# 5761-XH2 V6R1 System i Access for Web

## *Configuring Enterprise Identity Mapping*

**First Edition (February 2009)**
This edition supplements the V6R1 System i Access for Web Information Center documentation.

In order to enable Single sign-on (SSO) with WebSphere Application Server® and System i™ Access for Web, you must configure Enterprise Identity Mapping (EIM). This topic provides an overview of the steps to configure EIM. These steps are intended as a guide to administrators when planning and configuring the EIM environment.

EIM is part of the Network subcomponent of System i Navigator. For information about EIM, see the *Enterprise Identity Mapping* topic in the IBM i5/OS Information Center (http://www.ibm.com/systems/i/infocenter/).

Configuring EIM involves these steps:

- Create an EIM domain. See step 1.
- Add EIM domain to Domain Management. See step 2.
- Create EIM source user registry. See step 3.
- Create EIM identifier for each user. See step 4.
- Add associations to EIM identifiers. See step 5.

**Steps to configure Enterprise Identity Mapping:**

1. Create an EIM domain.

   EIM domain information is stored on a Lightweight Directory Access Protocol (LDAP) directory server. The LDAP administrator distinguished name and password is required in order to create an EIM domain.

   To create an EIM domain, follow these steps:

   a. In System i Navigator, expand **<*system_name*> > Network > Enterprise Identity Mapping**.

   b. Right-click **Configuration** and select **Configure** (or **Reconfigure**, if EIM has been previously configured) to start the EIM configuration wizard.

c. On the Welcome page, select **Create and join a new domain**.

   Select **Next**.

d. On the Specify EIM Domain Location page, select one of these as appropriate:

   - **On the local Directory server**
   - **On a remote Directory server**

   Select **Next**.

e. On the Configure Network Authentication Service page, select **No**. Select **Next**.

   **Note:** Network Authentication Service is not required for EIM in WebSphere Application Server environments. For more information about Network Authentication Service, see the *Network authentication service* topic in the IBM i5/OS Information Center (http://www.ibm.com/systems/i/infocenter/).

f. If you selected to have the EIM domain located on the local Directory server in step 1.d above, go to the next step.

   Otherwise, the Specify Domain Controller page is displayed. Specify the **Domain controller name** and **Port**. For example:

   Domain controller name: `ldap.mycompany.com`
   Port: `389`

   Select **Next**.

g. Either the Specify User for Connection or the Configure Directory Server page is displayed. Specify the **Distinguished name** and **Password** of the directory server administrator, as well as the directory server **Port** number, as appropriate. For example:

   Distinguished name: `cn=administrator`
   Password: `myadminpwd`
   Port: `389`

   Select **Next**.

h. On the Specify Domain page, provide a name for the EIM domain. For example:

   Domain: `EimDomain`

   Select **Next**.

i. On the Specify parent DN for Domain page, select **No**. Select **Next**.

j. If the directory server is active, a message is displayed indicating to end and restart the directory server for the changes to take effect.

   Select **Yes** to restart the directory server.

k. On the Registry Information page, select **Local i5/OS** and deselect **Kerberos**. Write down the Local i5/OS® registry name. This registry name will be used when creating associations for EIM identifiers. For example: `myi.mycompany.com`

Select **Next**.

l. On the Specify EIM System User page, let it default to using the directory server administrator distinguished name and password when performing EIM operations on behalf of operating system functions.

   Select **Next**.

m. On the Summary page, confirm the EIM configuration information.

   Select **Finish**.

2. Add EIM domain to Domain Management.

   To add the EIM domain to Domain Management, follow these steps:

   a. In System i Navigator, expand **<*system_name*> > Network > Enterprise Identity Mapping**.
   b. Right-click **Domain Management**, and select **Add Domain**.
   c. On the Add Domain dialog, select the EIM domain name specified in step 1.h of the Create an EIM domain step. For example: `EimDomain`

      Select **OK**.

   d. The domain is added to System i Navigator. Expand the domain by selecting the + next to the domain name.
   e. Specify the directory server administrator distinguished name and password at the Connect to EIM domain controller prompt.
   f. Two subcategories are displayed, User Registries and Identifiers.

3. Create EIM source user registry.

   To create an EIM source user registry, follow these steps:

   a. In System i Navigator, expand **<*system_name*> > Network > Enterprise Identity Mapping > Domain Management > <*domain_name*> > User Registries**.
   b. Right-click **User Registries**, and select **Add Registry > System**.
   c. On the Add System Registry dialog, provide a registry name. For exmaple:

      Registry: `WebSphereUserRegistry`

   d. Select **LDAP – short name** from the registry type selection list. Registry type **LDAP – short name** is not available in System i Navigator releases prior to V5R4M0. If you are using an earlier release of System i Navigator, specify `1.3.18.0.2.33.14-caseIgnore` as the registry type. This is the ObjectIdentifier-normalization (OID) form of registry types whose principals are identified by the LDAP short name attribute. This OID is mapped to "LDAP – short name" in V5R4M0 System i Navigator.

      Select **OK**.

4. Create EIM identifier for each user.

   An EIM identifier must be created for each user in the WebSphere user registry. When new users are added to the WebSphere user registry, an EIM identifier must be created for each new user.

   To create an EIM identifier for a user in the WebSphere user registry, follow these steps:

   a. In System i Navigator, expand **<*system_name*> > Network > Enterprise Identity Mapping > Domain Management > <*domain_name*> > Identifiers**.

   b. Right-click **Identifiers**, and select **New Identifier**.

   c. On the New EIM Identifier dialog, provide a unique identifier name and optional description. For example: `Thomas R. Smith`

      Select **OK**.

   d. Repeat steps 4.b and 4.c for each WebSphere user that uses System i Access for Web.

5. Add associations to EIM identifiers.

   Each EIM identifier requires two EIM associations. These associations link the WebSphere user identity (source identity) to an IBM i user profile (target identity). When new EIM identifiers are added to represent new users in the WebSphere user registry, repeat these steps to create the corresponding EIM associations.

   To add associations to an EIM identifier, follow these steps:

   a. In System i Navigator, expand **<*system_name*> > Network > Enterprise Identity Mapping > Domain Management > <*domain_name*> > Identifiers**. A list of identifiers is displayed in the right pane of System i Navigator.

   b. Right-click an identifier and select **Properties**. For example: `Thomas R. Smith`

   c. From the Associations tabbed page, select **Add** to add a WebSphere user registry source association.

   d. On the Add Association dialog, provide values for the following fields. You can specify a value or select **Browse...** to select from a list of known values.

      - **Registry:** Specify the source registry name from step 3.c of the Create EIM source user registry step. For example: `WebSphereUserRegistry`
      - **User:** Specify the user's WebSphere user identity. For example: `tsmith`
      - Association type: `Source`

      Select **OK** to add the source association.

   e. From the Associations tabbed page, select **Add** to add an i5/OS user profile target association.

f. On the Add Association dialog, provide values for the following fields. You can specify a value or select **Browse...** to select from a list of known values.

- **Registry:** Specify the target registry name from step 1.k of the Create EIM domain step. For example: `myi.mycompany.com`
- **User:** Specify the user's IBM i user profile name. For example: `TOMSMITH`
- Association type: `Target`

Select **OK** to add the target association.

g. Select **OK** to close the Properties dialog.