Oracle® Enterprise Single Sign-On Provisioning Gateway

Administrator's Guide

Release 11.1.2

E27317-02

March 2013

ORACLE®

Oracle Enterprise Single Sign-On Provisioning Gateway, Administrator's Guide, Release 11.1.2

E27317-02

Copyright ©1998, 2013, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Table of Contents

Preface

The Oracle Fusion Middleware Provisioning Gateway Administrator's Guide explains how to use the Provisioning Gateway Administrative Console to remotely add, modify, and delete application credentials directly within each user's Logon Manager credential store, eliminating the need for local credential capture and granting the user instant access to the target application.

Audience

This guide is intended for experienced administrators responsible for the planning, implementation, and deployment of Provisioning Gateway. Administrators are expected to understand single sign-on concepts and be familiar with Internet Information Services, Windows Registry settings, and the Oracle Enterprise Single Sign-On Administrative Console. Persons completing the installation and configuration procedure should also be familiar with their company's system standards

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Related Documents

For more information, see the other documents in the Oracle Enterprise Single Sign-On Suite documentation set for this release.

Oracle Enterprise Single Sign-On Suite

Release Notes

Installation Guide

Administrator's Guide

Secure Deployment Guide

User's Guide

Oracle Enterprise Single Sign-On Logon Manager

Deploying Logon Manager with a Directory-Based Repository

Configuring and Diagnosing Logon Manager Application Templates

Oracle Enterprise Single Sign-On Provisioning Gateway

Administrator's Guide

Command Line Interface Guide

Oracle Identity Manager Connector Guide

Sun Java System Identity Manager Connector Guide

IBM Tivoli Identity Manager Connector Guide

Oracle Enterprise Single Sign-On Universal Authentication Manager

Administrator's Guide

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Overview of the Provisioning Gateway Administrative Console

The Provisioning Gateway Administrative Console enables administrators to set up, gather, and manage information from the Provisioning Gateway Web service. The following modules can be accessed from the Provisioning Gateway Administrative Console:

- Settings
- Users
- Reports & Logs

Accessing the Provisioning Gateway Administrative Console

Open a Web browser and enter the following URL:

`https://yourserverhost/v-go pm console/logon.aspx`

where *yourserverhost* is the name of the server where you installed Provisioning Gateway.

The Provisioning Gateway Administrative Console Logon Page opens.

Version Information

The About module provides information about which versions of Provisioning Gateway and Microsoft .NET Framework are installed.

- **Product Version.** Indicates which version of Provisioning Gateway is installed.
- **.NET Framework.** Indicates which version of Microsoft .NET Framework is installed.

Logon Page

Enter your logon credentials to access the Provisioning Gateway Web Service and click **Log On**.

The username and password should be the same as the directory authentication credentials.

For example, for Active Directory or AD LDS (ADAM), the username would be in the format: *domainname**username*.

For Sun or IBM, the username would be in the format: *uid*=*username*.

The Provisioning Gateway server only recognizes credentials that it has access to. On AD or AD LDS (ADAM), those recognized credentials are domain accounts. For Sun and IBM, the account must exist in the storage. If no storage has been defined, the account is authenticated against the local accounts on the server where the Web service is running.

Security Settings

Provisioning Gateway can be run without changing the default security settings. Security can be increased by changing several of the settings.

You can edit the Provisioning Gateway security settings through the Microsoft .Net Framework ASP.NET Configuration Settings. These settings are then changed in the Provisioning Gateway configuration files:

- <*local directory*>\Provisioning Gateway\Service\web.config
- <*local directory*>\Provisioning Gateway\Console\web.config

Granting Access to the Provisioning Gateway Management Console

By default, all users are denied access to the Provisioning Gateway Management Console. You can assign users provisioning rights through the Oracle Enterprise Single Sign-On Administrative Console. You can perform the following actions on users:

- Provisioning a logon (adding, modifying, deleting credentials) for a user. Assign these rights in the "Provisioning" tab of a template.
- Deleting an SSO user. Do this on the "Delete SSO User Right" tab of the Provisioning Gateway node.

Configure these settings and publish them to the repository to grant users access to the Provisioning Gateway Management Console.

See the *Oracle Enterprise Single Sign-On Suite Administrator's Guide* for more information on using these settings.

Changing the Encryption Algorithm

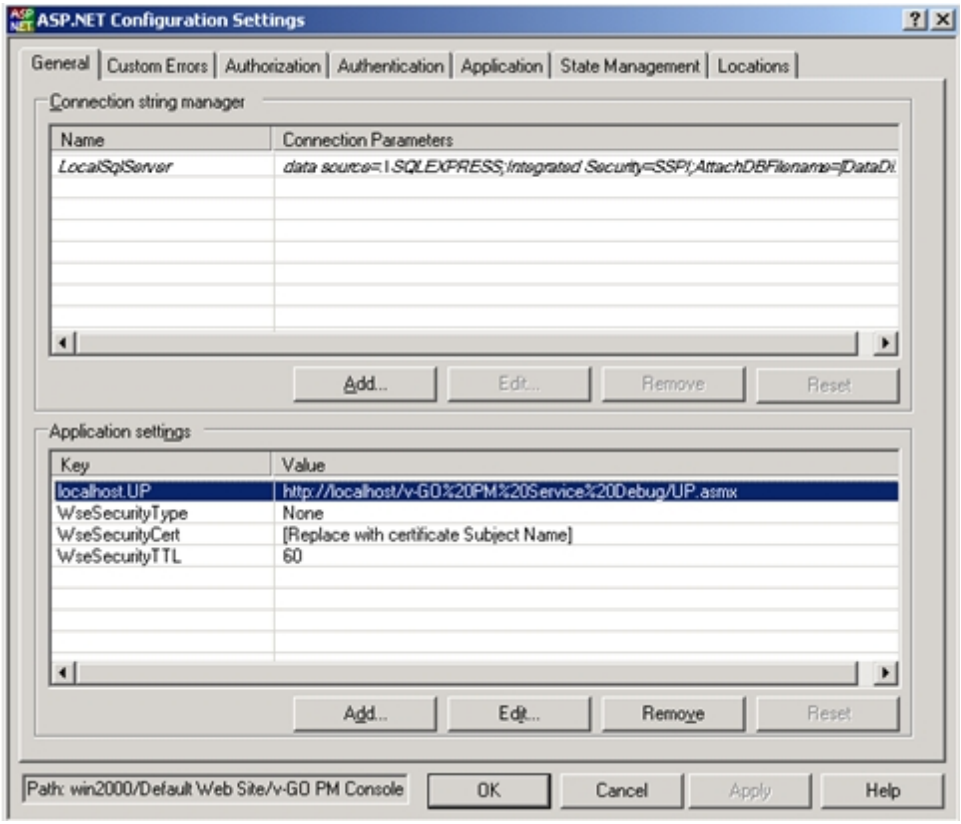
By default, the Provisioning Gateway Web service uses 3DES encryption. To increase security, you can change encryption to AES. In order to enable this feature, you must edit a setting in Oracle Service Properties:

1. Go to **Control Panel** > **Internet Information Services**.
2. Right-click the Provisioning Gateway Service Web site. Select **Properties**.
3. Click the **ASP.NET** tab. Verify that the ASP.NET version is set to 2.0.x. (If it is not set to 2.0, change the setting and click **Apply**.) Click **Edit Configuration**.
4. In the ASP.NET Configuration Settings dialog box, highlight **EncryptionAlgorithm** and click **Edit**.
5. In the Value field, replace 3DES with AES_256. This value causes the Provisioning Gateway Service to use the AES encryption method.

Enabling SSL

For testing purposes, you can enable SSL by changing the localhost.UP key in Provisioning Gateway Console Properties:

1. In the ASP.NET Configuration Settings dialog box, highlight localhost.UP and click **Edit**.



2. Go to **Control Panel** > **Internet Information Services**. Right-click the Provisioning Gateway Console Web site. Select **Properties**.
3. Click the **ASP.NET** tab. Verify that the ASP.NET version is set to 2.0.x. (If it is not set to 2.0, change the setting and click **Apply**.) Click **Edit Configuration**.
4. In the Value field, replace:
   http://localhost/Provisioning Gateway Service/UP.asmx
   by entering
   `https://localhost/Provisioning Gateway Service/UP.asmx`
5. You can now edit the properties for the Provisioning Gateway Service in IIS to turn on SSL.

Setting Permissions

When you install Oracle Enterprise Single Sign-On Provisioning Gateway (Provisioning Gateway), you must create a specific service account, at the domain level, in order for Provisioning Gateway to function properly. This guide describes how to increase security by creating such an account with a specific set of permissions to certain objects within Active Directory.

In order to increase security, Oracle now recommends that this service account be created as a member of the Domain Users group. (For the purposes of this document, the service account is named PMSERVICE; however, you can follow any naming convention you choose).

The instructions in this document describe how to:

- Create the service account (PMSERVICE) as a member of the Domain Users group.
- Grant a specific set of permissions to certain objects within Active Directory to the serviced account.
- Configure the Oracle Enterprise Single Sign-On Administrative Console.
- Create templates for provisioning.
- Provision a user.

The PMSERVICE account must also be a member of the local administrator's group on the IIS server that the Provisioning Gateway server-side components are installed on.

You will need an account with Domain Admin and Schema Admin privileges in order to complete certain tasks involving the installation of Logon Manager, extending the schema, installing software, and modifying certain permissions within Active Directory.

This guide is intended for experienced administrators and software engineers who are responsible for the installation, configuration, and maintenance of Provisioning Gateway and Oracle Enterprise Single Sign-On Logon Manager (Logon Manager). Administrators are expected to understand the installation, configuration, maintenance, and troubleshooting of the following Microsoft products and technologies:

- Windows® Server 2003
- Microsoft Active Directory
- Microsoft Internet Information Server (version 6.0)
- Oracle Logon Manager software in a Microsoft Active Directory environment, including installation of the Oracle Enterprise Single Sign-On Administrative Console and the Logon Manager Agent, schema extension, and configuring the Provisioning Gateway Agent through the Oracle Enterprise Single Sign-On Administrative Console.

General Recommendations and Notes

Microsoft recommends that you not install Internet Information Server (IIS) on a Domain Controller. Oracle recommends that you install the Provisioning Gateway Server-side components on a member server, not a Domain Controller.

The procedures and recommendations presented in this document have been tested in a controlled environment where the desired results were achieved. Oracle recommends that you test these procedures in a non-production environment that resembles your working network as closely as possible.

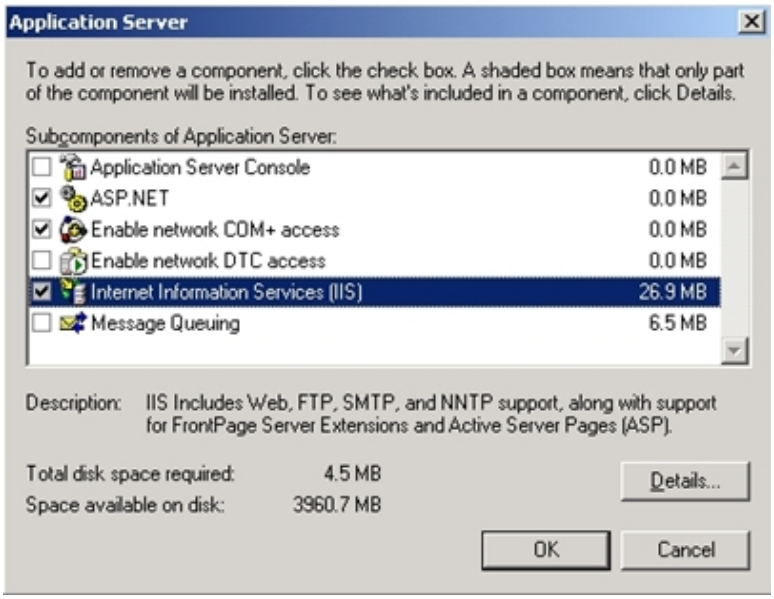
The procedures outlined in this document involve changes that can affect your entire domain. Specialized policies, trust, inheritance issues, and intra- and inter-site replication issues, particularly as they exist in large enterprises, cannot be fully tested outside of the actual environment.

As with any issues that could affect a large number of users, Oracle recommends a prudent, error-on-the-side-of-caution approach to testing and deploying this product by those who are responsible for installing, configuring, and maintaining it.

Installing the Server-Side Components

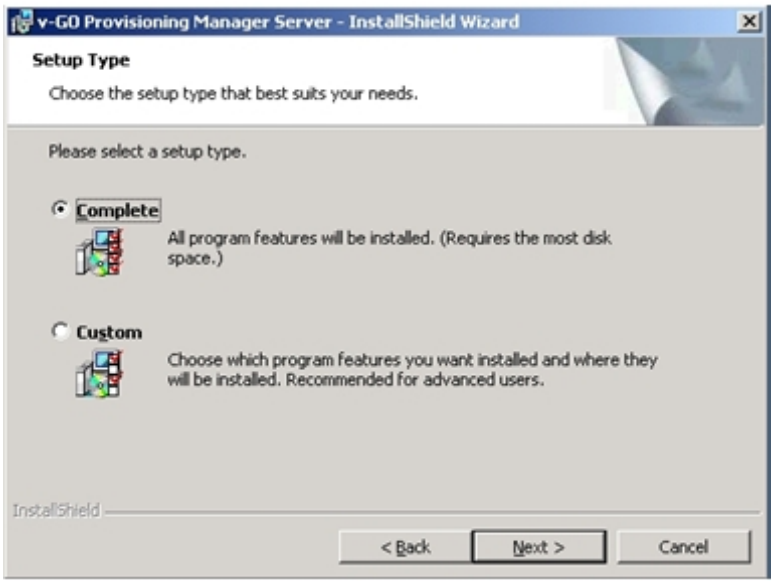
To install the Provisioning Gateway Server-side components:

1. On a domain controller, through a Terminal Server session to a domain controller, or through a workstation that has the Active Directory Users and Computers snap-on installed, create an account called PMSERVICE.
2. Provide the account with a very secure password.
3. Verify that the account is not required to change its password on next logon. This account need only be a member of the domain users group.
4. On a member server in your domain, log onto that machine as a domain-level administrator.
5. In the Application Server dialog box, verify that Internet Information Server 6.0, as well as the ASP.NET components, are installed:



You can install the .NET framework, version 2.0, manually by downloading it from the Microsoft Web site.

6. There are no special configurations or options to consider during the installation of the Provisioning Gateway Server-side components. Accept the defaults after agreeing to the End-User License Agreement.
7. In the Setup Type dialog box, select **Complete**.



As part of the installation process, one or more DOS windows will flash momentarily on this server as services start and stop. This is normal behavior during the installation process.

Installing the Logon Manager and Provisioning Gateway Agents

1. Install and configure Logon Manager on a workstation within your domain. Install the Oracle Enterprise Single Sign-On Administrative Console, the Logon Manager Agent, and extend your schema. Refer to the *Logon Manager Installation and Setup Guide* for more information.
2. Verify that Logon Manager is functioning properly.
3. Install the Provisioning Gateway client-side components on the workstation where you installed Provisioning Gateway. Refer to the *Provisioning Gateway Installation and Setup Guide* for more information.

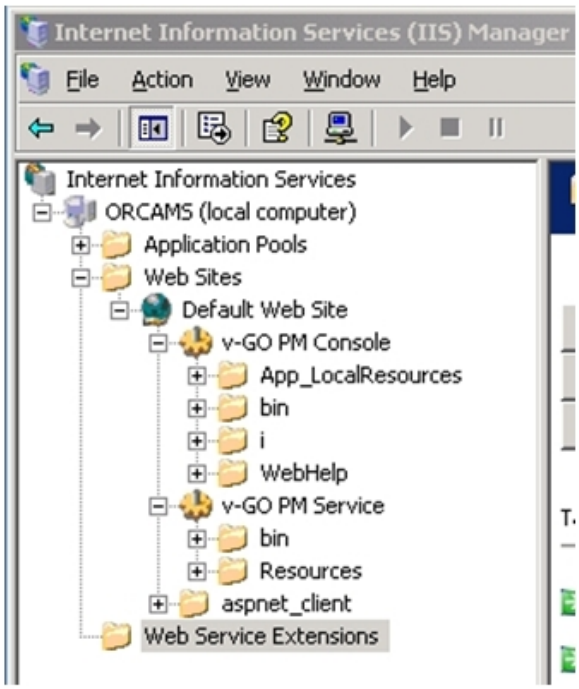
When you deploy the Logon Manager Agent to workstations, you must also deploy the Provisioning Gateway client-side component to each workstation where Logon Manager will reside.

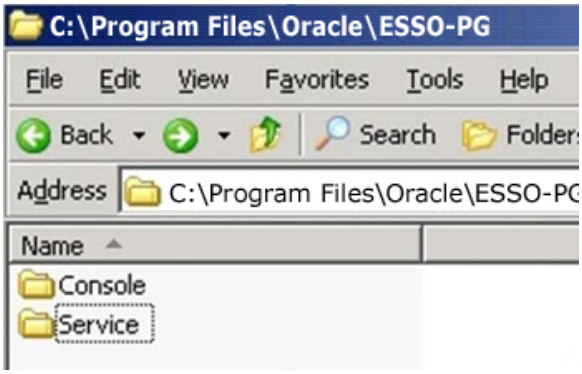
Verifying the Provisioning Gateway Server-Side Installation

To verify that you have successfully installed the Provisioning Gateway Server-side components on your IIS Member Server, look for the following:

- Virtual directories within IIS Manager
- Folders and files in the C:\Program Files\Oracle directories on the server.

Examples of these entities are shown in the following illustrations:

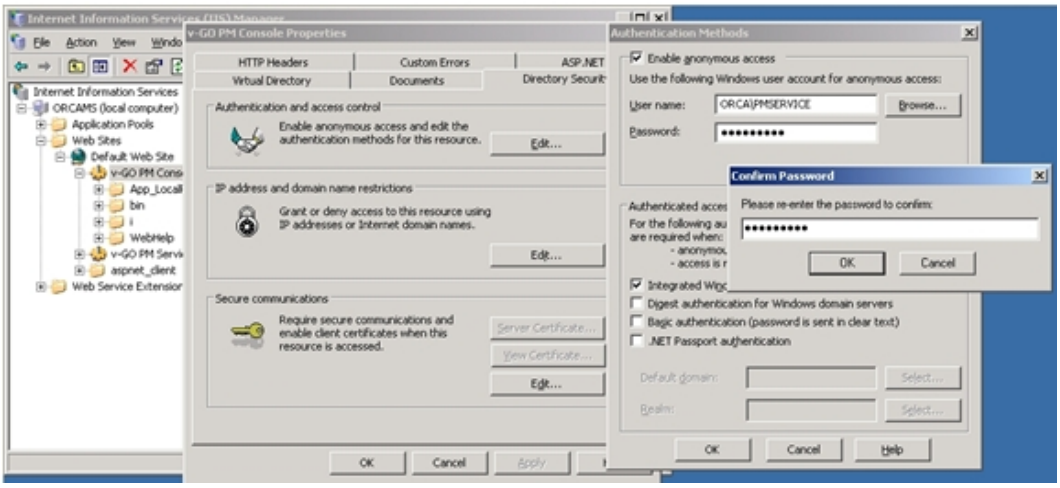




Configuring the Provisioning Gateway IIS Server

In order for the Provisioning Gateway Server-side components to function properly, you must make the PMSERVICE account a member of the local administrator's group on the IIS Server that houses the Oracle server-side components.

1. In the control panel of the Provisioning Gateway IIS member server, click the Local Users and Groups icon in the Computer Management Group.
2. Add the PMSERVICE account.
3. Open the Internet Information Server, then Default Website.
4. Locate the Provisioning Gateway Management Console and Provisioning Gateway Service virtual directories. For both directories, make the PMSERVICE account responsible for anonymous access.



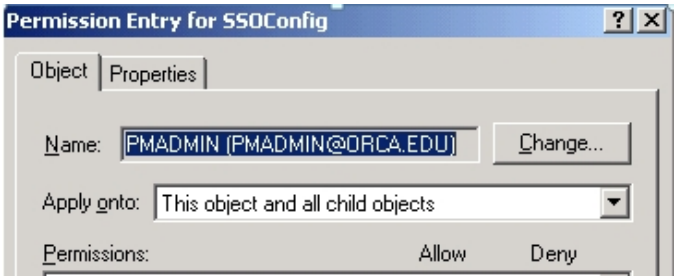
5. From the RUN line, type `iisreset` to restart the IIS service.

Granting Special Permissions to the PMSERVICE Account

The next procedure is to grant special rights to specific containers within Active Directory on a domain controller to the PMSERVICE account. Remember that, to Active Directory, the PMSERVICE account is simply an ordinary user account.

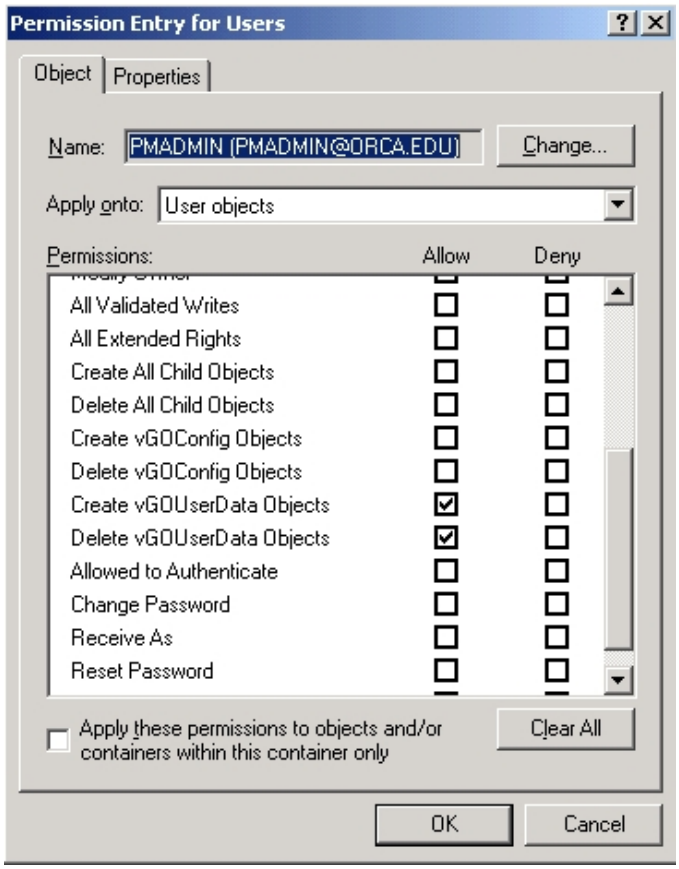
To grant the special permissions:

1. In the Permission Entry for SSOConfig dialog box, grant the PMSERVICE account read-only access to the SSOConfig container (the container where the application templates are stored) as shown in the following illustration:

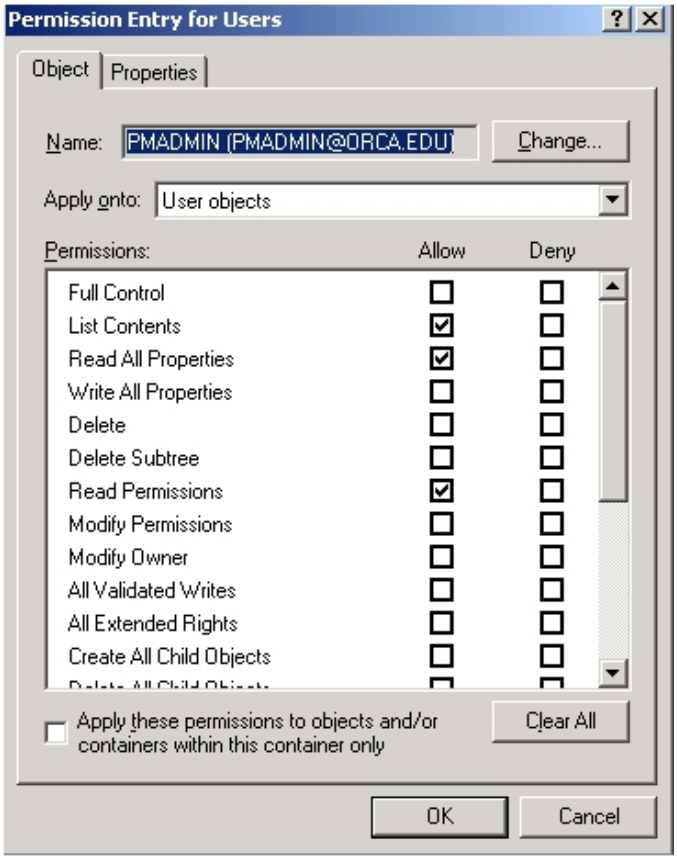


Steps 2 through 8 must be repeated for each Organizational Unit that exists within your organization that contains users.

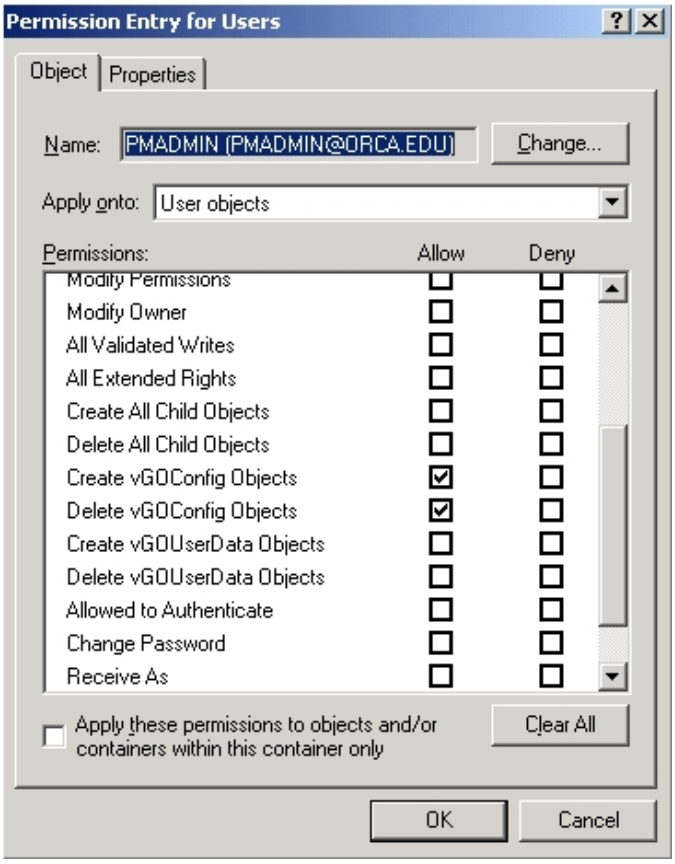
2. In the Permission Entry for the Users container grant the PMSERVICE the ALLOW permission applied onto the User objects as it pertains to both the Create vGOUserData Objects and Delete vGOUserData Objects.



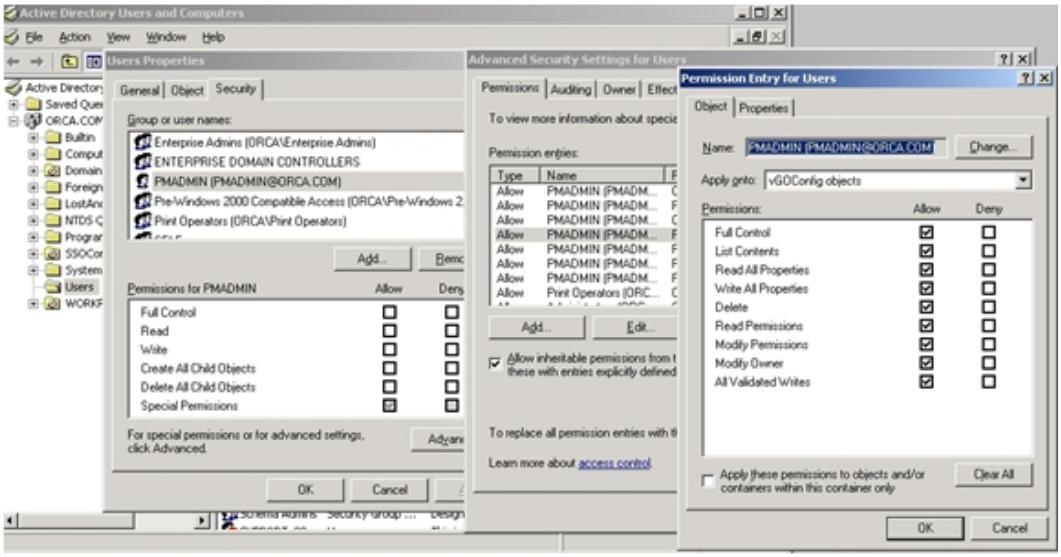
3. Grant List Contents, Read all Properties, and Read Permissions to the User Objects containers.



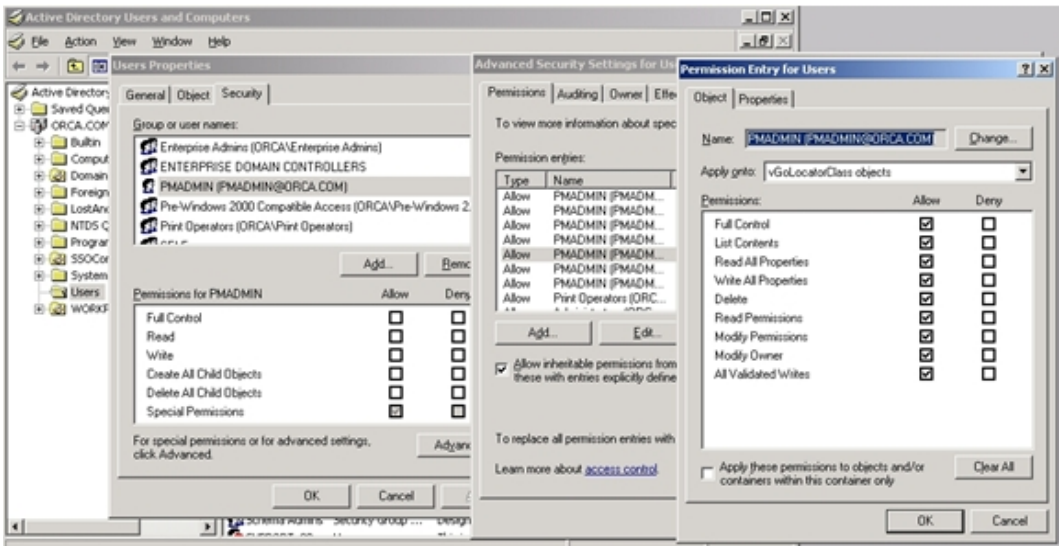
4. Grant the ALLOW permission applied onto the User objects as it pertains to both the Create vGOConfig Objects and Delete vGOConfig Objects.



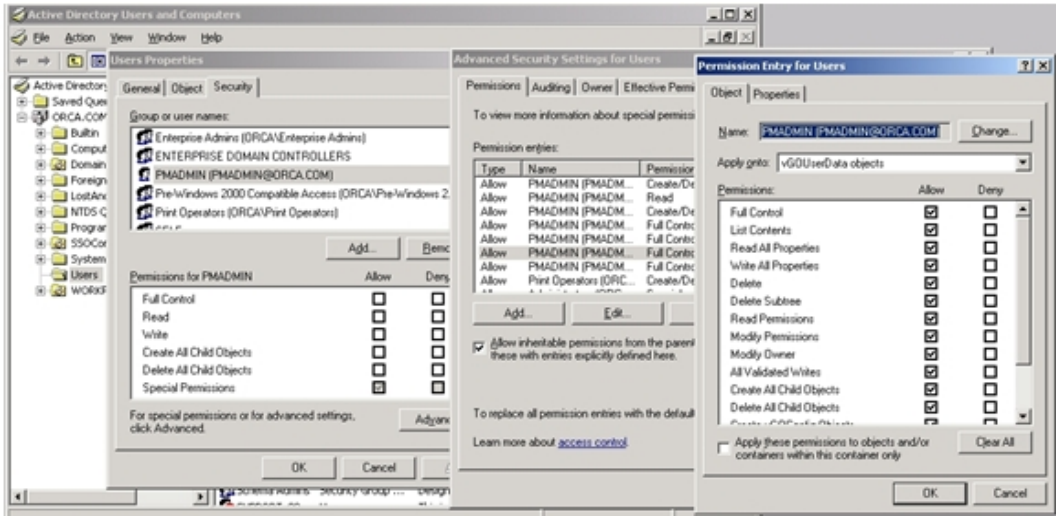
5. Grant FULL CONTROL to the PMSERVICE account as it applies to the vGOConfig objects.



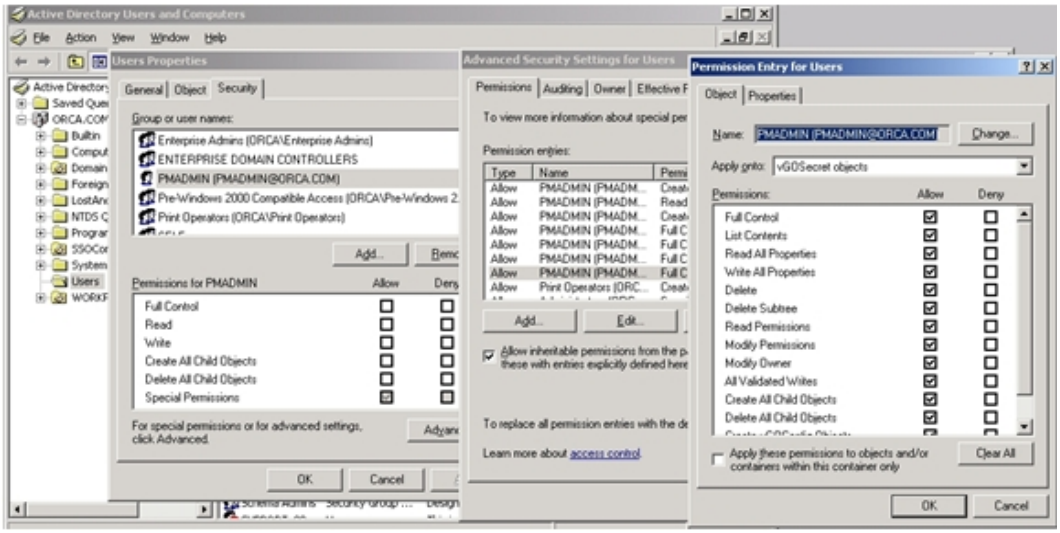
6. Grant FULL CONTROL to the PMSERVICE account as it applies to the vGOLocatorClass objects.



7. Grant FULL CONTROL to the PMSERVICE account as it applies to the vGOUserData objects.



8. Grant FULL CONTROL to the PMSERVICE account as it applies to the vGOSecret objects.


Active Directory Users and Computers
File Action View Window Help
Users Properties
General Object Security
Group or user names:
Enterprise Admins (ORCA\Enterprise Admins)
ENTERPRISE DOMAIN CONTROLLERS
PMADMIN (PMADMIN@ORCA.COM)
Pre-Windows 2000 Compatible Access (ORCA\Pre-Windows 2...
Print Operators (ORCA\Print Operators)
Add...
Permissions for PMADMIN
Allow
Full Control
Read
Write
Create All Child Objects
Delete All Child Objects
Special Permissions
For special permissions or for advanced settings, click Advanced.
OK
Cancel
Advanced Security Settings for Users
Permissions
Auditing
Owner
To view more information about special per
Permission entries:
Type
Name
Add...
Edit...
To replace all permission entries with the de
Learn more about access control.
Permission Entry for Users
Object
Properties
Name: PMADMIN (PMADMIN@ORCA.COM)
Change...
Apply onto: vGOSecret objects
Permissions:
Allow
Deny
Full Control
List Contents
Read All Properties
Write All Properties
Delete
Delete Subtree
Read Permissions
Modify Permissions
Modify Owner
All Validated Writes
Create All Child Objects
Delete All Child Objects
Apply these permissions to objects and/or containers within this container only
Clear All
OK
Cancel

Granting Provisioning Rights to Domain Users

If you want regular domain users (users who do not have administrative permissions to the AD repository) to have the ability to provision other users, you must create a security group for them in AD. Grant permissions to this new group as outlined in this manual. Add to this group the names of any users you want to enable to view provisioning activity using the PM Console.

The Provisioning Gateway Service User account should be included in this security group by default.

For details on creating user groups, see the Provisioning Gateway *Administrator's Guide*.

Settings

Settings > Web Service Account

Use the Web Service Account page to set or change the Anonymous Logon for IIS Web Services. The Provisioning Gateway Web service runs as this domain account. The Web Service Account dialog box displays the current Anonymous Logon account and provides a logon form for changing this account.

You must be authenticated to the Provisioning Gateway Console as a member of the administrator group of the Provisioning Gateway Web server to change the account

The Web service account requires the following privileges:

- Read and write access to the Registry path `HKLM\Software\Passlogix`.
- Connect, read, and write access to the storage if AD or AD LDS (ADAM).

To change the Web service account, type in the account **User Name** (in the format Domain\Username) and **Password**, confirm the password, and click **Save**.

Settings > Storage

Use the Storage page to view or change connection settings for the directory service (Oracle Internet Directory, Microsoft Active Directory, Microsoft AD LDS (ADAM), IBM LDAP Directory, or Sun Directory Server) that is used as the repository for Provisioning Gateway data.

Fields marked with an asterisk [*] are required

When you have completed your changes, click **Save Changes** to apply the new settings to Provisioning Gateway. After the storage settings are saved, you will be prompted to re-authenticate to Provisioning Gateway.

The information on this page is encrypted and saved to the registry under `HKLM\Software\Passlogix\PM\Server\Storage`.

Setting	Value
***Storage Type**	Choose one of the following storage locations: • Oracle Internet Directory • Oracle Directory Server Enterprise Edition • Oracle Virtual Directory • Sun Directory Server • Microsoft Active Directory • Microsoft AD LDS (ADAM) • IBM LDAP Directory • Novell eDirectory
***Server**	Enter either the name of the server or the IP address of the server.
***Root DN**	The root directory. For example, DC=mydir,DC=com.
Provide this setting for Oracle Directories, Active Directory, IBM LDAP Directory, Novell eDirectory, and Sun Directory Server storage only:	
***User Path(s)**	The fully qualified path indicating the location of user accounts. There can be unlimited paths to search. The paths are searched in the order they are entered and are separated by a semicolon (;). For example, CN=users,DC=mydir,DC=com
Provide these settings for Active Directory and or AD LDS (ADAM) storage only:	
Prepend Domain	Select this option to add the user's domain to the username when naming the user's container. For example, for the domain *passlogix* and user *jamesk*, the container is named *jamesk* with this flag disabled and *passlogix.jamesk* with this flag enabled.
Provide this setting for Active Directory storage only:	
Locate in User	Select to enable searching for Provisioning Gateway user data under the Active Directory user objects.
Provide this setting for Sun LDAP storage only.	
User Prepend	Specifies the user naming attribute for user objects in the directory.This setting is used to form the relative distinguished name (RDN) of a user object. Typical values include "CN" or "UID."
Provide these settings for Oracle Directories, IBM LDAP Directory, Novell eDirectory, or Sun Directory Server storage only:	
***Connect as User**	The user name of the directory administrator.
***Password**	The password of the directory administrator.

Setting	Value
Provide this setting for Oracle Directories, Active Directory, IBM LDAP Directory, Novell eDirectory, or Sun Directory Server storage only:	
Use secure connection (SSL)	Select to enable secure socket layer.
If using Configuration Objects or Role/Group support, provide these settings for all directory storage types:	
Use configuration objects instead of application list	Select to enable the use of configuration objects (COs) instead of application configuration lists, also known as the entlists. The Provisioning Gateway Server obtains the access control rights of its provisioning clients by searching the directory for provisioning objects. It finds only the objects it has access to.
Role/Group support	Select to enable Role/Group-based access control of administrative users. Enabling Role/Group support activates configuration object support. If Role/Group support is enabled, permissions should be specified. If no permissions are specified, by default, all users and groups are denied access for all actions. See Setting up Role and Group Support for information on setting up permissions.
Configuration and role/group objects root DN	Specifies where to begin the search for configuration and provisioning objects. The search moves from the specified locations downward. For example, *ou=vgoconfig,dc=test2003,dc=com* or *dc=passlogix,dc=com.* The path to this container must exist and contain at least one template prior to the input of these storage settings. The template can be in a sub-container rather than in the path itself. If this container does not exist, you will get an error message. See Setting up Role and Group Support for information on setting up permissions.

Settings > Event Log

Use the Event Log page to configure the server where events will be logged. When you have completed your changes, click **Save Changes** to apply the new settings to Provisioning Gateway.

Setting	Value
Database Type	Select the database you are using: • Oracle database • Microsoft SQL Server • Syslog Daemon The Syslog Daemon is not a database; however, you select it on the Event Log Settings page from the Database Type drop-down list in order to send events to the daemon. There are no parameters to set for the Syslog daemon. Configuration is done manually following installation. See the *Oracle Enterprise Single Sign-On Suite Installation Guide* for more information.
Provide this setting for Oracle Database only:	

Connection String	Enter the database connection string.
	For example, this string should be in the following form when using: Oracle using external authentication:
	`Provider=[OLE DB Provider] ;Data Source=[SID]; User Id=/;`
	Microsoft's Oracle OLE Provider:
	`Provider=MSDAORA ;Data Source=ORCL; User Id=/;`

Provide this setting for Microsoft SQL Server database only:	
Server	Enter the name of the server where events will be logged. SQL Server must be running on this machine, although the Provisioning Gateway database does not have to exist. If this is the first time this server is used by Provisioning Gateway, the Initialize Event Log box must also be checked so the Provisioning Gateway database is created. You cannot use the IP address of the server to specify the current machine. You must use the actual machine name (for example, pdevrx2). The name localhost cannot be used to refer to the local machine. You must use the name of the machine.
Provide this setting for the Oracle and SQL databases:	
Initialize Event Log	When enabled, this setting creates the Provisioning Gateway database on the specified server. If the database already exists, all existing data in the database is erased. Typically, this setting is used on the initial install and when you want to clear the log entries in the database. This setting is not saved.

Settings > Template Mapping

Use this page to map Logon Manager templates to Oracle Privileged Accounts Manager (OPAM) targets.

In order to perform any of the following functions, the user must be granted "Map Template" permissions in the Oracle Enterprise Single Sign-On Administrative Console.

1. In the Targets window, you will see the names of all available OPAM targets, followed by the name of the template mapped to it (in parentheses), if any.
2. Select a target and click the **Edit** button to edit the target's mapping properties.
3. In the template mapping Edit dialog, select a template to map to the OPAM target. If a template is already mapped to the target, it is selected when this dialog launches.

For more information about setting up template mapping and assigning permissions, see the *Oracle Enterprise Single Sign-On Administrator's Guide*.

Managing Users

Users > Manage SSO Users

This page allows you to search for users and to add, modify, or delete their credentials. Users can be searched for by name or by the logons they have.

Find Users

Show user(s) with User Name. Enter the user name to search for. Leave this field blank to perform a search on all users. In the drop-down list, select either **substring match** or **exact match**.

Only show users who have logons for. This list includes all the possible applications available to users in your organization. Select one or more application to filter the result to show only users who have logons for these applications.

Show additional information. The search results list the usernames. The search results can also show **Logons** or **Pending Provisioning Instructions**. Select either of these options if desired.

Click **Find Users** when all information has been entered.

Search Results

The results list the **User Name** and, depending on whether additional information was selected, **Logons** and, if applicable, any **Pending Provisioning Instructions**. Use the buttons (which highlight on mouse-over) to add, delete, and modify users. Click on a user's name to view or edit that user's profile.

Applications that are not predefined (for example, on-the-fly Web applications) cannot be provisioned.

Add New Logon

Delete SSO User or

Delete Logon or

Cancel Provisioning Request

Modify Logon

user 1 Click on User Name

Users

Users > Manage SSO Users > Add New Logon

This page allows you to create a provisioning instruction to add a new application logon for a specific user. This page is accessed by searching for a user on the Manage SSO Users page and clicking the button next to the **User Name**.

Add Logons

SSO User. The Logon Manager user name selected from the user search results.

Application. Lists all of the available applications. There is also an option to **not list applications that user already has a logon for**. After an application is selected, the Logon Information section refreshes and text boxes appear for each field required by the selected application.

Description. Allows you to modify a logon's description field as seen in the Logon Manager Logon Manager. This field is optional.

Logon Information

User ID. User's username or ID for the application.

Password/Confirm Password. User's password for the application.

> After the **User ID** field is created, it cannot be modified. If a User ID must be changed, you must delete the existing logon and add a new logon with a new User ID. Depending on the requirements of the application being added, you might be prompted for additional fields, such as a Third or Fourth Field. Similarly, some applications might not require all of the fields. In such cases, the unnecessary fields do not appear.
>
> When you have entered all the required information, click **Add Logon** to submit your add request.

Users > Manage SSO Users > Delete SSO User

This dialog asks if you are sure that you want to delete the selected SSO user. Click **OK** to delete or **Cancel** if do not want to delete this user. When you click **OK**, a message will confirm that this user has been deleted.

Access this dialog box by searching for a user on the Manage SSO Users page and clicking the button next to **User Name**.

Users > Manage SSO Users > Delete Logon

This dialog box asks if you are sure that you want to delete the selected logon. Click **OK** to delete or **Cancel** if do not want to delete this logon. When you click **OK**, a message will confirm that this logon has been deleted. Access this dialog box by searching for a user on the Manage SSO Users page and clicking the button next to **Logon**.

Users > Manage SSO Users > Cancel Request

This dialog asks if you are sure that you want to cancel the pending provisioning instruction. Click **OK** to cancel or **Cancel** if do not want to cancel this request. When you click **OK**, the page will refresh and the pending provisioning instruction will no longer be displayed. Access this dialog box

by searching for a user on the Manage SSO Users page and clicking the button next to **Pending Provisioning Request**.

Users > Manage SSO Users > Modify Logon

This page allows you to modify an application logon. Any fields that you leave blank on this page will not be changed. Access this page by searching for a user on the Manage SSO Users page and clicking the button next to **User Name**.

Logon to Modify

SSO User. The Logon Manager user name selected from the user search results.

Application. The application to be modified.

User ID. Username or ID for the application.

> After the User ID field is created, it cannot be modified. If a User ID must be changed, you must delete the existing logon and add a new logon with a new User ID.
>
> If a logon does not have User ID associated with it, the password field cannot be modified. A User ID must exist in order to modify the password. Logons that do not have a User ID associated with them should be deleted and recreated with a User ID, if a new one is required.

New Logon Information

Password/Confirm Password. User's password for the application.

Description. Allows you to modify a logon's description field as seen in the Provisioning Gateway Logon Manager.

Third Field. The third field for this logon.

Fourth Field. The fourth field for this logon.

> Third and Fourth Fields are required only if the identified application is configured with a Third or Fourth Field. Depending on the requirements of the application being added, you might be prompted for additional fields. Some applications might not require all of the fields. In such cases, the unnecessary fields do not appear.
>
> When you have entered all the necessary information, click **Modify Logon** to submit your modify request.

Users > Manage SSO Users > Edit User

This page displays the selected user's logons and any pending provisioning instructions. Access this page by searching for a user on the Manage SSO Users page and clicking on the user's name in the search results list.

Edit User

User Name	Displays the selected user's name.
	Click to add a new logon for this user
	Click to delete this user.
Logons	Lists the logons assigned to the user.

Use the links and buttons (which highlight on mouse-over) to add, delete, and modify user logons.

Delete All Logons	Removes all logon credentials from the user's directory.
Advanced Delete	Allows you to generate a custom delete request.
	Deletes the specific logon associated with this user.
	Changes a user's logon credentials for a specific logon.

If a logon does not have user ID associated with it, the password field cannot be modified. Any credentials that do not have a user ID associated with them should be deleted and replaced.

Pending Provisioning Items	Displays any provisioning instructions pending for the selected user. Displays the provisioning instruction (such as add or delete), the application, and the creation and execution date for the provisioning instruction. Click **Cancel Instruction** to delete this instruction from the repository.

Advanced Delete

SSO User. Displays the Logon Manager user name selected from the user search results.

Application. Lists the applications that can be deleted from this user. Select the application to delete from the drop-down list. The credential fields associated with the selected application are displayed. You must fill in all the credential fields exactly as they are stored in the directory:

- **User ID.** Enter the User ID.
- **Password/Confirm Password.** User's password for the application. These fields only appear if the application is configured to only have a password field.
- **Description.** Logon's description field as seen in the Logon Manager Logon Manager.
- **Third Field.** The third field for this application logon.
- **Fourth Field.** The fourth field for this application logon.

When you have entered all the information has been entered, click **Submit** to submit your delete request.

Users > Add New SSO User

This page allows you to create new Logon Manager users. This creates a storage object in the repository for the user. After the user is created, the Add New Logon page appears so that you can add applications for the new user.

Add New SSO User

User Name. Enter the user name to add. Click **Next**. The Add New Logon screen opens.

The user name must exist in the directory. If it does not, an error will occur.

Reports

Reports & Logs > Event Log

Use the Event log page to view the Provisioning Gateway event log. Events can be viewed by date periods and can be filtered by event type.

1. To select a date, click **Choose**.
2. Enter appropriate search parameters and click **View Log**. The log entries appear at the bottom of the screen:
   - Date/Time
   - Event Type
   - Provisioned User
   - Application
   - Execute Date
3. Click the  button for details on the status of the instruction.

The log is exportable to a CSV file, which can be loaded into many optional tools (Microsoft Excel, for example) for analysis.

1. To export the log file, click **Export Log**.
2. Select the export destination for the log file and click **OK**. These are the list of fields exported to this file:
   - Time Stamp
   - Event Type
   - User Name
   - Application
   - Execute Date
   - Provisioning Agent

Reports & Logs > Status Request

The Status page provides a summary of the status of the selected provisioning instruction.

State. The state of the instruction:

- Pending
- Retrieved
- Processed

Result. The result of the instruction:

- Success
- Failure
- Retrieved

Description. A detailed textual description of the instruction processing result.

Modified Date. The last time the instruction was modified. If the state of the instruction is "Pending," all the other fields are left blank.

Click **Back to Event Log** to return to the Event Log page.

Reports & Logs > Generate Report

Use the Generate Report page to download a CSV-formatted file containing all the data stored in the repository.

Select the type of report to generate:

Logons. This option generates an application report (user's credentials). This report contains the following fields:

- User DN (for example, cn=user1,ou=people,ou=vgo,dc=passlogix,dc=com)
- User name (for example, user1)
- Application Name
- Last Used Date
- Modified Date

Provisioning Instructions. This option generates a provisioning item report (user's provisioning instructions). This report contains the following fields:

- Instruction Type
- Instruction GUID
- Current Status
- Provisioned User
- Application
- Create Date/Time
- Execute Date/Time
- Provisioning Agent

Select the type of report to generate and click **Download Report**.

Obtaining a Certificate

In order to use Provisioning Gateway, you must obtain an X.509 Certificate for SSL and Certificate Chain from a trusted certificate authority.

Certificates can be obtained from any trusted certificate authority. This purpose of this guide is to demonstrate how certificates can be obtained through Microsoft® Certificate Services.

These instructions will guide you through installation of a standalone CA, which can be used to issue certificates to anyone, even non-Windows entities.

Certificates can be installed on Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 200 R2. The instructions and screen shots in this guide are primarily for Windows 2000. The instructions in this guide can easily be followed using either operating system.

The following articles from the Microsoft Web site can be referred to for information on installing certificates and setting up SSL:

"Install an Enterprise Root Certificate Authority (Windows 2003)", http://technet2.microsoft.com/windowsserver/en/library/4ffc15cf-f42f-43db-8eb9-fcd8c3102d621033.mspx

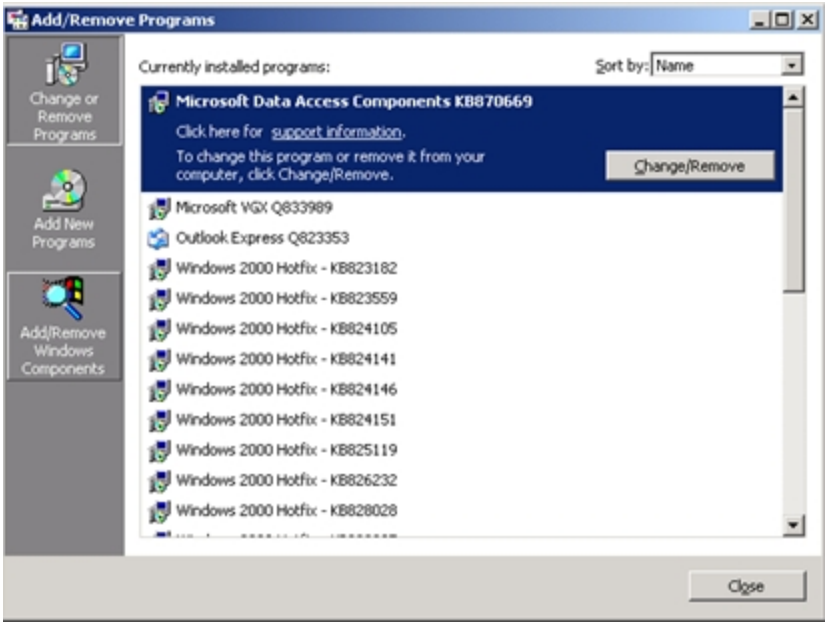
"How to Set Up SSL on a WebServer", http://technet2.microsoft.com/windowsserver/en/library/4ffc15cf-f42f-43db-8eb9-fcd8c3102d621033.mspx

The following pages contain the procedures involved in certificate setup:

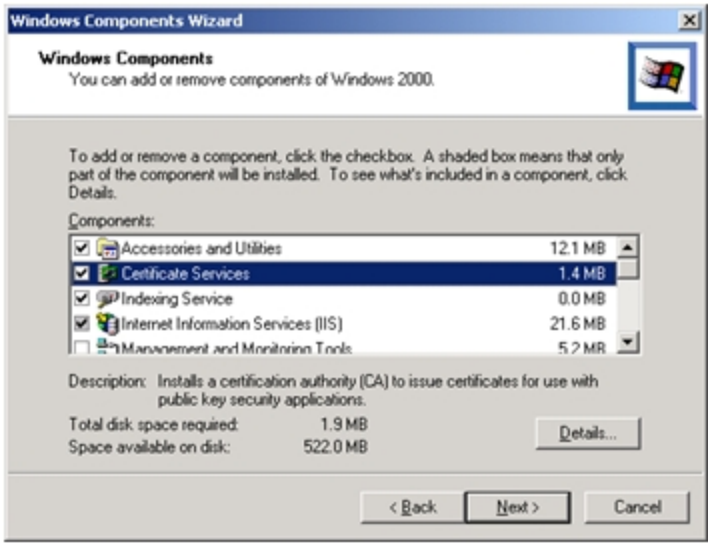
- Installing the Microsoft Certificate Authority
- Enabling SSL for Your Web Site
- Submitting a Certificate Request to a CA Manually

Installing the Microsoft Certificate Authority

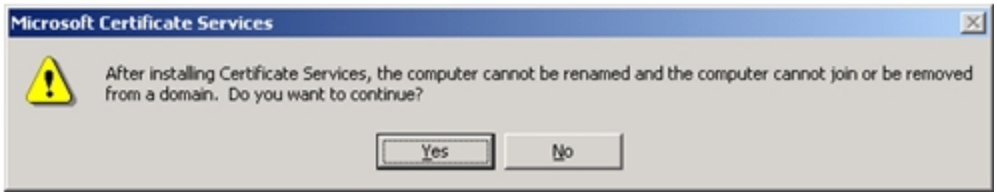
1. Click **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**.
2. Click **Add/Remove Windows Components**.



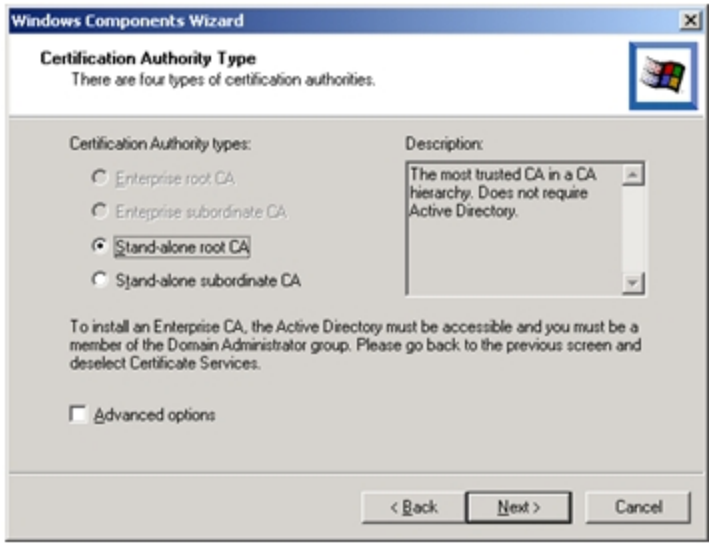
3. Check **Certificate Services** and click **Next**.



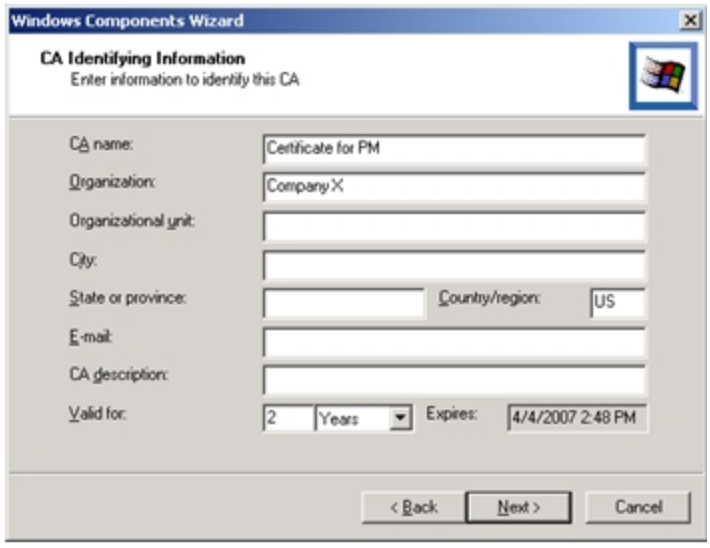
4. When you are asked if you want to continue, click **Yes**.



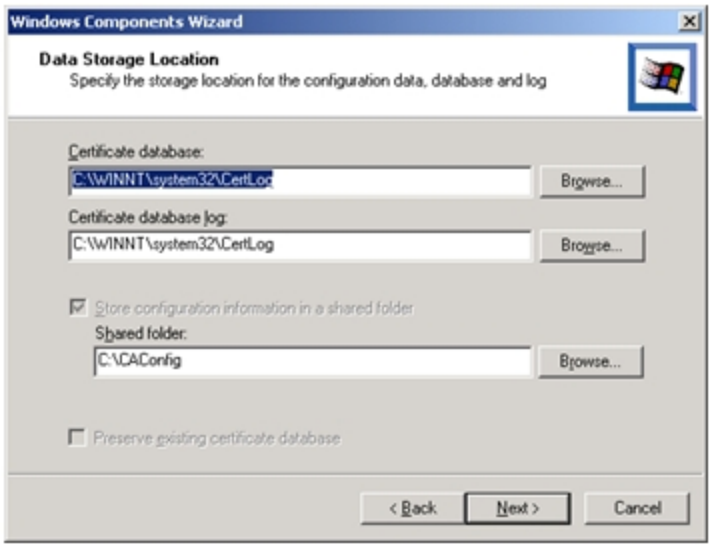
5. Select **Stand-alone root CA**.



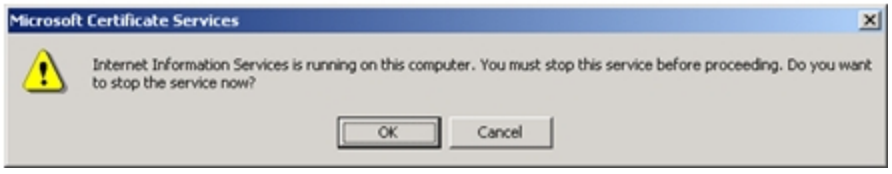
6. Enter CA Identifying Information. Enter the length of time that this certificate should be valid. Click **Next**.



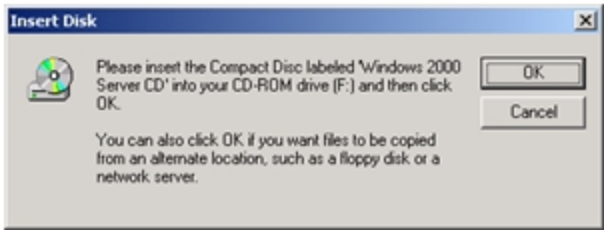
7. Specify the storage location for the configuration data. Click **Next**.



8. You might be prompted to stop IIS. If so, click **OK**.



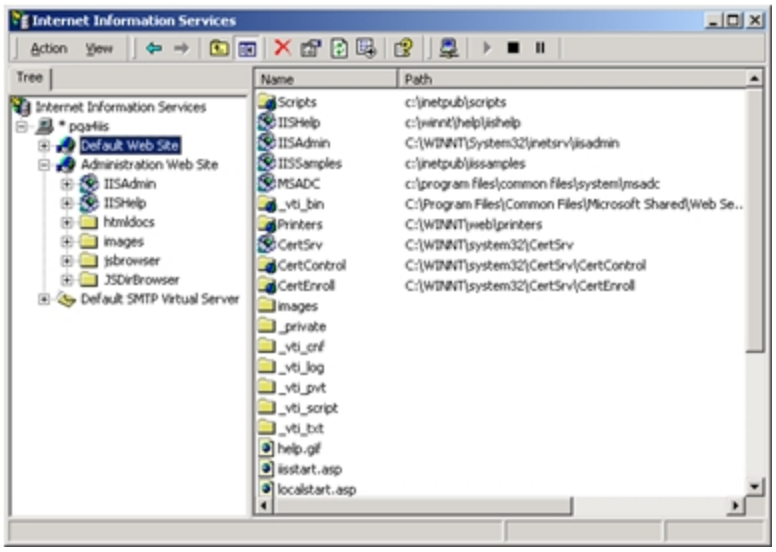
9. You might be prompted to insert the Windows CD. If so, insert it and click **OK**.



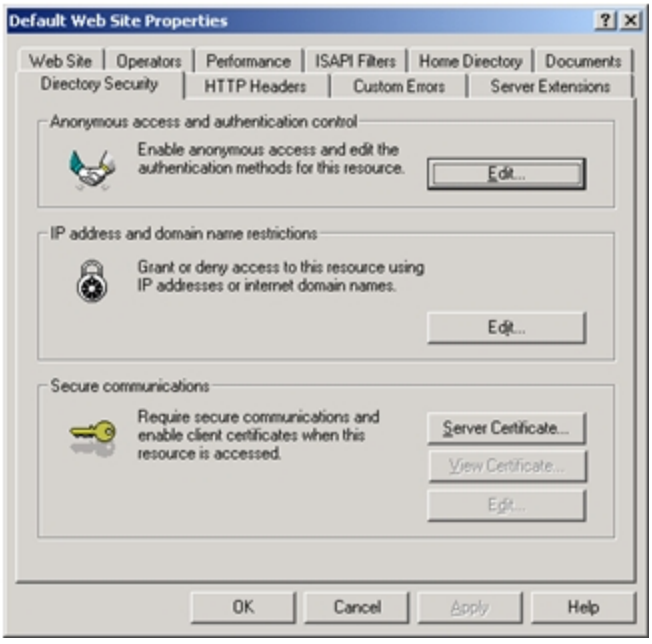
10. At this point, you might be prompted to enable ASP pages. You must select **Yes**.
11. Click **Finish**.

Enabling SSL for Your Web Site

1. Open Microsoft IIS and expand the Default Web Site. You will perform the following steps for each Provisioning Gateway Web site.
2. Right-click the Web site (for example, Default Web Site). Click **Properties**.

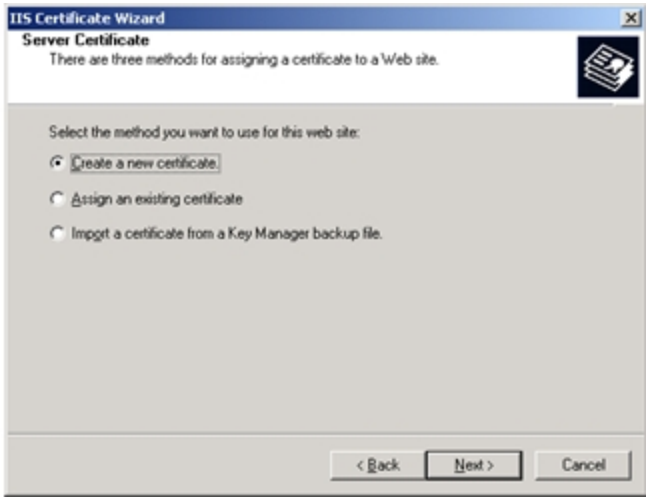


3. Select the **Directory Security** tab. Under **Secure communications**, click **Server Certificate**.

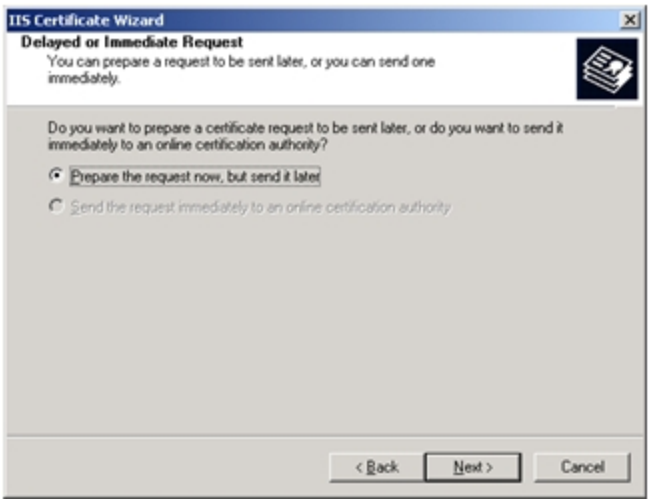


4. The Web Server Certificate Wizard appears. You will use the wizard to generate a request for a certificate. Click **Next**.

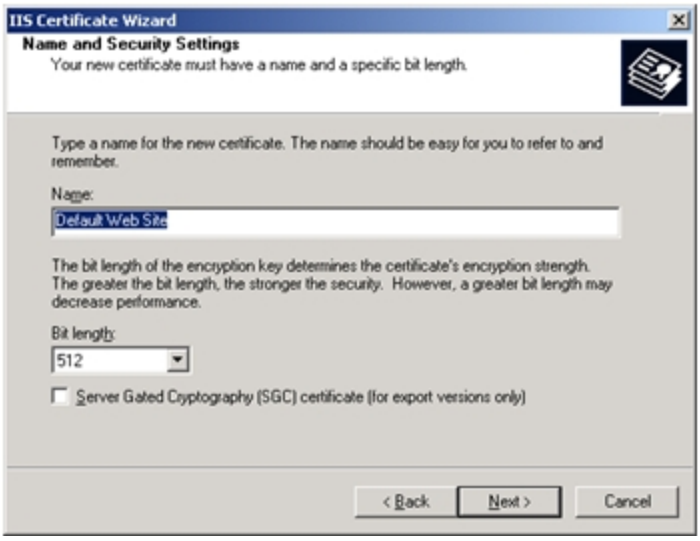
5. Select **Create a new certificate** and click **Next**.



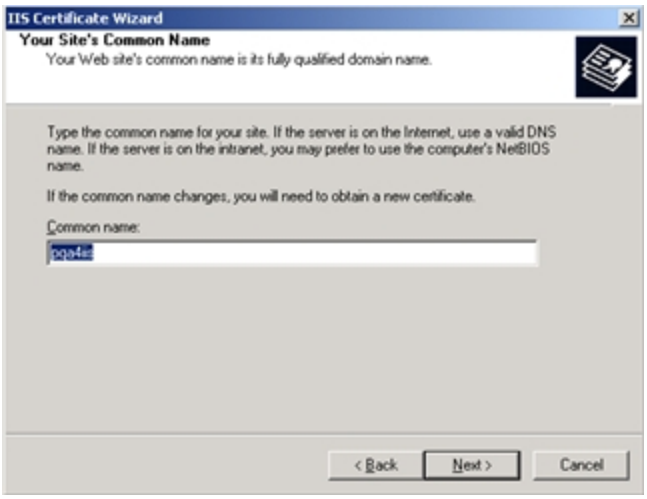
6. Select **Prepare the request now, but send it later** and click **Next**. If you have an Enterprise-level CA and the machine is part of the domain, a request can be directly prepared. The **Send the request immediately to an online certification authority** will be available. If you select this option, you do not need to follow the steps in Submitting a Certificate Request to a CA Manually.



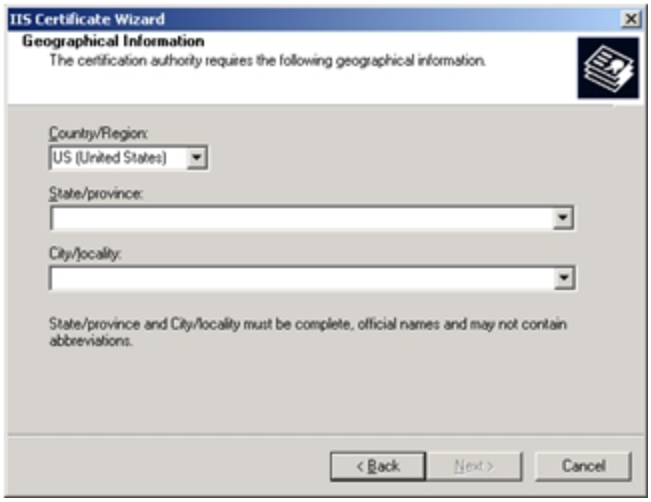
7. Enter a name for the new certificate. Ensure that the name is easy to refer to and to remember. Choose the bit length. The higher the bit length, the stronger the encryption, but the slower the performance. Choose a bit length that will balance strength and performance for your needs. For a root CA, you should use a key length of at least 2048 bits. This option is not available if you use existing keys. Click **Next**.



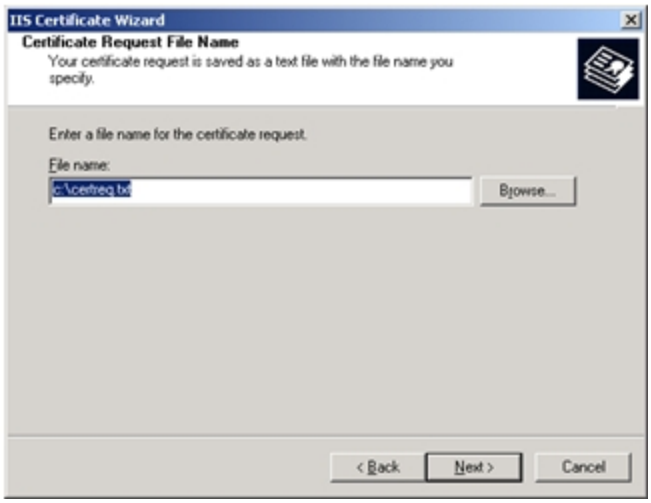
8. Enter your site's common name. This name must match the machine name or site URL. Click **Next**.



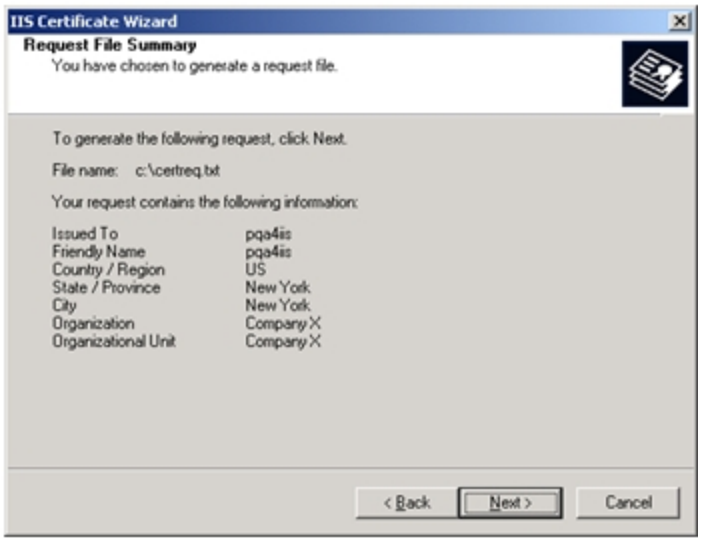
9. Enter your geographical information and click **Next**.



10. Enter a file name for the certificate request. Click **Browse** to locate it. Remember the location of this file as you will open it after completing the request.



11. Review the summary of your request. Click **Next**.

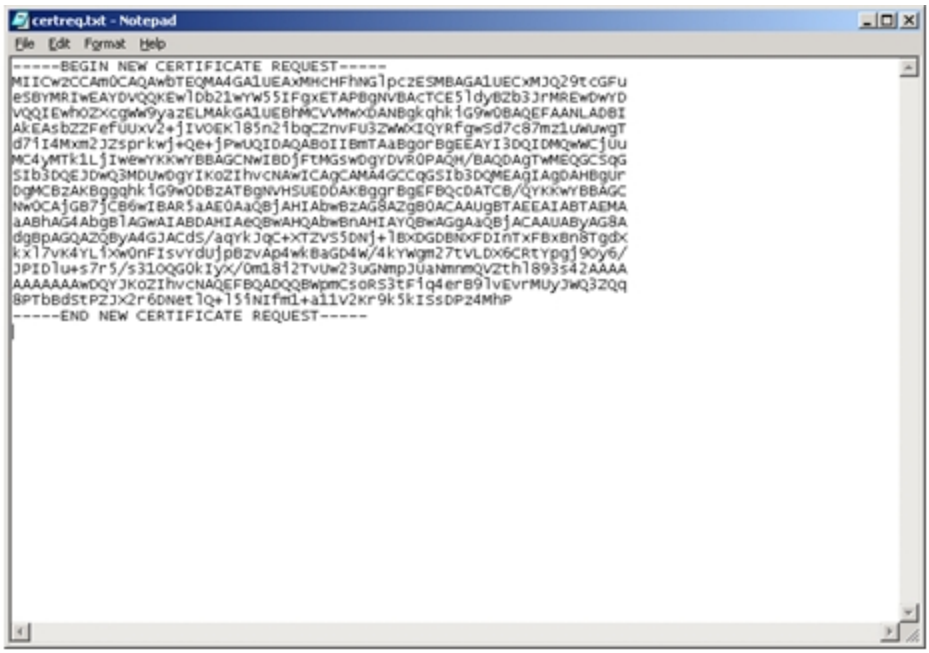


12. Click **Finish**.

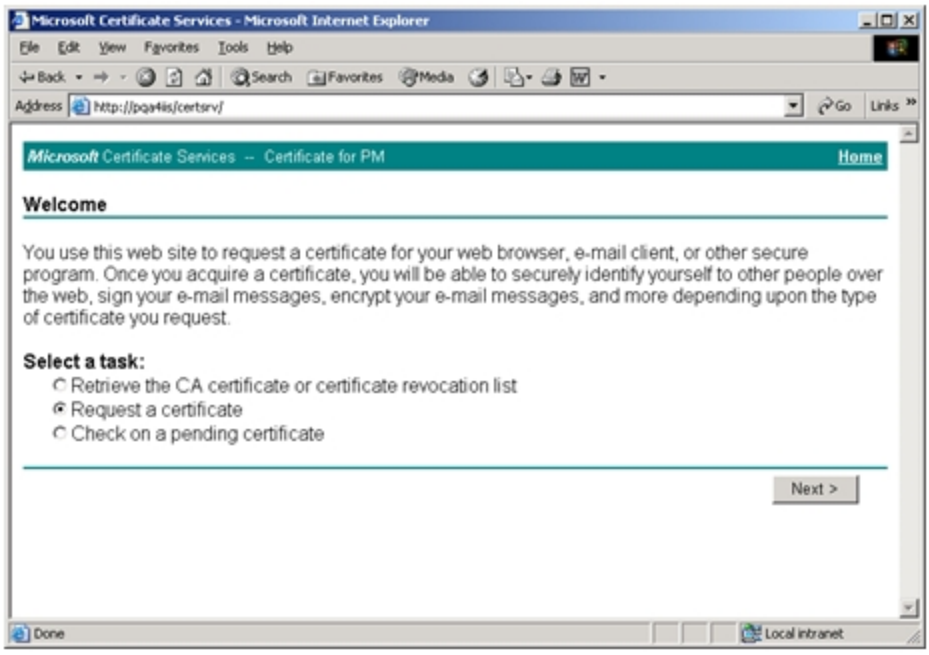

IIS Certificate Wizard
Completing the Web Server Certificate Wizard
You have successfully completed the Web Server Certificate wizard. A certificate request was created and saved to the file:
c:\certreq.txt
Send or e-mail this file to your certification authority, who will send you a response file containing your new certificate. Restart this wizard to attach the new certificate to your server.
Click here
for a list of certification authorities who offer services for Microsoft products.
To close this wizard, click Finish.
< Back
Finish
Cancel

Submitting a Certificate Request to a CA Manually

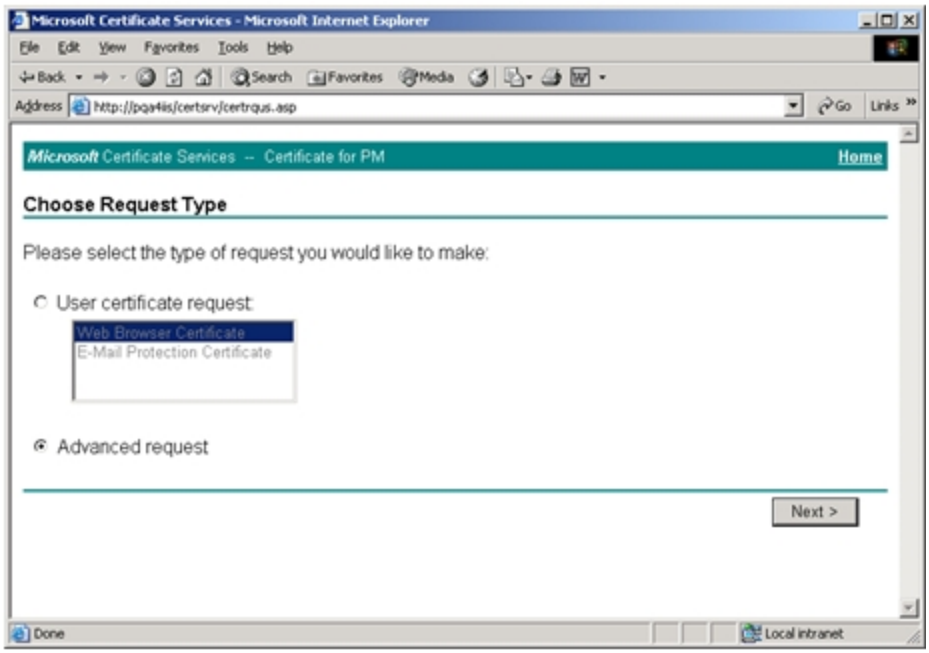
1. Locate the certificate request document (refer to Step 11 for the location). Open the text file and copy all of the contents to a clipboard. You will paste the contents into a request in Step 5.



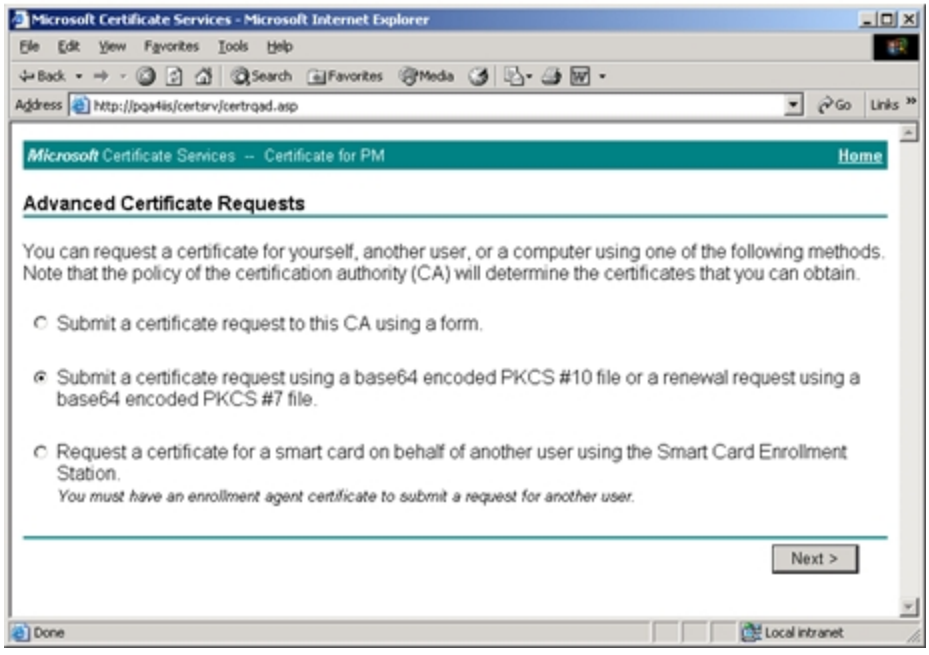
2. Open Microsoft Certificate Services. The URL is http://yourmachinename/certsrv/. Select **Request a Certificate** and click **Next**.



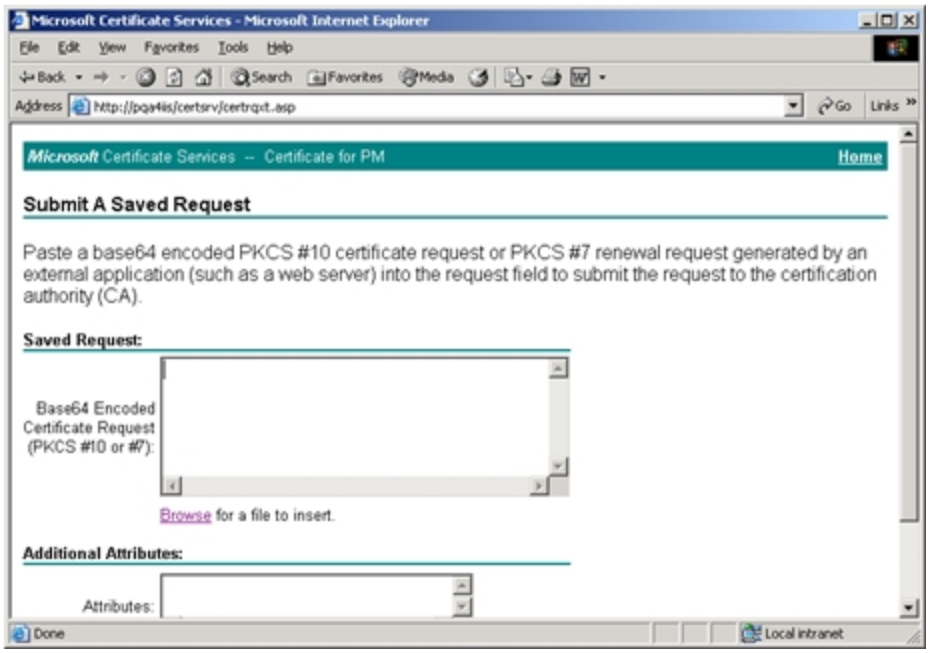
3. Select **Advanced Request** and click **Next**.

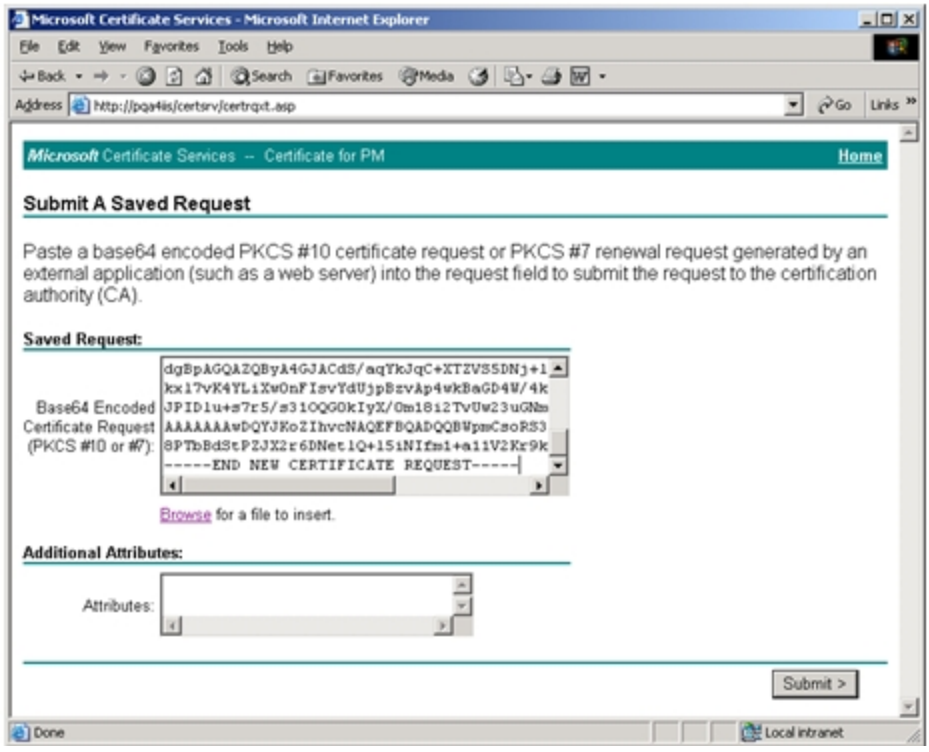


4. Select **Submit a certificate request using a base64 encoded... file** and click **Next**.

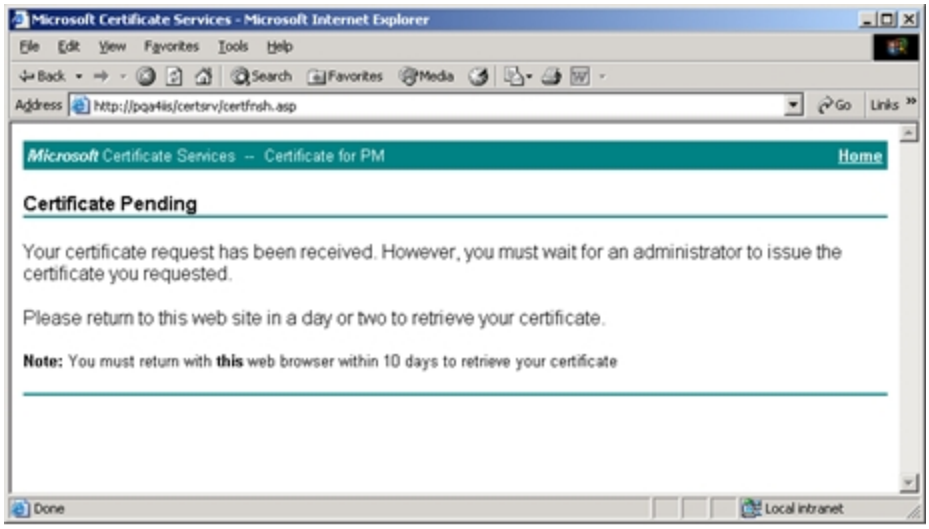


5. In the **Saved Request** text box, paste the contents of the certificate request file copied in Step 1 (or you can browse to locate the file and insert it). Click **Submit**.

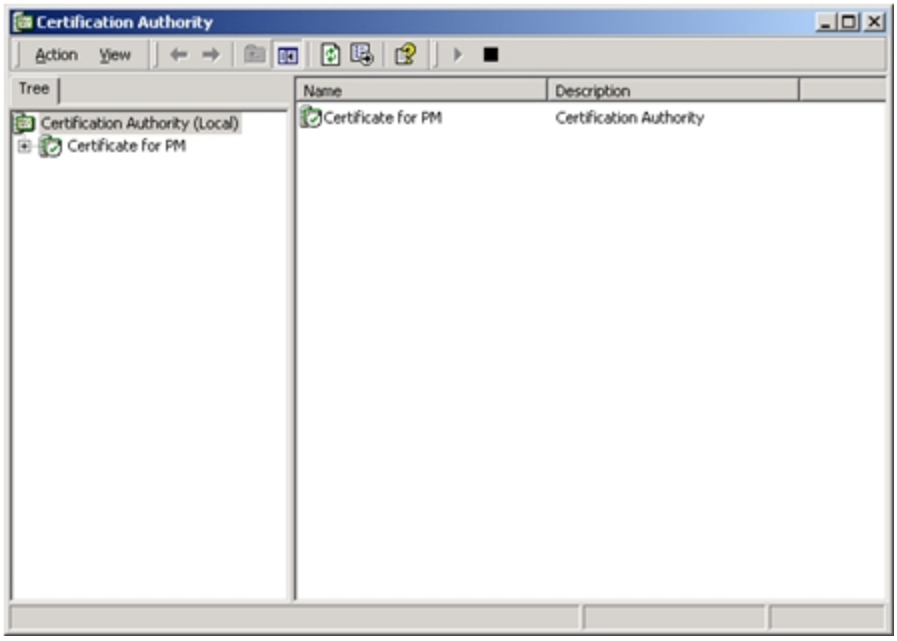

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://pqa4is/certsrv/certrqxt.asp
Go Links
Microsoft Certificate Services -- Certificate for PM
Home
Submit A Saved Request
Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).
Saved Request:
Base64 Encoded Certificate Request (PKCS #10 or #7):
Browse for a file to insert.
Additional Attributes:
Attributes:
Done
Local intranet


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://pqa4is/certsrv/certrqxt.asp
Go Links
Microsoft Certificate Services -- Certificate for PM
Home
Submit A Saved Request
Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).
Saved Request:
Base64 Encoded Certificate Request (PKCS #10 or #7):
dgBpAGQAZQByA4GJACdS/aqYkJqC+XTZVS5DNj+l
kxl7vK4YLiXwOnFIsvYdUjpBzvAp4wkBaGD4W/4k
JPIDlu+s7r5/s31OQGOkIyX/Om18i2TvUw23uGNm
AAAAAAAwDQYJKoZIhvcNAQEFBQADQQBWpmCsoRS3
8PTbBdStPZJX2r6DNetlQ+15iNIfm1+a11V2Kr9k
-----END NEW CERTIFICATE REQUEST-----
Browse for a file to insert.
Additional Attributes:
Attributes:
Submit >
Done
Local intranet

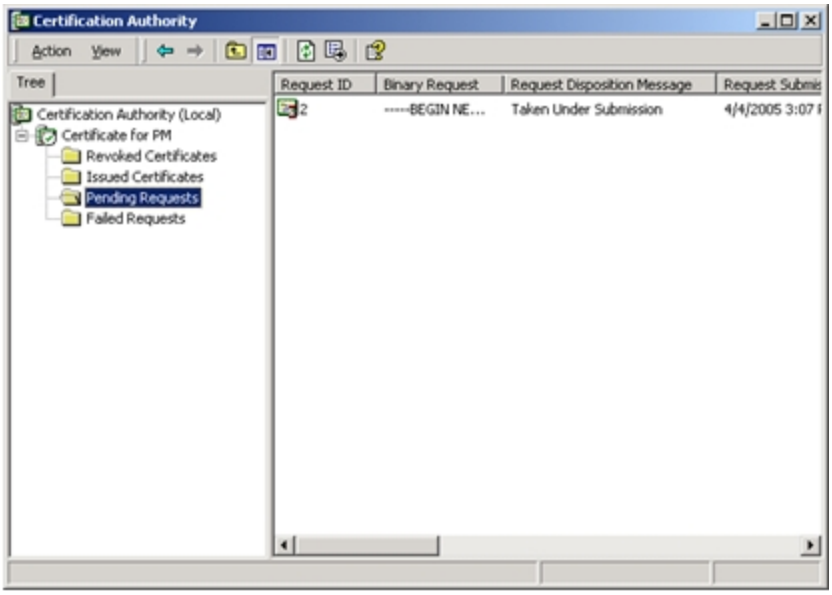
Your certificate request has been received and is pending.



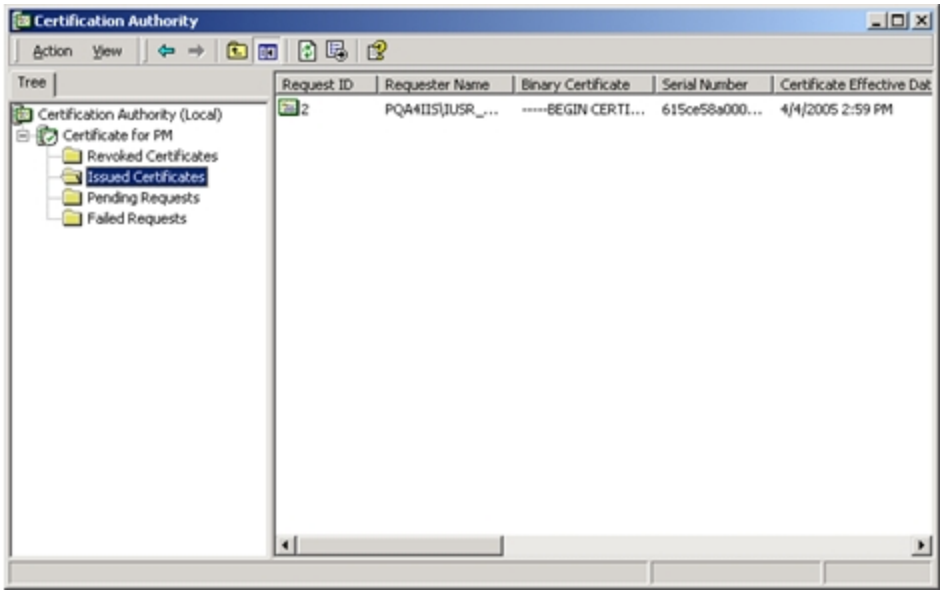
6. Open the Certificate Authority tool by clicking **Start** > **Programs** > **Administrative Tools** > **Certificate Authority**. Expand the certificate authority.



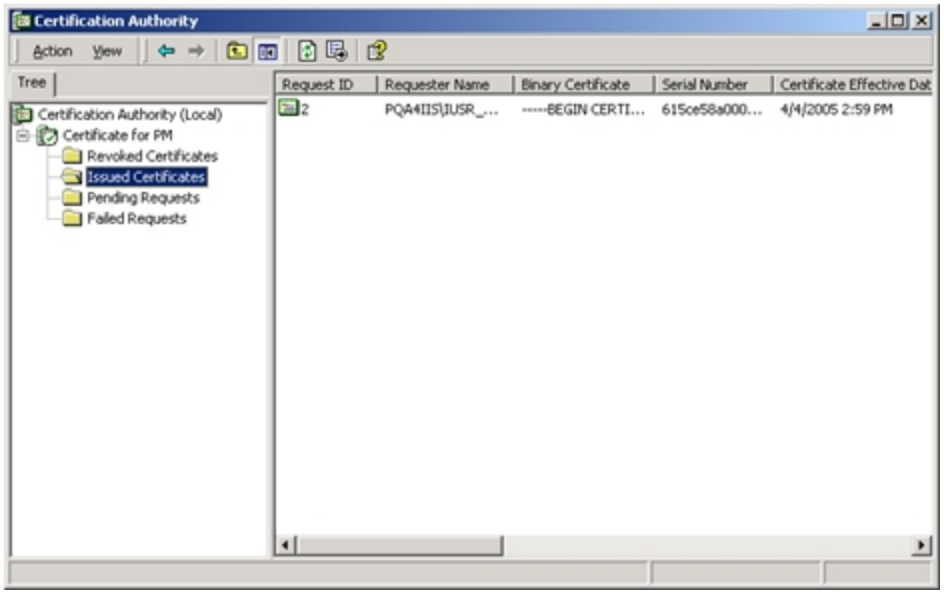
7. Click on the **Pending Requests** folder. Click the certificate request in the right pane, and click **All Tasks** > **Issue**.



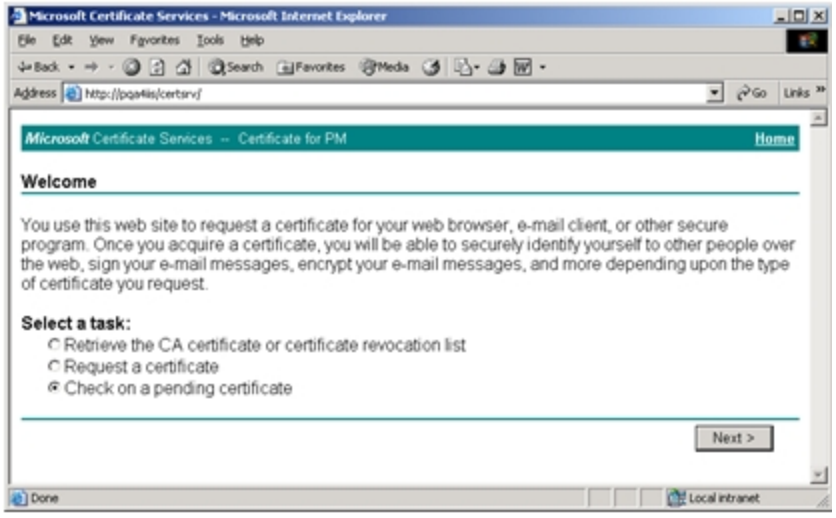
The **Pending Requests** folder is now empty.



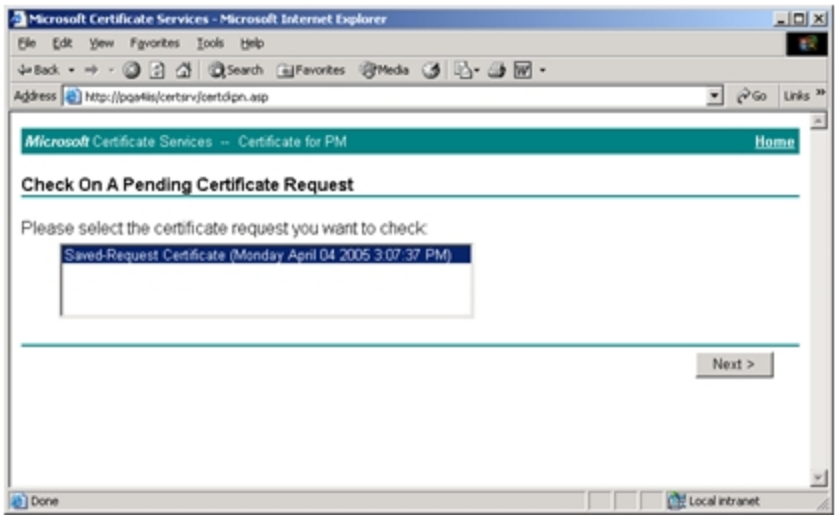
The certificate moves to the **Issued Certificates** folder.



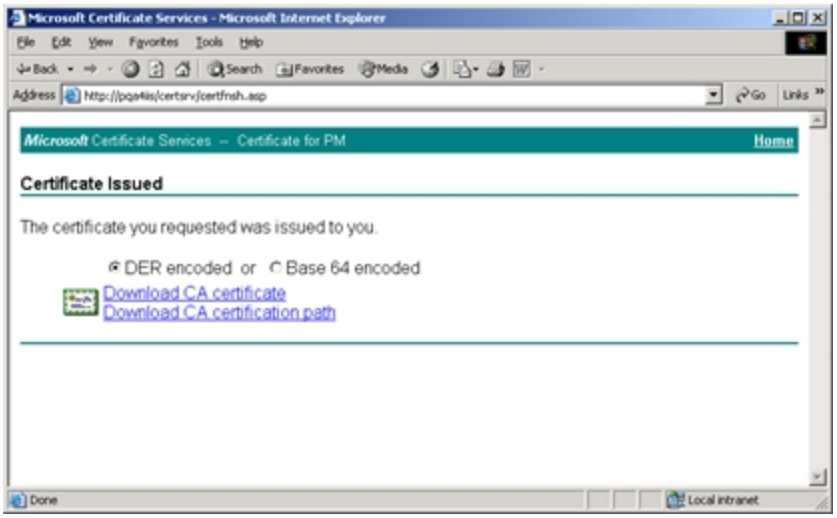
8. Open Microsoft Certificate Services. The URL is http://yourmachinename/certsrv/. Select **Check on a pending certificate** and click **Next**.



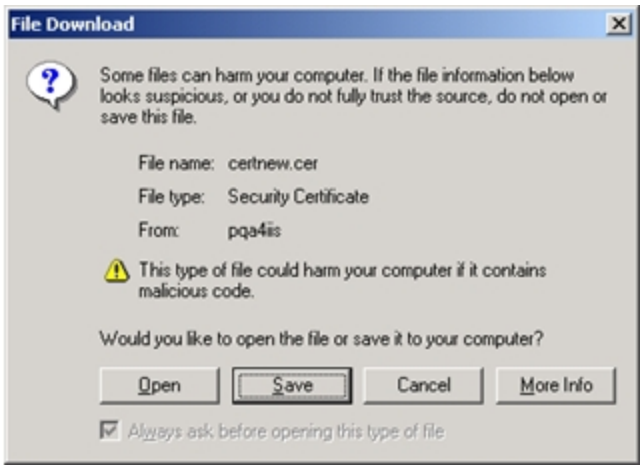
9. Select the certificate that was just created and click **Next**.



10. Click **Download CA certificate**. You can select either DER or Base 64 encoded.

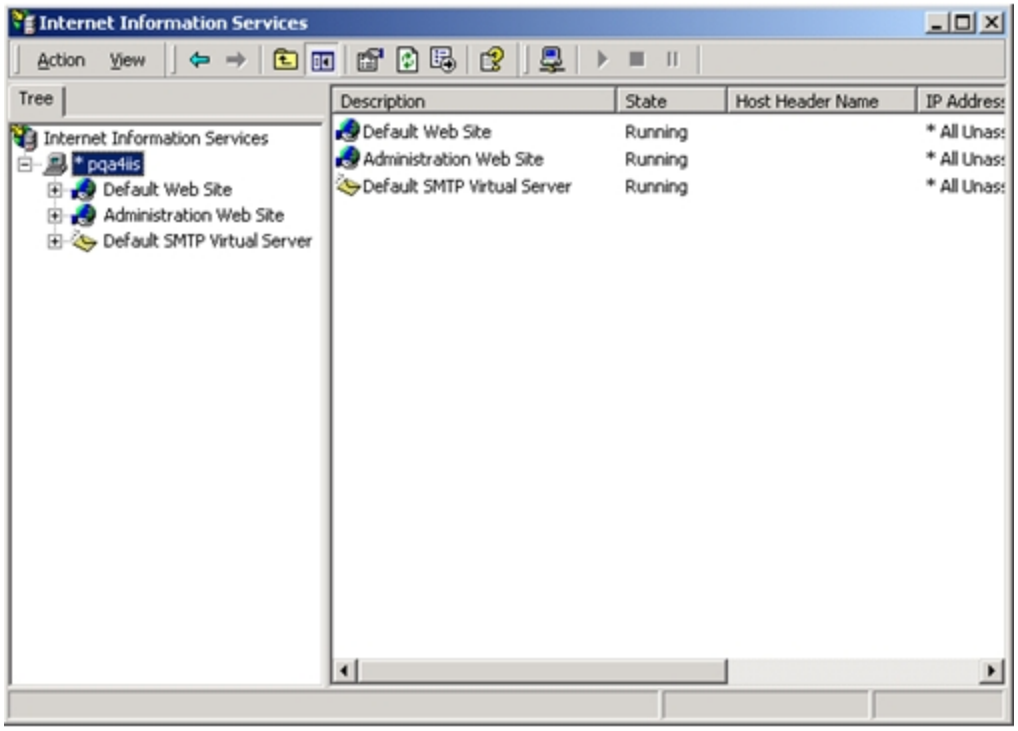


11. Save the file to a location on your computer. Download the certificate.

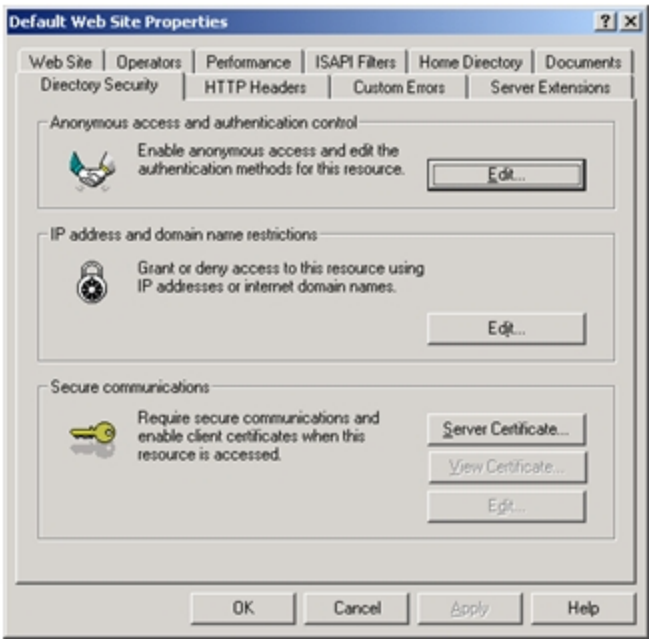


12. Locate the certificate that was just downloaded and double-click it to open it.

13. This certificate must now be installed into IIS. Open IIS and locate the Web site where Provisioning Gateway is installed. Right-click the Web site and click **Properties**.

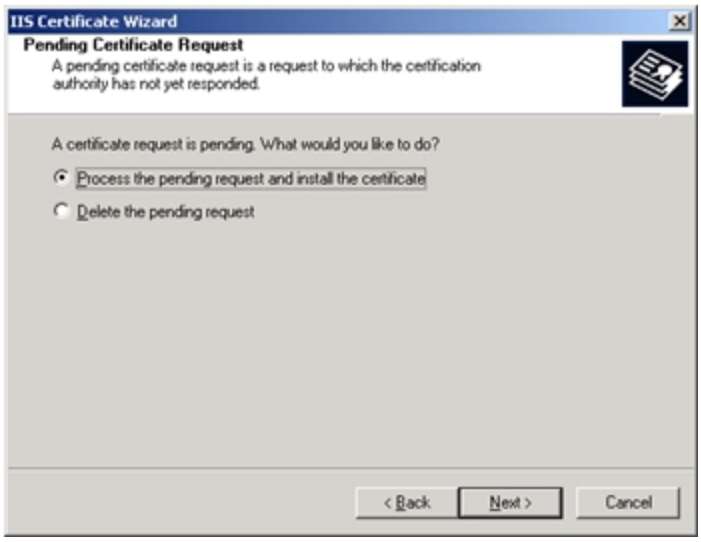


14. Select the **Directory Security** tab and click **Server Certificate**.

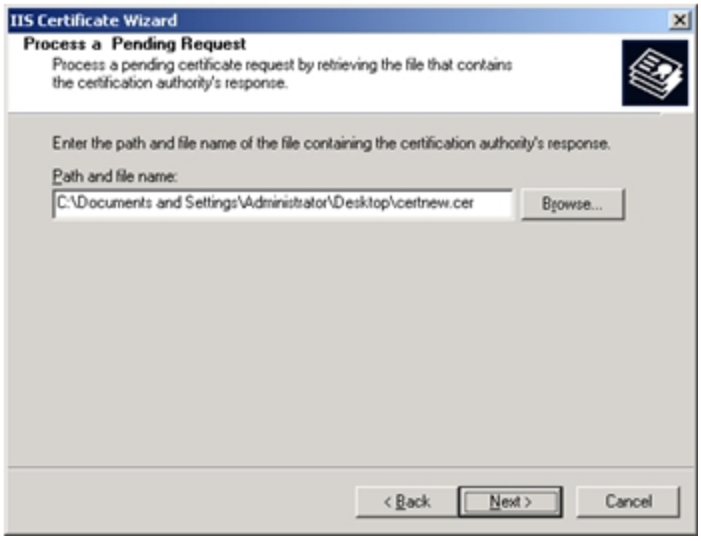


15. On the Web Server Certificate Wizard panel, click **Next**.

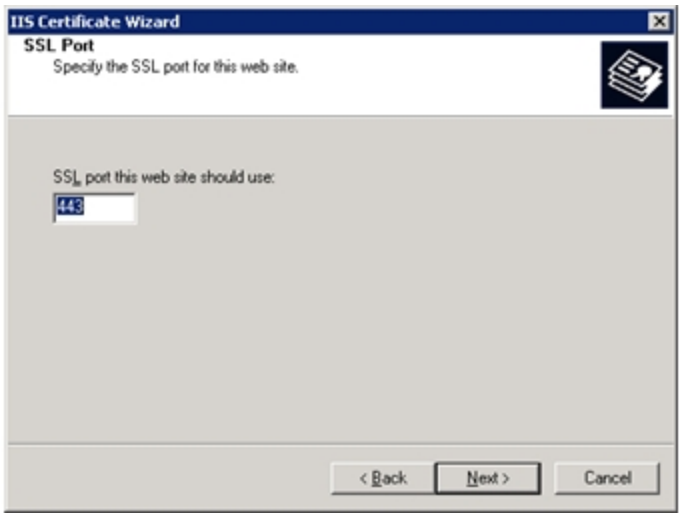
16. Click Process the pending request and install the certificate. Click **Next**.



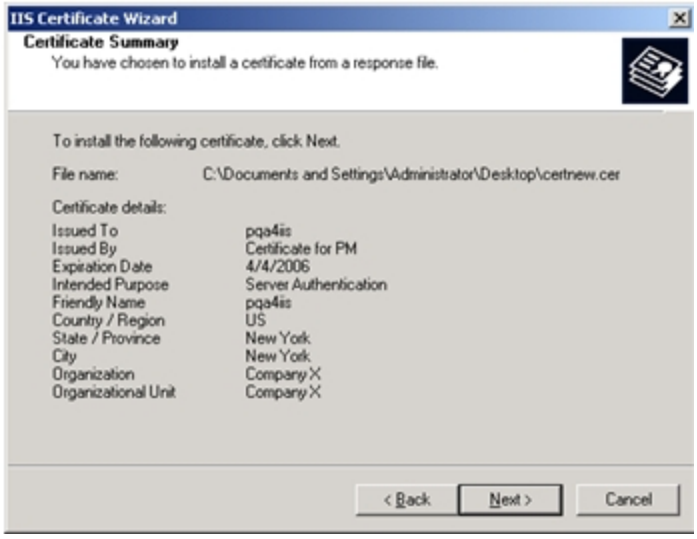
17. Browse to the location of the saved certificate file. Click **Next**.



18. The Wizard asks for the SSL port to use with this Web site. The default SSL Port is 443. Click **Next**.



19. Review the summary of your request. If there are any problems, you might have to issue a new certificate. If everything is correct, click **Next** to install the certificate.



20. When the IIS Certificate Wizard is done, click **Finish**.

Setting Up Role or Group Support

Provisioning Gateway Role/Group support provides the capability to manage provisioning rights for specific applications and users. These provisioning rights are configured and managed in the Oracle Enterprise Single Sign-On Administrative Console. To set up Role/Group support, open the Oracle Enterprise Single Sign-On Administrative Console by clicking **Start** > **Programs** > **Oracle**> **Logon Manager Console**.

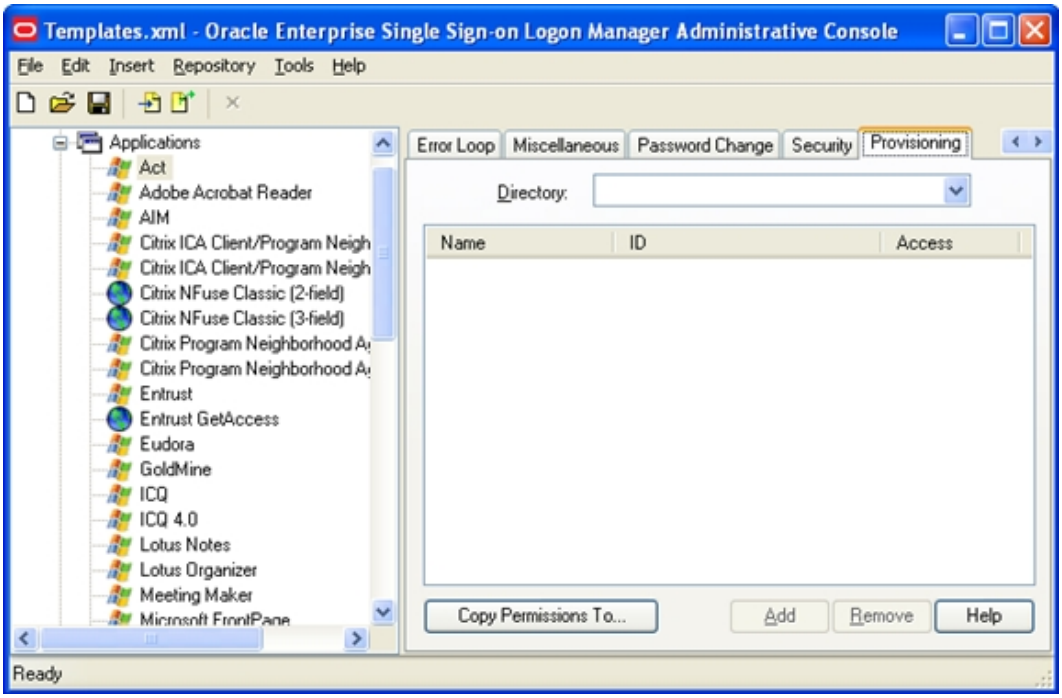
Two panels are available to manage provisioning rights:

- A Provisioning tab, which is located on the individual application panel. This tab enables you to manage provisioning rights for specific applications.
- A Provisioning Manager node, which is located in the Oracle Enterprise Single Sign-On Administrative Console tree (left pane). This node enables you to manage provisioning rights for users.

Using the Provisioning Tab

To access the **Provisioning** tab, expand **Applications** on the left side of the Oracle Enterprise Single Sign-On Administrative Console and double-click any application. Click the **Provisioning** tab.

From this tab, you can add or remove permissions. You can also select the level of access rights (add, modify, or delete applications) for those permissions.



Control	Value
Directory	Enables you to select the target directory server.
Name	Lists the groups or users who currently have access to this item.
ID	Lists the user's account name.
Access	Indicates the permissions that have been granted to the user or group (Add, Modify or Delete Logon). To change a user or group's access rights, right-click the user or group and select **Add Logon**, **Modify Logon**, or **Delete Logon** from the shortcut menu.
Copy Permissions To	Enables you to apply the provisioning rights for the current application to multiple applications. Click this button to display a dialog box listing all the applications. Select the applications that you want these provisioning rights to be copied to. Use **Ctrl**+click or **Shift**+click to select multiple entries. Click **OK**.
Remove	Removes selected users or groups from the list. Select a user or group to remove; use **Ctrl**+click or **Shift**+click to select multiple entries.

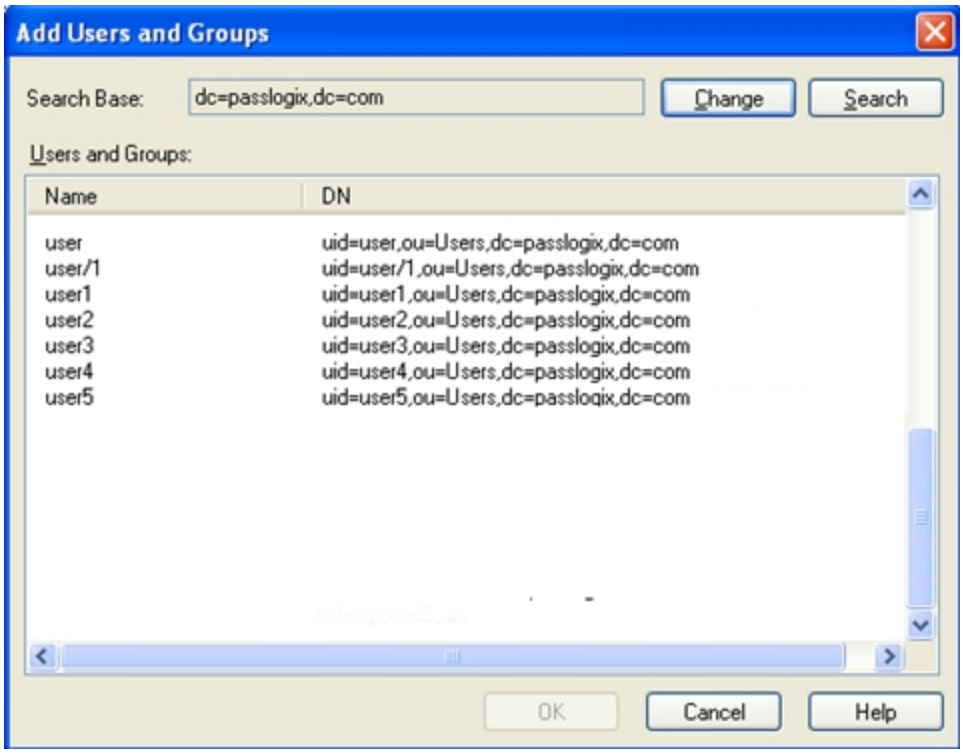
Adding Users or Groups

The dialog box that you use to add users or groups depends upon which directory server is being used:

- LDAP
- Active Directory or AD LDS (ADAM)

LDAP

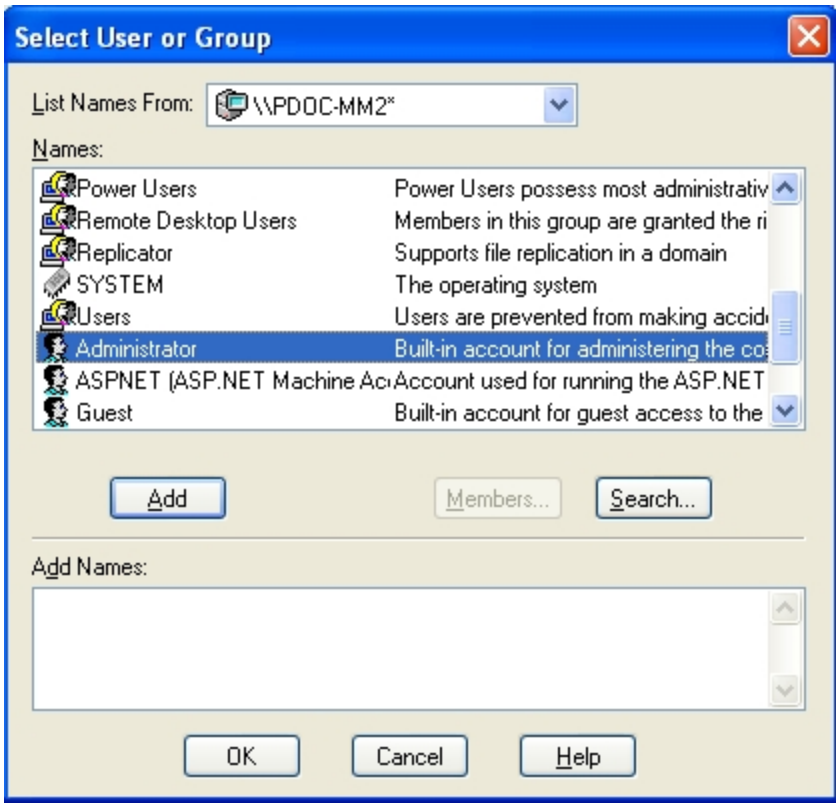
Use the Add Users and Groups dialog box to select the individual users or user groups that are to be added to the access list for the current configuration item (Add Logon, Modify Logon, or Delete Logon).



Control	Value
Search Base	The base (highest-level) directory to begin searching for user or group accounts. All subdirectories of the base directory are searched. Enter a location or click **Change** to browse the directory tree.
Change	Displays the Select Search Base dialog box to browse for a base directory for the search. Use this dialog box to browse to and select the base (highest-level) directory to search for user and group names. Click **OK** when finished.
Search	Begin searching the base directory for users and groups.
Users or Groups	Lists the search results. Select the names to be added to the access list for the current configuration item. Use **Ctrl**+click or **Shift**+click to select multiple entries. Click **OK** when finished to copy your selections to the access list.

Active Directory and AD LDS (ADAM)

Use the Select User or Group dialog box to select the individual users or user groups that are to be added to the access list for the current configuration item (Add Logon, Modify Logon, or Delete Logon).



Controls	Value
List Names From	Select an Active Directory domain or server.
Names	Lists the names of users and groups for the selected domain or server. Select one or more names to add to the access list.
Add	Copies users and groups selected in the Names list to the Add Names list. Use **Ctrl**+click or **Shift**+click to select multiple entries.
Members	When a group is selected the Names list, displays the Global Group Membership dialog box, which lists the members of the selected group.
Search	When a group is selected the Names list, displays the Global Group Membership dialog box, which lists the members of the selected group.
Add Names	Displays the names of the users or groups that you have you have added so far. Click **OK** to add these names to the access list for the current configuration item. You can type or edit user names in this list. However, entries are checked for invalid account names, and duplicate account selections are automatically removed when you click OK.

Using the Provisioning Manager Node

Use the **Provisioning Manager** node to manage provisioning rights for users. To access, click the **Provisioning Manager** node from the tree in the left pane. When you select the node, a pane (the right pane) is displayed with two tabs:

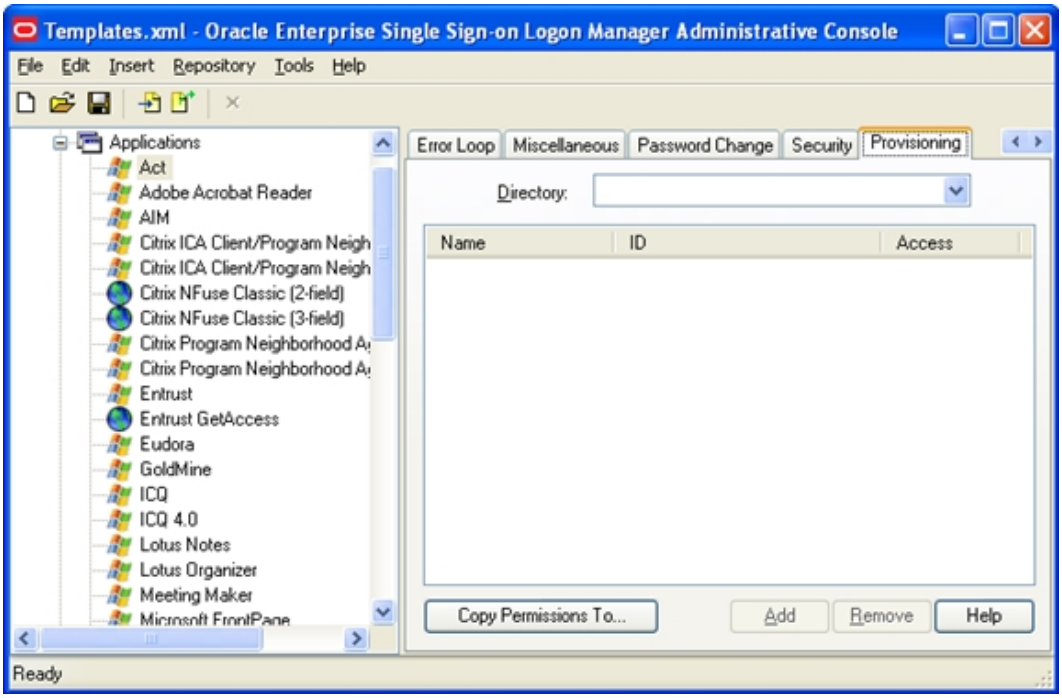
- Default Rights
- Delete SSO User Right

When you change the settings in this node, you must publish them to the repository in order for them to take effect. Right-click the **Provisioning Gateway** node in the Oracle Enterprise Single Sign-On Administrative Console, and select **Publish** .

Default Rights

Use the **Defaults Rights** tab to define the provisioning rights for each new application created. This feature sets standard rights for each application created. After each application is created, change the rights as needed.

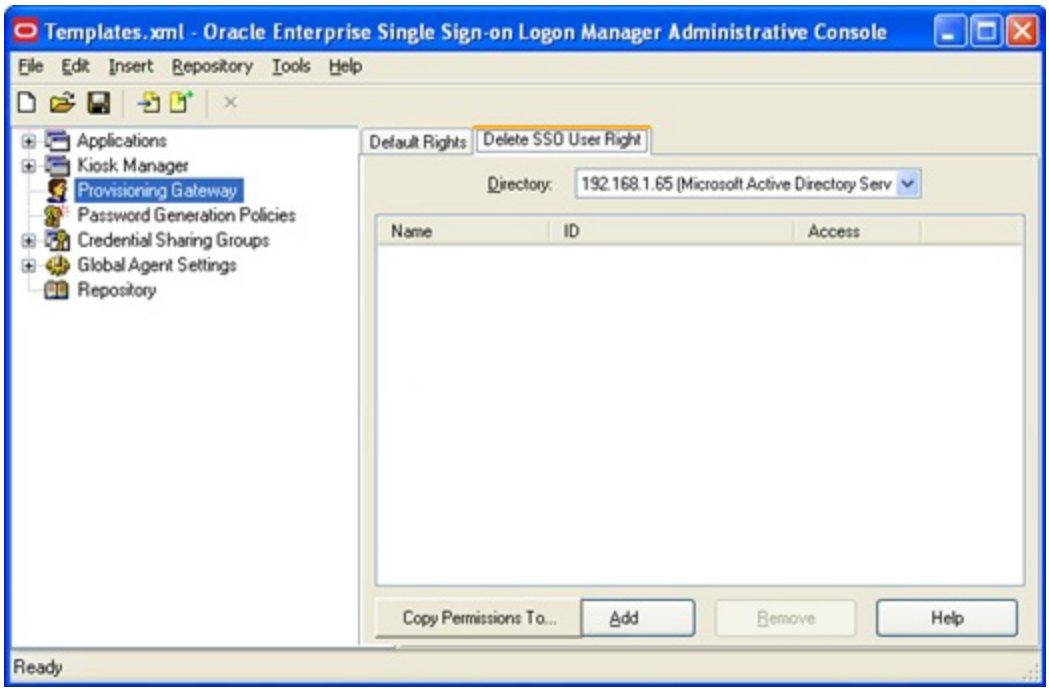
The controls on this tab function the same as the controls on the **Provisioning** tab.



Delete SSO User Right

Use the **Delete SSO User Right** tab to define the users to grant the Delete SSO User functionality to in the Provisioning Gateway Management Console.

The controls on this tab function in the same manner as those on the **Provisioning** tab.


Templates.xml - Oracle Enterprise Single Sign-on Logon Manager Administrative Console
File Edit Insert Repository Tools Help
Applications
Kiosk Manager
Provisioning Gateway
Password Generation Policies
Credential Sharing Groups
Global Agent Settings
Repository
Default Rights
Delete SSO User Right
Directory:
192.168.1.65 (Microsoft Active Directory Serv
Name
ID
Access
Copy Permissions To...
Add
Remove
Help
Ready