Implementing Security for ArcGIS Server for the Microsoft .NET Framework

Tom Brenneman

Sud Menon

Schedule

Please!
Turn OFF cell phones
and paging devices

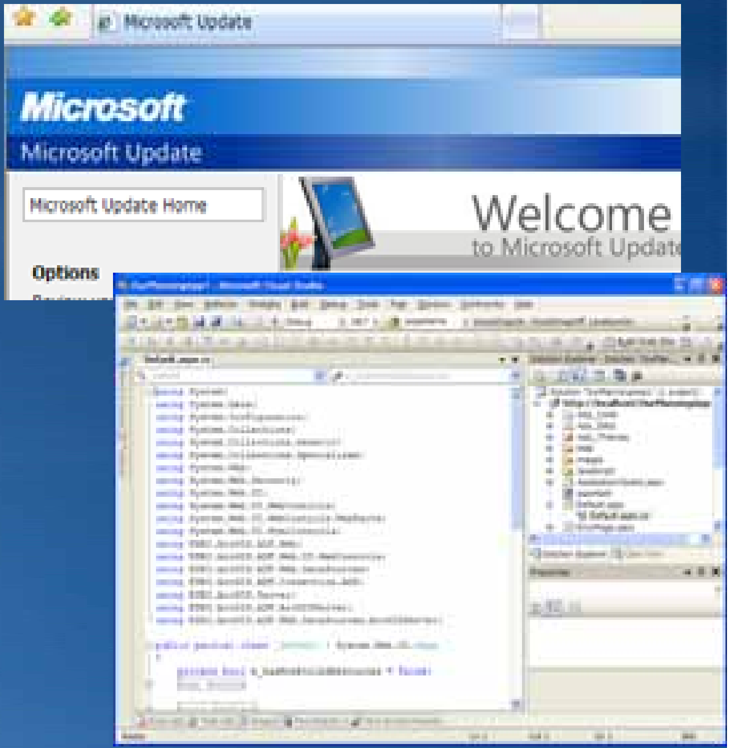
- **Security overview**
- **Setup and configuration**
- **Securing GIS Web services**
  - **Using the token service**
- **Securing Web applications**
  - **Web ADF applications**
  - **JavaScript/Flex API applications**

- **We will answer questions at the end on the session**

Please complete the session survey!

Security overview

- ArcGIS Server security provides access control
  - Which users can access particular services and applications
- Remember other security tasks
  - Security during transmission
  - Operating system – updates, virus protection
  - Code – SQL injection, cross-site scripting, etc.
  - Physical security
  - User education – phishing, etc.

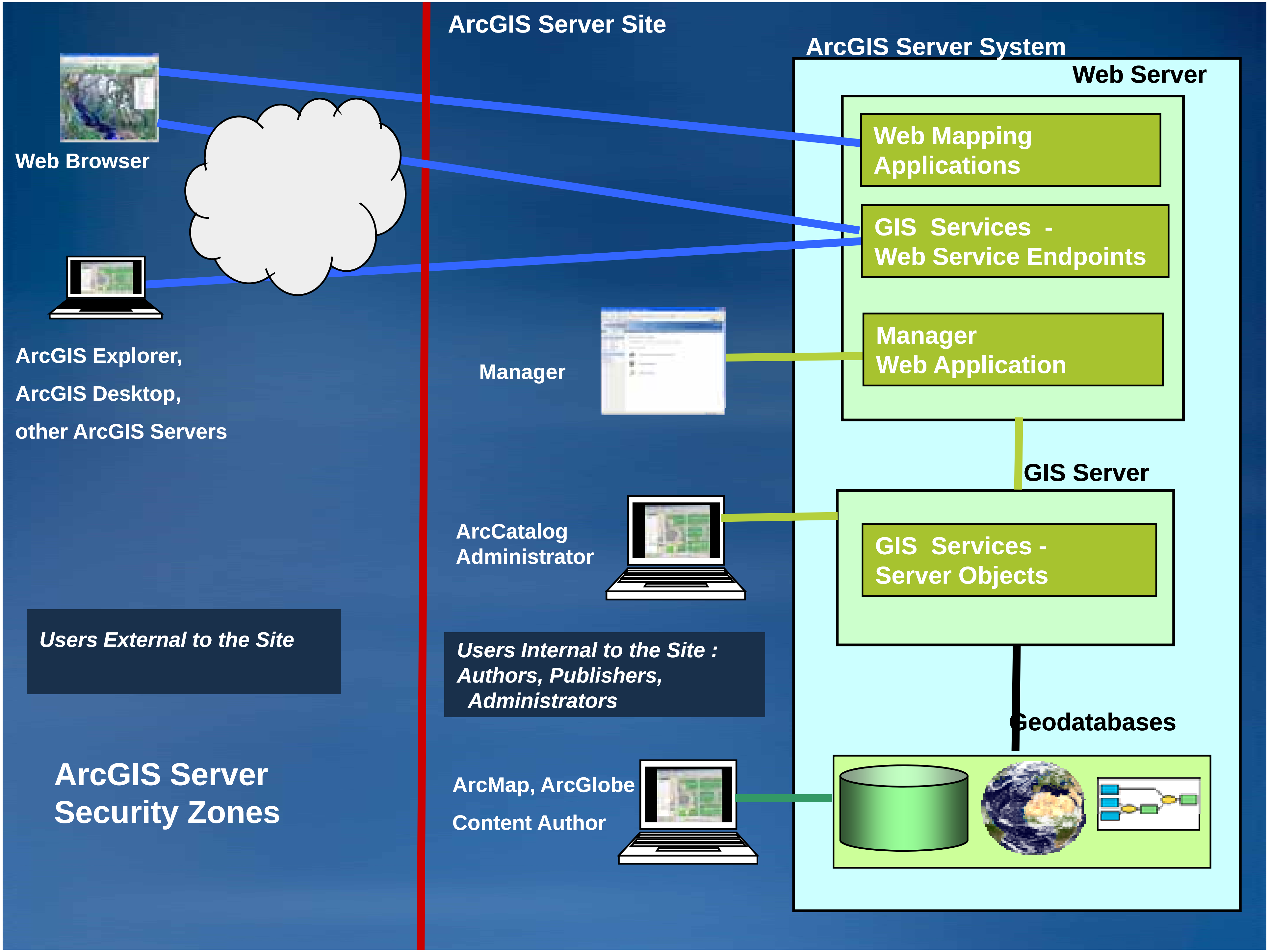


Access control model

- ArcGIS Server has role-based access control

- Uses standard IIS or ASP.NET security
- IIS
  - Basic, Digest, Integrated Windows
- ASP.NET
  - Membership and role provider framework

ArcGIS Server Security Zones



Web Browser

ArcGIS Explorer,

ArcGIS Desktop,

other ArcGIS Servers

Users External to the Site

ArcGIS Server Site

Manager

ArcCatalog
Administrator

Users Internal to the Site :
Authors, Publishers,
Administrators

ArcMap, ArcGlobe

Content Author

ArcGIS Server System

Web Server

Web Mapping
Applications

GIS Services -
Web Service Endpoints

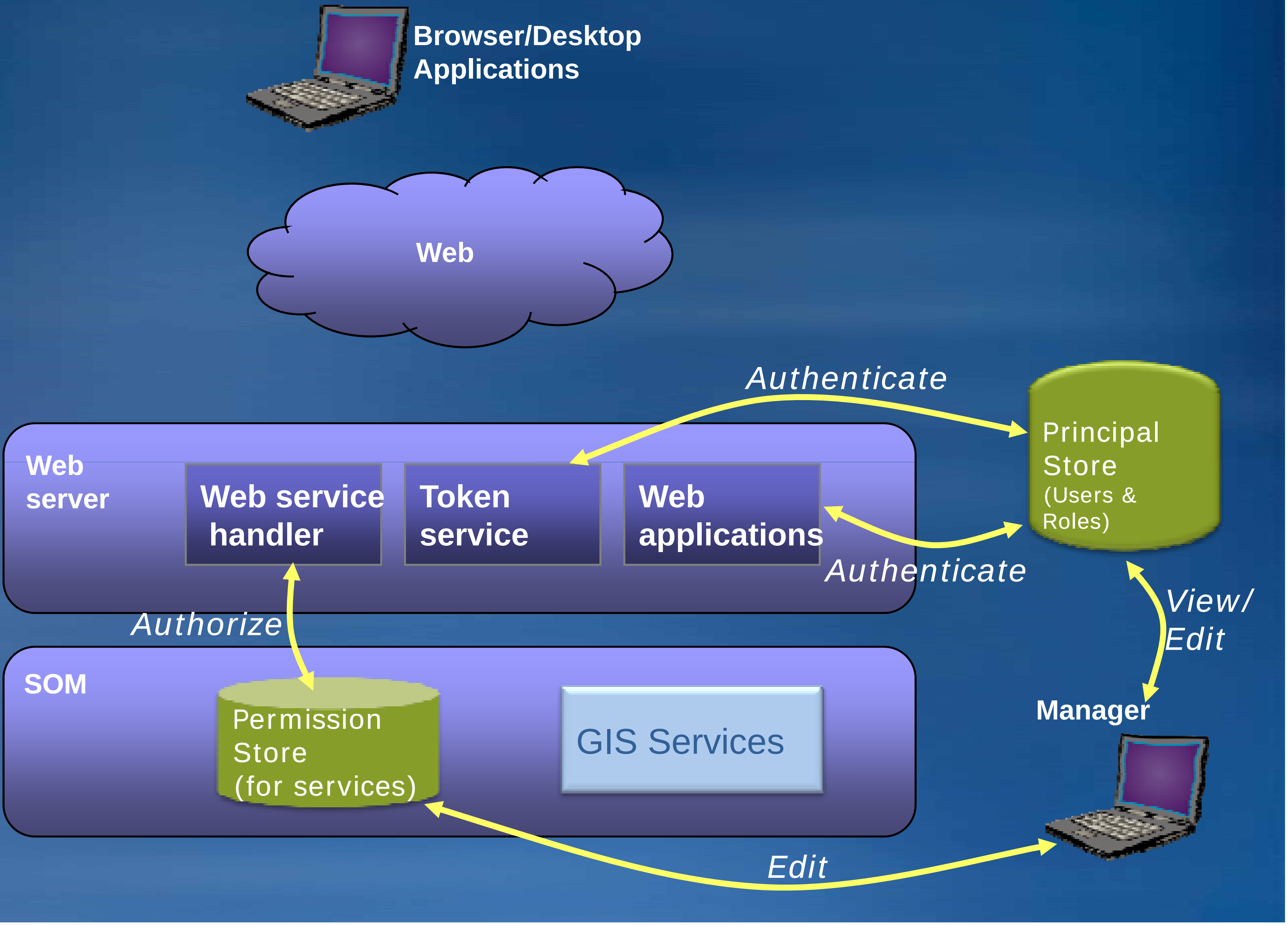
Manager
Web Application

GIS Server

GIS Services -
Server Objects

Geodatabases

Security model



Steps to securing services and applications

1. **Decide where users and roles will be stored**
2. **Install supporting items as needed**
   - **Secure Sockets Layer (SSL) certificate for Web server**
   - **SQL Server (Express)**
   - **Custom provider**
3. **Configure security in Manager**
   - **Configure location for users and roles**
   - **Add and manage users and roles**
4. **Secure Web application(s) using Manager***

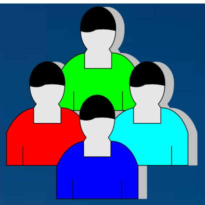
   - and/or -

5. **Secure GIS Web services using Manager**

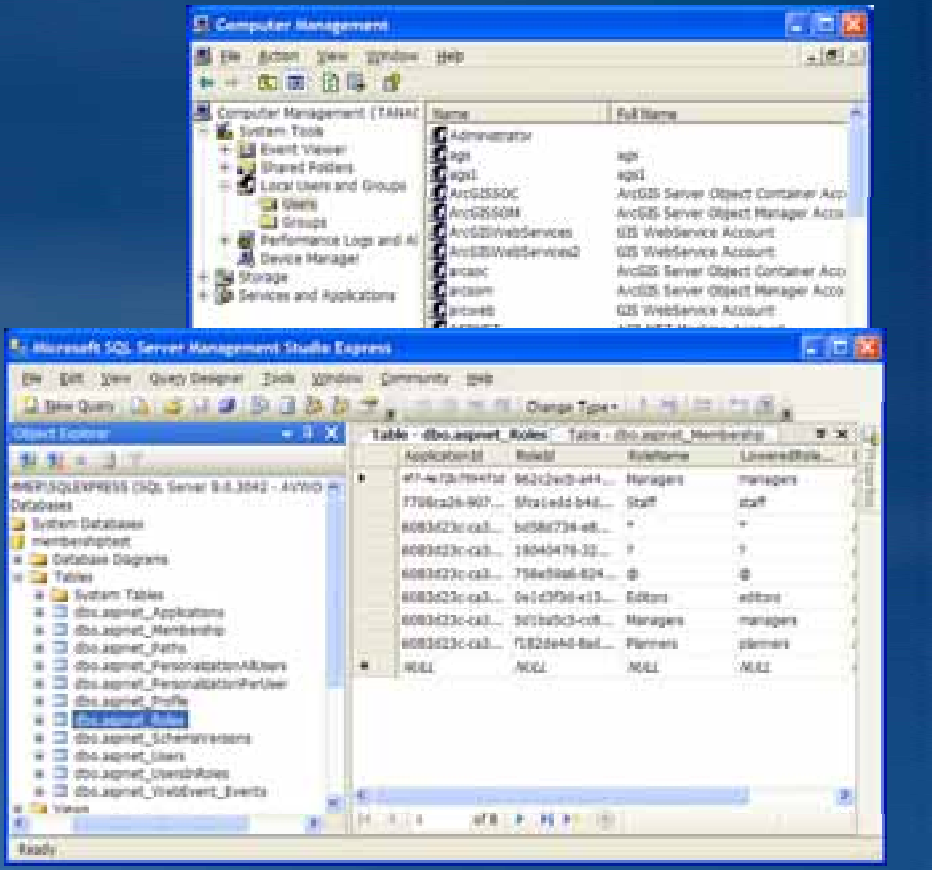
*or other tools for custom applications

Adapted from ArcGIS Server Help, "Internet security checklist"

Decide where users and roles will be stored



- Windows users and groups
  - Manage with operating system tools
- SQL Server
  - Full or Express version
  - Tables store users and roles in .NET membership format
- Custom provider
  - Oracle, Active Directory, XML, etc.
  - To use, acquire a .NET membership/role provider



Computer Management

Computer Management (TANAC
- System Tools
  - Event Viewer
  - Shared Folders
  - Local Users and Groups
    - Users
    - Groups
  - Performance Logs and Al
  - Device Manager
- Storage
- Services and Applications

Name	Full Name
Administrator	
ags	ags
ags1	ags1
ArcGISSOC	ArcGIS Server Object Container Acc
ArcGISSOM	ArcGIS Server Object Manager Acco
ArcGISWebServices	GIS WebService Account
ArcGISWebServices2	GIS WebService Account
arcsoc	ArcGIS Server Object Container Acc
arcsom	ArcGIS Server Object Manager Acco
arcweb	GIS WebService Account

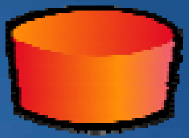
Microsoft SQL Server Management Studio Express

AWRF\SQLEXPRESS (SQL Server 9.0.3042 - AVWO
- Databases
  - System Databases
  - membershiptest
    - Database Diagrams
    - Tables
      - System Tables
      - dbo.aspnet_Applications
      - dbo.aspnet_Membership
      - dbo.aspnet_Paths
      - dbo.aspnet_PersonalizationAllUsers
      - dbo.aspnet_PersonalizationPerUser
      - dbo.aspnet_Profile
      - dbo.aspnet_Roles
      - dbo.aspnet_SchemaVersions
      - dbo.aspnet_Users
      - dbo.aspnet_UsersInRoles
      - dbo.aspnet_WebEvent_Events
    - Views

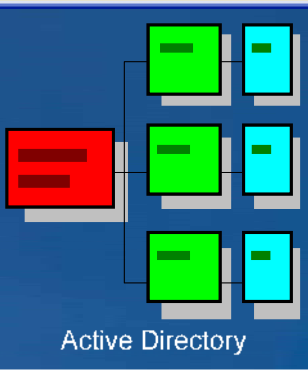
Table - dbo.aspnet_Roles | Table - dbo.aspnet_Membership

ApplicationId	RoleId	RoleName	LoweredRole...
4f7-4e73b7f9471d	962c2ec5-a44...	Managers	managers
7706ca26-907...	5fca1edd-b4d...	Staff	staff
6083d23c-ca3...	bd58d734-e8...	*	*
6083d23c-ca3...	18040479-32...	?	?
6083d23c-ca3...	758e59a6-624...	@	@
6083d23c-ca3...	0e1d3f30-e13...	Editors	editors
6083d23c-ca3...	501ba5c3-c8...	Managers	managers
6083d23c-ca3...	f182de4d-8ad...	Planners	planners
NULL	NULL	NULL	NULL

Ready

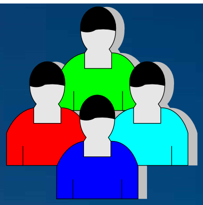


Oracle



Active Directory

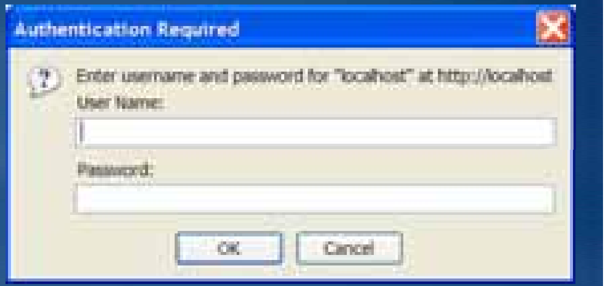
Decide where users and roles will be stored



- User and role store usually same place, but can have
  - Windows users + SQL Server roles
  - Windows users + roles in custom provider
  - SQL Server users + roles in custom provider
- Built-in SQL Server roles
  - Everyone (*): all users permitted whether provide login or not
  - Authenticated Users (@): users who provide a valid login
  - Anonymous (?): users who do not provide a login
  - Add can manually add to custom provider

How will users be authenticated?

- Authenticate = verify identity of the user
- If users in SQL Server or custom provider
  – Web Applications: ASP.NET Forms authentication
  – Web Services: Tokens service
- If Windows users, options are:
  – IIS-controlled authentication
    - Integrated Windows
    - Basic
    - Digest
  – Token authentication
    - Only supported if roles are in SQL Server

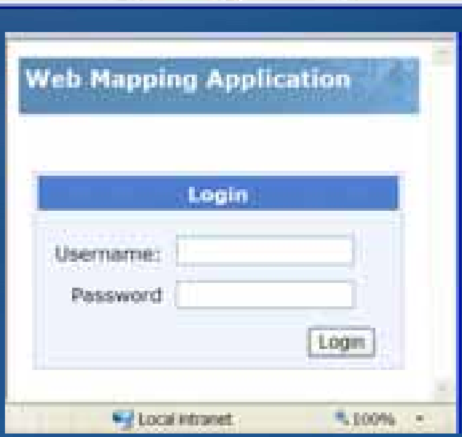


Authentication Required

Enter username and password for "localhost" at http://localhost

User Name:

Password:



Web Mapping Application

Login

Username:

Password

Demo

Configuring security using SQL

Session agenda

- Security overview
- Setup and configuration
- **Securing GIS Web services**
  - Using the token service
- Securing Web applications
  - Web ADF applications
  - JavaScript/Flex API applications

Securing ArcGIS Server services

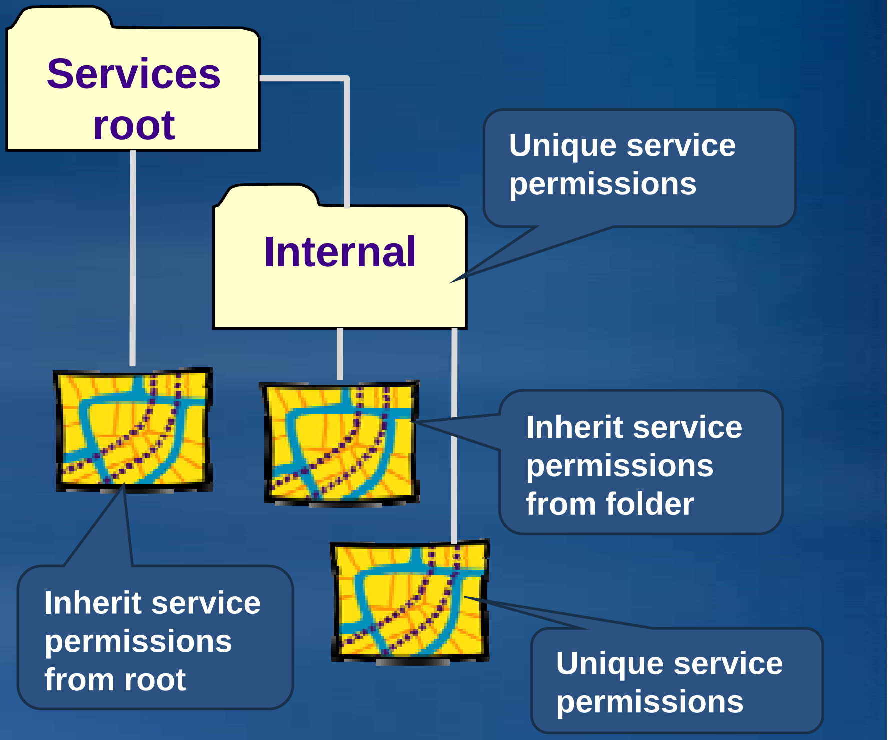
- Two ways to connect to an ArcGIS Server service

  1. Local connection
     - Works only on intranets
     - Access to all server functionality
     - User must be a member of the agsusers or agsadmin groups

  2. Web service (“Internet”) connections
     - SOAP, REST, WMS, KML
     - Works on intranets and over Internet
     - Security model introduced at 9.3

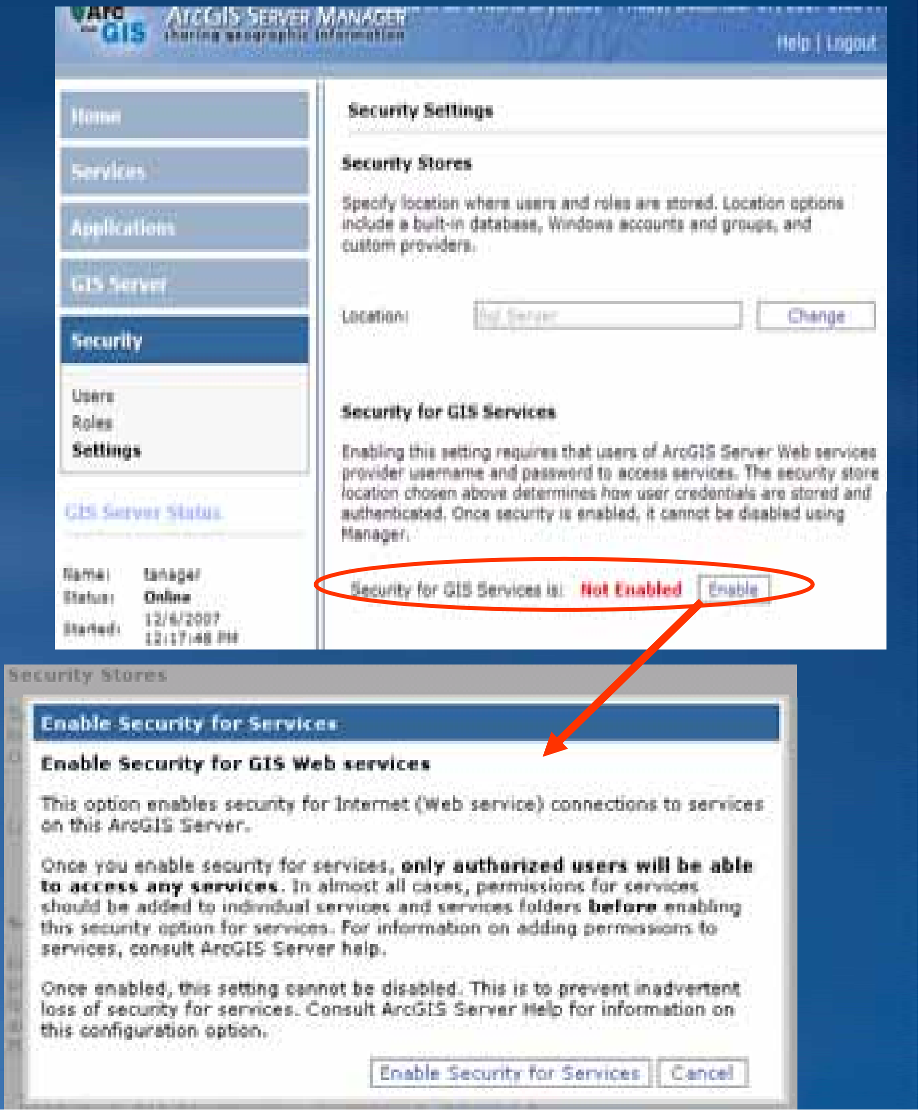
Securing GIS Web services

- Services inherit folder permissions
- Good practice to secure folders
- Permissions changes cascade to all children
  - Set permissions on root first


Services root
Internal
Unique service permissions
Inherit service permissions from folder
Inherit service permissions from root
Unique service permissions

Transitioning ArcGIS Server from open access to secure access

- Enabling security for services is set separately from permissions
  - Security-Settings tab
- With no security, everyone has access to everything
- With security, by default, everyone has access to nothing
  - If you enable security before changing permissions, no one will be able to use existing services



Security Settings

Security Stores

Specify location where users and roles are stored. Location options include a built-in database, Windows accounts and groups, and custom providers.

Location: GIS Server

Security for GIS Services

Enabling this setting requires that users of ArcGIS Server Web services provider username and password to access services. The security store location chosen above determines how user credentials are stored and authenticated. Once security is enabled, it cannot be disabled using Manager.

Security for GIS Services is: Not Enabled

Name: tanager
Status: **Online**
Started: 12/6/2007 12:17:48 PM

Enable Security for GIS Web services

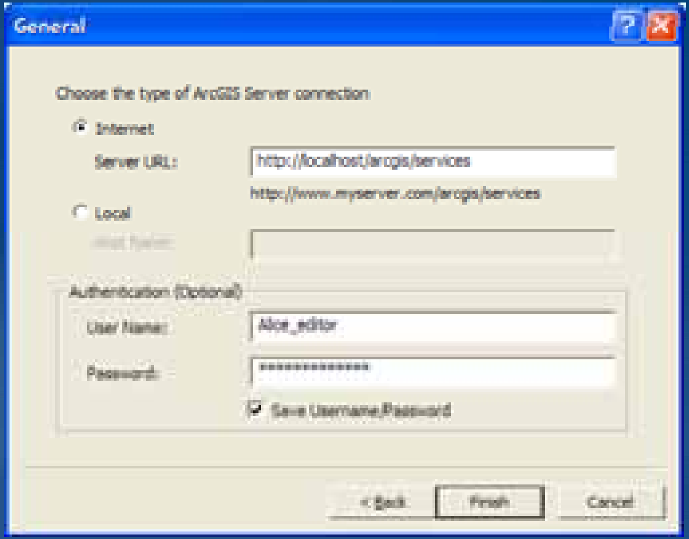
This option enables security for Internet (Web service) connections to services on this ArcGIS Server.

Once you enable security for services, **only authorized users will be able to access any services**. In almost all cases, permissions for services should be added to individual services and services folders **before** enabling this security option for services. For information on adding permissions to services, consult ArcGIS Server help.

Once enabled, this setting cannot be disabled. This is to prevent inadvertent loss of security for services. Consult ArcGIS Server Help for information on this configuration option.

Using secured services

- **ArcGIS Desktop, ArcGIS Explorer**
  - **Provide identify in connection dialog**
- **.NET Web applications**
  - **Manager: use “Access secured services”**
  - **Visual Studio: add identity in the resource manager**
- **SOAP, REST and JavaScript applications**
  - **Use token or Windows authentication**
  - **More on this shortly**



Choose the type of ArcGIS Server connection

● Internet

Server URL: http://localhost/arcgis/services

http://www.myserver.com/arcgis/services

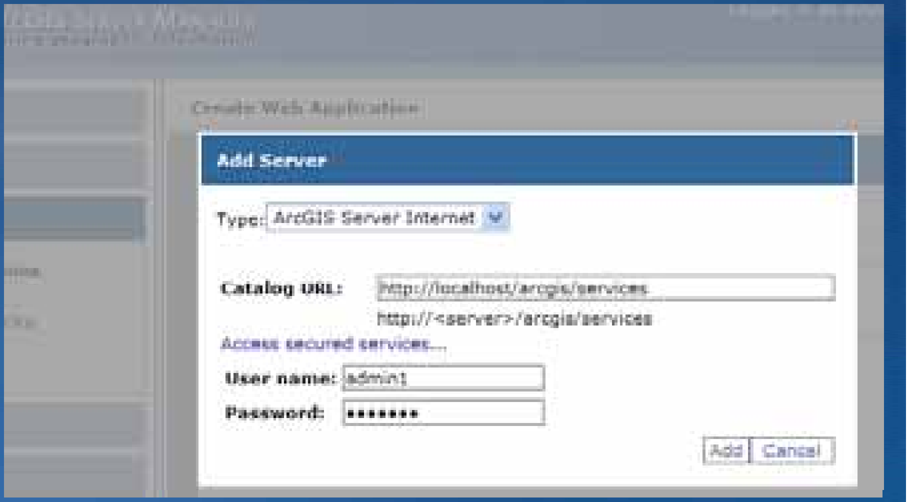
○ Local

Authentication (Optional)

User Name: Alice_editor

Password: **************

☑ Save Username/Password



Type: ArcGIS Server Internet

Catalog URL: http://localhost/arcgis/services

http://<server>/arcgis/services

Access secured services...

User name: admin1

Password: ••••••••

Demo

Securing GIS Web services

Session agenda

- Security overview
- Setup and configuration
- Securing GIS Web services
  - Using the token service
- Securing Web applications
  - Web ADF applications
  - JavaScript/Flex API applications

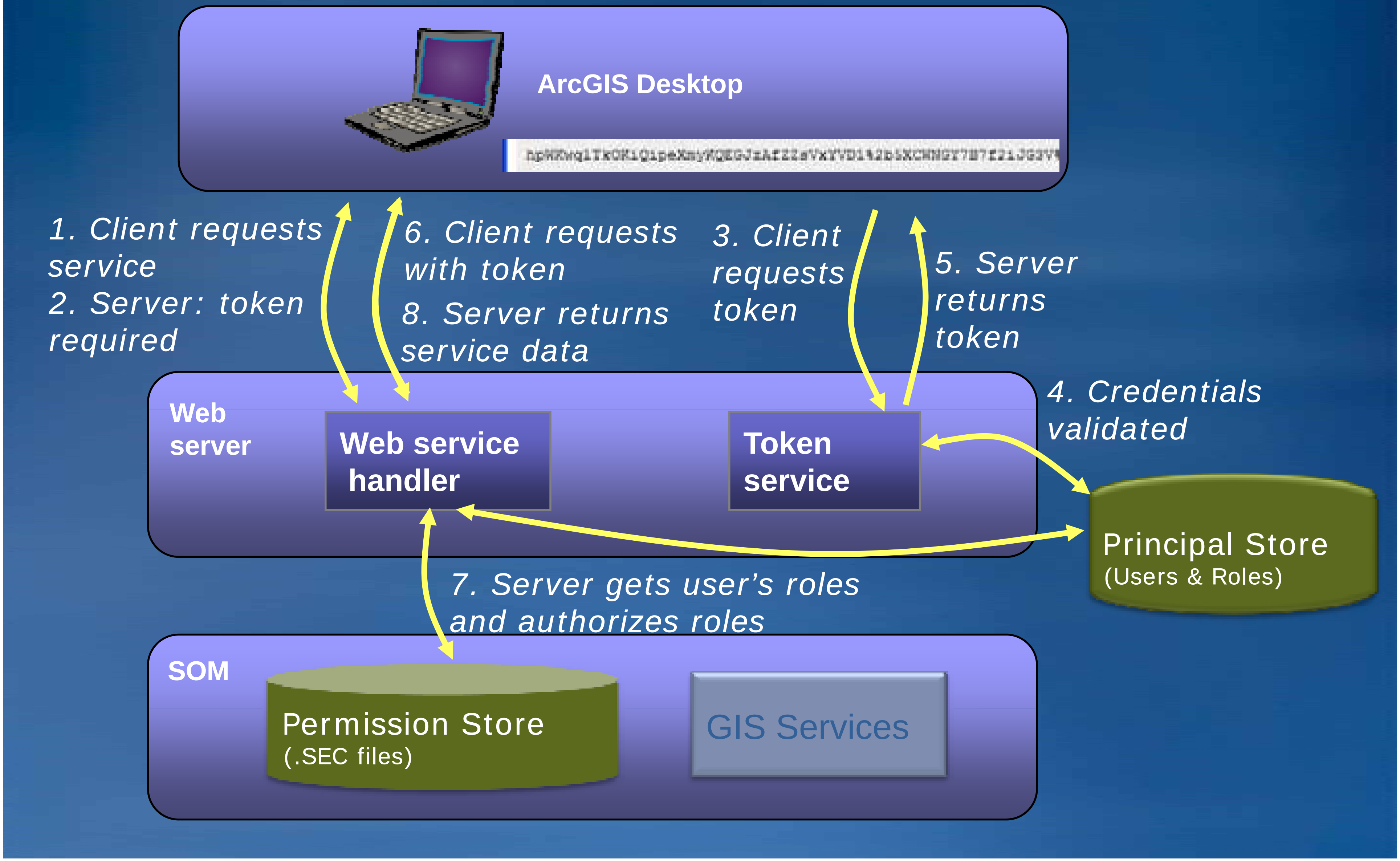
The Token service

- User authentication web service

- Why do we need it?
  - .NET provides no mechanism for web service security
    - Forms just for applications
  - Web service security when using and ASP.NET membership / role provider

- Used only with GIS Web services
  - Not used by default with Windows users
  - Not used to authenticate Web application users

How does the Token service work?



ArcGIS Desktop

1. Client requests service

2. Server: token required

6. Client requests with token

8. Server returns service data

3. Client requests token

5. Server returns token

4. Credentials validated

Web server

Web service handler

Token service

Principal Store
(Users & Roles)

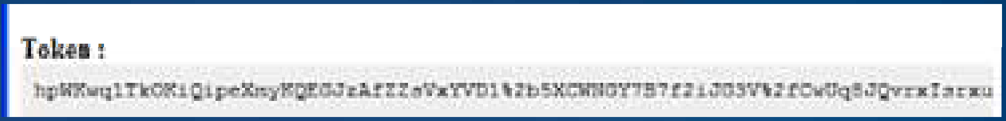
7. Server gets user's roles and authorizes roles

SOM

Permission Store
(.SEC files)

GIS Services

What is in a Token?



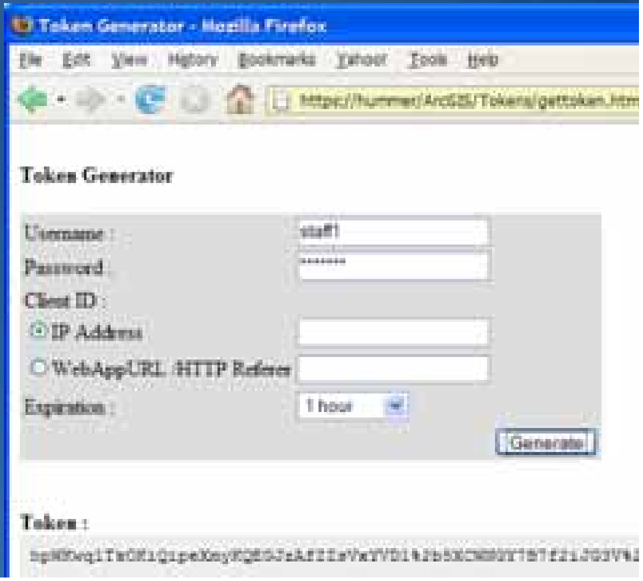
Token :

```
hpWKwq1TkOKiQipeXmyKQEGJzAfZZsVxYVD1%2b5XCWNGY7B7f2iJ03V%2fCwUq8JQvrxIsrxu
```

- Token is a string with encrypted information:
  - – User name
  - – Expiration time
  - – Optional: ID of the client
    - IP address or Web URL (HTTP Referrer)
    - If included, expiration can be a longer time period (weeks/months)
      - – Used by most clients – Desktop, ADF, JavaScript/REST applications, etc.
    - If not included, shorter expiration time – needs to be renewed

Working with the Token service

- Most clients will work with tokens automatically
  - Desktop (ArcMap, ArcCatalog, ArcGlobe) and Engine
  - ArcGIS Explorer
  - Web ADF (.NET and Java) and Mobile ADF
- Some clients will require explicit token management
  - SOAP-based clients not using ADF
    - Use server-side code to acquire and use token
    - See Developer Help for details and examples
  - JavaScript/REST clients
    - Developer obtains a token from get-token Web page
    - Developer embeds token in the Web application code
    - Access token on the server via a proxy page


Token Generator - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
https://hummer/ArcGIS/Tokens/gettoken.htm

Token Generator

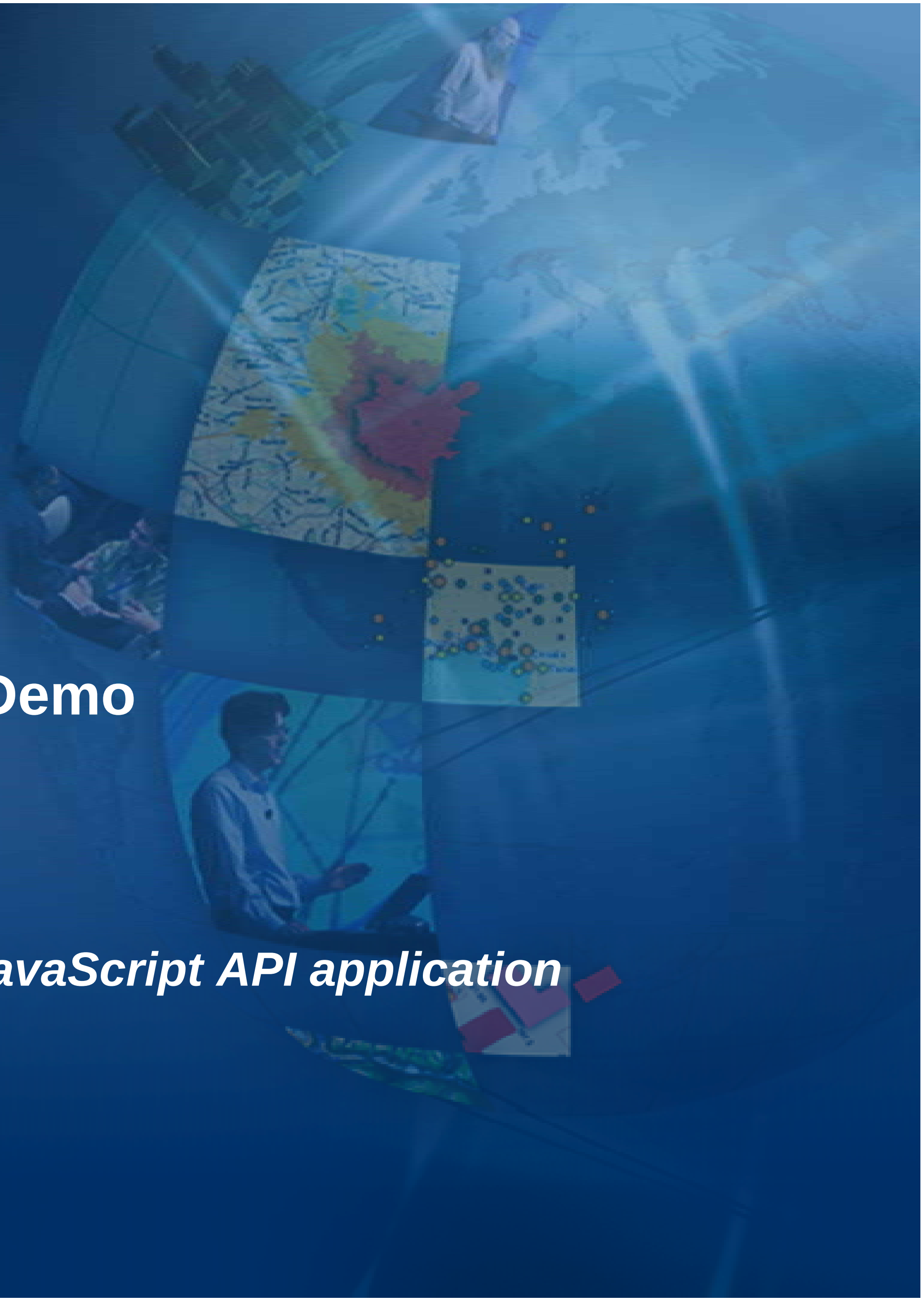
Username : staff1
Password : ********
Client ID :
● IP Address
○ WebAppURL /HTTP Referer
Expiration : 1 hour

Generate

Token :
hpMKwqiTsOKiQipeXmyKQEGJzAfZIzVwYVD1%2b5XCMBOY7B7f2iJO3V%

Working with the Token service (continued)

- GIS service can provide the Token service URL
- Requesting a token
  - Requires HTTPS by default
  - Example: https://myserver/arcgis/tokens?request=getToken&username=myUser&password=secret&clientId=ip.127.0.0.1&expiration=120
- Using a token
  - Append the token to the URL of the server
    - http://myserver/arcgis/services/USA/MapServer?token=hpWKwqlTkUHDWOGpp%...
  - Use HTTPS for maximum security over unsecure networks
    - Needed to guard against token hijacking and replay attacks
- Refreshing the token
  - If token may expire, include code to renew it
  - Server returns HTTP error code of 498 for expired token



Demo

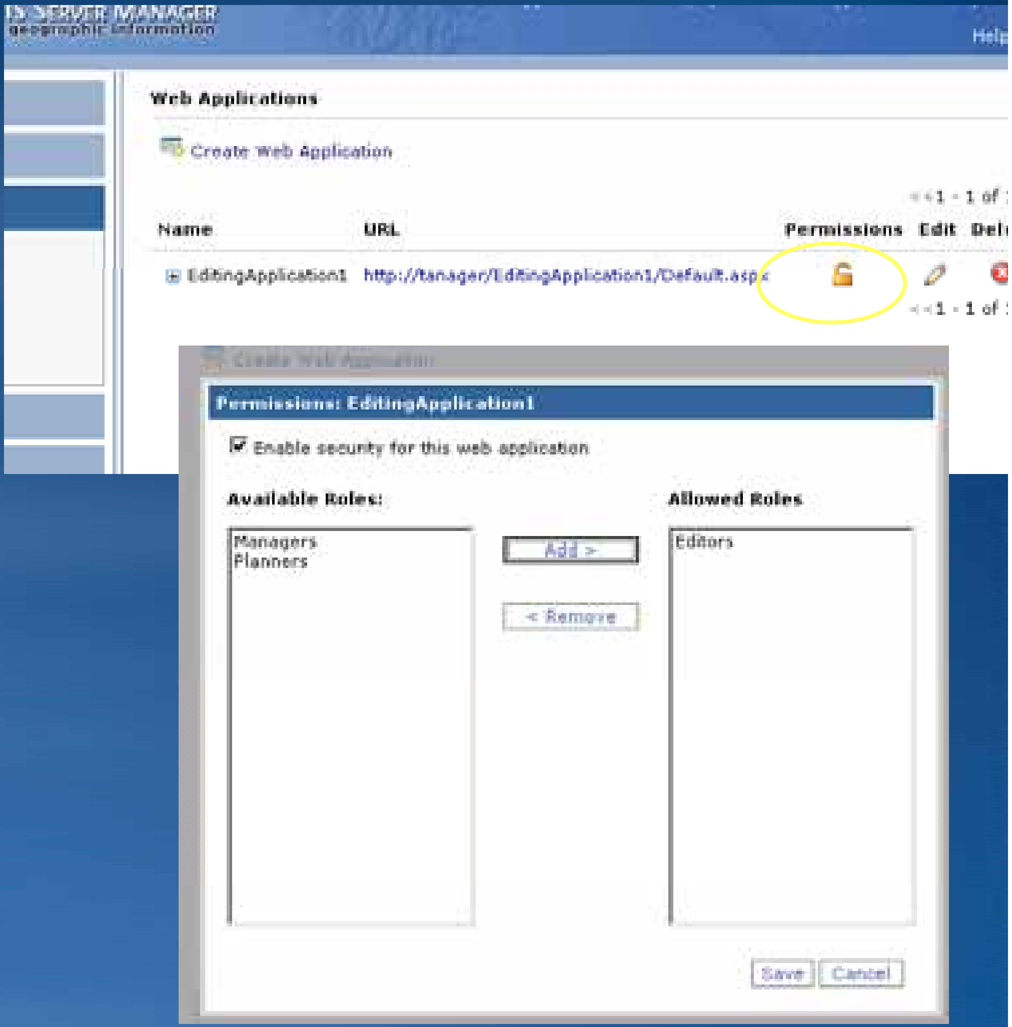
Using tokens in a JavaScript API application

Session agenda

- Security overview
- Setup and configuration
- Securing GIS Web services
  - Using the token service
- Securing Web applications
  - Web ADF applications
  - JavaScript/Flex API applications

Securing Web ADF applications with Manager

- Security button in Manager Applications
- Enable security
- Add permitted role(s)
  - Notice role-based security, not user-based
- Permission rules are stored in the application
  - Web.config - <authorization> element



Web Applications

Create Web Application

<< 1 - 1 of 1

Name	URL	Permissions	Edit	Del
EditingApplication1	http://tanager/EditingApplication1/Default.aspx			

<< 1 - 1 of 1

Create Web Application

Permissions: EditingApplication1

☑ Enable security for this web application

Available Roles:

Managers
Planners

Allowed Roles

Editors

Securing a Web ADF application outside of Manager

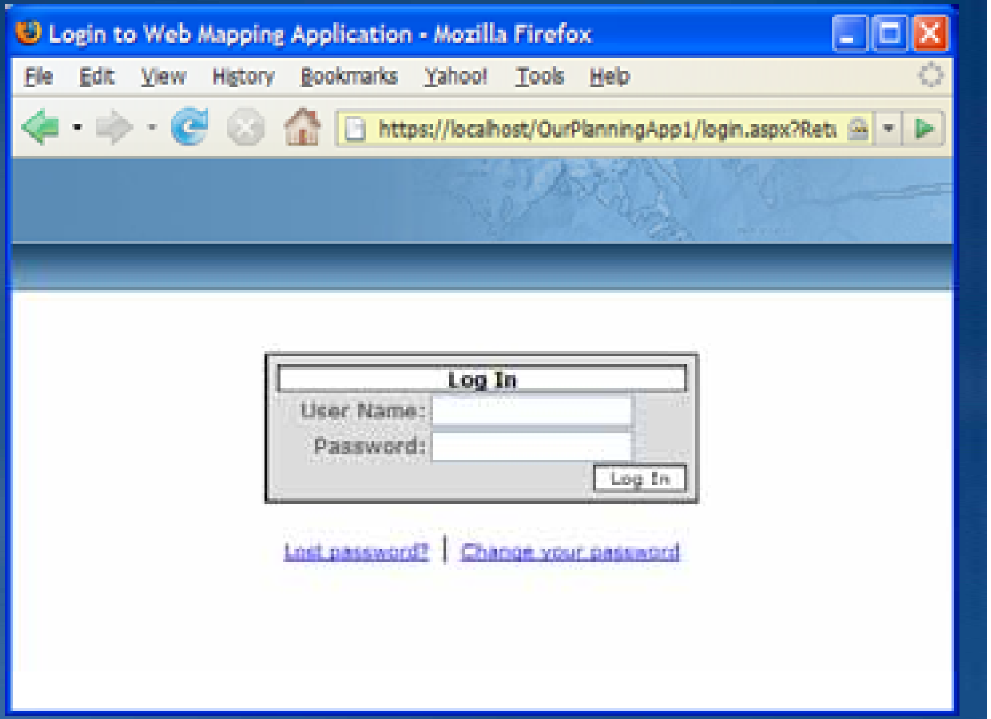
- Q: How do you secure a Web ADF application created with Visual Studio?
- A: Add the provider and permissions manually to web.config
  - Copy provider settings from /ArcGIS/Security/web.config
    - Connection string for SQL Server
    - Membership and provider elements
  - Add allow/deny rules

```
<authorization>
  <allow roles=“Editors” />
  <deny users=“*” />
</authorization>
```

  - Add login.aspx page if not using Web Mapping Application template

Using a secured Web ADF application

- User will be prompted to login
  - Login.aspx page when users in SQL Server or custom provider
  - Pop-up dialog with Windows users
- Application page
  - Displays login name
  - Logout link
    - When logged in with forms authentication


Login to Web Mapping Application - Mozilla Firefox

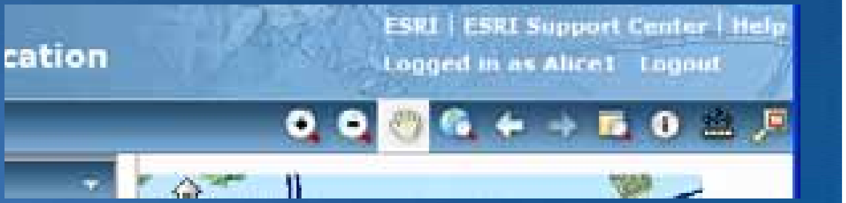
https://localhost/OurPlanningApp1/login.aspx?Retu

Log In

User Name:

Password:

Lost password? | Change your password



Demo

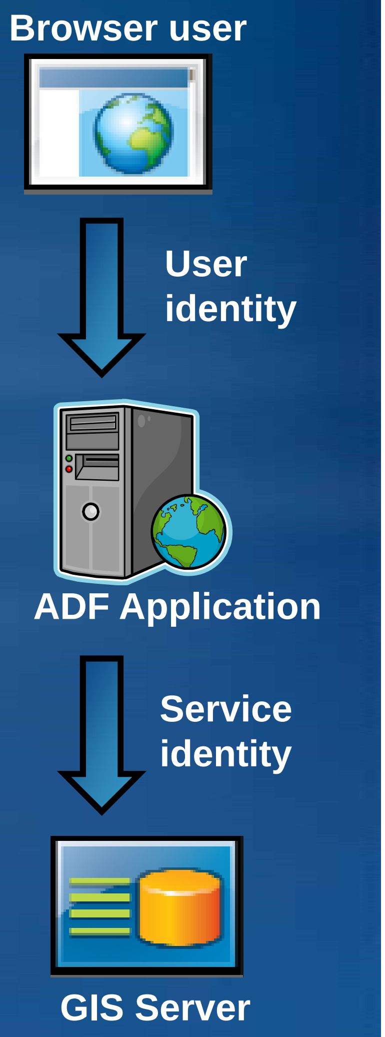
Securing a Web application in Manager

Securing applications that use client-side APIs: JavaScript APIs, Flex API, Silverlight API

- Can’t secure applications with only client-side code
- Using windows
  - Secure using OS
- Using ASP.NET
  - Wrap code in .aspx page
  - Use same approach shown earlier for securing the application outside of Manager

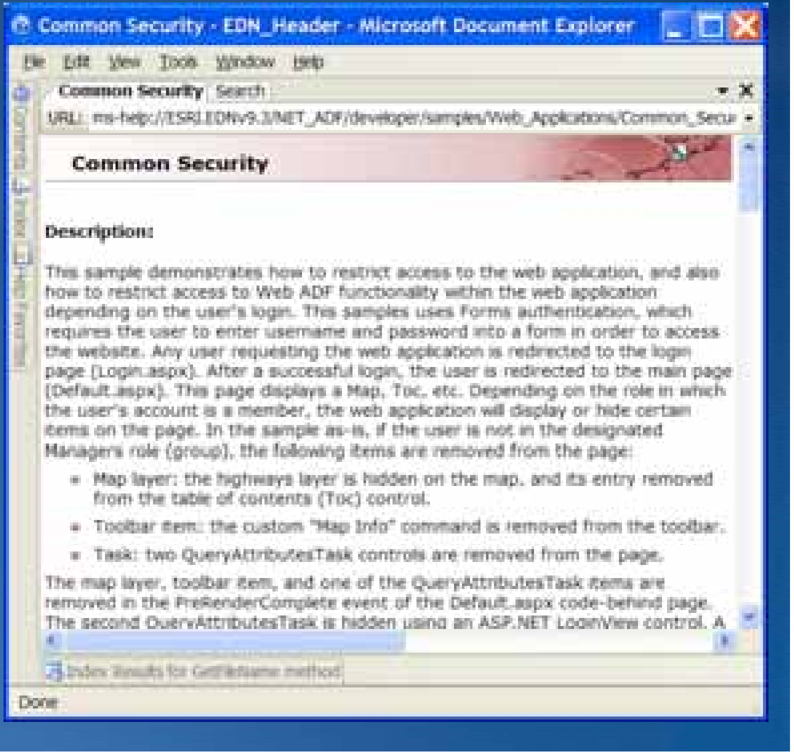
Passing user identity to the GIS service

- Scenario: Secure application with dynamic services based on user
  - User logs into the application
  - User sees only the services they have access to
- SecurityPassthrough samples
  - Passes user's identity to GIS service at runtime
  - Three samples:
    - SecurityPassthrough_Forms: Users/roles in SQL Server; Web service (Internet) connection to the GIS service
    - SecurityPassthrough_Win: Users/roles in Windows; Local connection to the GIS service
    - SecurityPassthrough_WinInternet (available for 9.3.1): Users/roles in Windows; Web service (Internet) connection to the GIS service



Controlling application content based on role

- Question: How can I show or hide content depending on the role?
  - Tools, tasks, layers, map, etc.
- Answer: Developer must add code
  - Wrap Web ADF controls in LoginView controls
  - Get user's role
  - Remove or add content depending on role
  - See sample in Developer Kit
    - "Common_Security"



Common Security - EDN_Header - Microsoft Document Explorer
File Edit View Tools Window Help
Common Security Search
URL: ms-help://ESRI.EDNv9.3/NET_ADF/developer/samples/Web_Applications/Common_Secu
Index Results for GetFileName method
Done

Common Security

Description:

This sample demonstrates how to restrict access to the web application, and also how to restrict access to Web ADF functionality within the web application depending on the user's login. This samples uses Forms authentication, which requires the user to enter username and password into a form in order to access the website. Any user requesting the web application is redirected to the login page (Login.aspx). After a successful login, the user is redirected to the main page (Default.aspx). This page displays a Map, Toc, etc. Depending on the role in which the user's account is a member, the web application will display or hide certain items on the page. In the sample as-is, if the user is not in the designated Managers role (group), the following items are removed from the page:

- Map layer: the highways layer is hidden on the map, and its entry removed from the table of contents (Toc) control.
- Toolbar item: the custom "Map Info" command is removed from the toolbar.
- Task: two QueryAttributesTask controls are removed from the page.

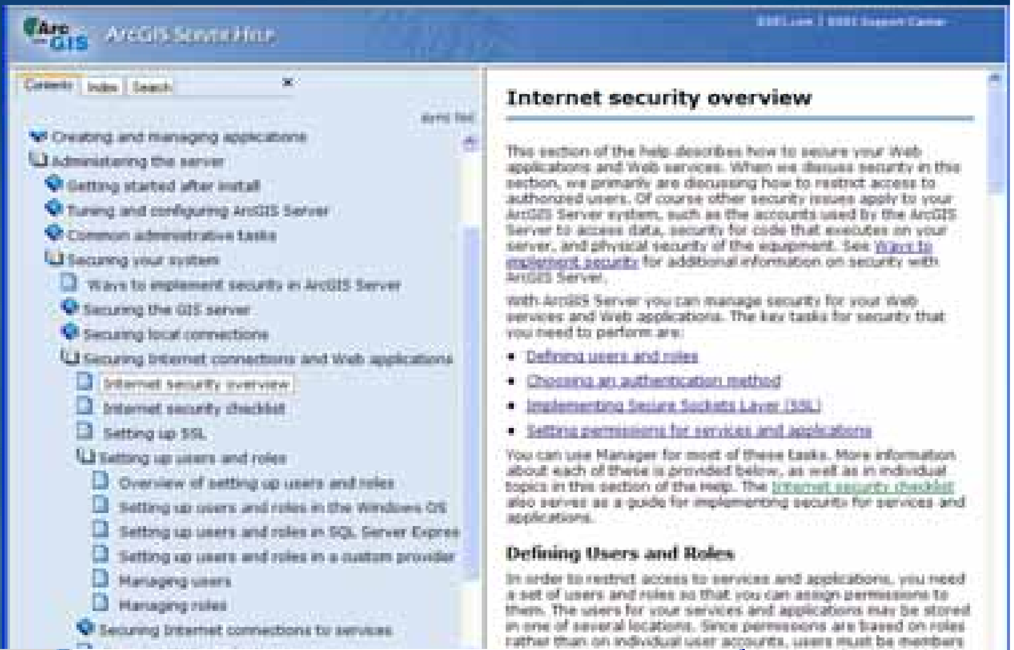
The map layer, toolbar item, and one of the QueryAttributesTask items are removed in the PreRenderComplete event of the Default.aspx code-behind page. The second QueryAttributesTask is hidden using an ASP.NET LoginView control. A

Demo

Modifying Web application content based on user’s role

Security resources for ArcGIS Server

- Server Help
- Web ADF Developer Help
- Help for JavaScript APIs
  - ArcGIS JavaScript
  - Virtual Earth
  - Google Maps
- Flex API Help
- Silverlight API Help



- Creating and managing applications
- Administering the server
  - Getting started after install
  - Tuning and configuring ArcGIS Server
  - Common administrative tasks
  - Securing your system
    - Ways to implement security in ArcGIS Server
    - Securing the GIS server
    - Securing local connections
    - Securing Internet connections and Web applications
      - Internet security overview
      - Internet security checklist
      - Setting up SSL
      - Setting up users and roles
        - Overview of setting up users and roles
        - Setting up users and roles in the Windows OS
        - Setting up users and roles in SQL Server Express
        - Setting up users and roles in a custom provider
        - Managing users
        - Managing roles
    - Securing Internet connections to services

Internet security overview

This section of the help describes how to secure your Web applications and Web services. When we discuss security in this section, we primarily are discussing how to restrict access to authorized users. Of course other security issues apply to your ArcGIS Server system, such as the accounts used by the ArcGIS Server to access data, security for code that executes on your server, and physical security of the equipment. See Ways to implement security for additional information on security with ArcGIS Server.

With ArcGIS Server you can manage security for your Web services and Web applications. The key tasks for security that you need to perform are:

- Defining users and roles
- Choosing an authentication method
- Implementing Secure Sockets Layer (SSL)
- Setting permissions for services and applications

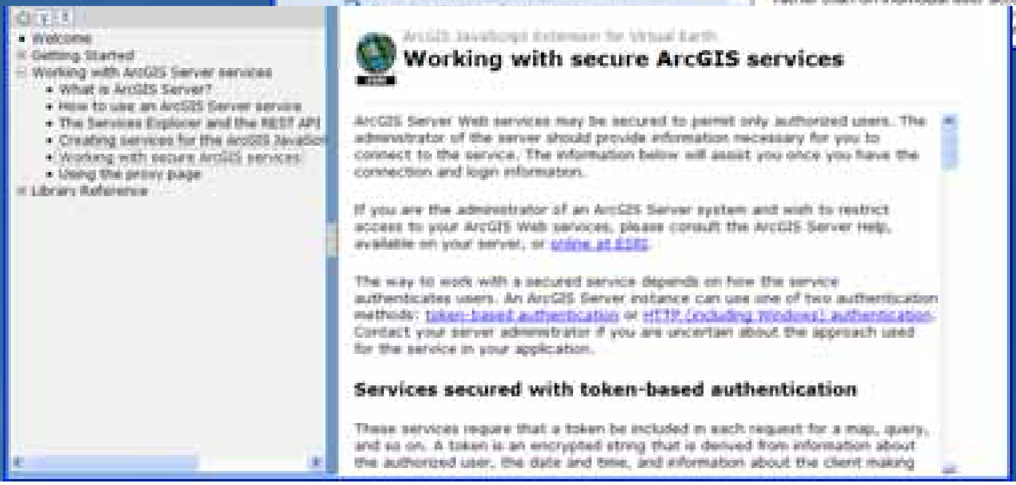
You can use Manager for most of these tasks. More information about each of these is provided below, as well as in individual topics in this section of the help. The Internet security checklist also serves as a guide for implementing security for services and applications.

Defining Users and Roles

In order to restrict access to services and applications, you need a set of users and roles so that you can assign permissions to them. The users for your services and applications may be stored in one of several locations. Since permissions are based on roles rather than on individual user accounts, users must be members

veral choices for the location for

tform standards for user and



- Welcome
- Getting Started
- Working with ArcGIS Server services
  - What is ArcGIS Server?
  - How to use an ArcGIS Server service
  - The Services Explorer and the REST API
  - Creating services for the ArcGIS JavaScrip
  - Working with secure ArcGIS services
  - Using the proxy page
- Library Reference

ArcGIS JavaScript Extension for Virtual Earth

Working with secure ArcGIS services

ArcGIS Server Web services may be secured to permit only authorized users. The administrator of the server should provide information necessary for you to connect to the service. The information below will assist you once you have the connection and login information.

If you are the administrator of an ArcGIS Server system and wish to restrict access to your ArcGIS Web services, please consult the ArcGIS Server Help, available on your server, or online at ESRI.

The way to work with a secured service depends on how the service authenticates users. An ArcGIS Server instance can use one of two authentication methods: token-based authentication or HTTP (including Windows) authentication. Contact your server administrator if you are uncertain about the approach used for the service in your application.

Services secured with token-based authentication

These services require that a token be included in each request for a map, query, and so on. A token is an encrypted string that is derived from information about the authorized user, the date and time, and information about the client making

Summary

- Manager at 9.3+ enables users to
  - Configure user and role stores
  - Secure Web applications
  - Secure GIS Web services
- Clients work with security
  - Desktop, Engine and Web ADF work seamlessly
  - SOAP and JavaScript clients may require working with tokens
- Use standard ASP.NET methods for finer-grain security in applications

Additional Resources

Questions, answers and information…

- ***Tech Talk***
  - *Outside this room right now!*
- **Meet the team**
  - **6:00 – 7:00 pm during the party in Oasis 2**
- ***Other sessions***
  - ***Advanced Map Caching Topics Wednesday 2:45 – 4:00 pm***
- ***ESRI Resource Centers***
  - **PPTs, code and video**

resources.esri.com

- ***Social Networking***

www.twitter.com/ESRIDevSummit

tinyurl.com/ESRIDevSummitFB

Want to Learn More?

ESRI Training and Education Resources

- Instructor-Led Training
  - ArcGIS Server: Web Administration Using the Microsoft .NET Framework
  - Developing Applications with ArcGIS Server Using the Microsoft .NET Framework
- Free Web Training Seminars
  - ArcGIS Server Setup and Administration
  - Building Applications with ArcGIS Server Using the Microsoft .NET Framework
  - Implementing Security for ArcGIS Server .NET Solutions

http://www.esri.com/training

Questions