Session: 500121

Agenda key: 33MI

System i Access for Web Security Considerations

http://www.ibm.com/eserver/iseries/access/web/

Mark Vanderwiel
IBM Rochester – System i Access for Linux and Windows Development
vanderwl@us.ibm.com

Doug Beauchene
IBM Rochester – System i Access for Web Development
dougbeau@us.ibm.com

i want stress-free IT.

i want control.

i want an i.

System i Access for Web Sessions/LABs

22CC	409136		Get to the Web Fast with System i Access for Web
25LA	520027	NEW!	LAB: Getting Started with System i Access for Web
32MI	409160		Database Access with System i Access for Web
33MI	500121		System i Access for Web – Security Considerations
35MI	410068		System i Access for Web – Setup and Configuration
36MF	440281		Run 5250 through a Browser using System i Access for Web
41LA	450047	🎖	LAB: System i Access for Web: Installation and Configuration
42LA	450047	🎖	LAB: System i Access for Web: Installation and Configuration
44MN	420016		Build a Home Page to i5/OS using System i Access for Web
45MN	420015		Tips and Techniques for System i Access for Web
53LA	420063		LAB: Test Drive System i Access for Web
55MM	470021		System i Access for Web runs in a Portal
56MM	480144		Programming with System i Access for Web

🎖 **Voted "Best Traditional Lab" at Spring and Fall 2005 COMMON**

Try out System i Access for Web for yourself!

Start your browser and connect to the following web site:
http://iseriesd.dfw.ibm.com/webaccess/iWAHome (case sensitive)

User ID = WUSER **Password = DEMO2PWD**	**This shows the basic look of Access for Web as we ship it. You can try various functions -- including working with printer output, creating database requests, etc. Click on the 5250 tab, sign onto the i5/OS, then start an RPG application called BOATS and run it.**
User ID = BOATADMIN **Password = DEMO2PWD**	**This is an example of how a customer might design a web page for their use. You will see that an end user could start the same BOATS application by clicking on the 5250 session -- or they could have used WebFacing to run the application. You will also see other links that would let a user work with spoolfile information, work with IFS, run database requests, etc..**

Agenda

Security considerations in the web environment relative to System i Access for Web

- System i Access for Web overview
  - What is it
  - The environment it runs in
- Environment security
  - SSL and VPN
- Authentication security options
  - How does the user authenticate to System i Access for Web?
  - How does System i Access for Web authenticate with i5/OS?
  - System i Access for Web in a WebSphere Single Signon (SSO) environment
  - Special considerations for 5250 and database
- System i Access for Web and Portal
  - How are things different?
- System i Access for Web runtime (usage) security
  - Use of policies
  - Custom homepage/template
- Additional information
  - Websites
  - Application Server Authentication: WebSphere Global Security
  - Application Server Authentication: EIM domain configuration
  - Application Server Authentication: EIM Identity Token Connector

What is System i Access for Web?

V5R3/V5R4 i5/OS

End users can leverage business information, applications, and resources across an enterprise by extending 5/OS resources to the client desktop through a web browser

- Provides a web-based view of i5/OS applications and resources through a browser

- Runs on i5/OS

- Requires no software be installed on the client other than a browser

- Provides two offerings:

  - Web application
  - Portal application

- Windows
- Linux
- Macintosh
- UNIX....

Mozilla

Netscape

Opera

Opera

Internet Explorer

Firefox
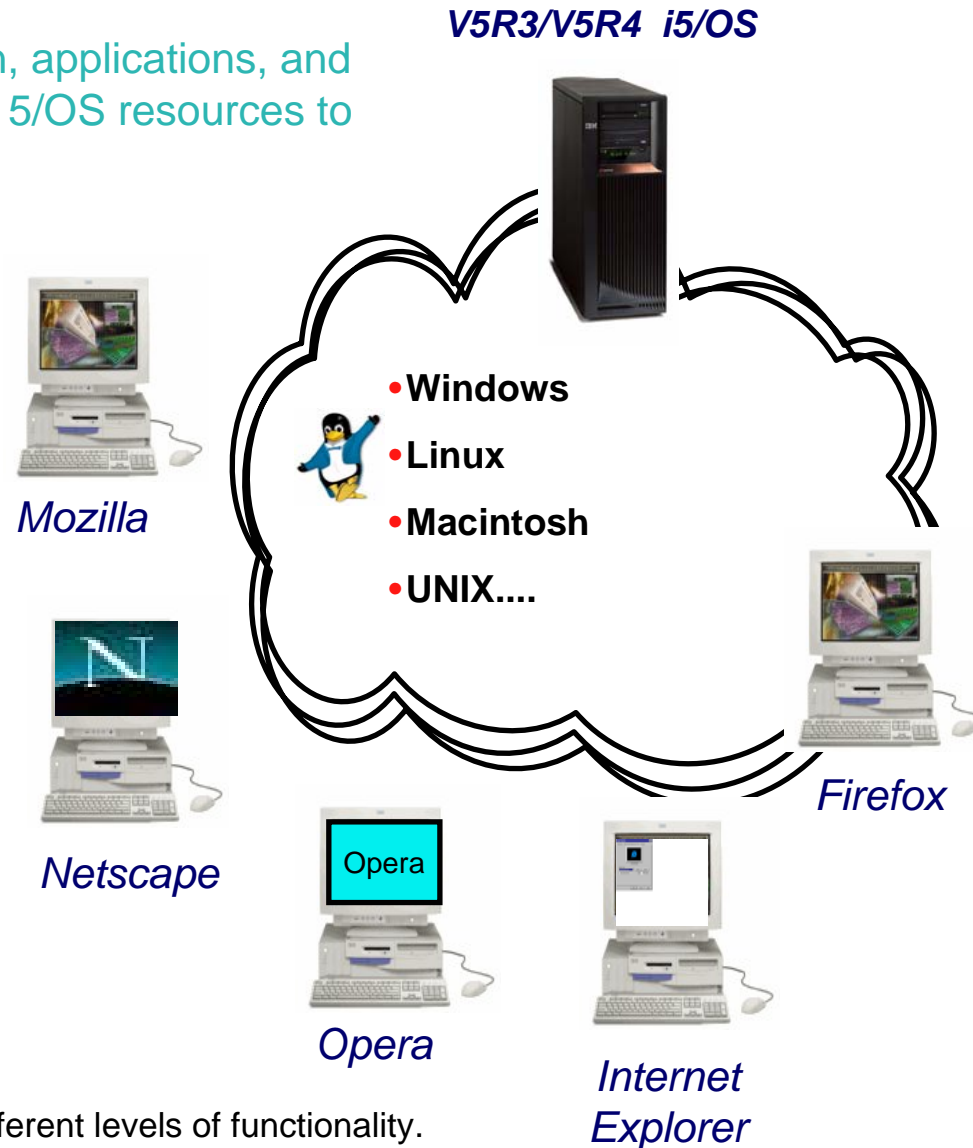
Note: Web application and portal application have different levels of functionality.

System i Access for Web Environment

HTTP
HTTPS

Web Browser

System i Access for Web

TN5250,
sockets

HTTP
web server

Web Application
Server

i5/OS host servers
5250 applications
Database
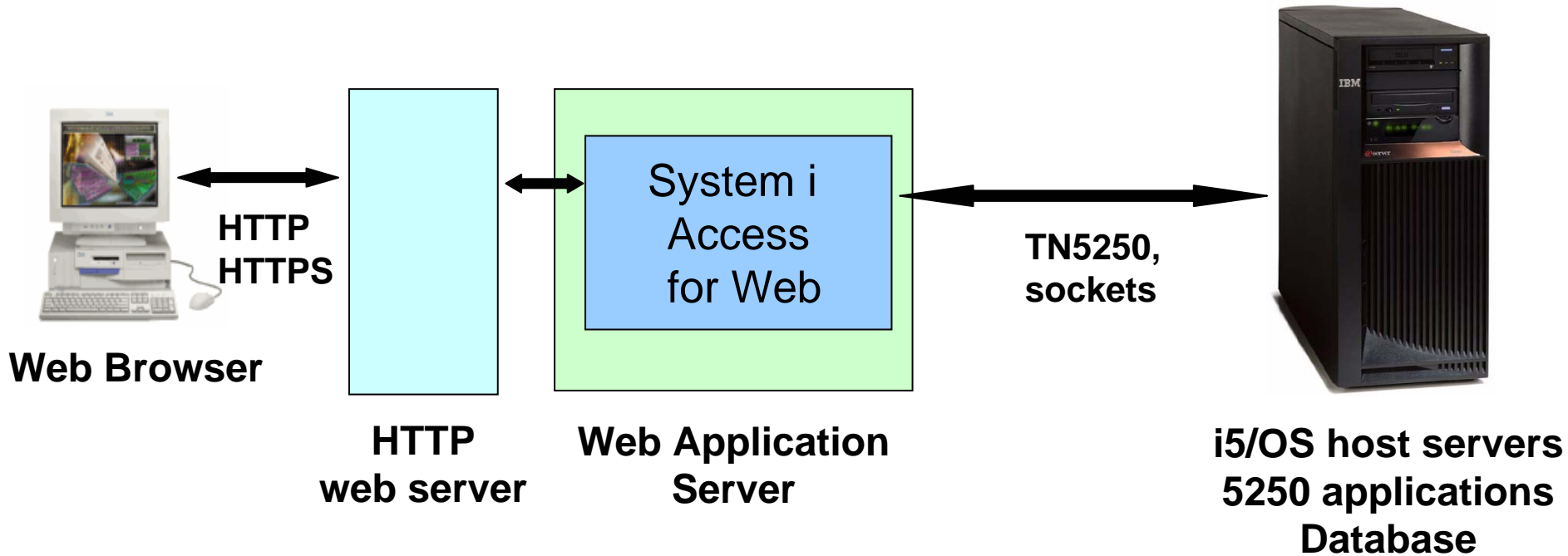
Agenda

Environment security

- SSL and VPN

System i Access for Web Environment (continued)

HTTP or HTTPS

sockets
i5/OS host server ports
telnet port

System i Access for Web
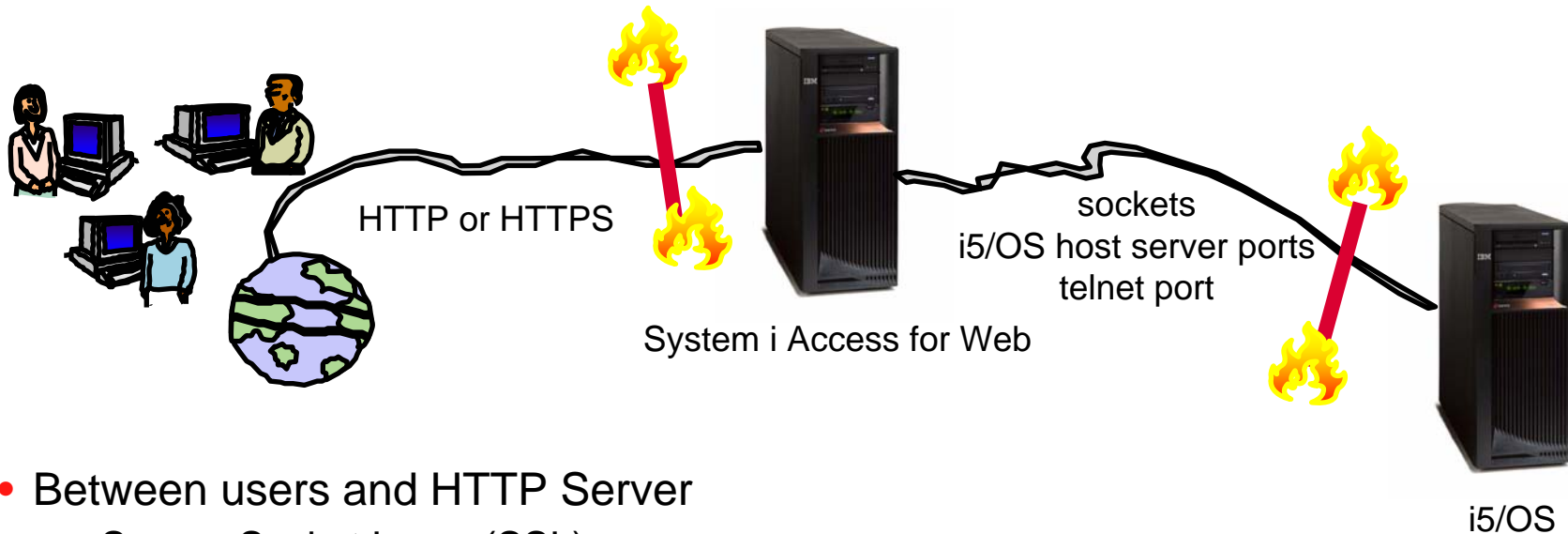
i5/OS

- Between users and HTTP Server
    - Secure Socket Layer (SSL)
    - Virtual Private Networking (VPN)
    - Firewalls
- Between System i Access for Web and i5/OS
    - VPN
    - Firewalls

Secure Sockets Layer

- Used for data confidentiality between Web browser and HTTP server
  - Digital certificates used to determine trust relationships
  - Point to Point encryption for all data (PC App to Server App)
  - Part of the standard HTTPS protocol

- See Info Center for specific details on Configuration and Setup.
  - See the "Configure WebSphere Security" topic

- Levels of SSL
  - TLSv1, SSLv3 recommended, use 128-bit or higher
  - SSLv2 should not be used anymore. Disable in clients and server (APAR SE25734)

Virtual Private Networking

- Used for data confidentiality between Web browser and HTTP server
  - Digital certificates and User authorization used establish tunnel
  - End to End encryption for all data (PC to Server tunnel)
  - Allows any protocol, including standard HTTP

- See Info Center for specific details on Configuration and Setup.
  - See the "Virtual Private Networking" topic

- Redbooks
  - IBM System i Security Guide for IBM i5/OS Version 5 Release 4 (SG24-6668-01)
  - OS/400 V5R2 Virtual Private Networks (REDP-0153-01)

Agenda

Authentication security options

- How does the user authenticate to System i Access for Web?
- How does System i Access for Web authenticate with i5/OS?
- System i Access for Web in a WebSphere Single Signon (SSO) environment
- Special considerations for 5250 and database

Authentication

- Authentication is verifying the identity of the user

- System i Access for Web supports two types of authentication
  - Application
    - System i Access for Web handles the authentication
  - Application Server
    - WebSphere Application Server handles the authentication

- Specified by the AUTHTYPE parameter on the CFGACCWEB2 command
  - Application: AUTHTYPE(*APP)
  - Application Server: AUTHTYPE(*APPSVR)

Authorization

- Authorization is verifying that authenticated users have permission to access requested resources

- System i Access for Web uses the i5/OS user profile and object level security to authorize access to i5/OS resources

- System i Access for Web provides application level control of access to functions through policies
  - Policies can be administered at the i5/OS user and group profile levels

My Home Page	**Policies**		
My Folder			
Print	Profile: **JHANSEN**		
Messages			
Jobs	**Action**	**Category**	**Description**	**Access**
5250	✎	5250	5250 user interface custom settings.	Allowed
Database	✎	Command	Run batch command custom settings.	Allowed
Files	✎	Customize	Preferences and policy administration custom settings.	Allowed
Command	✎	Database	Database tables, requests, and run SQL custom settings.	Allowed
Download	✎	Database connections	Create and edit database connection definitions.	Allowed
Customize	✎	Download	Download packages custom settings.	Allowed
• Preferences	✎	Files	Integrated file system and file share custom settings.	Allowed
• Policies	✎	General	Page layout, language and character set custom settings.	Allowed
• Settings	✎	Jobs	Work with jobs custom settings.	Allowed
• Transfer configuration	✎	Mail	Send mail custom settings.	Allowed
Other	✎	Messages	Display messages, send messages, and message queue custom settings.	Allowed

Application Authentication

- System i Access for Web handles authentication

- i5/OS user profile and password
  - Hostname specified by the TGTSVR parameter on the CFGACCWEB2 command

- Method: HTTP basic authentication
  - RFC2617
  - User profile and password are encoded (not encrypted) in the HTTP headers and should be protected

Application Server Authentication

- WebSphere handles authentication

- WebSphere credentials
    - Typically a user ID and password
    - Authenticated with the active WebSphere user registry

- System i Access for Web uses Enterprise Identity Mapping (EIM) to map the authenticated WebSphere user identity to an i5/OS user profile
    - System i Access for Web identifies the user by the mapped i5/OS user profile
    - i5/OS user profile is used to authorize access to i5/OS resources using object level security

Application Server Authentication (continued)

- System i Access for Web supports two methods of gathering credentials
  - HTTP basic authentication
    - User ID and password are encoded (not encrypted) in the HTTP headers and should be protected
  - Form-based authentication
    - User ID and password are clear text and should be protected

- Specified by the AUTHMETHOD parameter on the CFGACCWEB2 command
  - HTTP basic authentication: AUTHMETHOD(*BASIC)
  - Form-based authentication: AUTHMETHOD(*FORM)
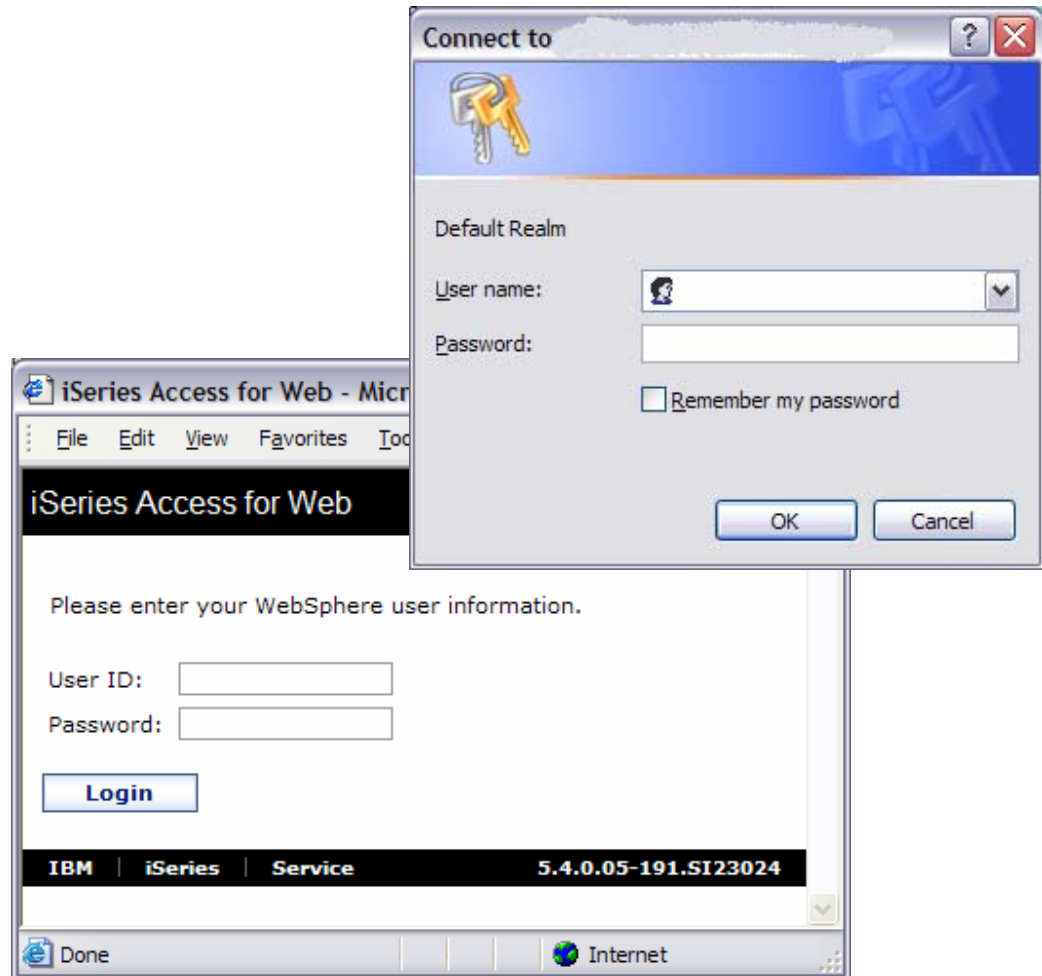
Application Server Authentication Required Configuration

- WebSphere with global security enabled and an active user registry to authenticate users

- An EIM domain configuration for i5/OS to enable mapping of WebSphere user identities to i5/OS user profiles

- The EIM Identity Token Connector (resource adapter) installed and configured in WebSphere
  - Used to request identity tokens (encrypted data strings that represent the authenticated WebSphere user identity) which are input to EIM lookup operations.

- **Note**: See Additional Information charts at the end of this presentation for more information on the above required configuration.

Application Server Authentication
Configure System i Access for Web

- Configure System i Access for Web
  - CFGACCWEB2
    AUTHTYPE(*APPSVR)
    AUTHMETHOD(*FORM) …
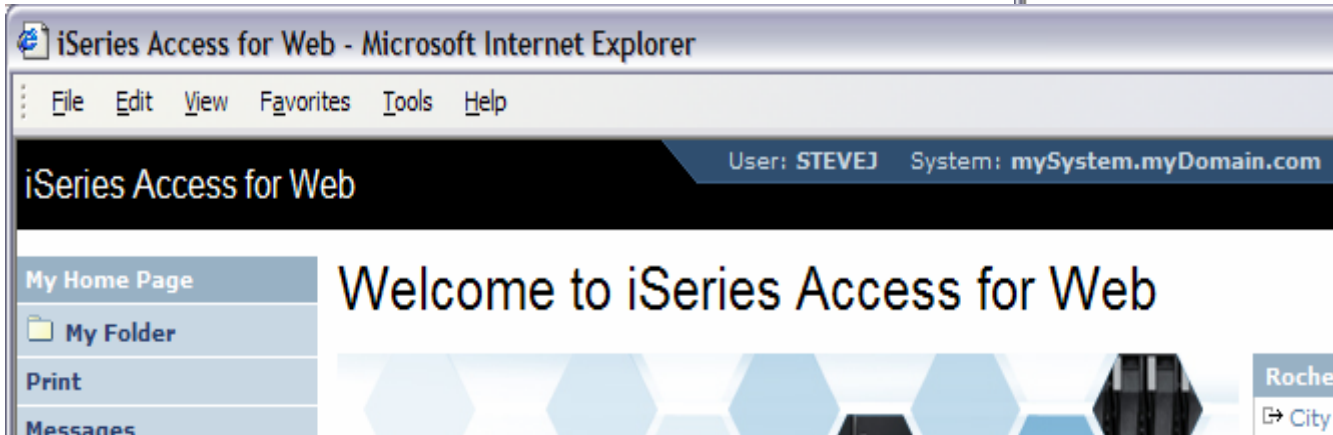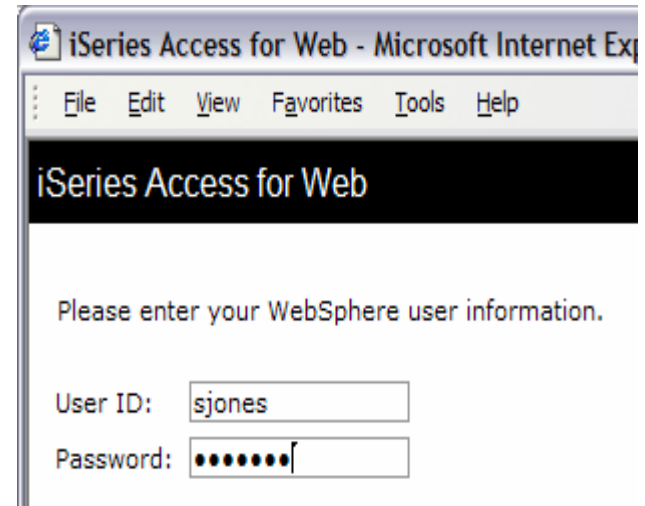
Application Server Authentication WebSphere Single Signon (SSO)

- Allows users to authenticate one time when
  - Accessing WebSphere resources and Lotus Domino resources
  - Accessing resources in multiple WebSphere Application Server domains

- Requirements for WebSphere SSO
  - Use the same user registry
  - Set the domain name service (DNS) domain
  - Share the LTPA keys (export/import)

- Refer to the WebSphere Information Center for details
  - Search for "single signon"

- System i Access for Web Information Center contains a example of setting up the WebSphere SSO environment.

Application Server Authentication WebSphere SSO (continued)

- Enable SSO

- Specify DNS domain

- Share LTPA keys

Global security > LTPA

| Generate Keys | Import keys | Export Keys |

General Properties

* Password

●●●●●●●●●●

* Confirm password

●●●●●●●●●●●

Additional Properties

Single signon (SSO)

Trust association

Authentication

⊟ Authentication mechanisms

LTPA

⊞ Authentication protocol

⊞ JAAS Configuration

⊞ Resources

⊟ Security

  ▪ Global security

  ▪ SSL

⊞ Environment

⊞ System administration

Global security > Single signon (SSO)

General Properties

☑ Enabled

☐ Requires SSL

Domain name

myDomain.com

☑ Interoperability Mode

☑ Web inbound security attribute propagation

| Apply | OK | Reset | Cancel |

5250 Sessions

Start Session

Server
Server: [   ]
Port: [23]
Code page: [37 ▼]

Workstation ID ❓
○ Use user ID
⦿ Specify workstation ID [   ]
☐ Avoid duplicates for this user
☑ Avoid duplicates with other users

General ❓
Initial macro: [▼]
☐ Bypass signon
☐ Display HTML data in fields

[**Start Session**]

- 5250 sessions can be started to any system running i5/OS

- Must provide user profile and password on i5/OS Sign On screen

Sign On

System . . . . . :
Subsystem . . . . :   QINTER
Display . . . . . :   QPADEV0006

User . . . .   [   ]
Password . . . .   [   ]
Program/procedure . . . .   [   ]
Menu . . . .   [   ]
Current library . . . .   [   ]

RELEASE: V05R03M00
DRIVER: 2600722

USE OF THIS SYSTEM IS FOR IBM   MANAGEMENT APPROVED PURPOSES ONLY.
USE IS SUBJECT TO AUDIT AT   ANY TIME BY IBM MANAGEMENT.

(C) COPYRIGHT IBM CORP. 1980, 2003.

37   6,53

5250 Session Bypass Signon

- QRMTSIGN system value must be *VERIFY

- Select bypass signon when starting or configuring a session

Configure New Session

General

Session: mySession   * required

Default view: Web

Initial macro:

☑ Bypass signon

☐ Display HTML data in fields

☑ Enable advanced JavaScript functions

Server

Server: mySystem.myDomain.com

Port: 23

Start Session

Server

Server: mySystem.myDomain.com

Port: 23

Code page: 37

Workstation ID

○ Use user ID

◉ Specify workstation ID

☐ Avoid duplicates for this user

☑ Avoid duplicates with other users

General

Initial macro:

☑ Bypass signon

☐ Display HTML data in fields

Start Session

- System i Access for Web must be configured for application authentication or bypass signon is not available
    - CFGACCWEB2 AUTHTYPE(*APP) …

5250 Session Signon Macro

- Record a macro to sign on

- Edit the macro
  - Replace user profile with [user]
  - Replace password with [password]

- Select as initial macro when starting session

Macro: **Signon**

[cursor 6,53][erasefld][user]cursor 7,53][erasefld][password][enter][wait][enter][wait]

Server ❓

Server: mySystem.myDomain.com

Port: 23

Code page: 37

Workstation ID ❓

○ Use user ID
◉ Specify workstation ID [_____]
☐ Avoid duplicates for this user
☑ Avoid duplicates with other users

General ❓

Initial macro: Signon ▼

☐ Bypass signon
☐ Display HTML data in fields

Start Session

5250 Session
Signon Macro (continued)

- Select as initial macro when configuring a session

- System i Access for Web must be configured for application authentication or [password] substitution in macros will not work
  - CFGACCWEB2 AUTHTYPE(*APP) …

Configure New Session

General

Session: mySession   * required

Default view: Web

Initial macro: Signon

☐ Bypass signon

☐ Display HTML data in fields

☑ Enable advanced JavaScript functions

Server

Server: mySystem.myDomain.com

Database Connections

- A Database connection defines characteristics of the JDBC connection to the database
  - Target database
  - JDBC driver
  - Other attributes

- System i Access for Web uses the IBM Toolbox for Java JDBC Driver

- Additional database connections are created using Customize function
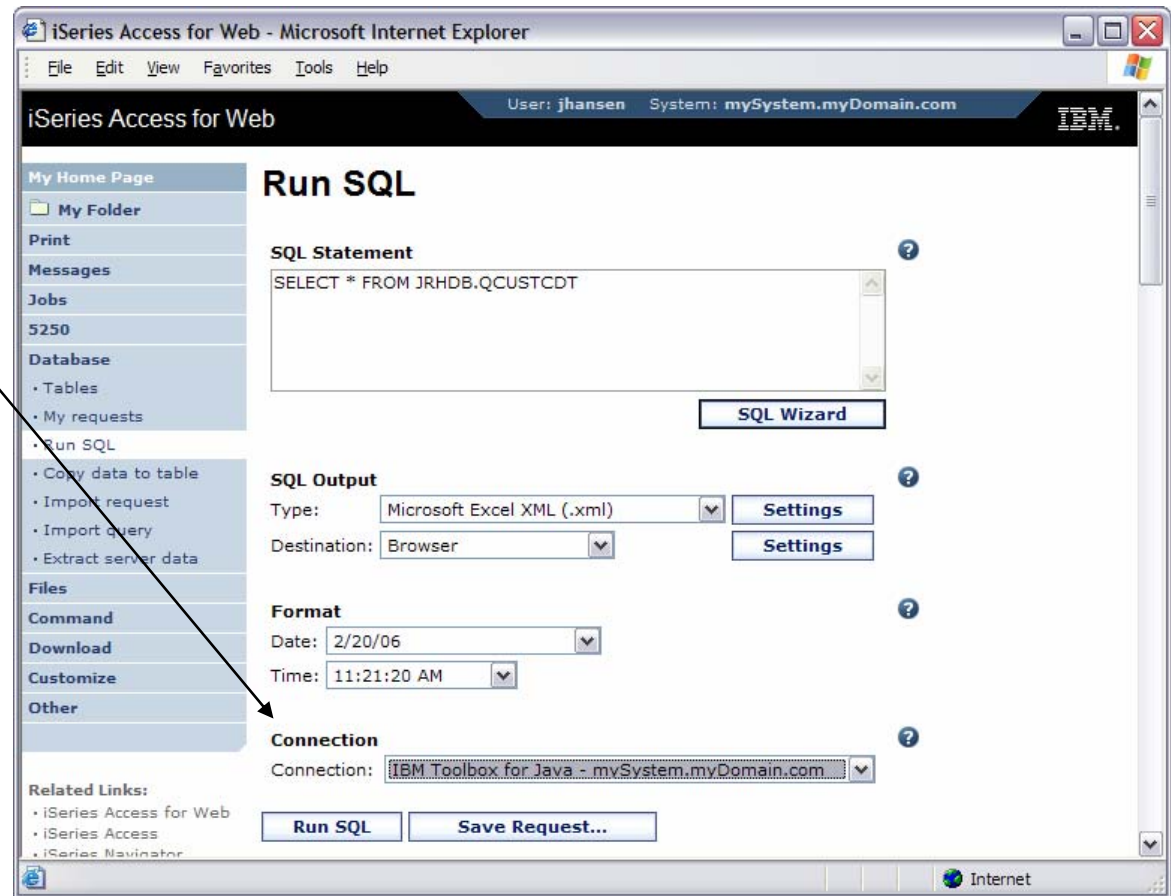
Adding Database Connections

- Two types of database connection definitions are supported
  - Driver manager
  - Data source

- Data sources are managed by WebSphere and can be used by other applications

Database Connection Considerations

- Application Authentication
  - Driver manager connections
    - System i Access for Web always specifies the authenticated user profile and password when getting a connection from the driver manager
    - Credentials can be specified as properties on the JDBC URL for the IBM Toolbox for Java JDBC Driver
      - Override values specified when getting a connection from the driver manager

  - Data source connections
    - System i Access for Web always specifies the authenticated user profile and password when getting a connection from a data source.

Database Connection Considerations (continued)

- Application Server Authentication
  - Driver manager connections
    - Credentials can be specified as properties on the JDBC URL for the IBM Toolbox for Java JDBC Driver
      - If credentials are not specified, System i Access for Web will use identity tokens and EIM
    - Credentials must be specified as properties on the JDBC URL for other drivers

  - Data source connections
    - A component-managed authentication alias must be configured
    - Credentials from the authentication alias are always used

Agenda

System i Access for Web and Portal

- How are things different?

Portal

- Portal provides a single point of personalized interaction with applications, content, processes and people

- Integrate data and applications from various sources into one user experience
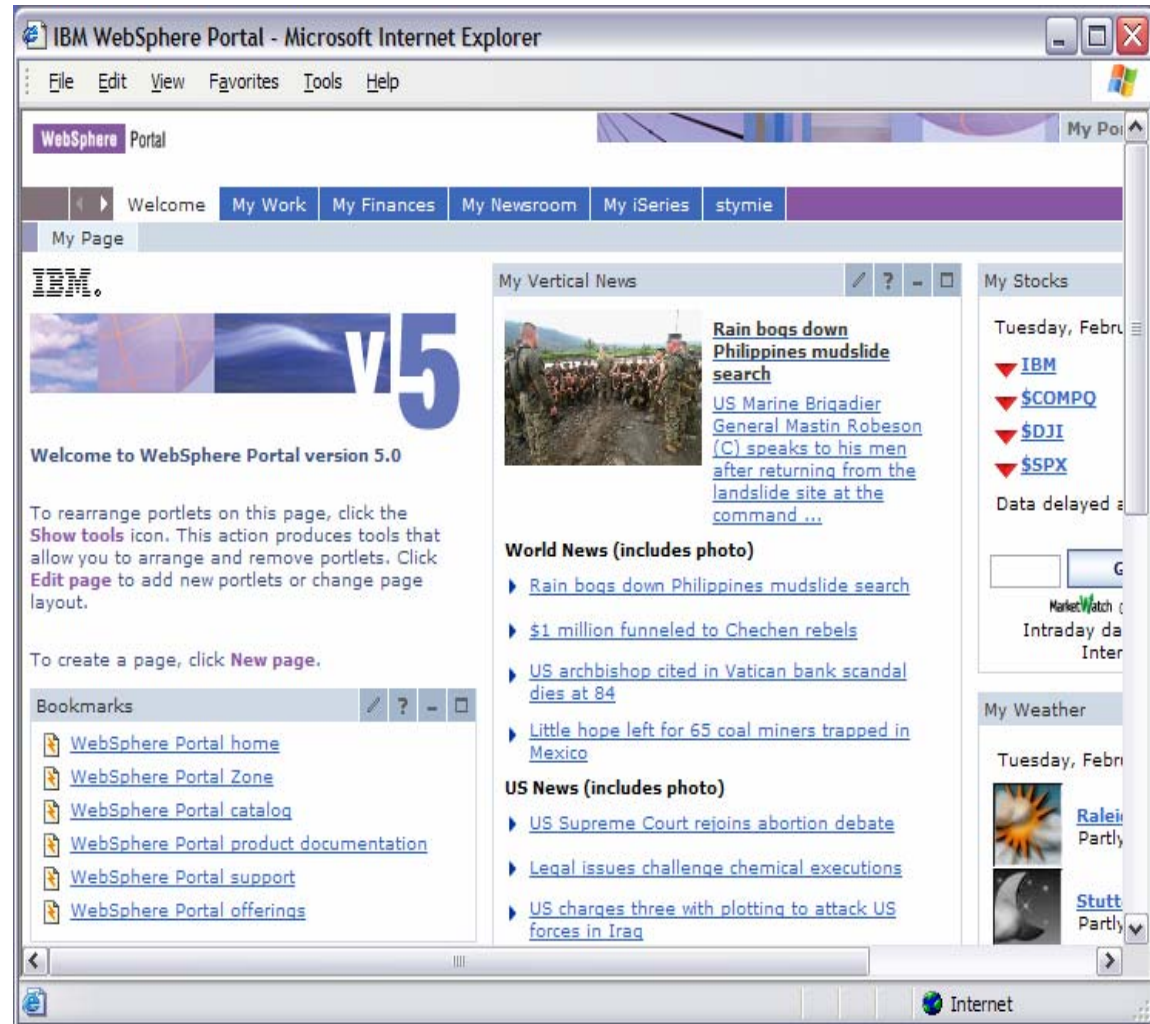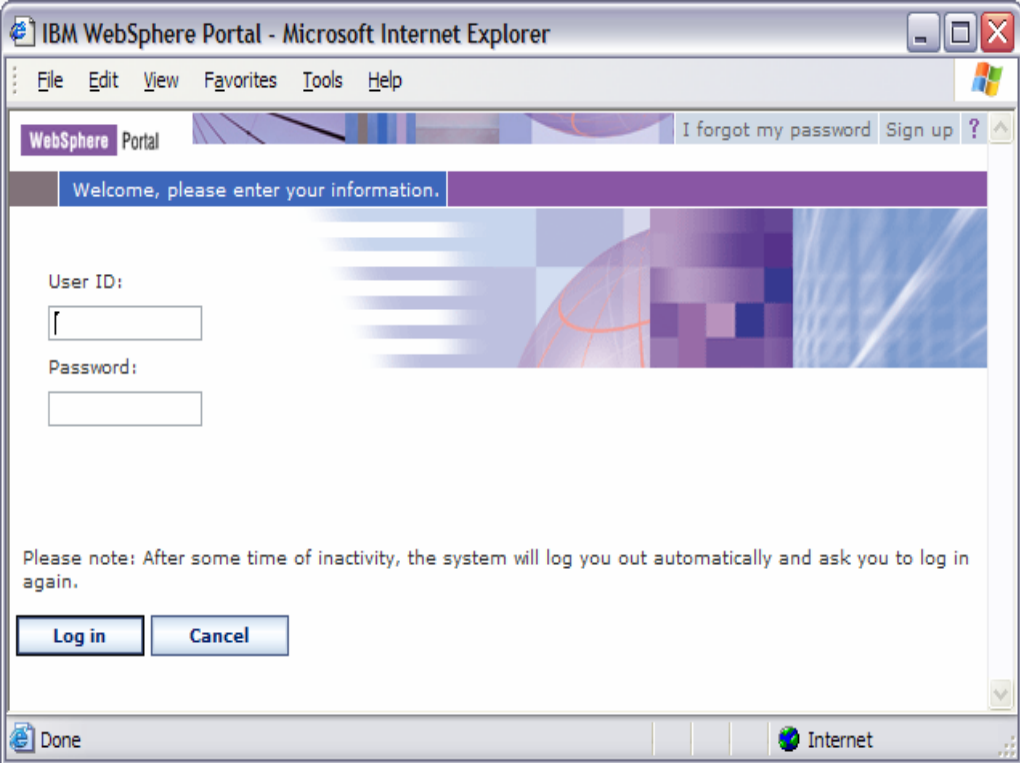
Portal Application

- System i Access for Web portlets integrate access to i5/OS resources in a portal environment

- Function is similar to the web application
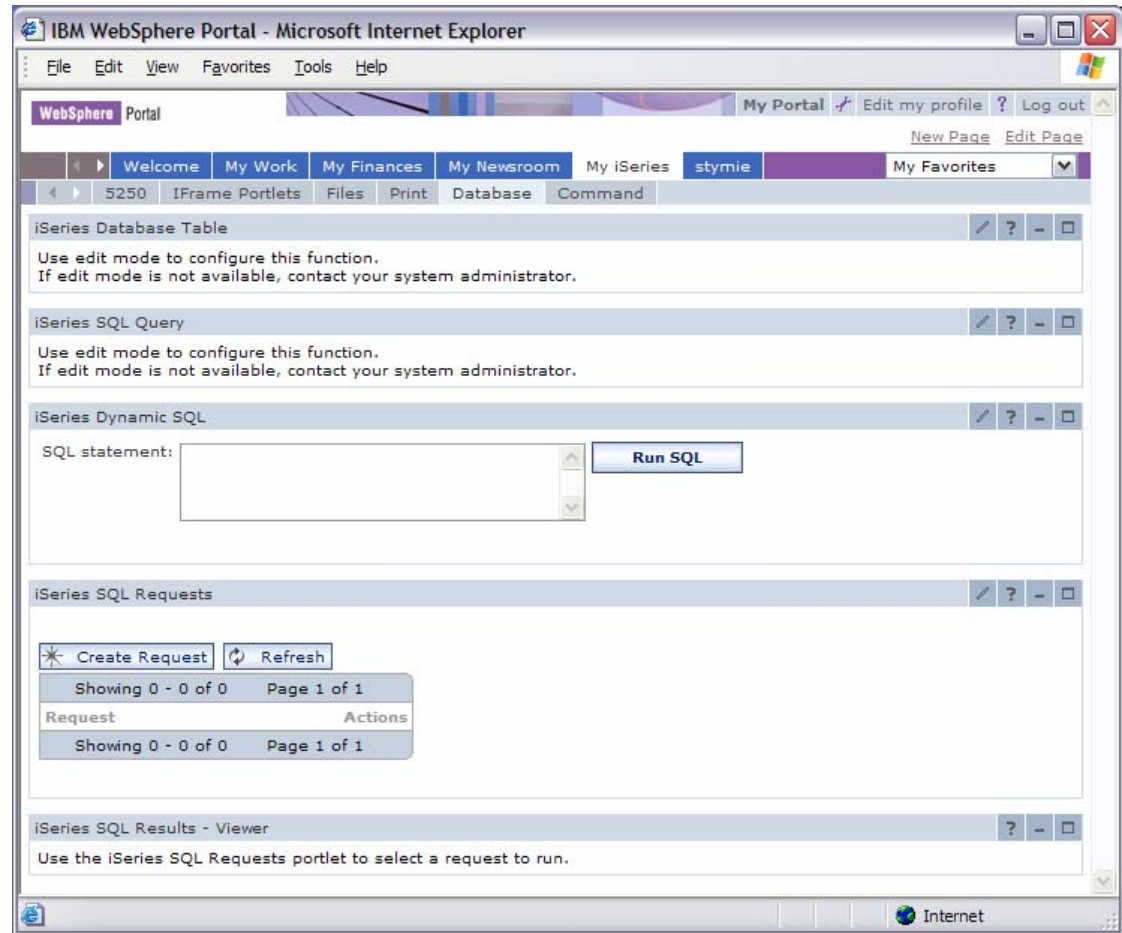
Portal Authentication

- Portal handles authentication

- Portal credentials
  - Authenticated with the active user registry

- Form-based authentication
  - User ID and password are clear text and should be protected

- Use Portal interfaces to control access to pages and portlets

System i Access for Web Portlet Authentication

- Setting to specify the hostname of system for accessing i5/OS resources
  - Default is the hostname of the system where Portal is running

- Setting to specify the credential to use when accessing i5/OS resources
  - Used to authenticate to i5/OS
  - i5/OS user profile and object level security are used to authorize access to i5/OS resources

- Settings can be controlled by the Portal administrator

iSeries File List

Edit Portlet Settings

☐ **Server**

Server: mySystem.myDomain.com

☐ **Authentication**

○ Use credential specific to this portlet window

    User:

    Password:

    Confirm password:

○ Use credential set with iSeries Credentials portlet

    Credential: myCredentials

○ Use system shared credential set by administrator

    Credential: deployment.keystore

◉ Use authenticated WebSphere credential

Authentication Options

- Use credentials specific to this portlet
  - Specify the i5/OS user profile name and password
  - Specific to this portlet window for this user

  Use credential specific to this portlet window

  User: stevej
  Password: ••••••
  Confirm password: ••••••

- Use credential set with System i Access for Web Credentials portlet
  - Select the name of a credential maintained with the iSeries Credentials portlet
  - Credential contains an i5/OS user profile name and password

  Use credential set with iSeries Credentials portlet

  Credential: myCredentials
  myCredentials
  mySystem.myDomain.com [System]

  Use system s

Authentication Options (continued)

- Credentials portlet lets users create and manage their own list of credentials
  - User created credentials are not available to other users
- Administrator can create system credentials using the WebSphere Portal Credentials Vault administration function
  - System credentials are available to all users
  - Each user sets their own i5/OS user profile name and password
- Manage credential values in one place

Authentication Options (continued)

- WebSphere Portal Credentials Vault administration function

Authentication Options (continued)

- Use system shared credential set by administrator
  - Created and managed by administrator using the WebSphere Portal Credentials Vault administration function
  - Common to all portal users

Authentication Options (continued)

- Use authenticated WebSphere credential
  - Uses identity tokens and EIM to map the authenticated WebSphere user identity to an i5/OS user profile

  ◉ Use authenticated WebSphere credential

- Requires:
  - EIM domain configuration on each i5/OS where resources will be accessed
    - All in the same EIM domain
  - EIM Identity Token Connector installed
    - J2C connection factories configured with JNDI names eis/iwa_IdentityToken and eis/IdentityToken
  - EIM identifier target associations for each i5/OS that will be accessed

5250 Sessions

- Bypass signon
  - QRMTSIGN system value must be *VERIFY
  - Settings to enable bypass signon and specify the credential to use

- No macro support

Agenda

System i Access for Web runtime (usage) security

- Use of policies
- Custom homepage/template

Controlling access for System i Access for Web

3 methods using System i Access for Web to control access

- Administration policies
  - Administrators can use the Customize function to set policies for users and groups of users.

- User Preferences
  - Users can set their own Preferences for things like
    - What tabs are available in the navigation bar
    - How to view output (default rows/columns per page)
    - How to filter output

- Customize the Home page and template
  - Administrators can use the Customize function to replace the default System i Access for Web home page with their own home page.
  - Administrators can use the Customize function to replace the default template that defines the layout, look, and feel of System i Access for Web pages
  - Style sheets - The look of the System i Access for Web page content is now controlled by external style sheets.

Controlling access for System i Access for Web

Home page

Controlling access for System i Access for Web

Product functionality

Controlling access for System i Access for Web

Sample for a user that can only run preconfigured database queries

Controlling Access - How & Who?

- The Customize function allows administrators to set policies for users and groups of users.

- These policies control...
  - Functions a user can perform.
  - How certain information is presented to the user.

- When a function is restricted...
  - Its navigation bar content is removed.
  - Access to the servlet is restricted.
  - It takes effect immediately.

- Administrators with *SECADM special authority are automatically authorized to administer settings for users and groups of users to which they have authority.

- These administrators can then grant other user profiles permission to administrate System i Access for Web functions.

Controlling Access - Strategies

- System i Access for Web ships with a set of default policy settings.

- These default policy settings allow most functions to be available for all users.

- As an administrator, you may not want users to access all functions.

- A quick strategy to restrict a function from all users
  – First, grant an administrator to have access to all functions
  – Use the Customize Group Profiles function and customize the *PUBLIC group profile.
  – Every user is a member of this group.
  – You could "Deny" a function for all users to restrict access.
  – You could then "Allow" specific users access to some functions that were restricted.

- Only users that have been allowed access will be able to use that function.

Notes: Controlling Access - Strategies

- System i Access for Web ships with a set of default policy settings. The default policy settings allow most of the System i Access for Web functions to be available for all users. Without any customization, users accessing System i Access for Web could begin using most of the available functions.

- As an administrator of this product, you may not want your users to be able to access all of these functions. It is the responsibility of an administrator to restrict functions they do not want their users to be able to access.

- One of the quickest strategies that can be deployed to restrict a function from all users is to use the Customize Group Profiles function and customize the *PUBLIC group profile.

- This group profile is defined such that every user is a member of this group. So, for example, if you were to customize the *PUBLIC profile and set the "Browse files" and "File shares" file functions to "Deny", you would restrict file system access from this product for all users.

- If some of your users required access to this function, you could specifically customize their user profiles and set this function back to "Allow". In this way, only users that have been specifically allowed access will be able to use that function, all others would not have access.

- It should be noted that the *PUBLIC group profile includes the administrator user ID that is used to customize other group and user profiles. If you were to deny functions for *PUBLIC, this would affect the administrator user profile. As you customize System i Access for Web for *PUBLIC, you may want to consider specifically allowing your administrator user profile to have access so that it is not locked out of System i Access for Web functions.

Controlling Access - Setting policies

Administrator actions on user & group profiles

Action	Description
Edit	This action is always available. Use this option to create or modify policy settings for the specified user or group profile.
View all policies	Select this action to view all of the policy settings currently being used for the profile.
View group membership	Select this action to display the Group Membership page that lists the group and supplemental group profiles (by name) the user profile has been assigned membership.
View group members	Select this action to display the Group Membership page that lists the user profiles (by name) that are currently members of the group profile.
Copy	This action is only available when the user or group profile currently has specific policy settings. It allows you to copy all of the policy settings from this profile to one or more other profiles.
Reset	This action is only available when the user or group profile currently has policy settings. It allows you to remove all of the policy settings specific to this profile.

Controlling Access - Setting policies (continued)

Controlling Access - Setting policies (continued)

Controlling Access - Setting policies (continued)

Administrator Action on each policy setting

Action	Description
Use current setting	This is the default action that is pre-selected. If the setting is not modified, no action is performed. If the setting is modified, it will be added to the user or group profile record in the System i Access for Web policies file.
Apply setting to profile	Select this action to add the current setting to the user or group profile record in the System i Access for Web policies file. The setting will be written to the user or group profile record, even if it was not modified. You would use this action to ensure the user or group profile gets this setting. This is because a different policy setting may be used based on the user profile being a member of one or more i5/OS group profiles.
Reset to default	Select this action to remove the setting from the user or group profile record in the System i Access for Web policies file. This option is only available if the user or group profile record currently contains a specific setting for this policy.

Controlling Access - Setting policies (continued)

The "Derived From" column (displayed when editing policy and preference settings) indicates where the policy setting that will be used for this user profile was found.

Action	Description
Profile setting	Indicates the setting is currently specific to the profile being customized. The setting had previously been applied to this profile.
Group – (groupName)	Indicates the setting is not specific to the profile being customized, but is being derived from the specified i5/OS group profile and the user is a member of this group.
*PUBLIC setting	Indicates the setting is not specific to the profile being customized. No setting was found in any i5/OS group profile memberships. The setting is being derived from the *PUBLIC group settings. This is a special group profile available to System i Access for Web administrators. All user profiles are automatically members of this special group profile. Administrators can modify this group profile to easily apply settings to all System i Access for Web users.
Shipped default	Indicates the setting is not specific to the profile being customized, no setting was found in any i5/OS group profile memberships, or the special *PUBLIC group profile. The setting is being derived from a shipped default value.
Parent policy	Indicates the function is a sub-function of a higher level category, and its policy setting is being controlled by a top level policy setting. For example, Tables is a sub-function of Database. If Database is restricted, Tables will be restricted as well and would show its being controlled by a parent policy.

Controlling Access - Setting policies (continued)

Example: 5250 Access

- The following screen shots step through setting up the items necessary to allow a group of users to use a single pre-configured 5250 session.

- In this example, ONEMANAGER is one of the user profiles in the MANAGERS group.

- This example shows
  - Creating a 5250 session configuration to be used by the management team
  - Making a shortcut of the 5250 session available to the MANAGERS group profile.
  - Restricting access to other functions in System i Access for Web.

- When the policy is set, it takes effect immediately.

Example: 5250 Access - Before

- Access the 5250 tab System i Access for Web Main page as user ONEMANAGER.
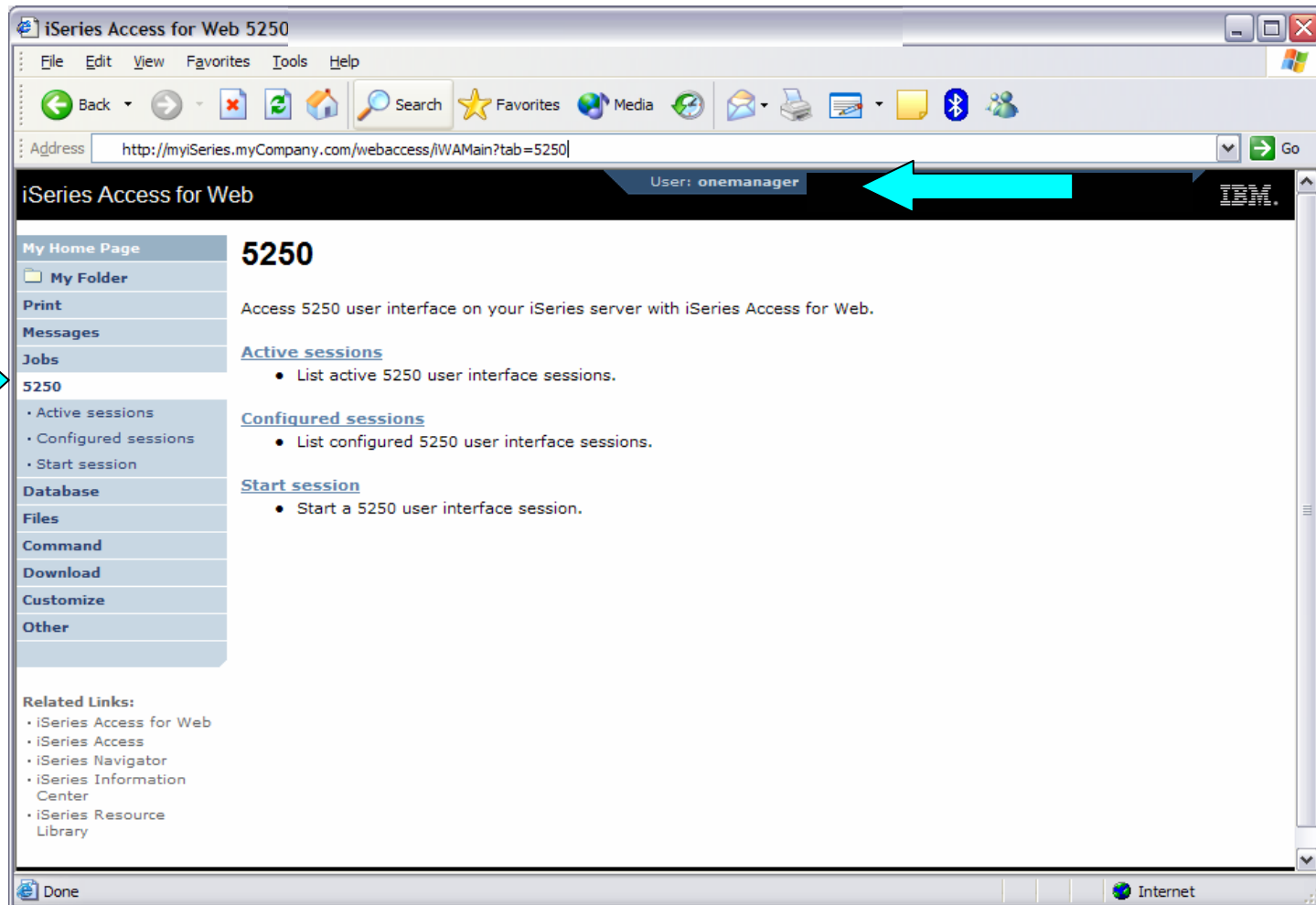
Example: 5250 Access - Policies

- Policies - the starting point for customization of a specific user or group.
- This is a new browser session, where we signed on as an administrator.

Example: 5250 Access - Categories

- Determine which categories need to be restricted/modified.

Example: 5250 Access – Other

- Turn off the other non-5250 functions. Set top level to Deny.
- Repeat for each category that should be restricted for the MANAGERS group.

Example: 5250 Access – Functional Setup

- The administrator goes to the Configured Sessions link on the 5250 tab. Select the "Configure new session" link.

Example: 5250 Access – Functional Setup

- The administrator configures the 5250 session settings to be used by the managers.
- Settings include the server to connect to, color schemes, and many other options.

Example: 5250 Access – Functional Setup

- The saved session is only available to the administrator that is currently signed on.
- The session must be shared to the managers. Use the "Create Shortcut" action.

Example: 5250 Access – Functional Setup

- Name the shortcut whatever you wish.
- Session can be shared with MANAGERS group, *PUBLIC, or individual profiles.

Example: 5250 Access – Back to Customize

- Go back to 5250 in Customize – Policies for the MANAGERS group profile.
- Select the shortcut to use as the default session settings for the MANAGERS.
- Select settings to lock MANAGERS out of starting/configuring new sessions.

Example: 5250 Access – More 5250 Settings

- Set all 5250 policies to Deny, except Configured Sessions and Start Configured Sessions.
- You may also want to allow them to access My Keypads and My Macros.

Example: 5250 Access – After

- Now managers can only start a pre-configured 5250 session, or reconnect to an active session

Controlling access to integrated e-mail

- System i Access for Web allows you to e-mail...
  - Database query results, printer output PDFs, command completion notifications, etc.

  - E-mail notifications can also be sent when items are placed into personal folders.

- Using the Mail function...
  - Users must first have an email address configured for their user profile. The administrator may configure this or allow users to configure their own email address in the Mail policy settings.

  - The administrator must also specify the name of the SMTP mail server to be used by the user profile or group in the Mail policy settings.

  - If the user has an SMTP user ID and SMTP domain defined in an i5/OS directory entry, those values will be used, unless other values are entered into the System i Access for Web policy settings.

  - Individual users may be restricted from using the Mail function within policy settings.

New for V5R4

- Style sheet support
  - Allows look-and-feel customization of System i Access for Web content

- Transfer configuration data from one user to another
  - Move and copy operations supported for:
    - 5250 sessions and macros
    - Saved commands
    - Database requests
    - My Folder items
    - Policies

- New home page support
  - Usable navigation content
  - Update information and product links

- New product look
  - Using cascading style sheet shipped with product
  - Action links are now images

Transfer Configuration Data

Home Page Customization

- A default home page is displayed when the iWAHome servlet is invoked.
  - http://<mySystem.myCompany.com>/webaccess/iWAHome
  - It's a starting point to highlight functions.
  - It's an example of how to build your own home page or pages that access System i Access for Web functionality.

- The Customize function allows you to replace the default home page.

- Default home page replacement can be done for all users (*PUBLIC), or can be changed for only certain users and/or groups of users.

- Additional Information
  - "Build a quick and easy Web site with System i Access for Web" - Janet Weber
    - http://www.ibm.com/servers/eserver/iseries/access/pdf/build_website_article.pdf
    - iSeries 400 Experts Journal
  - iSeries News article

Template file customization

- System i Access for Web has a default look for it functional pages.
  - This look is controlled by a template file and cascading style sheet.

- The template file has sections to specify
  - Header/footer areas of functional pages.
  - Where System i Access for Web content is placed in the page.

- The Customize function allows you to replace the default template file.

- Default template file replacement can be done for all users (*PUBLIC), or can be changed only for certain users and/or groups of users.

HomePage before – iWAHome servlet

HomePage after – iWAHome servlet

http://<system>/webaccess/iWAHome

HomePage after – iWAHome (another example)

Home Page/Template Customization Example (continued)

- Custom template

Additional Information

- Product web site
  - URL: http://www.ibm.com/eserver/iseries/access/web/
  - Latest information, articles, FAQs, fix information

- Information Center, Version 5 Release 4
  - URL: http://www.ibm.com/eserver/iseries/infocenter/
  - Connecting to iSeries, iSeries Access, iSeries Access for Web

- WebSphere Application Server for i5/OS information
  - URL: http://www.ibm.com/eserver/iseries/software/websphere/wsappserver

- Product help
  - Available on System i Access for Web pages

Additional Information

Application Server Authentication: WebSphere Global Security

- The following charts provide additional information on configuring WebSphere Application Server global security

Application Server Authentication WebSphere with Global Security Enabled

- Refer to the WebSphere Information Center for details
  - Search for "configuring global security"

Application Server Authentication WebSphere with Global Security Enabled (continued)

- Configure the active user registry

- Configure the authentication mechanism
  - Lightweight Third Party Authentication (LTPA)
  - Enable Single Signon (SSO)
    - Additional properties of LTPA configuration

User registries
- Custom
- LDAP
- Local OS

Authentication
- ⊟ Authentication mechanisms
  - LTPA
- ⊞ Authentication protocol
- ⊞ JAAS Configuration

Global security > **LDAP User Registry**

Configuration

General Properties
* Server user ID
[ ]
* Server user password
[ ]
Type
[IBM Tivoli Directory Server ▼]

Global security > **LTPA**

Configuration

[Generate Keys] [Import keys] [Export Keys]

General Properties
* Password
[ ]
* Confirm password
[ ]

Additional Properties
- Single signon (SSO)
- Trust association

Application Server Authentication WebSphere with Global Security Enabled (continued)

- Configure global security settings

  - Enable global security

  - Active authentication mechanism

  - Active user registry

Global security

Configuration

General Properties

☑ Enable global security

☐ Enforce Java 2 security

☐ Enforce fine-grained JCA security

☐ Use domain-qualified user IDs

＊ Cache timeout

600   seconds

☑ Issue permission warning

Active protocol

CSI and SAS ▼

Active authentication mechanism

Lightweight Third Party Authentication (LTPA) ▼

Active user registry

Lightweight Directory Access Protocol (LDAP) user registry ▼

☐ Use the Federal Information Processing Standard (FIPS)

Additional Information

Application Server Authentication: EIM domain configuration

- The following charts provide additional information on Enterprise Identity Mapping (EIM) domain configuration.

Application Server Authentication EIM Domain Configuration

- An EIM domain is a directory within a Lightweight Directory Access Protocol (LDAP) server
  - A collection of identifiers, associations and registries
  - Used to map identities from one registry to another registry

- System specified by TGTSVR parameter on the CFGACCWEB2 command must be part of an EIM domain
  - Configured using System i Navigator
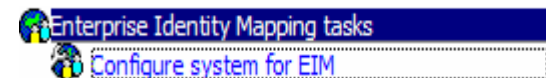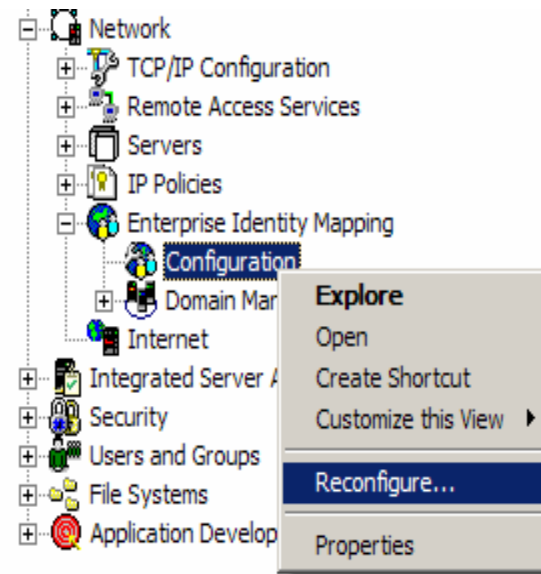
Application Server Authentication
EIM Domain Configuration (continued)

- Create and join a new domain, or join an existing domain
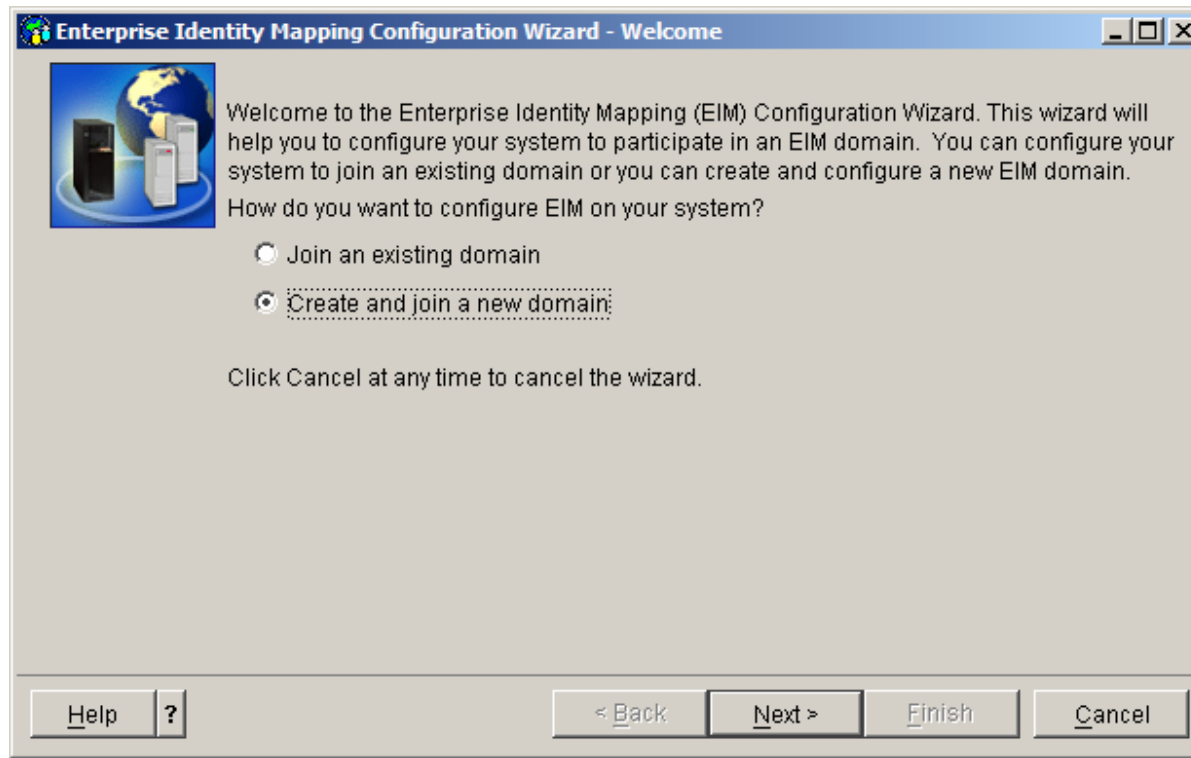
Application Server Authentication
EIM Domain Configuration (continued)

- Choose the Directory (LDAP) server to contain the EIM domain.
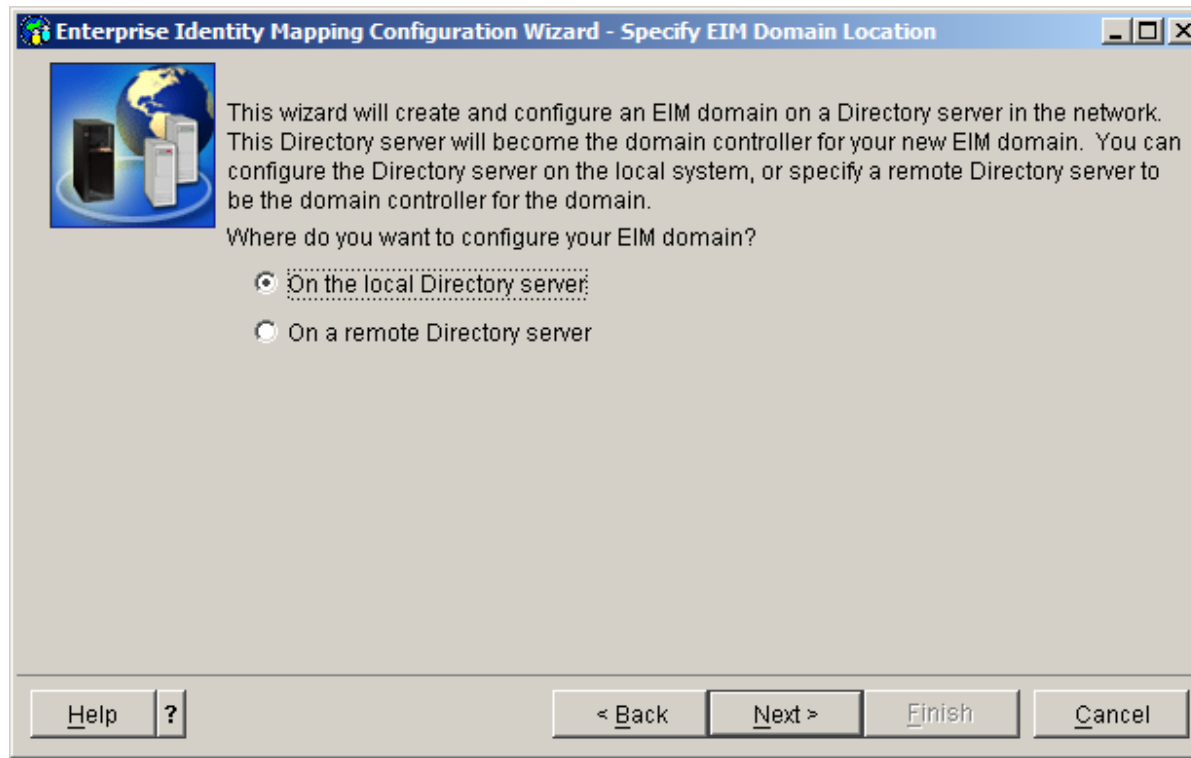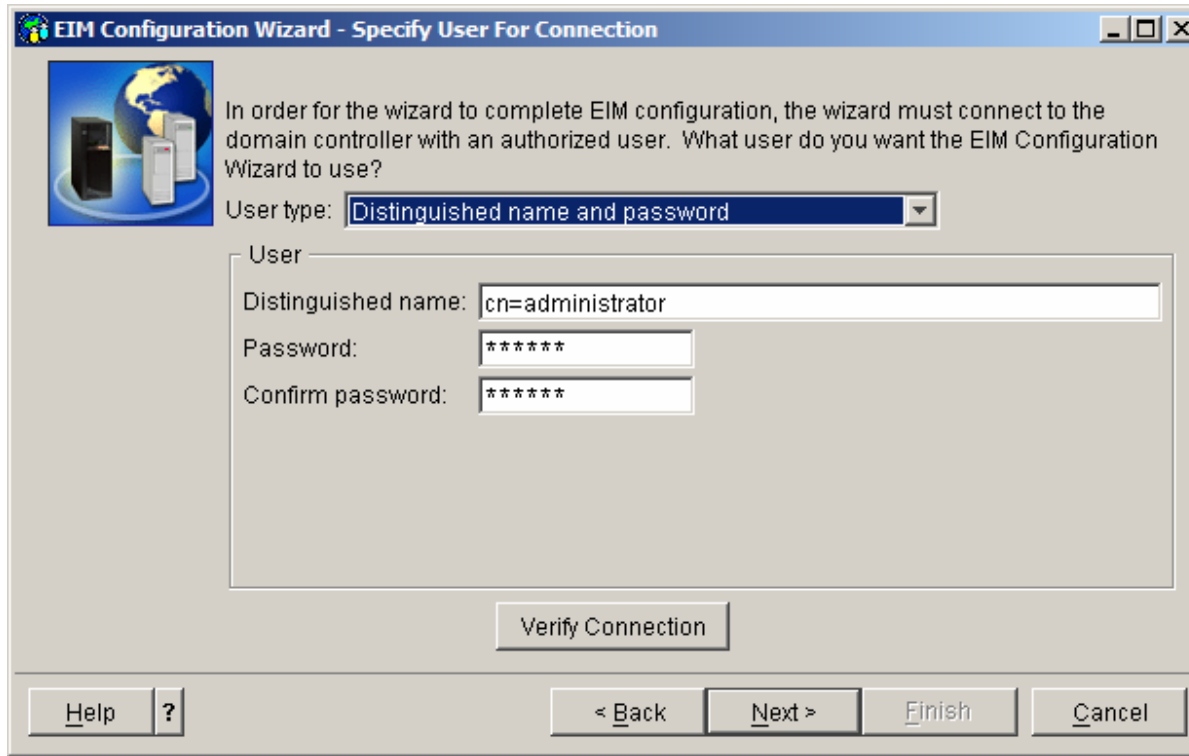
Application Server Authentication
EIM Domain Configuration (continued)

- Network Authentication Service (Kerberos) is not needed
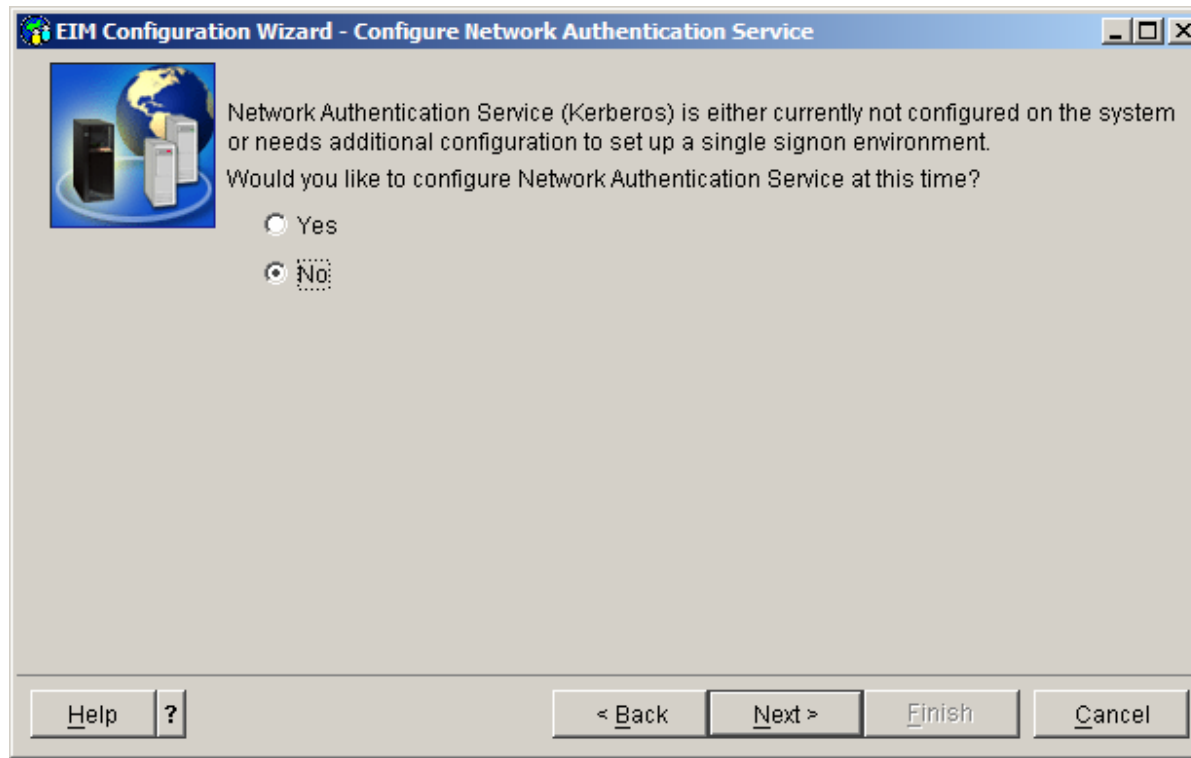
Application Server Authentication
EIM Domain Configuration (continued)
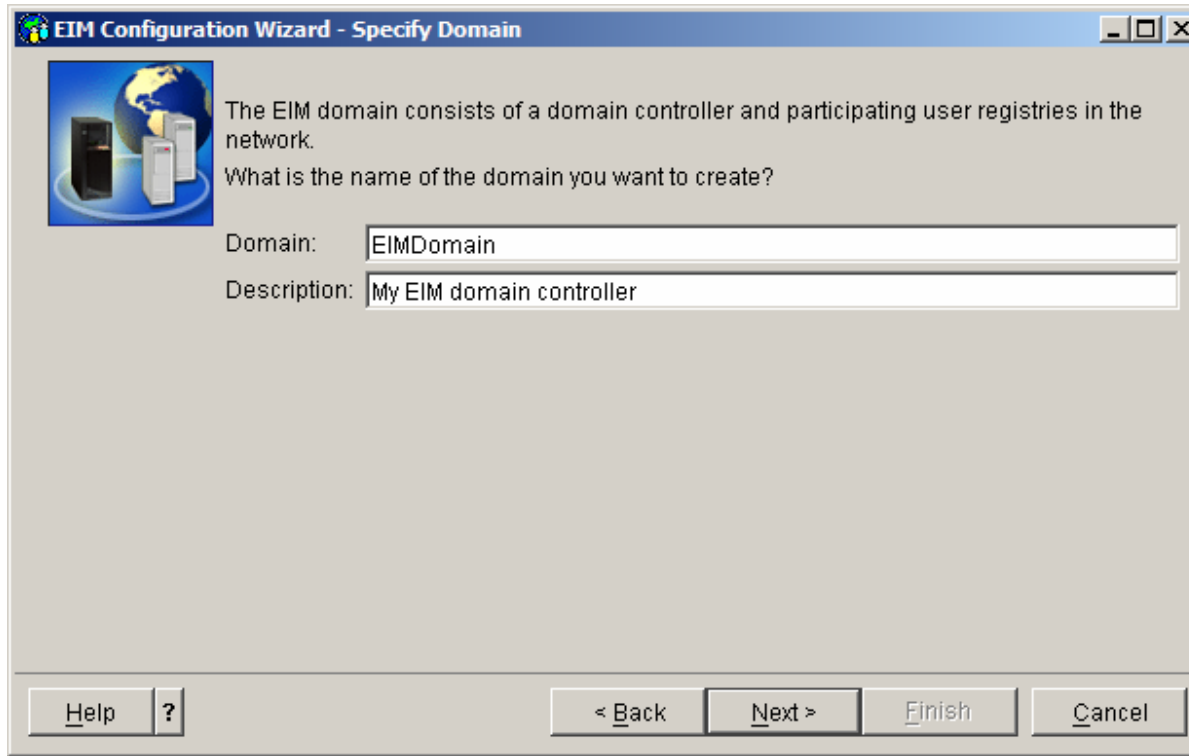
- Specify administrator credentials for the Directory (LDAP) server

Application Server Authentication
EIM Domain Configuration (continued)

- Specify a name for the EIM domain

Application Server Authentication
EIM Domain Configuration (continued)

- Specify the location within the directory for the EIM domain

Application Server Authentication
EIM Domain Configuration (continued)

- Create an EIM registry to represent the i5/OS user registry

Application Server Authentication
EIM Domain Configuration (continued)

- Specify credentials for i5/OS to use when accessing EIM on the Directory server

Application Server Authentication
EIM Domain Configuration (continued)

- Confirm the information and select Finish to create the EIM domain
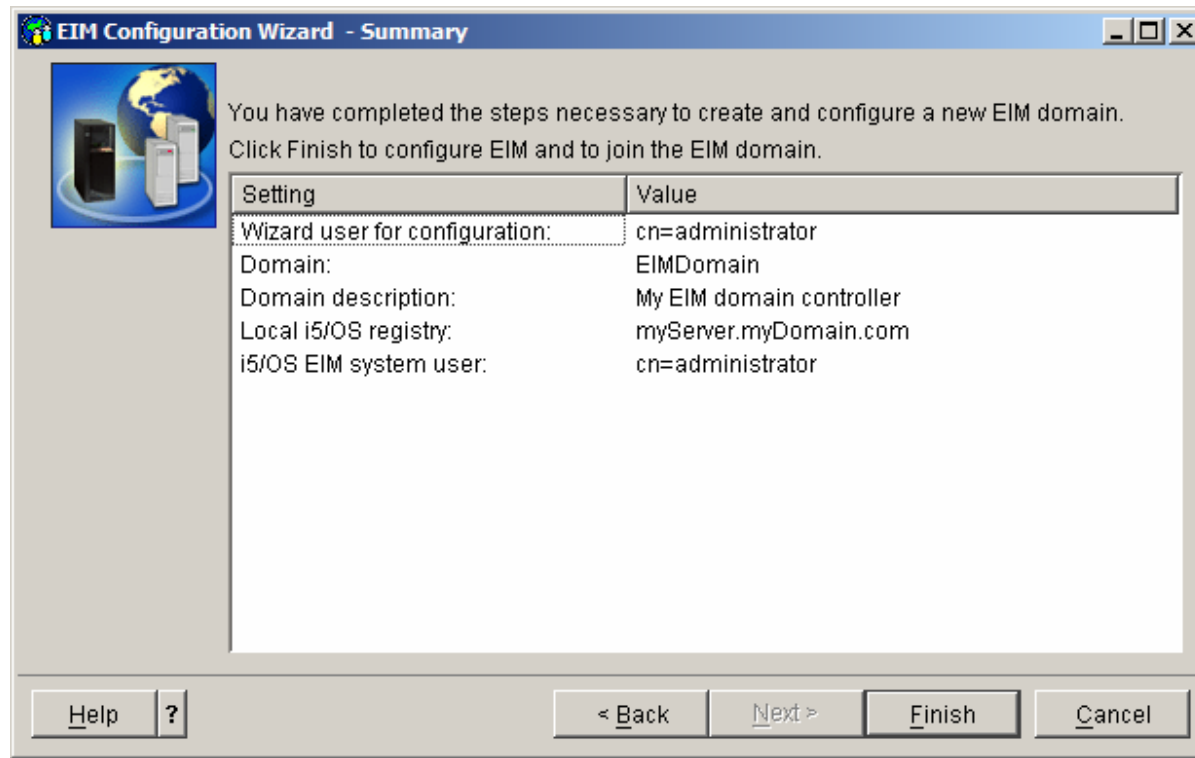
Application Server Authentication
EIM Domain Configuration (continued)

- Create an EIM registry to represent the active WebSphere user registry
  - Specify registry name
  - Specify registry type
    - LDAP – short name
    - For System i Navigator prior to V5R4, specify 1.3.18.0.2.33.14-caseIgnore

Add System Registry - EimDomain

Domain:	EimDomain
Registry:	WebSphereUserRegistry
Type:	LDAP - short name
Description:	Registry used to contain source associations for Websphere users
User registry URL:	

Address aliases

Alias:	
Type:	DNS host name

Add

Alias	Type

Remove

- Enterprise Identity Mapping
  - Configuration
  - Domain Management
    - EIM
      - User Registries
      - Identifiers

Enterprise Identity Mapping tasks
- Add a new system registry
- Add a new application registry
- Add a new group registry
- Create a new identifier

OK   Cancel   Help   ?
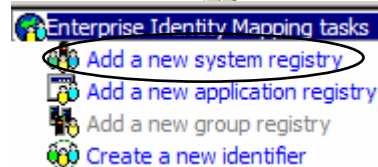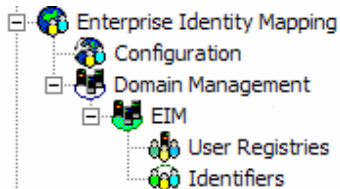
Application Server Authentication
EIM Domain Configuration (continued)

- Create an EIM identifier to represent each WebSphere user
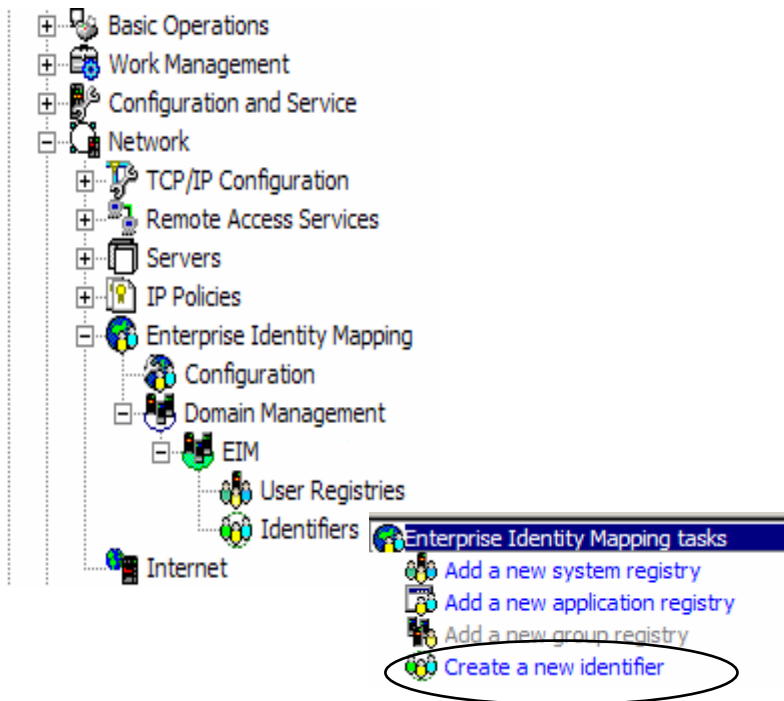
Application Server Authentication EIM Domain Configuration (continued)

- Create EIM associations for each identifier

Application Server Authentication
EIM Domain Configuration (continued)

- Source association describes relationship to WebSphere user ID

- Browse and select registry representing the WebSphere user registry

- Specify WebSphere user ID
  - LDAP short name
  - May need to be qualified with security domain realm
    - ldap.myDomain.com:389/sjones

- Select 'Source' as association type
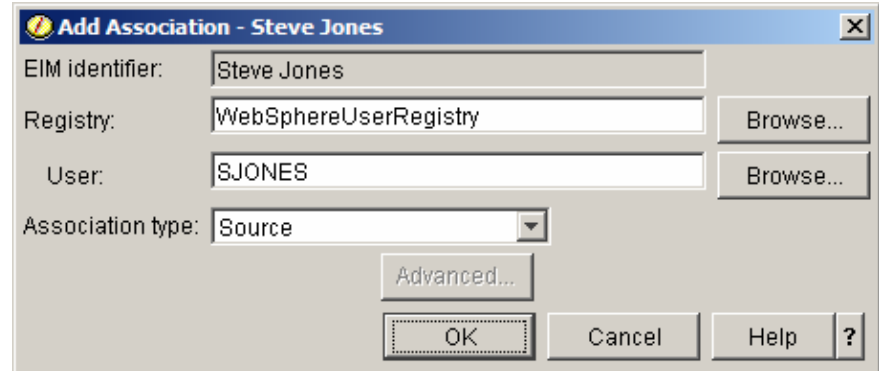
Application Server Authentication
EIM Domain Configuration (continued)

- Target association describes relationship to i5/OS user profile

- Browse and select registry representing the i5/OS user registry

- Specify i5/OS user profile

- Select 'Target' as association type

Add Association - Steve Jones	
EIM identifier:	Steve Jones
Registry:	mySystem.myDomain.com Browse...
User:	STEVEJ Browse...
Association type:	Target
	Advanced...
	OK Cancel Help ?
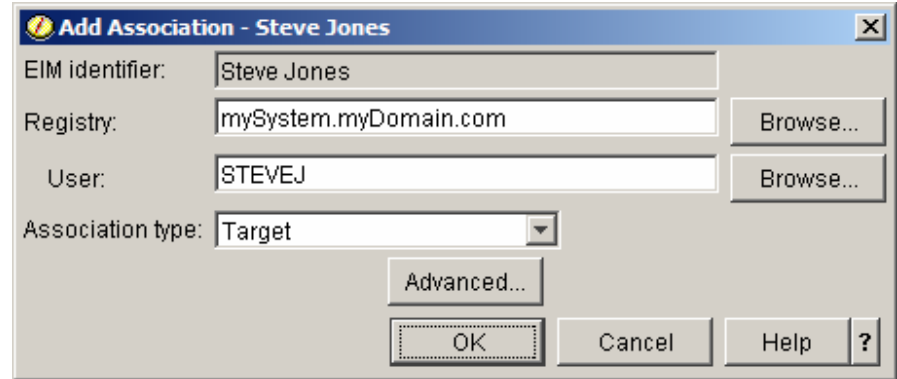
Application Server Authentication
EIM Domain Configuration (continued)

- These associations allow the WebSphere user identity SJONES to be mapped to the mySystem.myDomain.com i5/OS user profile STEVEJ

- As users are added to the WebSphere user registry, identifiers with associations must be added to the EIM domain

Additional Information

Application Server Authentication: EIM Identity Token Connector

- The following charts provide additional information on Enterprise Identity Mapping (EIM) Identiry Token Connector configuration

Application Server Authentication
EIM Identity Token Connector

- The EIM Identity Token Connector is a resource adapter that conforms to the J2EE Connector Architecture (JCA) specification

- Connector must be installed in WebSphere

- Create a J2C authentication entry

- Configure Java 2 Connector (J2C) connection factories

- Connection factories are used to request identity tokens
  – Identity tokens are encrypted data strings representing the authenticated WebSphere user identity

- Identity tokens are passed to the i5/OS host servers and input to EIM lookup operations which map the WebSphere user identity to an i5/OS user profile

Application Server Authentication
EIM Identity Token Connector (continued)

- Install the connector in WebSphere
  - /QIBM/ProdData/OS400/security/eim/idTokenRA.rar
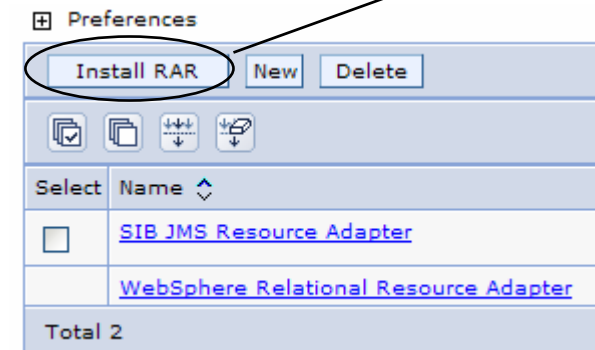
Application Server Authentication
EIM Identity Token Connector (continued)

- Create J2C authentication entry
  – LDAP administrator credentials

Application Server Authentication
EIM Identity Token Connector (continued)

- Create connection factories

Application Server Authentication
EIM Identity Token Connector (continued)

- Use the following JNDI names
  - eis/iwa_IdentityToken
  - eis/IdentityToken

- Select the J2C authentication entry created earlier

Resource adapters > **Identity Token Connector** > **J2C connection factories** > **New**
General Properties

* Scope
`cells:        _iwa60:nodes:        _iwa60`

* Name
`CF1`

JNDI name
`eis/IdentityToken`

Description

* Connection factory interface
`javax.resource.cci.ConnectionFactory`

Category

Component-managed authentication alias
Component-managed authentication ali
`_iwa60/idTokenAlias`

Container-managed authentication
Container-managed authentication alias
use resource reference authentication se
`.wa60/idTokenAlias`

Authentication preference (deprecated i
reference authentication settings instead
`BASIC_PASSWORD`

Mapping-configuration alias (deprecated
reference authentication settings instead
`DefaultPrincipalMapping`

Additional Properties

- Connection pool properties
- Advanced connection factory properties
- Custom properties

Apply OK Reset Cancel

Application Server Authentication
EIM Identity Token Connector (continued)

- Set custom properties on factories
  - LdapHostName
  - LdapHostPort
  - EimDomainName
  - SourceRegistryName
- Optional properties
  - ParentDomain
  - KeyTimeoutSeconds
  - KeySize
  - …

Resource adapters > Identity Token Connector > J2C connection factories > CF1 > Custom properties

Name ◇	Value ◇	Description ◇
LdapHostName	ldap.myDomain.com	Required. The fully qualified TCP/IP host name of the LDAP server hosting the EIM domain controller. For example: myLDAPServer.com
LdapHostPort	389	Optional. The port number of the LDAP server.
EimDomainName	EIMDomain	Required. The simple (undistinguished) name of the EIM domain this resource adapter is using. For example: Auth Tokens Domain
ParentDomain		Optional. The LDAP DN value for the parent domain of the EIM domain this resource adapter is using. For example: dc=myServer, dc=myCompany, dc=com
SourceRegistryName	WebSphereUserRegistry	Required. The name of the EIM registry in which the authenticated username has a source mapping.
KeyTimeoutSeconds	1200	Optional. The number of…

Application Server Authentication
EIM Identity Token Connector (continued)

- System i Access for Web will use the connection factories in the following order
  - eis/iwa_IdentityToken
  - eis/IdentityToken

- Can create just one of the factories
  - If eis/iwa_IdentityToken connection factory is not created, WebSphere logs will have lots of JNDI lookup errors
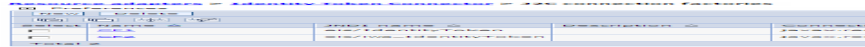
Trademarks and Disclaimers

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at
http://www.ibm.com/legal/copytrade.shtml.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered
    trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Other company, product, or service names may be trademarks or service marks of others.

Information is provided "AS IS" without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual
environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does
not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information,
including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or
any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance,
function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here
to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any
user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage
configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements
equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact
your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.