Enterprise Portal Administration Guide

Microsoft Corporation

Published: May 2008

Microsoft Dynamics is a line of integrated, adaptable business management solutions that enables you and your people to make business decisions with greater confidence. Microsoft Dynamics works like and with familiar Microsoft software, automating and streamlining financial, customer relationship and supply chain processes in a way that helps you drive business success.

U.S. and Canada Toll Free 1-888-477-7989

Worldwide +1-701-281-6500

www.microsoft.com/dynamics

Table of Contents

Enterprise Portal Administration Guide

Enterprise Portal for Microsoft Dynamics™ AX gives you access to business information and allows you to participate in business processes using a Web browser.

About installing Enterprise Portal and Role Centers

Enterprise Portal and Role Centers are installed using Microsoft Dynamics AX Setup. For more information about installing Enterprise Portal, see "Install Enterprise Portal and Role Centers" in the Microsoft Dynamics AX Installation guide.

What's new in Enterprise Portal

Microsoft Dynamics AX provides a set of Web modules that give you access to Microsoft Dynamics AX data and allow you to participate in business processes using Web-based Microsoft Dynamics AX forms. These modules and the portal system are collectively called Enterprise Portal. Enterprise Portal is built on Microsoft® Windows® SharePoint® Services or Microsoft Office SharePoint Server.

What's new

Enterprise Portal includes the following new features and modules.

Feature or module	Description
Role Centers	Microsoft Dynamics AX and the Enterprise Portal framework include customizable home pages called Role Centers. Role Centers display reports and other business intelligence information, transaction data, alerts, links, and common tasks associated with a user's role in the company. Role Centers are available in both Enterprise Portal and the Microsoft Dynamics AX client.
Purchase Requisition	Purchase Requisition enables employees to enter requests for equipment, supplies, and other materials using Enterprise Portal. When the purchasing department approves a requisition, purchase orders automatically are created in the Microsoft Dynamics AX client.
Customer Relations Management (CRM)	CRM provides the tools necessary to create and maintain a comprehensive set of data about customers and their information using Enterprise Portal. Employees can track information about prospective customers from the first point of contact, to customer purchases, to post-sale activities. CRM integrates with Financials and Supply Chain Management.

Feature or module	Description
Service Management	Service Management enables technicians to manage various aspects of their service requests using Enterprise Portal. Technicians can manage resource assignments, time tracking, customer history, future service plans, and resolution details.
Access to multiple companies	Users who have access to multiple Microsoft Dynamics AX companies can use the company list to access the Enterprise Portal pages for another company, rather than having to open a separate Web site.

Administration enhancements

Some of the biggest changes and enhancements in Enterprise Portal address the needs of Enterprise Portal administrators.

Area	What's new
Windows SharePoint Services/Office SharePoint Server	This version of Enterprise Portal requires either Windows SharePoint Services 3.0 or Office SharePoint Server.
Installation	Enterprise Portal is installed using Microsoft Dynamics AX Setup. Setup verifies whether Internet Information Services (IIS) and either Windows SharePoint Services or Office SharePoint Server already are installed on the server. If these applications are not installed, Setup prompts you to install them. For more information about installing Enterprise Portal, see "Install Enterprise Portal and Role Centers" in the Microsoft Dynamics AX Installation guide.
Business Connector proxy configuration	Setup automates the process of configuring the proxy in various locations on the Enterprise Portal server. Setup prompts you for the proxy credentials when you install Enterprise Portal, and then configures the proxy credentials in the following locations: • Microsoft Dynamics AX • Windows user groups • IIS • Microsoft SQL Server™
IIS	Setup automates the process of configuring security, ASP.NET, and application pools in IIS.
Site creation and deployment	By default, when you install Enterprise Portal, Setup automatically creates an Enterprise Portal site, extends that site in Windows SharePoint Services or Office SharePoint Server, and deploys the

Area	What's new
	site. For more information about creating and deploying an Enterprise Portal site, see "Creating Enterprise Portal sites" in the Enterprise Portal Administration guide, which is available from the Help menu in the Microsoft Dynamics AX client.
User profiles	You can use these profiles to assign users to specific Role Centers. Microsoft Dynamics AX includes several default profiles that are defined for common roles. You can customize these profiles or create new ones. For more information about Role Centers, see Administering Role Centers. For more information about user profiles, see Manage user profiles for Role Centers.

Creating Enterprise Portal sites

This section provides information to help you create and view Enterprise Portal Web sites. The following topics are included:

- Create an Enterprise Portal intranet site
- Create an Enterprise Portal extranet site
- Create an Enterprise Portal Internet site
- View an Enterprise Portal Web site

Create an Enterprise Portal intranet site

When you install the Enterprise Portal framework, Setup creates an Enterprise Portal intranet site by default. If you will be using the default intranet site, you do not need to complete the steps listed in this topic, unless you want to create another intranet site.

This topic describes how to manually create intranet sites using SharePoint Central Administration after you installed Enterprise Portal using Setup. You might want to do this if you chose not to create the default intranet site when you installed Enterprise Portal, or if you want to create multiple Enterprise Portal intranet sites. For more information about installing Enterprise Portal, see "Install Enterprise Portal and Role Centers" in the Microsoft Dynamics AX Installation guide.

Important considerations

- Enterprise Portal is designed to be a top-level site. If you installed Enterprise Portal on Office SharePoint Server, delete the top-level site collection using SharePoint Central Administration (**Start** > **Administrative Tools** > **SharePoint 3.0 Central Administration** > **Application Management** > **Delete Site Collection**). If you create the Enterprise Portal site as a subsite of an existing site collection, users might need to use additional navigation steps to complete tasks, and it might be more complicated for administrators to manage site permissions.
- You cannot create company-specific Enterprise Portal intranet sites. If users have access to multiple companies, they can select which company to view information for using the **Company** list in Enterprise Portal.

To create an Enterprise Portal intranet site

1. In the Microsoft Dynamics AX client, click **Administration** > **Setup** > **Internet** > **Enterprise Portal** > **Web sites**.
2. Click the **Create site** button.
3. Enter information in the **Web Application**, **Title and Description**, and **Web Site Address** sections.

Important:

You must enter a unique title and description for each Enterprise Portal site. If you create a new Web site using SharePoint Services or IIS Manager, and a title or site description matches an existing site, Enterprise Portal will not deploy on the new site.

4. Under **Template Selection**, click the **Custom** tab.
5. Click **Microsoft Dynamics AX Enterprise Portal**.
6. Enter information in the **Site Owners** and **Quota** sections, and then click **OK**.

Enable the Web server in Windows Firewall

After you create the SharePoint site, you must enable the Web server in Windows Firewall so users can access the site. If you do not enable the Web server in Windows Firewall, you can view the site on the local server, but no other users can view the site.

1. Click **Start** > **Control Panel** > **Windows Firewall**.
2. Click the **Advanced** tab.
3. In the **Network Connection Settings** section, click **Settings**.
4. Select **Web Server (HTTP)** and click **OK**.

Note:

By default, when you enable **Web Server (HTTP)** through the firewall, you enable port 80. If you configured the Enterprise Portal site for a port other than port 80, enable that port on the **Exceptions** tab in Windows Firewall.

Next steps

After you have created an intranet site, see the following topics to finish configuring and securing your site:

- Configuring Enterprise Portal
- Configuring Enterprise Portal security
- Give users access to an Enterprise Portal intranet site

Create an Enterprise Portal extranet site

You can create an extranet site for Enterprise Portal so employees, customers, and vendors can access Microsoft Dynamics AX information and participate in business processes using a Web browser.

Before you create an extranet site

1. Set up and configure a perimeter network. A perimeter network enhances the security of the Enterprise Portal configuration by using firewalls and domain controllers to restrict access to Microsoft Dynamics AX data. For more information, see Configuring a perimeter network for Enterprise Portal.
2. Obtain a secure sockets layer (SSL) certificate from a certificate authority. SSL is a cryptographic system for encrypting data sent over the Web.

3. Verify that the Enterprise Portal framework is installed. You can view the virtual server URL in the **Manage deployments** form (**Administration** > **Setup** > **Internet** > **Enterprise Portal** > **Manage deployments**). For more information about installing Enterprise Portal, see "Install Enterprise Portal and Role Centers" in the Microsoft Dynamics AX Installation guide.

To create an Enterprise Portal extranet site

1. Click **Administration** > **Setup** > **Internet** > **Enterprise Portal** > **Web sites**.
2. Click the **Create site** button.
3. Enter information in the **Web Application**, **Title and Description**, and **Web Site Address** sections.

Important:

You must enter a unique title and description for each Enterprise Portal site. If you create a new Web site using SharePoint Services or IIS Manager, and a title or site description matches an existing site, Enterprise Portal will not deploy on the new site.

4. Under **Template Selection**, click the **Custom** tab.
5. Click **Microsoft Dynamics AX Enterprise Portal**.
6. Enter information in the **Site Owners** and **Quota** sections, and then click **OK**.
7. Use IIS to assign the SSL certificate to the Web site you just created (**Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**).
   - Under **Web sites**, right-click the new site and click **Properties**.
   - Click **Directory Security**.
   - Under **Secure Communications**, click **Server Certificate**.
   - Complete the **Web Server Certificate Wizard**.
8. Restart IIS. Open a command prompt, type **iisreset/noforce**, and press ENTER.
9. Verify that the site is configured for SSL. Click **Administration** > **Setup** > **Internet** > **Enterprise Portal** > **Web sites**. Locate the site you just created and verify that the **External URL** field shows https.
10. View the site in a browser. Select the site in the **Web sites** form and click **View in Browser**.

Next steps

After you have created an extranet site, see the following topics to finish configuring and securing your site:

- Configuring Enterprise Portal
- Configuring Enterprise Portal security
- Give users access to an Enterprise Portal extranet site

Create an Enterprise Portal Internet site

You can create an Internet site using Enterprise Portal so potential customers can view your organization's product catalog, fill out a questionnaire, or sign up to become a customer. This topic describes how to manually create an Enterprise Portal Internet site.

Note:

Enterprise Portal Internet sites do not display company-specific data.

Before you begin

This topic assumes that you have already installed the Enterprise Portal framework using Setup. If you did not install the Enterprise Portal framework already, do so now. For more information about installing Enterprise Portal, see "Install Enterprise Portal and Role Centers" in the Microsoft Dynamics AX Installation guide.

Create a new Web application in SharePoint Central Administration

By default, when you install the Enterprise Portal framework using Setup, the system creates a Web application and a Web site that use Integrated Windows authentication. You cannot use the default Web application and Web site for an Enterprise Portal Internet site because an Enterprise Portal Internet site must use Anonymous authentication. The following procedure describes how to use SharePoint Central Administration to create a new Web application that is configured for Anonymous authentication.

1. Open SharePoint Central Administration (**Start** > **Programs** > **Administrative Tools** > **SharePoint 3.0 Central Administration**).
2. Create a new Web application (**Application Management** > **Create or extend Web application** > **Create a new Web application**).
3. Click **Create a new IIS Web site**.

   Important:

   Do not change the **Authentication Provider** settings. You will configure this application for Anonymous authentication after you have created the site collection, as described later in this topic. You can adjust the **Port**, **Host Header**, and **Path** settings as necessary, or you can leave the default settings.
4. In the **Application Pool** section, click **Configurable**, and then enter the credentials for the Business Connector proxy.
5. Enter information in the remaining sections and click **OK**.

Deploy Enterprise Portal on the new Web application

1. In the Microsoft Dynamics AX client, click **Administration** > **Setup** > **Internet** > **Enterprise Portal** > **Manage deployments**.
2. Select the **Enabled** check box for the virtual server URL for the Web application you just created.
3. Open a command prompt, type **iisreset**, and press ENTER.

Create a site using the Public template

Enterprise Portal includes separate templates for internal sites and public sites. Use this procedure to create a site using the public template.

1. Open **SharePoint Central Administration** (**Start** > **Programs** > **Administrative Tools** > **SharePoint 3.0 Central Administration**).
2. Create a new site collection (**Application Management** > **Create site collection**).
3. In the **Web Application** section, select the application that you created in the "Create a new Web application in SharePoint Central Administration" procedure.
4. Enter a title and description.

Important:

You must enter a unique title and description for each Enterprise Portal site. If you create a new Web site using SharePoint Services or IIS Manager, and a title or site description matches an existing site, Enterprise Portal will not deploy on the new site.

5. Specify a URL.
6. In the **Template Selection** section, click **Custom**, and then click **Microsoft Dynamics Public**.
7. Specify collection administrators and quota details.
8. Click **OK**.
9. After the new SharePoint site collection is created, open a command prompt, type **iisreset /noforce**, and press ENTER.

Configure anonymous authentication in IIS

You must configure the Web site to use anonymous authentication in IIS.

1. Open IIS manager (**Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**).
2. Expand the **Web Sites** directory, right-click the site that you created in the previous procedure, and click **Properties**.
3. Click **Directory Security**, and then click **Edit** in the **Authentication and access control** section.
4. Click **Enable Anonymous authentication**, and then click **OK**.

   Note:

   You do not need to change the user name or password.

   The **Inheritance Overrides** dialog box opens.
5. Click **Select All**, and then click **OK**.

View the site as an anonymous user

You might not be able to view the Enterprise Portal Internet site if you are logged on to your corporate network and your credentials have already been authenticated using Windows Integrated authentication.

To view the site as an anonymous user, you must enable anonymous logon user authentication in your Web browser. The following procedure describes how to enable anonymous logon user authentication for Internet Explorer. If you are using a Web browser other than Internet Explorer, consult that product's documentation for information about enabling anonymous logon user authentication.

1. Open Internet Explorer.
2. Click **Tools** > **Internet Options** > **Security** > **Internet** or **Local intranet** > **Custom level**.
3. Under **User Authentication**, select **Anonymous logon**.
4. Open the Web site in your Web browser.

Next steps

- Register the site IP address and a URL with a domain name service so users can find the site on the Internet.
- Configure the guest account and a guest user group so users can access the Enterprise Portal Internet site. For more information, see Give users access to an Enterprise Portal Internet site.

View an Enterprise Portal Web site

You can view an Enterprise Portal Web site using one of the following methods:

- Enter the URL in the address field of your Web browser. The default URL is http://server_name/sites/DynamicsAX.
- Select a site in the **Administration of Web sites** form and click the **View in Browser** button (**Administration** > **Setup** > **Internet** > **Enterprise Portal** > **Web sites**).

Configuring Enterprise Portal

This section provides information to help you configure Enterprise Portal user relations, document handling options, and other parameters and settings. The following topics are included:

- Configure Enterprise Portal using the Configuration Wizard
- Specify user relations
- Set up documents for viewing in Enterprise Portal
- Set up transaction summaries for Enterprise Portal
- Specify Enterprise Portal parameters
- Set up Enterprise Portal Search

Configure Enterprise Portal using the Configuration Wizard

The **Enterprise Portal Configuration Wizard** helps you set up user groups, document management, and transaction summary parameters for Enterprise Portal. You can configure these options before or after installing the Enterprise Portal templates and files using Setup.

To configure Enterprise Portal using the Configuration Wizard

1. Click **Administration** > **Setup** > **Internet** > **Enterprise Portal** > **Configuration wizard**.
2. Complete the configuration wizard. For more information about the fields and options in the wizard, see Enterprise Portal Configuration Wizard (form).

Next steps

If you have not already done so, install Enterprise Portal. For more information about installing Enterprise Portal, see "Install Enterprise Portal and Role Centers" in the Microsoft Dynamics AX Installation guide. If you have installed Enterprise Portal, review the topics in Configuring Enterprise Portal security.

Specify user relations

When you specify user relations, you identify a user's relationship to your organization. Users can be internal, such as employees, or external, such as vendors, customers, or business relations. After you specify user relations, a user's information (such as employee ID or customer account ID) is automatically displayed in applicable fields on Enterprise Portal pages. Certain Enterprise Portal pages, for example Human Resources and Shop Floor Control, can only be viewed if a user is assigned a user relation.

Note:

Users must be listed in the **User** form before you can specify user relations for them.

User relations do not enforce security in Enterprise Portal. Enterprise Portal security is enforced through user groups in Microsoft Dynamics AX and SharePoint groups. For more information, see Configuring Enterprise Portal security.

1. Click **Administration** > **Setup** > **User relations**.
2. On the **Overview** tab, click the **Wizard** button. Complete the steps in the wizard.

Set up documents for viewing in Enterprise Portal

By default, Enterprise Portal does not display any documents. To display documents, you must map document types to document categories. Document categories determine which types of documents can be displayed on specific Enterprise Portal module sites. The list of document categories is fixed, but the categories are general enough to encompass most document types.

For example, if your organization uses Microsoft Visio® diagrams, you must map the .vsd document type to a document category in Enterprise Portal. If the .vsd document type is not mapped to a category, users cannot view Visio diagrams in Enterprise Portal.

After you map document types to document categories, you must specify which document categories are visible on each Enterprise Portal module site, and then specify which document categories are visible for external users. Document categories act as a sort of filter by allowing only users with the appropriate permissions to view certain types of documents, and then only on the designated module site.

This topic describes how to set up documents for viewing in Enterprise Portal using the **Enterprise Portal Configuration Wizard**.

You can also specify which document categories appear in Enterprise Portal modules on the **Documents** tab in the **Enterprise Portal parameters** form (**Administration** > **Setup** > **Internet** > **Enterprise Portal** > **Parameters**).

Note:

This topic does not describe how to add new document types to Microsoft Dynamics AX. For information about adding new document types, and other document management tasks, see Using document management in the Applications and Business Processes Help.

1. Click **Administration** > **Setup** > **Internet** > **Enterprise Portal** > **Configuration wizard**.
2. Click **Next** until the **Map document types to document categories** page is displayed.

   The document types that are listed on this page are the document types in the **Basic** > **Setup** > **Document management** > **Configuration wizard** form.
3. Select a document type to display in Enterprise Portal, and then select the document category that it should be mapped to.
4. After you have specified a document category for each document type to display in Enterprise Portal, click **Next**.

Note:

Categories can contain multiple document types, but a document type cannot be mapped to multiple categories.

5. On the **Configure module document categories** page, right-click each category and click **New category**.

Note:

Use the **Online customer** and **Online vendor** options to specify which document categories can be viewed by external users (customers or vendors). If you do not specify any document categories for these items, external users will not be able to view any documents in Enterprise Portal.

6. After you have specified which document categories appear in each module, click **Next** and complete the wizard.

Set up transaction summaries for Enterprise Portal

You can configure Enterprise Portal to display totals or balances – called transaction summaries – for the following types of transactions:

- Purchase totals, including quantity, amount, weight and volume
- Customer balances
- Inventory on hand
- Vendor balances

Generating transaction summaries can adversely affect the performance of the database server. We recommended that you configure a batch job to generate transaction summaries during off-peak hours. Configuring a batch job for transaction summaries requires that you:

- Create a batch group, which enables you to add multiple batch jobs to the processing list at one time.
- Associate the transaction summary batch job with a batch group, and specify how often the batch job is processed.
- Add the batch group to the batch queue.

Create a batch group (optional)

You can use batch groups to add multiple batch jobs to the batch queue at one time. For more information, see Create a batch group in the Applications and Business Processes Help.

1. In the Microsoft Dynamics AX client, click **Basic** > **Setup** > **Batch** > **Batch groups**.
2. Press CTRL+N to create a new batch group, and then close the form.

Configure transaction summaries

You can use the **Transaction summary** form to specify how often transaction summaries are generated. For more information, see Transaction summary (Class Form) in the Applications and Business Processes Help.

Note:

You also can configure transaction summaries using the **Enterprise Portal Configuration Wizard**. For more information, see Configure Enterprise Portal using the Configuration Wizard.

1. In the Microsoft Dynamics AX client, click **Administration** > **Setup** > **Internet** > **Enterprise Portal** > **Transaction summary**.
2. Associate the transaction summary to a group from the **Batch group** list.
3. Select the **Batch processing** check box to run the job as a batch without its being associated with a batch group.
4. Click **Recurrence** to specify how often the transaction summary is run.
5. Click **OK** to close the form. A message is displayed stating that the transaction summary job has been added to the batch queue.

Start batch processing

1. In the Microsoft Dynamics AX client, click **Basic** > **Periodic** > **Batch** > **Processing**.
2. In the **Group** list, select the batch group that you associated with the transaction summary job, and then click **OK**.

   The job starts processing according to the schedule you defined. For more information, see Processing batch jobs in the Applications and Business Processes Help.

Specify Enterprise Portal parameters

Enterprise Portal parameters determine the following:

- The types of documents users can access in Enterprise Portal
- The number sequences for items that are displayed in Enterprise Portal

Caution:

Although you can change the parameters at any time, these changes might affect the Enterprise Portal pages and temporarily disrupt user connectivity to those pages.

1. Click **Administration** > **Setup** > **Internet** > **Enterprise Portal** > **Parameters**.
2. Select the parameters. For a description of the fields and options in this form, see Enterprise Portal parameters (form).
3. Click **OK**.

Set up Enterprise Portal Search

If you enable Enterprise Portal Search, users can search records in the Microsoft Dynamics AX database, as well as documents, announcements, discussions, and list items that are stored in Microsoft Windows SharePoint Services or Microsoft Office SharePoint Server. If you do not set up Enterprise Portal Search as described here, search results return data from the SharePoint site, such as documents or announcements, but the results do not include Microsoft Dynamics AX data.

Before you begin

- Users will see only search results that they have access to based on Microsoft Dynamics AX security features, including user groups, record-level security, and domains.
- Enterprise Portal Search does not integrate with the Search center on Office SharePoint Server. This means that users cannot search for Microsoft Dynamics AX data using the Search center.
- After you have set up Search, users can view search results by navigating to the search results page in Enterprise Portal.
- Set up the Microsoft Dynamics AX data crawler as described in "Setting up the Data Crawler for a global search" in the System and Application Setup Help.

Note:

For information about configuring tables you created in Microsoft Dynamics AX so those tables can be searched, see “How to: Configure a Table for Search” in the Microsoft Dynamics SDK.

Setting up Enterprise Portal search

After you finished setting up and configuring the Microsoft Dynamics AX data crawler, you can use the following procedures to set up Enterprise Portal search.

Start SharePoint Services Search

This procedure describes how to start the search service in Windows SharePoint Services.

1. Verify that the full-text search service is enabled for the Microsoft Dynamics AX database. By default, this service is enabled in Microsoft SQL Server.
2. Open **SharePoint Central Administration** (**Start** > **Programs** > **Administrative Tools** > **SharePoint 3.0 Central Administration**).
3. Click the **Operations** tab.
4. Under **Topology and Services**, click **Services on server**.
5. Click **Windows SharePoint Services Search**. The **Configure Search Services** pages opens.
6. In the **Service Account** and **Content Access Account** sections, enter the Business Connector proxy credentials.
7. Verify the details in the **Search Database** section.
8. Specify an indexing schedule.

Note:

Indexing can consume resources on the server. Consider specifying an indexing schedule during off-peak hours.

9. Click **Start** to start the Windows SharePoint Services Search.

Associate the SharePoint Search Service with the Enterprise Portal content database

This procedure describes how to associate the SharePoint Search Service with the content database used by Enterprise Portal. If you do not complete this procedure, SharePoint search will not return data from the Enterprise Portal database.

1. Open **SharePoint Central Administration** (**Start** > **Programs** > **Administrative Tools** > **SharePoint 3.0 Central Administration**).
2. Click the **Applications Management** tab.
3. Under **SharePoint Web Application Management**, click **Content database**.
4. In the **Web Application** drop-down list, click the Enterprise Portal application.
5. In list of databases, click the content database used by Enterprise Portal.
6. Under **Search Server**, select the Enterprise Portal server.
7. Click **OK**.

Search Enterprise Portal

Use this procedure to search Microsoft Dynamics AX data on Enterprise Portal.

1. Open your Enterprise Portal Web site.
2. Set the search drop-down list to **Dynamics AX**.
3. Click a module site where you want to perform a search (for examples, Sales).
4. Enter a search term and click the search button.

Configuring Enterprise Portal security

This section provides information to help you plan your Enterprise Portal security model, including information about Enterprise Portal groups, permissions, user access, and perimeter network configuration. The following topics are included:

- About Enterprise Portal security
- About Enterprise Portal roles and user groups
- Configuring a perimeter network for Enterprise Portal

About Enterprise Portal security

This topic describes various aspects of Enterprise Portal security, such as Enterprise Portal security components, a process overview for securing Enterprise Portal, and best practices.

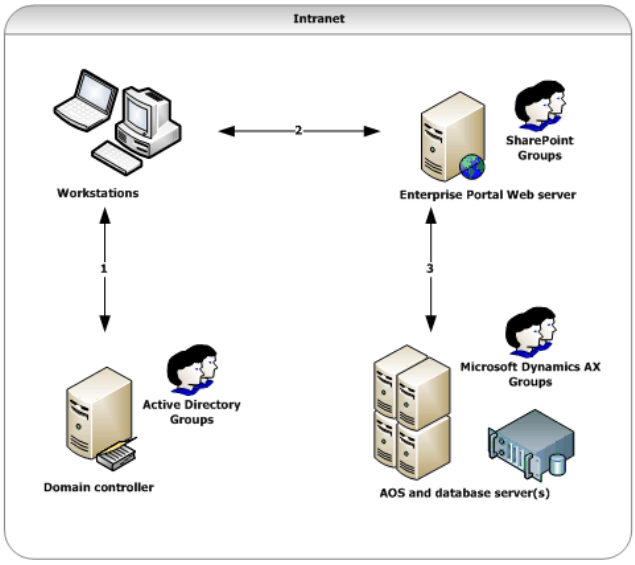
Enterprise Portal security components

Enterprise Portal security uses a combination of the following:

- Microsoft Active Directory® directory services
- Windows SharePoint Services or Office SharePoint Server users and groups
- Microsoft Dynamics AX access control

Figure 1 illustrates how the combination of these services and features determines user access and the content shown on Enterprise Portal.

Figure 1: Enterprise Portal security access in an intranet deployment



1. A user attempts to log on to the network. The user's credentials must be listed in Active Directory on the domain controller.
   - If the user is not listed in Active Directory, the user cannot access any resources on the network.
   - If the user is listed in Active Directory, the user can attempt to access the Enterprise Portal site using a Web browser.
2. The IIS Web server receives the request for the Enterprise Portal page. The Web server verifies whether the user is listed in Microsoft Dynamics AX and in Windows SharePoint Services or Office SharePoint Server to determine if the user can access the Enterprise Portal site.
   - If a user is not listed in both, that user is denied access to the site.
   - If the user is listed in both, that user can access the site, and the Web server sends a request to the AOS server to determine which data and content should be displayed (if any).
3. The AOS server receives the request for Microsoft Dynamics AX data.
   - If the user is not listed in any Microsoft Dynamics AX groups, the user sees an empty Enterprise Portal page in their Web browser.
   - If the user is listed in one or more groups, the Enterprise Portal page displays content and data defined by the user group permissions.

The Enterprise Portal security components in an extranet deployment can include one or more firewall devices and multiple domain controllers, but the process of determining page access and the content shown on pages is the same.

Process for configuring Enterprise Portal security

By default, only the administrator who installed Enterprise Portal can access the site. The process for configuring Enterprise Portal security then is a process of giving users access to the site and assigning users to Microsoft Dynamics AX groups so they can view content on the site.

1. Install Enterprise Portal. For more information about installing Enterprise Portal, see "Install Enterprise Portal and Role Centers" in the Microsoft Dynamics AX Installation guide.
2. Add users to Active Directory. If your organization has a core Microsoft Dynamics AX installation running, users might already be listed in Active Directory. If a user is listed in the **Users** form and the **Enabled** option is selected, the user already exists in Active Directory.
3. Enable the default Enterprise Portal user groups (a subset of the Microsoft Dynamics AX user groups) by completing the **Enterprise Portal Configuration Wizard**. For more information, see Configure Enterprise Portal using the Configuration Wizard.
4. Add users to groups according to each user's role in the company. For information about Enterprise Portal roles and corresponding user groups, see About Enterprise Portal roles and user groups.
5. Set up and configure a perimeter network (for extranet deployments). For more information, see Configuring a perimeter network for Enterprise Portal.

6. Give users access to the site. For more information, see Giving users access to Enterprise Portal sites.
7. Specify user relations (required for the Shop Floor Control and Human Resources module sites). For more information, see Specify user relations.

Enterprise Portal security best practices

The following best practices can help you be diligent and proactive toward maintaining a more secure Enterprise Portal environment.

- Configure your servers to automatically download and install updates from Microsoft Update. If your organization prefers to not install updates automatically, schedule a regular time to review and install updates.
- Verify with management each user's role and Microsoft Dynamics AX group assignments. If you add a user to the wrong group, that user could have access to data and content that is not intended for them. If necessary, review the About Enterprise Portal roles and user groups topic with management to create an accurate list of each user's role and corresponding group assignments.
- If a user leaves your organization or company, remove that user from Active Directory, the SharePoint site, and the list of users in Microsoft Dynamics AX.

About Enterprise Portal roles and user groups

An Enterprise Portal role is a job function, such as a sales representative or an employee manager. For example, if a sales representative in your organization intends to use Enterprise Portal, that user must belong to several groups so they can view the necessary pages and data.

This topic describes the Enterprise Portal roles and user groups that are enabled in Microsoft Dynamics AX after you complete the **Enterprise Portal Configuration Wizard**. You can create additional roles as necessary, but you will need to determine which user group or combination of user groups allows users in that role to view the content and data necessary to do their jobs.

Identifying roles and user groups

Use the information in this topic as follows:

1. Create a list of all internal and external users who require access to Enterprise Portal.
2. Identify each user's role and map it to one of the Enterprise Portal roles described in this topic.
3. For each user, note the user groups that correspond to their role. The table that follows includes a list of corresponding user groups for each role.
4. Add each user to the groups that correspond to their role so they can view content and data on Enterprise Portal.

After you assign users to groups, you must give users access to Enterprise Portal. For information, see Giving users access to Enterprise Portal sites.

Note:

If users are assigned to more than one role, they must be assigned to the corresponding user groups for all roles. You cannot assign a user to both an internal role and an external role. For example, a user cannot be both an internal employee and a vendor.

Role	Description	Required group membership
Absence approver (internal)	Gives users access to the absence approval functionality in the employee self-service pages. Users can: • Approve absence requests for some or all employees. • Approve absence registrations for some or all employees.	EP_HRMA EP_HRME EP_Int EP_Empl
Administrator (internal)	Gives users access to configure and administer Enterprise Portal. Users can: • Manage Web users. • Configure options for users, Accounts receivable, Inventory management, and customer self-service pages. • Control setup options, such as style sheets and languages. • Refresh the Microsoft Dynamics AX data from within Enterprise Portal.	EP_Admin EP_Empl EP_Int EP_HRME
Applicant (external)	Gives users access to the employee self-service pages and users can apply for a job.	EP_HRAp
Business relation (external)	Gives users access to the business relation self-service pages. Users can: • Browse the product catalog. • Complete questionnaires.	EP_BR

Role	Description	Required group membership
Consultant (internal)	Gives users access to the Project module site. Users can: • Register hours on projects. • Browse invoices and invoice proposals. • Browse hour, cost, revenue, item, and on-account transactions. • View and create reports for total hours per project. • View and create reports for hours per journal. • Complete and analyze questionnaires. • View and delete their alerts. • View and disable their alert rules.	EP_Empl EP_Cons EP_Int EP_HRME
Customer (external)	Gives users access to the customer self-service pages. Users can: • Browse the product catalog. • Add items to the shopping basket. • Create orders online. • Add items to the shopping basket without ordering, and then return to the shopping module at a later time to finish their orders. • Complete questionnaires.	EP_Cust EP_Ext
Employee manager (internal)	Gives users access to the employee self-service pages. Users can: • Browse and update personal information, such as appraisal interviews, benefits, courses,	EP_HRMM EP_HRME EP_Empl EP_Int

Role	Description	Required group membership
	emergency contacts, development plans, loans, and resume qualifications for managed employees. • Perform various managerial activities, such as recruitment project tasks. • View various manager reports. • Access performance management tools.	
Employee (internal)	Gives users access to the employee self-service pages. Users can: • Browse and update personal information, such as appraisal interviews, benefits, courses, emergency contacts, development plans, equipment loans, and resume qualifications. • Access various employee activities, such as absence request registration and absence registration. • View various employee reports.	EP_Empl EP_Int EP_HRME
Enterprise Portal Shop Floor Control (SFC) employee role (internal)	Gives users access to the electronic timecard. Users can: • Register time and attendance. • Register personal project hours. • Register personal time spent on indirect activities. • Register personal time on production jobs.	EP_JMGS EP_Empl

Role	Description	Required group membership
Guest (external)	Gives anonymous Web users access to log on to the Enterprise Portal customer site with limited functionality. Users can: • Browse the product catalog (but they cannot place orders). • Create a registration request to become a customer.	EP_Cust EP_Ext
Questionnaire Administrator (internal)	Gives users access to the questionnaire self-service pages. Users can: • Access analytical tools, such as questionnaire statistics. • Schedule and distribute questionnaires. • Access administrator reports. • Access results and evaluations for all participants.	EP_QuAd
Questionnaire participant (external)	Gives users access to the questionnaire self-service pages. Users can: • Access and complete questionnaires. • View various reports that are available to participants. • View their own results and evaluations.	EP_Qupa
Sale representative (internal)	Gives users access to various sales-related forms and reports. Users can perform tasks within these areas: • Business relations: Create and edit	EP_Sale EP_Empl EP_Int EP_HRME

Role	Description	Required group membership
	• Leads: Create and edit • Opportunities: Create and edit • Quotation: Create, edit, accept, and send (mail/letter) • Sales order: Create, edit, and send (mail/letter) • Customer: Create and edit • Credit note: Create, update, and send (mail/letter) • Contact person: Create, edit, and delete • Prices: Update price and discount • Product information: Send (mail/letter) • Questionnaire: Complete and analyze • Alerts: View and delete their alerts • Alerts: View and disable their alert rules Users can view and create the following reports: • Sales analysis • Lead analysis • Pipeline analysis • Sales versus target • New leads trend • Win analysis • Month-over-month closing trend • Pipeline by sales process and stage • Leads summary by source type	

Role	Description	Required group membership
	• Sales by week, month, quarter, and year (current year and the year before) (list and graph) • Sales by region • Sales by customer • Price list by customer • Sales price list by customer (all customers/by customer) • Customer turnover • Sales by person • Price list • Sales prices • Price/discount list • Top 100 (by revenue and margin) • Blanket orders • Sales forecast per item (all customers/by customer)	
Technician (internal)	Gives users access to service orders and service agreements. Users can: • Create, view, and edit service orders. • Create, view, edit, and delete service order lines. • Create, view, and edit repair lines. • View service object relation lines. • View service task relation lines. • View service agreements.	EP_Tech EP_Empl
Vendor (external)	Gives users access to the vendor self-service pages. Users can: • Change their address,	EP_Vend EP_Ext

Role	Description	Required group membership
	telephone number, Web site address, telex, fax, language, and e-mail addresses. Some fields, such as account number, currency, balance, and balance in currency, are read-only fields. • Set up and change contact person information (title, name, phone extension, phone, mobile phone, pager, e-mail address, and personal address). • View purchase orders (header and lines). • View items (read-only mode). • View journals (purchase order, packing slip, and invoice). • Update prices and discounts. • View delivery due date. • View supply performance. • View supply capacity. • Complete questionnaires.	

Configuring a perimeter network for Enterprise Portal

This section describes how to secure Enterprise Portal using either a traditional perimeter network or a standard perimeter network. The following topics are included:

- Configure a traditional perimeter network for Enterprise Portal
- Configure a standard perimeter network for Enterprise Portal

Configure a traditional perimeter network for Enterprise Portal

This topic describes how to set up a traditional perimeter network to support Enterprise Portal. A traditional perimeter network enhances the security of the Enterprise Portal configuration by using two firewalls and two domain controllers to restrict access to Microsoft Dynamics AX data. This topic also describes how to configure ports on the firewall devices and establish the appropriate trust level between domain controllers.

Caution:

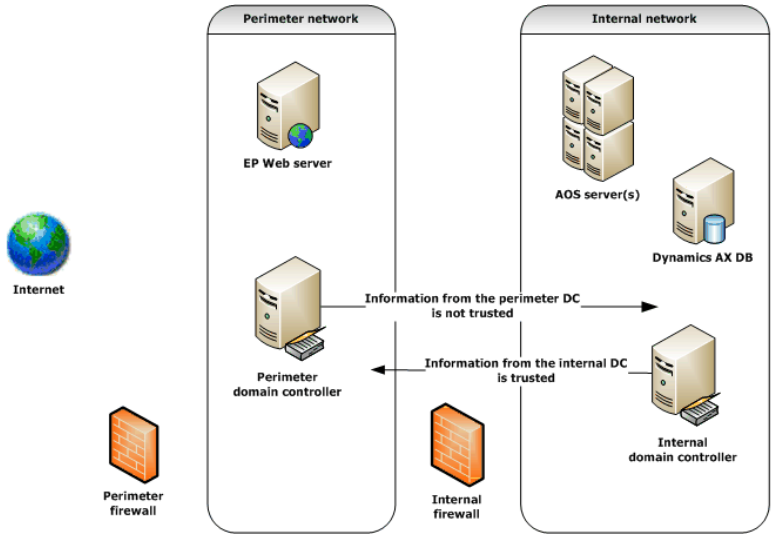
If you do not have experience setting up and configuring network security, contact your Microsoft Certified Partner for assistance. If you do not set up the perimeter network correctly, your system might be vulnerable to security threats.

Although a traditional perimeter network is recommended, you also can set up a standard perimeter network using Microsoft ISA Server and a single firewall device. For more information, see Configure a standard perimeter network for Enterprise Portal.

About traditional perimeter networks

A traditional perimeter network contains two Microsoft Active Directory® directory service domain controllers separated by firewall devices in two distinct networks, as shown in Figure 1.

Figure 1: A traditional perimeter network



The perimeter network contains the Enterprise Portal Web server that is running IIS, and an Active Directory domain controller. The perimeter domain controller hosts accounts for those users who are external to the organization and who require Enterprise Portal access. These user accounts are set up on the perimeter domain controller as follows:

1. External users have no rights on the internal domain.
    a. External users cannot log on to the machine as a local user (log on locally)
    b. External uses cannot access the internal network
2. The internal network contains a complete installation of Microsoft Dynamics AX. This includes the following components:
    a. An Active Directory domain controller that contains the accounts for all internal Microsoft Dynamics AX users
    b. A database that stores Microsoft Dynamics AX data and a list of both internal and external Microsoft Dynamics AX users
    c. A Microsoft Dynamics AX AOS

The internal domain controller has a one-way trust with the perimeter domain controller. This means that information that is sent by the internal domain controller is trusted, but information that is sent by the perimeter domain controller is not trusted. This enhances network security by ensuring that the perimeter domain controller is not able to communicate to the internal domain controller which users are internal to the domain or which users are administrators. If the information that is sent by the perimeter domain was trusted, a malicious user might compromise the internal domain controller, and thereby access data in the internal domain.

Setting up a traditional perimeter network

This section describes how to configure ports and a one-way trust for a traditional perimeter network that supports Enterprise Portal.

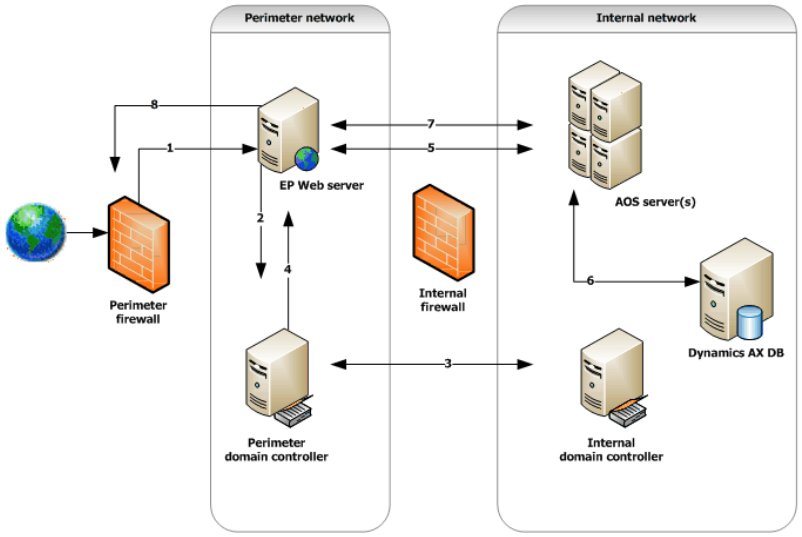
Install and configure Enterprise Portal on a perimeter network

If you have not already done so, install Enterprise Portal on the Web server in the perimeter network. For more information about installing Enterprise Portal, see "Install Enterprise Portal and Role Centers" in the Microsoft Dynamics AX Installation guide.

Configure ports

This section describes how to configure ports in the perimeter network and the internal network so users can access the appropriate Microsoft Dynamics AX information using Enterprise Portal. Table 1 at the end of this section provides a complete list of ports and the associated direction, connection, and connection type information.

Figure 2: A request for an Enterprise Portal page



A request is processed as follows:

1. By default, the Enterprise Portal Web server receives the request from the firewall on TCP port 80 (or 443, if your Web server is configured for Secure Sockets Layer [SSL] encryption). The firewall therefore must have port 80 or 443 open for incoming Internet requests. All outbound traffic is permitted, which means that all ports are open for traffic going from the perimeter network to the Internet.
2. After the Web server receives the request, it sends the request to the perimeter domain controller on UDP port 53 to verify whether the user is an external or internal user.
3. The perimeter domain controller and the internal domain controller communicate by using various ports, as shown in Table 1 at the end of this section.
4. The perimeter domain controller identifies the user and then returns the request to the Web server on UDP port 53.
5. The Web server authenticates the user and then sends the request to the AOS on TCP port 2712. The Web server and the AOS communicate by using the Business Connector proxy account.
6. The AOS communicates with the Microsoft Dynamics AX SQL Server database on port 1433.
7. After the AOS retrieves the necessary data from the database, it returns the request to the Web server on the default TCP port, 2712.
8. The Web server completes the request by sending the page to port 80 or 443.

Table 1: Ports for a traditional perimeter network to support Enterprise Portal

Port	Direction	Connection	Type	Notes
80 or 443 (by default)	Inbound/ Outbound	Perimeter firewall to the Enterprise Portal Web server	TCP	Verify which ports are used in your environment
2712 (by default)	Inbound/ Outbound	Enterprise Portal server to Microsoft Dynamics AX AOS	TCP	Verify which port is used in your environment
53	Inbound/ Outbound	DNS	UDP	None
135	Outbound	Internal domain controller to perimeter domain controller	TCP	None
135	Inbound	Perimeter domain controller to internal domain controller	TCP	None
445	Outbound	Internal domain controller to perimeter domain controller	TCP	None
445	Inbound	Perimeter domain controller to internal domain controller	TCP	None
1638	Outbound	Internal domain controller to perimeter domain controller	TCP	None
1638	Inbound	Perimeter domain controller to internal domain controller	TCP	None
389	Outbound	Internal domain controller to perimeter domain	UDP	None

Port	Direction	Connection	Type	Notes
		controller		
389	Inbound	Perimeter domain controller to internal domain controller	UDP	None
None	Outbound	Internal domain controller to perimeter domain controller	UDP equals domain	None
None	Inbound	Perimeter domain controller to internal domain controller	UDP equals domain	None

If necessary, use Telnet or Netmon to verify these ports. For more information about configuring firewall ports, see How to configure a firewall for domains and trusts.

Configure DNS

The following procedures describe how to configure your Domain Name System (DNS) to create a one-way trust between the domain controllers in your network. For Enterprise Portal, the perimeter network domain controller should trust the internal domain controller, but the internal domain controller should not trust the perimeter domain controller.

To create the one-way trust, complete the following procedures:

- Configure zone transfers on both domain controllers
- Create a secondary zone on both domain controllers
- Create trust from the internal domain controller to the perimeter domain controller

Configure zone transfers on both domain controllers

Complete this procedure to ensure that the domain controllers can communicate with each other.

1. Log on to the internal domain controller by using an account that is a member of the domain administrators group.
2. Open DNS (**Start** > **Programs** > **Administrative Tools**).
3. In the **DNS console**, expand the local name server.
4. Expand **Forward Lookup Zones**, right-click the domain name, and then click **Properties**.
5. Click the **Zone Transfers** tab.
6. Select **Allow Zone Transfers**, and then select **Only to the Following Servers**.
7. Enter the IP address for the perimeter network domain controller, and then click **Add**.
8. Click **OK**, and then restart the DNS server.
9. Repeat this procedure for the perimeter domain controller.

Create a secondary zone on both domain controllers

Complete this procedure to ensure that the domain controllers know each other's fully qualified domain names.

1. Log on to the internal domain controller by using an account that is a member of the Domain Administrators group.
2. Open DNS(**Start** > **Programs** > **Administrative Tools**).
3. In the **DNS console**, expand the local name server.
4. Right-click **Forward Lookup Zones**, click **New Zone**, and then click **Next**.
5. On the **Zone type** page, select **Secondary zone**, and then click **Next**.
6. On the **Zone Name** page, enter the fully qualified domain name of the perimeter network, and then click **Next**.
7. Enter the IP address for the perimeter domain controller, and then click **Next**.
8. Click **Finish** to complete the wizard, and then restart the DNS server.
9. Repeat this procedure for the perimeter domain controller.

Create a one-way trust between the domain controllers

Complete this procedure to set up the one-way trust between the internal domain controller and the perimeter domain controller.

1. Log on to the perimeter domain controller by using an account that is a member of the Domain Administrators group.
2. Open Active Directory Domains and Trusts (**Start** > **Programs** > **Administrative Tools**).
3. In the console tree, right-click the domain name for the domain that you want to administer, and then click **Properties**.
4. Click the **Trust** tab.
5. Click **New Trust**, and then click **Next**.

6. On the **Trust Name** page, enter the fully qualified domain name for the internal domain, and then click **Next**.
7. Select **One Way: Outgoing**, and then click **Next**.
8. Select **Both this domain and the specified domain**, and then click **Next**.
9. Enter the domain administrator credentials for the internal domain, select **Domain Wide Authentication**, and then click **Next**.
10. Click **Next** twice, and then click **Yes** to confirm outgoing trust.
11. Click **Finish**.

Important:

The IIS server and the AOS cannot communicate unless the IIS server can resolve the AOS IP address and name by using an LMHosts file. You must create an LMHosts file to resolve NetBIOS names as described in the following section.

Resolve computer names

Microsoft Dynamics AX uses the Remote Procedure Call (RPC) to communicate with the AOS. NetBIOS is a requirement of RPC. The IIS server and the AOS cannot communicate unless the IIS server can resolve the AOS IP address and name by using an LMHosts file.

Follow these steps to resolve the computer names.

1. Create an LMHosts file on the IIS server in the perimeter network. For information about how to create this file, see How to Write an LMHosts File for Domain Validation and Other Name Resolution Issues.
2. Add the AOS IP address and the AOS name in the LMHosts file on the IIS server.

Verify security and access

To verify the security of your traditional perimeter network, create a user account on the perimeter domain controller, and then configure the user as an external user in Microsoft Dynamics AX. After you create the external user account, open a page on an external Enterprise Portal site (for example, a page such as a questionnaire that has been set up for external access). The external user should be able to access this site.

Next, attempt to access an internal Enterprise Portal site. Verify that the external user receives an access denied message or is redirected to the external site (depending on how you configured Enterprise Portal and IIS).

Finally, verify that you can access the internal site using your internal credentials. If any of these access attempts fail, verify the procedures in this document.

Configure a standard perimeter network for Enterprise Portal

We recommend using a traditional perimeter network for your Enterprise Portal network environment. A traditional perimeter network enhances the security of the Enterprise Portal configuration by using two firewalls and two domain controllers to restrict access to Microsoft Dynamics AX data. For more information, see Configure a traditional perimeter network for Enterprise Portal.

If a traditional perimeter network is not a feasible option for your organization, consider using a standard perimeter network that uses Microsoft ISA Server as your perimeter network's firewall server. You can access the Microsoft Business Solutions Perimeter Network Configuration Wizard on the Web to help you install and configure your standard perimeter network.

Caution:

If you do not have experience setting up and configuring network security, contact your Microsoft Certified Partner for assistance. If you do not set up the perimeter network correctly, your system might be vulnerable to security threats.

Giving users access to Enterprise Portal sites

This section provides information to help you configure Microsoft Dynamics AX roles and user groups and SharePoint groups so that users can access Enterprise Portal sites. The following topics are included:

- Give users access to an Enterprise Portal intranet site
- Give users access to an Enterprise Portal extranet site
- Give users access to an Enterprise Portal Internet site

Give users access to an Enterprise Portal intranet site

By default, only the administrator who installed Enterprise Portal has access to it. Other internal users can access Enterprise Portal after you have added each user to an Enterprise Portal user group in the **User groups** form, and then given each user access to the SharePoint site for Enterprise Portal.

Before you begin

Verify that the following tasks have been completed:

- You are a member of the local Administrators group on the Enterprise Portal server and a member of the Administrators group in Microsoft Dynamics AX.
- Users are listed in the **User** form in Microsoft Dynamics AX.
- You have a list of users who require access to Enterprise Portal, their roles in the organization, and their corresponding Enterprise Portal user groups. For more information about determining which user groups correspond to Enterprise Portal roles, see About Enterprise Portal roles and user groups.

Important For security reasons, we recommend that users and groups have the least amount of privileges necessary to do their jobs.

Add users to Enterprise Portal user groups

User groups determine the content shown in Enterprise Portal. Users must be a member of at least the EP_Int (Enterprise Portal Internal user) group before they can access Enterprise Portal. If a user does not belong to the EP_Int group or any other Enterprise Portal groups, the user sees a blank page when they access the site. The EP_Int group and all other Enterprise Portal default user groups are created in Microsoft Dynamics AX after you complete the **Enterprise Portal Configuration Wizard**. After you complete the wizard, you must add users to the Enterprise Portal groups. To learn how to add users to groups, see Manage user groups.

Give users access to the Enterprise Portal site

After you add users to Enterprise Portal groups, you must give users access to the Enterprise Portal SharePoint site. If a user does not have access to the site, the user will see an access error when viewing the site.

1. Open the Enterprise Portal site in your Web browser. The default URL is http://server_name/sites/DynamicsAx.
2. On the **Site Settings** page, under **Users and Permissions**, click **People and groups**.
3. On the toolbar, click **New** > **Add Users** or **New** > **New Group** to add users or create a new group on the current site.

   We recommend assigning users to SharePoint groups when possible to help minimize the amount of time spent administering individual user accounts.

Note:

You can add all the members of an Active Directory group by entering the domain and group name as a new user. You can also add all authenticated users by clicking the **Add all authenticated users** link on the **Add Users** page.

4. Grant each user or group permissions for the site. You might need to speak with the user's manager or group manager to determine the desired permissions.

Other internal users now can access the Enterprise Portal site.

Give users access to an Enterprise Portal extranet site

By default, only the administrator who installed Enterprise Portal has access to it. External users can access Enterprise Portal after you have added each user to an Enterprise Portal user group in the **User groups** form, and then given each user access to the SharePoint site for Enterprise Portal.

Before you begin

Verify that the following tasks have been completed:

- Your perimeter network is set up. External users cannot access Enterprise Portal unless you have set up and configured a perimeter network. For more information, see Configuring a perimeter network for Enterprise Portal.
- You are a member of the local Administrators group on the Enterprise Portal server and a member of the Admin group in Microsoft Dynamics AX.
- Users are listed in the **User** form in Microsoft Dynamics AX.
- You have a list of users who require access to Enterprise Portal, their roles in the organization, and their corresponding Enterprise Portal user groups. For more information about determining which user groups correspond to Enterprise Portal roles, see About Enterprise Portal roles and user groups.

Important:

For security reasons, we recommend that users and groups have the least amount of privileges necessary to do their jobs.

Add users to Enterprise Portal user groups

User groups determine the content shown in Enterprise Portal. External users must be a member of at least the EP_Ext (Enterprise Portal external user) group before they can access Enterprise

Portal. If an external user does not belong to the EP_Ext group or any other Enterprise Portal groups, the user sees a blank page when they access the site. The EP_Ext group and all other Enterprise Portal default user groups are created in Microsoft Dynamics AX after you complete the **Enterprise Portal Configuration Wizard**. After you complete the wizard, you must add external users to the Enterprise Portal groups. To learn how to add users to groups, see Manage user groups.

Give users access to the Enterprise Portal site

After you add users to Enterprise Portal groups, you must give users access to the Enterprise Portal SharePoint site. If a user does not have access to the site, the user will see an access error when viewing the site.

1. Open the Enterprise Portal site in your Web browser. The default URL is http://server_name/sites/DynamicsAx.

   The URL might be different if you are using SSL. You can verify the URL and view the site using the **Web sites** form (**Administration** > **Setup** > **Internet** > **Enterprise Portal** > **Web sites**).
2. On the **Site Settings** page, under **Users and Permissions**, click **People and groups**.
3. On the toolbar, click **New** > **Add Users** or **New** > **New Group** to add users or create a new group on the current site.

   We recommend assigning users to SharePoint groups when possible to help minimize the amount of time spent administering individual user accounts.

Note:

You can add all the members of an Active Directory group by entering the domain and group name as a new user. You can also add all authenticated users by clicking the **Add all authenticated users** link on the **Add Users** page.

4. Grant each user or group permissions for the site.

The external users now can access the Enterprise Portal site.

Give users access to an Enterprise Portal Internet site

Microsoft Dynamics AX creates a Guest user account during installation. The Guest user account allows anonymous Web users to log on to an Enterprise Portal Internet site with limited access. Web users who log on with the Guest account can view the product catalog, complete questionnaires, and sign up to become customers, but they cannot view any other information. All anonymous Web users connect to Enterprise Portal using the same Guest user account.

This topic describes how to enable the Guest user account and the Guest user group, and how to add the Guest user account to the Guest user group. You must complete all the procedures in this topic before users can access an Enterprise Portal Internet site.

Enable the Guest user account

By default, the Guest user account is disabled. You must enable this account before anonymous users can access the Enterprise Portal Internet site.

1. In the Microsoft Dynamics AX client, click **Administration** > **Common Forms** > **Users**.
2. On the **Overview** tab, select the **Guest** user account.
3. Select the **Enabled** check box.
4. Close the form to save changes.

Enable the Enterprise Portal Guest user group

Before users can access an Enterprise Portal Internet site, you must enable the Enterprise Portal Guest user group. The Enterprise Portal Guest user group is enabled when you configure Enterprise Portal using the Configuration Wizard. If you have not already done so, configure Enterprise Portal now using the Configuration Wizard. For more information, see Configure Enterprise Portal using the Configuration Wizard.

Add the Guest user account to the Enterprise Portal Guest user group

After you have configured Enterprise Portal, you must add the Guest user account to the Enterprise Portal Guest user group.

1. In the Microsoft Dynamics AX client, click **Administration** > **Setup** > **User groups**.
2. Click **EP_Gues**.
3. Click the **Users** tab.
4. Select the **Guest** user account in the **Remaining users** list box and click the left arrow button (**<**) to move the user account into the **Selected users** list box.
5. Press CTRL+S to save changes.

Next step

If you have not already done so, you can create an Enterprise Portal Internet site. For more information, see Create an Enterprise Portal Internet site.

Maintaining Enterprise Portal

This section provides information to help you maintain Enterprise Portal sites. The following topics are included:

- Delete an Enterprise Portal site
- Disable an Enterprise Portal virtual server

Delete an Enterprise Portal site

To delete an Enterprise Portal site, you first must delete the SharePoint site, and then delete the site from the list of Web sites in Microsoft Dynamics AX.

Note:

You cannot delete an Enterprise Portal site if it contains other virtual directories or subsites. You must delete any subsites before you can delete the top-level Enterprise Portal site.

Delete the SharePoint site

To delete the SharePoint site, you must be a site administrator who has a Full Control permission level.

1. Open the Enterprise Portal site in your Web browser.
2. Go to the **Site Settings** page for the top-level Enterprise Portal Web site.
3. Under **Site Administration**, click **Delete this site**.
4. Click **Delete** to confirm.

Delete the site in Microsoft Dynamics AX

To delete the site in Microsoft Dynamics AX, you must be a member of the Administrators group in Microsoft Dynamics AX.

1. Click **Administration** > **Setup** > **Internet** > **Enterprise Portal** > **Web sites**.
2. Select the site to delete and then press ALT+F9.

Note:

Deleting the SharePoint site does not delete the Web application. If you will not be using or creating any Enterprise Portal sites, you can delete the Web application using SharePoint Central Administration, or you can disable the virtual server in Microsoft Dynamics AX. For more information, see the Windows SharePoint Services documentation or Disable an Enterprise Portal virtual server.

Disable an Enterprise Portal virtual server

If you disable an Enterprise Portal virtual server, all Enterprise Portal Web sites on the virtual server are no longer accessible to users. You might choose to disable a virtual server if you need to perform routine maintenance, including service pack installations, hot fixes, or security updates.

To disable the virtual server, you must be a member of the Administrators group in Microsoft Dynamics AX.

1. Click **Administration** > **Setup** > **Internet** > **Enterprise Portal** > **Manage deployments**.
2. Clear the **Enabled** option for the virtual server, and then close the form.

You can enable the virtual server again by selecting the **Enabled** option in the **Manage deployments** form.