamen
        - Einrichten von Enterprise-Anmeldenamen
        - Provider für Enterprise-Anmeldenamen
          - Konfigurieren von Active Directory Federation Services 2.0
          - Konfigurieren von NetIQ Access Manager 3.2
          - Konfigurieren von OpenAM 10.1.0
          - Konfigurieren von Shibboleth 2.3.8
          - Konfigurieren von SimpleSAMLphp 1.10
    - Unterstützte HTML zum Konfigurieren der Website
  - Einladen von Benutzern
  - Verwalten von Benutzerrollen
  - Verwalten von Elementen
  - Verwalten von Gruppen
  - Verwalten von Benutzerprofilen
  - Entfernen von Mitgliedern

Konfigurieren von Active Directory Federation Services 2.0

Sie können Active Directory Federation Services 2.0 (AD FS) im Microsoft Windows Server-Betriebssystem als Identity-Provider für Enterprise-Anmeldenamen in ArcGIS Online konfigurieren. Die Konfiguration umfasst zwei Hauptschritte: die Registrierung des Enterprise-Identity-Providers bei ArcGIS Online und die Registrierung von ArcGIS Online beim Enterprise-Identity-Provider.

Schritt 1: Registrieren von AD FS als Enterprise-Identity-Provider bei ArcGIS Online

Schritte:

1. Überprüfen Sie, ob Sie angemeldet und Administrator Ihrer Organisation sind.
2. Klicken Sie im oberen Bereich der Website auf die Schaltfläche **Eigene Organisation**. Ihre Organisationsseite wird geöffnet.
3. Klicken Sie auf die Schaltfläche **Einstellungen bearbeiten**.
4. Klicken Sie links auf der Seite auf den Link **Sicherheit**.
5. Klicken Sie im Abschnitt **Enterprise-Anmeldenamen** auf die Schaltfläche **Identity Provider festlegen**.
6. Geben Sie in dem daraufhin angezeigten Fenster einen Namen für den Identity-Provider ein.
7. Stellen Sie mithilfe einer der drei im Folgenden genannten Optionen Metadateninformationen für den Identity-Provider bereit:
   - **URL** – Wählen Sie diese Option, wenn Zugriff auf die URL der AD FS-Verbundmetadaten besteht. Diese lautet in der Regel `https://<adfs-server>/federationmetadata/2007-06/federationmetadata.xml`.
   - **Datei** – Wählen Sie diese Option, wenn kein Zugriff auf die URL besteht. Rufen Sie eine Kopie dieser Datei aus AD FS ab, und laden Sie die Datei mit der Option **Datei** in ArcGIS Online hoch.
   - **Parameter** – Wählen Sie diese Option, wenn kein Zugriff auf die URL oder die Datei besteht. Geben Sie die Werte manuell ein, und stellen Sie die erforderlichen Parameter bereit: Anmelde-URL, Bindungstyp und Zertifikat. Wenden Sie sich an Ihren AD FS-Administrator, um diese Informationen zu erhalten.

Schritt 2: Registrieren von ArcGIS Online als vertrauenswürdigen Service-Provider bei AD FS

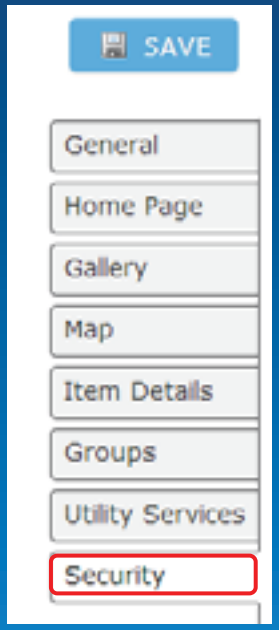
Schritte:

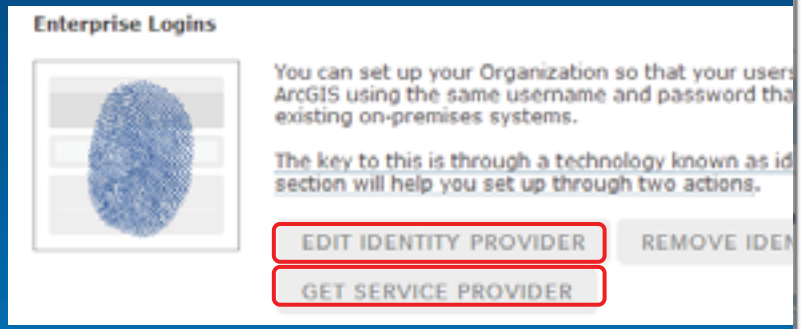
1. Öffnen Sie die AD FS 2.0-Verwaltungskonsole.
2. Wählen Sie **Vertrauensstellungen der vertrauenden Seite** > **Vertrauensstellung der vertrauenden Seite hinzufügen**.

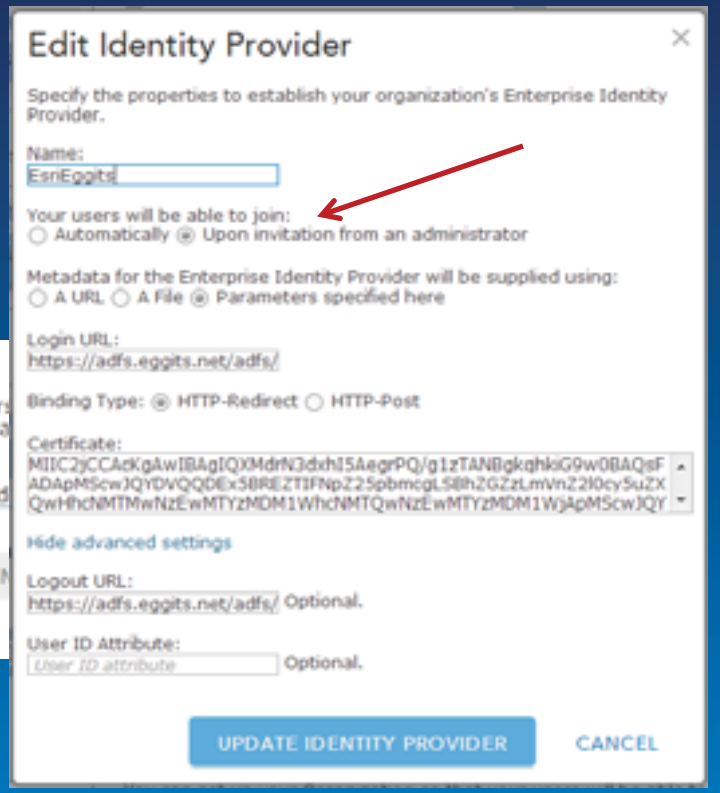
3. Klicken Sie im **Assistenten zum Hinzufügen einer Vertrauensstellung der vertrauenden Seite** auf die Schaltfläche **Start**.

Und so geht’s:


Esri Consulting
EDIT SETTINGS
INVITE USERS
UPGRADE SUBSCRIPTION

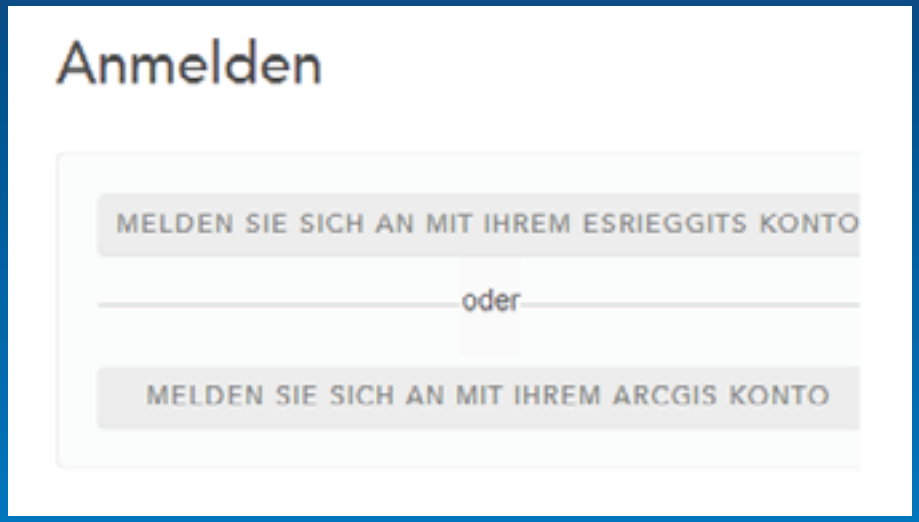

SAVE
General
Home Page
Gallery
Map
Item Details
Groups
Utility Services
Security


Enterprise Logins
You can set up your Organization so that your users
ArcGIS using the same username and password tha
existing on-premises systems.
The key to this is through a technology known as id
section will help you set up through two actions.
EDIT IDENTITY PROVIDER
REMOVE IDEN
GET SERVICE PROVIDER


Edit Identity Provider
Specify the properties to establish your organization's Enterprise Identity Provider.
Name:
EsriEggits
Your users will be able to join:
Automatically
Upon invitation from an administrator
Metadata for the Enterprise Identity Provider will be supplied using:
A URL
A File
Parameters specified here
Login URL:
https://adfs.eggits.net/adfs/
Binding Type:
HTTP-Redirect
HTTP-Post
Certificate:
MIIC2jCCAdKgAwIBAgIQXMdrN3dxhI5AegrPQ/g1zTANBgkqhkiG9w0BAQsF
ADApMScwJQYDVQQDEx5BREZTIFNpZ25pbmcgLS8hZGZzLmVnZ2l0cy5uZX
QwHhcNMTMwNzEwMTYzMDM1WhcNMTQwNzEwMTYzMDM1WjApMScwJQY
Hide advanced settings
Logout URL:
https://adfs.eggits.net/adfs/ Optional.
User ID Attribute:
User ID attribute
Optional.
UPDATE IDENTITY PROVIDER
CANCEL


esri-de-3.maps.arcgis.com
urn:oasis:names:tc:SAML:2.0:metadata
urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol
https://esri-de-3.maps.arcgis.com/sharing/rest/oauth2/saml/signin
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
Esri Consulting
https://esri-de-3.maps.arcgis.com

Demo Enterprise Login



Fazit

ArcGIS Online …

… bietet die Möglichkeit SSO zu verwenden

... verwendet dabei etablierte Industriestandards

… kann nahtlos in IT-Infrastrukturen integriert werden

… wird einfacher und sicherer

Applikationen mit OAuth 2.0

OAuth-Definition

“OAuth is an open standard for authorization. OAuth provides a method for clients to access server resources on behalf of a resource owner (such as a different client or an end-user).”

- **Quelle: Wikipedia**

Um was geht es?

Als Entwickler kann man zwei Typen von Applikationen für ArcGIS Online bauen, die auf geschützte Dienste zugreifen:

- **Applikation adressiert Nutzer, die einen Account in der ArcGIS Online-Subskription haben. Die Nutzer melden sich selbst über die Plattform an → User Login**

- **Applikation adressiert Nutzer, die der ArcGIS Online-Plattform unbekannt sind. Die Applikation meldet sich stellvertretend für den Nutzer an → App Login**

In Kurzform

App

+

Named User

=

User Login

App

+

Anonymous User

=

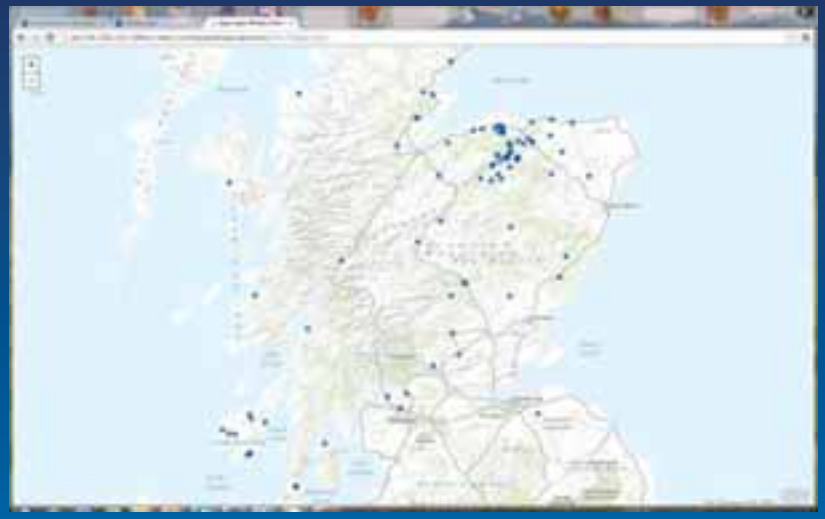
App Login

Demo OAuth mit User Login

Zusammenfassung

- Analog zur vorhandenen Absicherung über Token-Service
- Service-Aufrufe können der Applikation zugeordnet werden
- Industrie-Standard

Demo OAuth mit App Login



Zusammenfassung

- Die Applikation meldet sich an, nicht ein Benutzer
  - Jeder kann die Anwendung nutzen
  - Achtung: Credit-Verbrauch!
- Service-Aufrufe können der Applikation zugeordnet werden
- App Secret muss gut geschützt werden!

Portal

- Kein SAML oder OAuth
- SSO über Anbindung LDAP/AD
- Absicherung von Diensten über „klassischen“ Token-Service

Fragen

consulting@esri.de