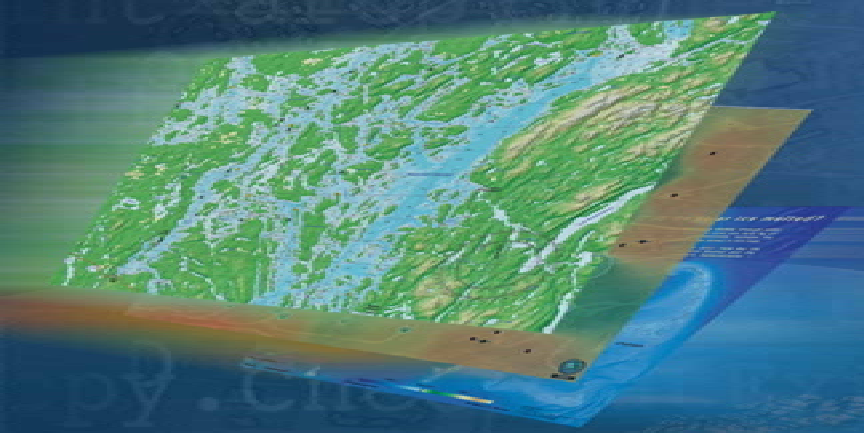
ESRI Developer Summit

March 22–25, 2010
Palm Springs, CA

Securing Your ArcGIS Server for the Microsoft .NET Framework Site

Tom Brenneman

Lloyd Heberlie



Schedule

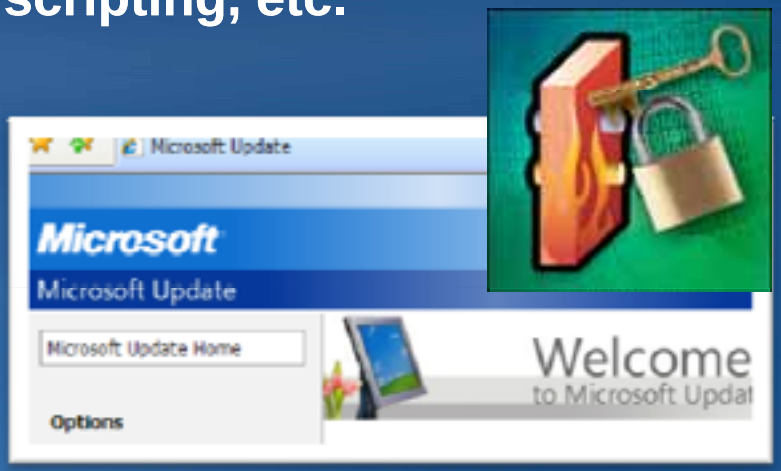
- Security overview
- Setup and configuration
- Securing GIS Web services
- Using the token service
  - Using a proxy page
- Securing Web applications
- Security pass through

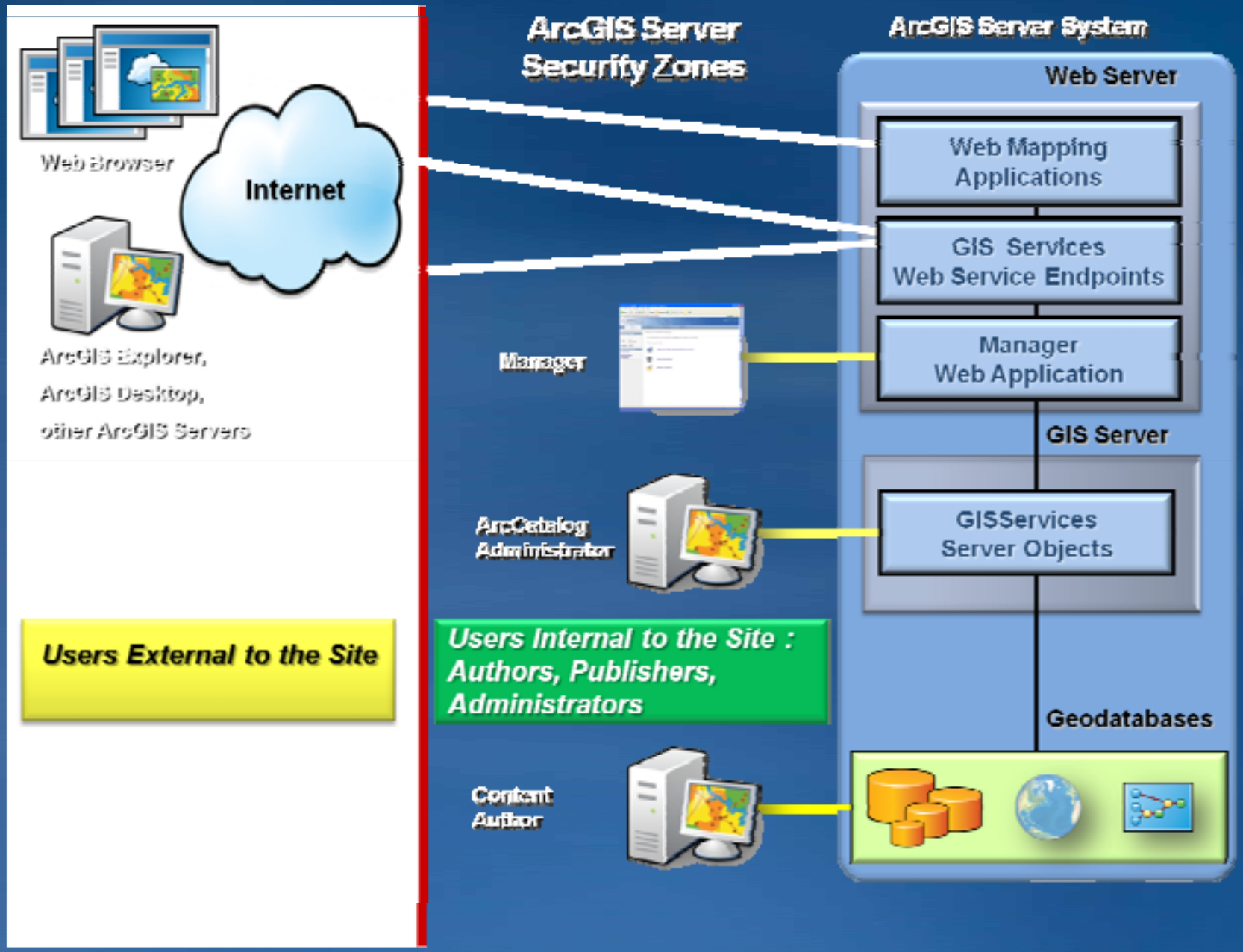
- We will answer questions at the end on the session

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.




ArcGIS Server
Security Zones
ArcGIS Server System
Web Server
Web Browser
Internet
Web Mapping
Applications
GIS Services
Web Service Endpoints
ArcGIS Explorer,
ArcGIS Desktop,
other ArcGIS Servers
Manager
Manager
Web Application
GIS Server
ArcCatalog
Administrator
GISServices
Server Objects
Users External to the Site
Users Internal to the Site :
Authors, Publishers,
Administrators
Geodatabases
Content
Author

Access control model for web users

- ArcGIS Server has role-based access control

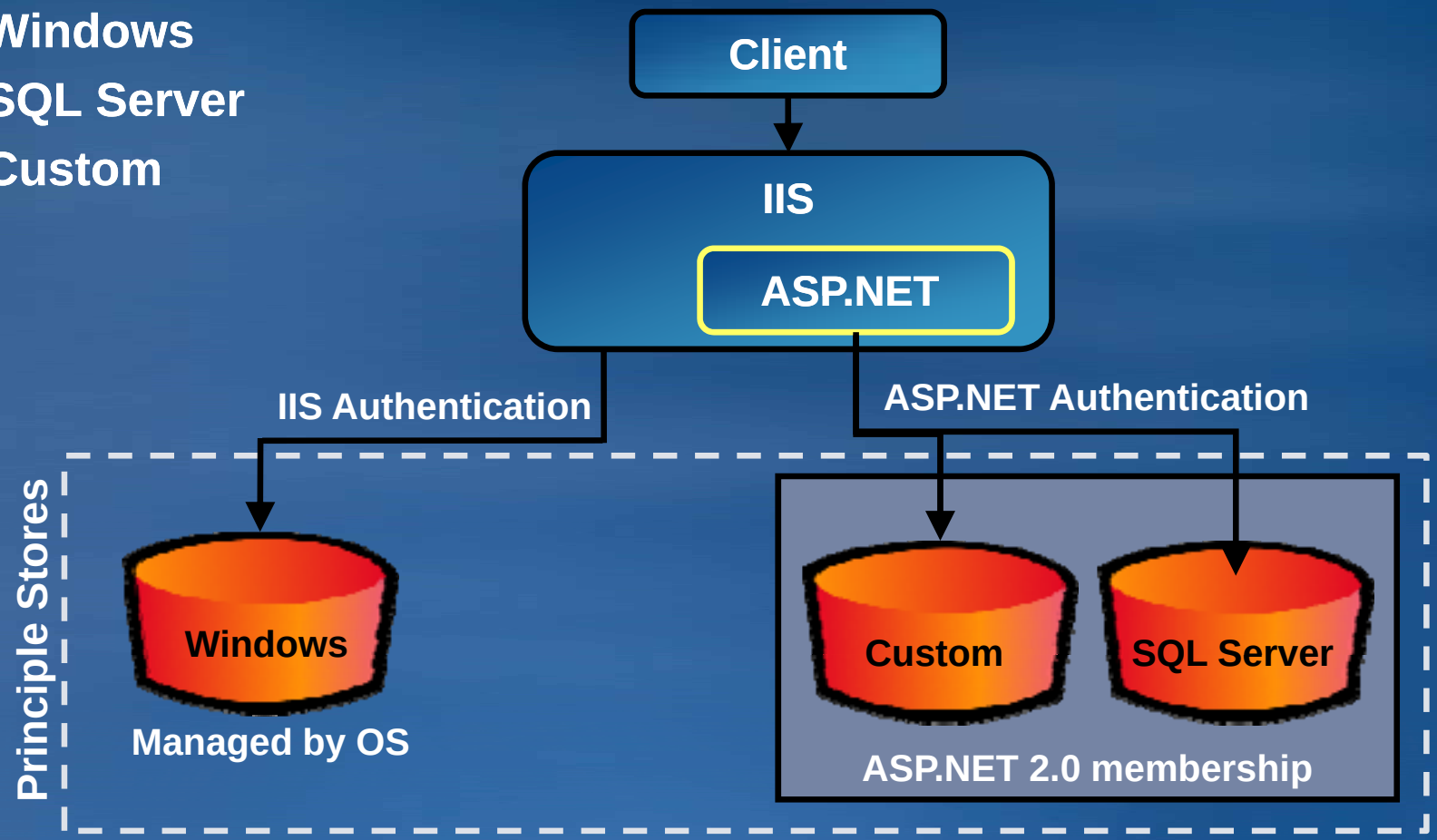
- Uses standard IIS or ASP.NET security
- IIS
  - Basic, Digest, Integrated Windows
- ASP.NET
  - Membership and role provider framework

Two phases of access control

- Authentication
  - Verification of user credentials
  - User name and password
- Authorization
  - Verification that user has access to specific resource
  - All authorization in ArcGIS Server based on roles

Authenticating users

- Authentication requires storage location for principles
  - Windows
  - SQL Server
  - Custom



Configuring security

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

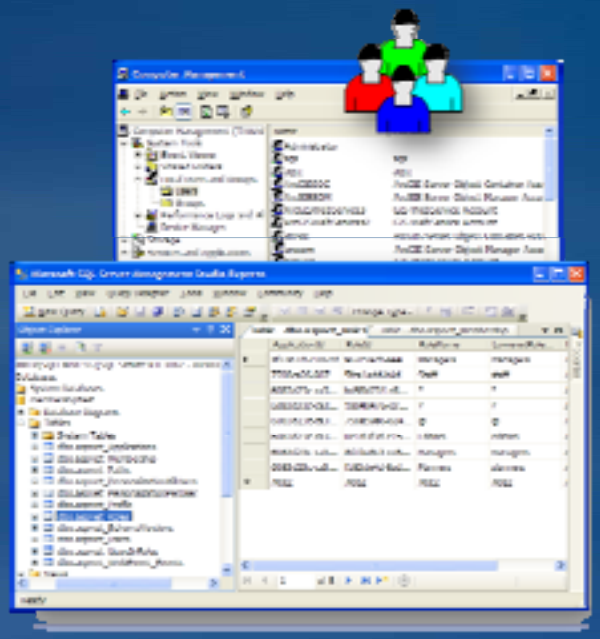
  - and/or -

- Secure GIS Web services using Manager

*or other tools for custom applications

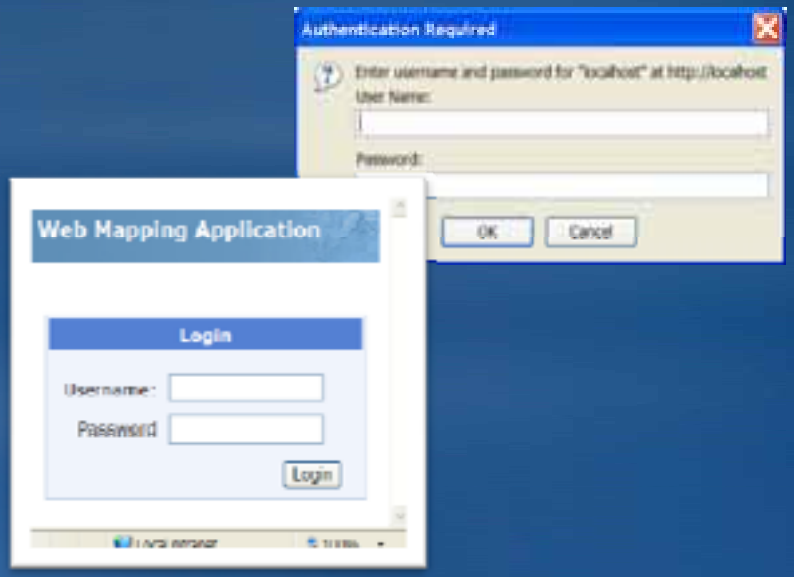
Decide where users and roles will be stored

- 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



How will users be authenticated?

- 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

More details on users and roles

- 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

Session agenda

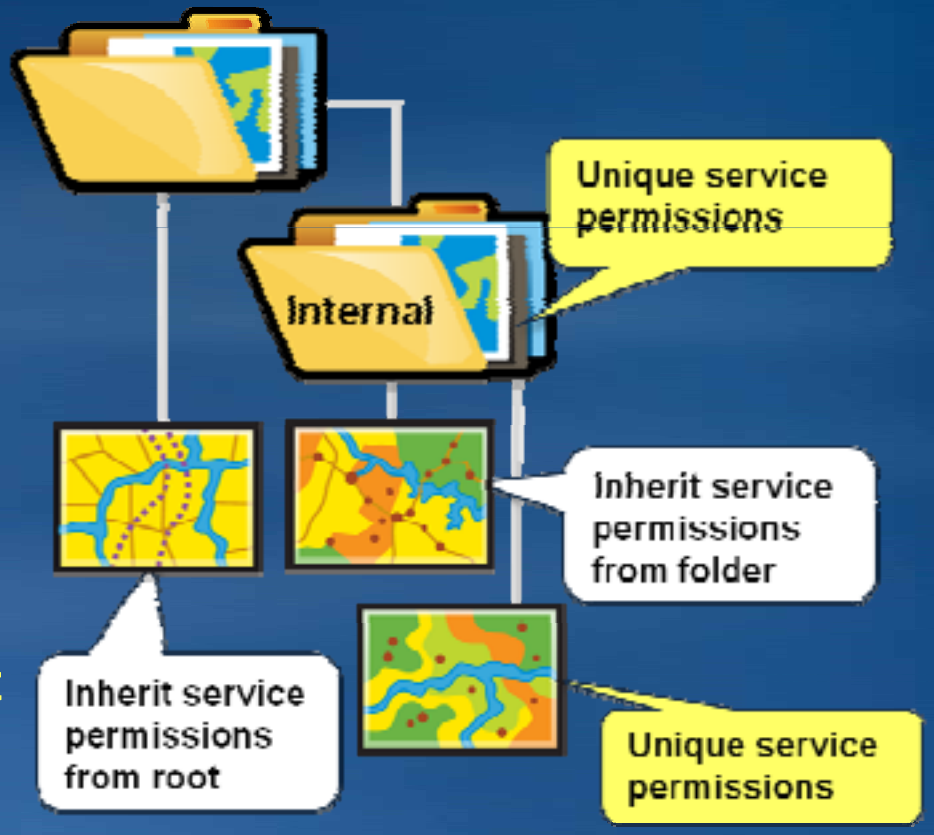
- Security overview
- Setup and configuration
- **Securing GIS Web services**
- Using the token service
  - Using a proxy page
- Securing Web applications
- Security pass through

Securing ArcGIS Server services

- Two ways to connect to an ArcGIS Server service
- Local connection
  - Works only on intranets
  - Access to all server functionality
  - User must be a member of the agsusers or agsadmin groups
- Web service (“Internet”) connections
  - SOAP, REST, WMS, KML
  - Works on intranets and over Internet

Securing GIS Web services

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

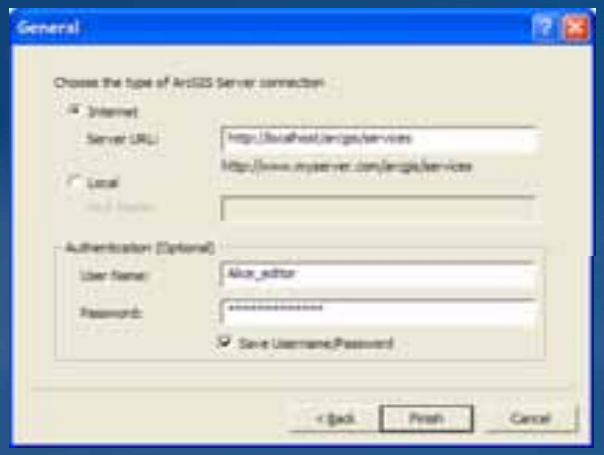


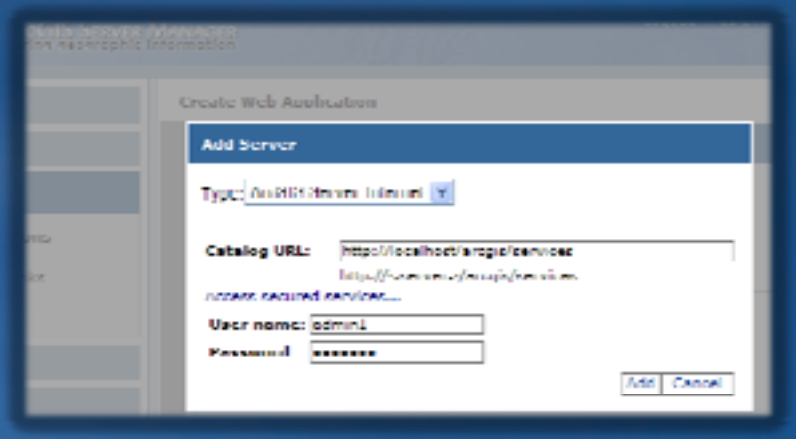
Transitioning ArcGIS Server from open access to secure access

- Enabling security for services is set separately from permissions
  - Security-Settings tab
- With no security, everyone has access to everything
- If you enable security before changing permissions, no one will be able to use existing services

Using secured services

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





When to use SSL for services

- Using IIS security (windows for users and groups)
- Data being displayed in dynamic service is sensitive
- Attributes of a query contain sensitive information
- Require Encrypted Web Access for folders and services
  - AGS Manager or ArcCatalog
  - You can't set encrypted access on a service, it has to be a folder

ESRI Developer Summit

March 22–25, 2010
Palm Springs, CA

Demo

Securing GIS Web services

Session agenda

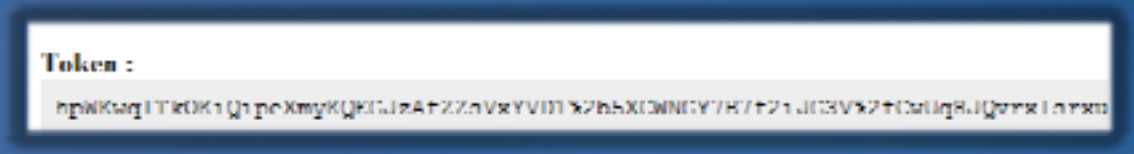
- Security overview
- Setup and configuration
- Securing GIS Web services
- Using the token service
  - Using a proxy page
- Securing Web applications
- Security pass through

The Token service

- User authentication web service
  - Token provided to access services
  - Uses HTTPS by default
- 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

What is in a Token?

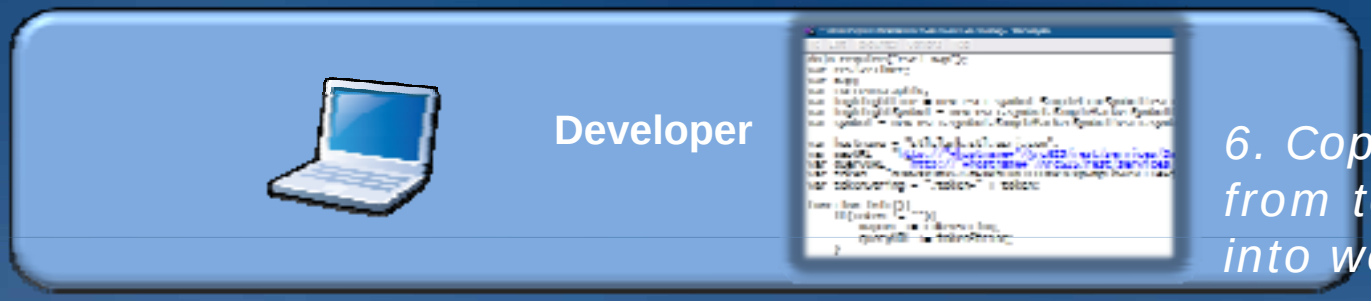
- Token is a string with encrypted information:
  - User name
  - Expiration time
  - Client ID (optional)
    - IP address or Web URL (HTTP Referrer)
    - If included, expiration can be a longer time period (weeks/months)
      - Used by most clients – Desktop, ADF, Web API/REST applications, etc.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



Working with the Token service

- Most clients will work with tokens automatically
  - ArcGIS Desktop, ArcGIS 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
  - Web API/RESTclients
    - Developer obtains a token from get-token Web page
    - Developer embeds token in application or proxy

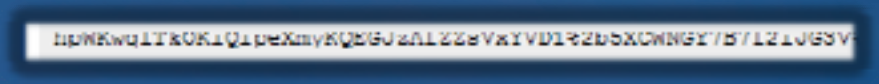
How developers commonly use the Token service

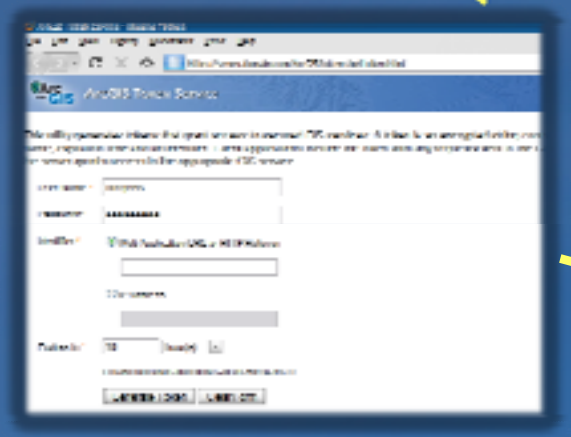


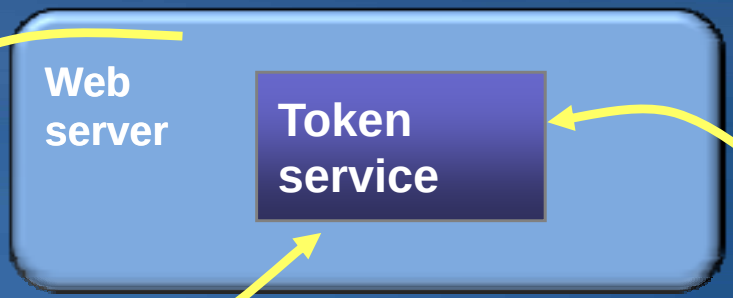
6. Copy/Paste token from token page into web app code

1. Developer uses Token service page
2. Enter required information

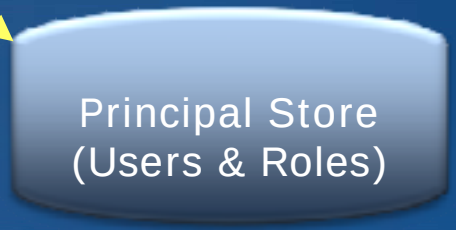
5. Service returns token







4. Credentials validated

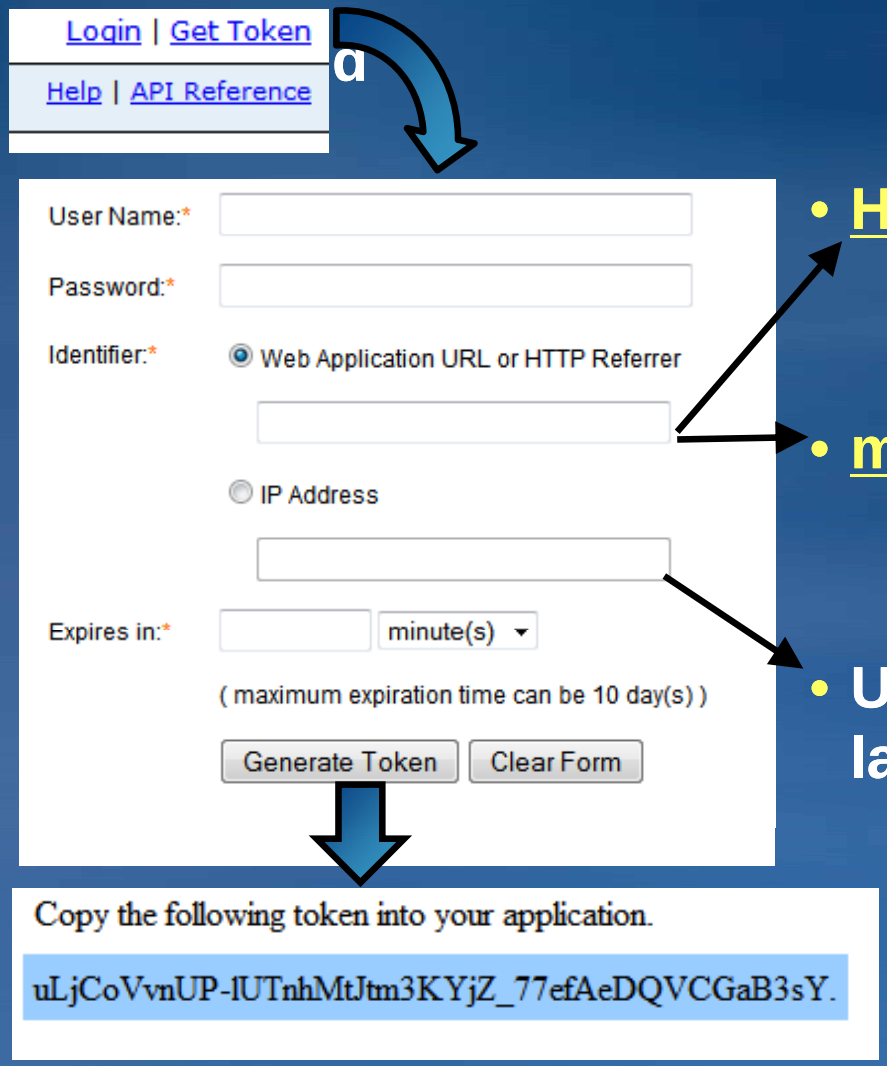


3. Client requests token

How the Web APIs/REST clients use the Token

Getting a token

Services Directory



- HTTP://myWebAppHost/myApp
  - App must be accessed via HTTP
- myWebAppHost/myApp
  - App can be accessed via HTTP or HTTPS
- Use IP with proxy page (more later)

Using a token

- GIS service can provide the Token service URL
- Append the token to the URL of the server
  - http://myserver/arcgis/services/USA/MapServer?token=hpWKwq...
- Use HTTPS for maximum security over unsecure networks
  - Needed to guard against token hijacking and replay attacks

ESRI Developer Summit

March 22–25, 2010
Palm Springs, CA

Demo

Using secure services in a flex application

Using a proxy page for token management

- Tokens in web API applications expire
  - HTTP error code of 498
  - Refresh embedded tokens periodically (source / config file update)
- Proxy page
  - Embed token using servers IP address as referrer
    - Pro: Token not exposed to client
    - Con: Tokens must still be updated in proxy page
  - Embed user name and password for dynamic token generation
    - Pro: No ongoing maintenance
    - Con: User name and password is unencrypted on the server
- Forum post contains dynamic proxy: http://forums.esri.com/Thread.asp?c=158&f=2396&t=297001

Proxy page security

- Proxy page contains no security logic
  - If left unsecure proxy provides unsecure back door to services
- Include proxy in web application and secure the application
- See Using the proxy page in JavaScript API help

ESRI Developer Summit

March 22–25, 2010
Palm Springs, CA

Demo

Using a proxy page for token management

Session agenda

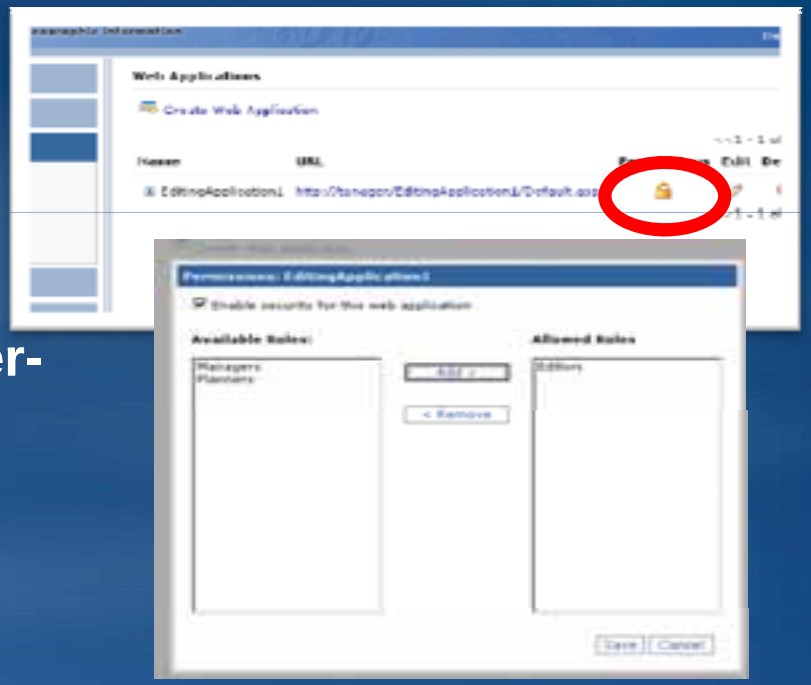
- Security overview
- Setup and configuration
- Securing GIS Web services
- Using the token service
  - Using a proxy page
- Securing Web applications
- Security pass through

Application security considerations

- Server based applications (.NET or Java Web ADF)
  - Only application needs to be secured
  - Web services are accessed from the server
- Browser based applications (JavaScript, Flex, Silverlight)
  - Application and web services need to be secured
  - Web services are accessed from the browser

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
- User will be prompted to login
  - ASP.Net security: Login.aspx page
  - IIS Security: Pop-up dialog



Securing Web API applications

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

ESRI Developer Summit

March 22–25, 2010
Palm Springs, CA

Demo

Securing a Web API application

Session agenda

- Security overview
- Setup and configuration
- Securing GIS Web services
- Using the token service
  - Using a proxy page
- Securing Web applications
- Security pass through

Passing identity from Web ADF application to services

- 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:
    - SecurityPassthrough_Win:
    - SecurityPassthrough_WinInternet
    - Common_Security – Page content controlled by logged in user

Passing identity from Web API application to services secured using windows

- JavaScript, Flex, and Silverlight
  - It just works
- Integrated Windows / Basic automatically pass credentials from application to web services

Passing identity from Web API application to services secured using ASP.NET

- Web application requests token from tokens services
  - Tokens service parameters
    - username
    - password
    - clientid (ref.[URL], ip.[IP ADDRESS])
    - Expiration (minutes)
  - E.g. : https://host/ArcGIS/tokens/?request=getToken&username=user&password=pass&clientid=ref.myAppHost&expiration=10
- Append token to layer
- Silverlight – must use short lived token – see February 15 2010
  - Refresh token using a timer

ESRI Developer Summit

March 22–25, 2010
Palm Springs, CA

Demo

Modifying Web application content based on user's role

Security resources for ArcGIS Server

- ArcGIS Server Resource Center
  - http://resources.esri.com
  - Accessing secure services: Web APIs
- Enterprise Resource Center
  - http://resources.esri.com/enterprisegis/
- Supporting Resources for ArcGIS Server
  - http://resources.esri.com/arcgisserver/index.cfm?fa=support
  - ArcGIS Server Manager Help
  - Web APIs, REST, SOAP Developer Help

Summary

- ArcGIS Server Manager 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 REST clients may require working with tokens
- Use standard ASP.NET methods for finer-grain security in applications

Additional Resources

- Other sessions
  - Advanced Map Caching Topics
- Social Networking
  - twitter @esridevsummit
  - facebook facebook.com/esridevsummit

Want to Learn More?

ESRI Training and Education Resources

- **Instructor-Led (Classroom) Training**
  - **ArcGIS Server: Web Administration Using the Microsoft .NET Framework**

- **Self-Study (Virtual Campus) Training**
  - **ArcGIS Server Setup and Administration**
  - **Implementing Security for ArcGIS Server .NET Solutions**

http://www.esri.com/training

Questions

- Thank you
- Please fill out the survey