Microsoft Dynamics® GP 2010

Web Services Installation and Administration Guide

Publication date

March 2010 - Last updated March 31, 2010

Contents

INTRODUCTION

Introduction

Welcome to Web Services for Microsoft Dynamics® GP. This documentation explains how to install and administer these services so they can be used by applications that integrate with Microsoft Dynamics GP. Before you begin installing and using the services, take a few moments to review the information presented here.

What's in this manual

The Microsoft Dynamics GP Web Services Installation and Administration Guide is designed to give you an in-depth understanding of how to install and administer these services. Information is divided into the following parts:

- Part 1, **Web Service Basics**, explains what is provided by the services for Microsoft Dynamics GP and describes the architecture.
- Part 2, **Installation**, describes how to install and configure the services.
- Part 3, **Security**, explains how to configure security for the services.
- Part 4, **Running the Web Service**, describes the day-to-day operation of the web services.

To learn about creating applications that use the Web Services for Microsoft Dynamics GP, refer to the documentation included with the Web Services for Microsoft Dynamics GP Software Development Kit (SDK).

Symbols and conventions

To help you use this documentation more effectively, we've used the following symbols and conventions within the text to make specific types of information stand out.

Symbol	Description
	The light bulb symbol indicates helpful tips, shortcuts, and suggestions.
	Warnings indicate situations you should be aware of when completing tasks.
Margin notes summarize important information.	Margin notes call attention to critical information and direct you to other areas of the documentation where a topic is explained.

Convention	Description
Part 1, **Web Service Basics**	Bold type indicates a part name.
Chapter 7, "Policy"	Quotation marks indicate a chapter name.
Installing web services	Italicized type indicates a section name.
`using System.IO;`	This font is used to indicate script examples.
Web Services Description Language (WSDL)	Acronyms are spelled out the first time they're used.
TAB or ALT+M	Small capital letters indicate a key or a key sequence.

Product support

Technical support for Web Services for Microsoft Dynamics GP can be accessed using the following methods.

- **Telephone support –** Technical Support at (888) 477-7877 between 8:00 a.m. and 5:00 p.m. Central Time, Monday through Friday. International users can contact Technical Support at (701) 281-0555.
- **Internet** – Technical support is also available online through CustomerSource or PartnerSource. Go to www.microsoft.com/Dynamics/GP and click the CustomerSource or PartnerSource link.

Part 1: Web Service Basics

This portion of the documentation contains basic information you should know before deploying Web Services for Microsoft Dynamics GP. The following information is discussed:

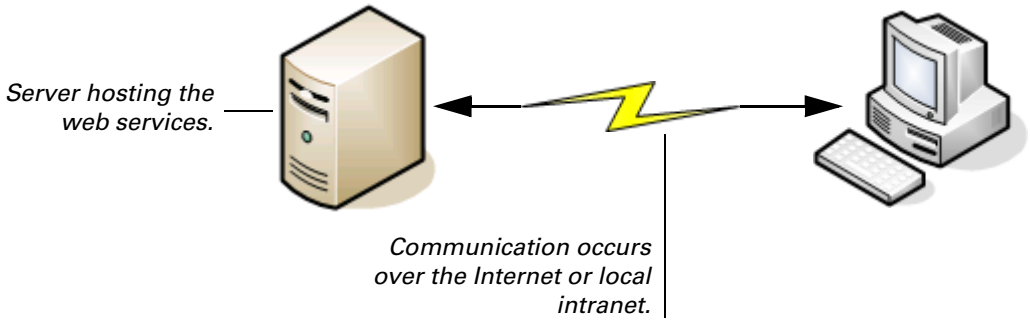
- Chapter 1, "Dynamics GP Web Service Overview," provides an overview of web services and what the Dynamics GP service provides.
- Chapter 2, "Web Service Architecture," describes the parts that make up the Web Services for Microsoft Dynamics GP, and how these parts work together.

Chapter 1: Dynamics GP Web Service Overview

Web Services for Microsoft Dynamics GP provide an ideal way for external applications to integrate with the data contained in the accounting system. The following topics introduce the Web Services for Microsoft Dynamics GP:

What is a web service?

In the most general terms, a web service is defined as a software system that is designed to support machine-to-machine interaction over a network. More specifically, web services are software systems that provide data and services to other applications. Web services use standard Internet transport protocols such as Hypertext Transfer Protocol (HTTP) and standard XML-based document formats such as Simple Object Access Protocol (SOAP) to exchange information.



Windows Communication Foundation (WCF) is used as the foundation to implement the Web Services for Microsoft Dynamics GP. WCF became part of the .NET Framework beginning with version 3. WFC provides support for many standard protocols that can be used for web services.

Web service benefits

In general terms, web services provide several key benefits for software systems:

1. *Based on industry standards*
   Applications that can interact with with services should be able to access the data and services provided by the web service.

2. *Development tool independence*
   Any development tool that supports the web service standard should be able to interact with the web service.

3. *Insulation from future changes*
   Web services attempt to keep the web service interface unchanged, even though the data and code behind the web service may change in future versions of a product. This helps applications that use the web service to keep working, even though the application behind the web service has changed.

4. *Secure access to data.*
   Web services can tightly control access to the data and services they are making available.

What the Dynamics GP service provides

The Microsoft Dynamics GP service provides access to the primary documents in the accounting system. Some of the document types include:

- Customers
- Vendors
- Sales documents
- Purchase documents
- Receivables transactions
- Payables transactions
- General ledger transactions
- Accounts

Through the web service, integrating applications can retrieve documents, create new documents, update existing documents, and delete or void documents.

The Microsoft Dynamics GP service is fully integrated with the Dynamics Security Service. The administrator of the web service can configure security so only specified users are allowed to perform actions like creating or updating sales documents.

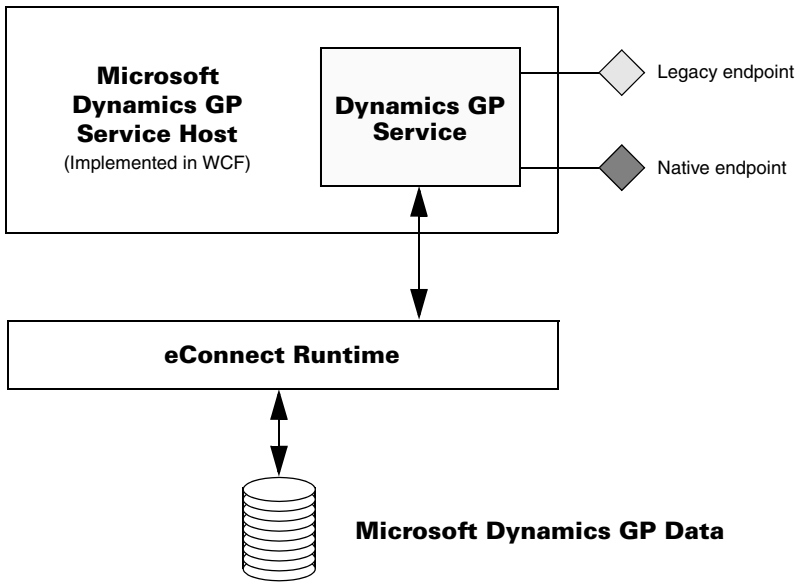
Chapter 2: Web Service Architecture

When deploying the Web Services for Microsoft Dynamics GP, it will be helpful to understand the architecture used to implement them. Information about the architecture is divided into the following sections:

- *Web service foundation*
- *Configurations*
- *Security*
- *Policy*
- *Exception logging*

Web service foundation

Web Services for Microsoft Dynamics GP is constructucted on a base of Windows Communication Foundation (WCF) and eConnect. The architecture is shown in the following illustration.



Windows Communication Foundation

The preferred foundation for web services on the Microsoft Windows Server platform is the Windows Communication Foundation. WCF provides a versatile framework that can be used to implement several types of web services. WCF is used to implement the Microsoft Dynamics GP Service Host. This is a Windows service that can host several WCF services for Microsoft Dynamics GP. One of these is the Dynamics GP service. The Dynamics GP Service provides a *legacy* endpoint and *native* endpoint. External applications use these web service endpoints to access data in Microsoft Dynamics GP.

Legacy endpoint The legacy web service endpoint uses the **BasicHttpBinding**. This endpoint has the characteristics of a standard ASMX-based web service, just like a web service that was created with ASP.NET. Release 9 and Release 10 of Web Services for Microsoft Dynamics GP were ASMX-based web services that were implemented using ASP.NET. Applications can use the legacy endpoint of the Dynamics GP service just like they had used the ASP.NET-based web service from the previous releases.

Native endpoint The native web service endpoint uses the **WSHttpBinding**. This endpoint is similar to legacy endpoint, but has better performance and default security. The native endpoint can also use additional web service features such as reliable messaging. The code that applications use to connect to the native endpoint of the Dynamics GP service is different from the code to connect to the legacy endpoint.

When you use an application that integrates with the Dynamics GP service, it is the responsibility of the applicaton developer to tell you which endpoint the application is accessing.

eConnect

The Dynamics GP web service uses eConnect to provide access to the data managed by the accounting system. eConnect is a set of SQL stored procedures and supporting code used by integrating applications to access data in Microsoft Dynamics GP. Data validation logic is built into eConnect, helping ensure the integrity of any data written to the database through the web services.

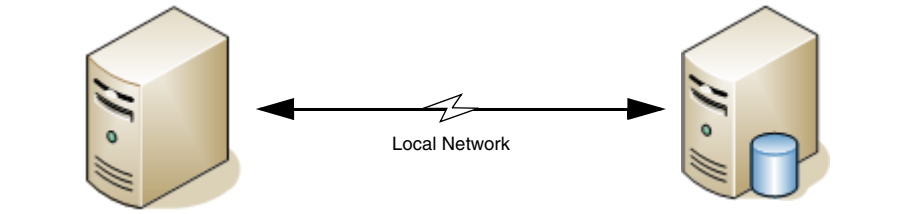
The eConnect interfaces can still be used when the Dynamics GP web service is installed. This allows you to run integrations based directly on eConnect on the same installation as the Dynamics GP web service.

Configurations

Two common configurations are used with Web Services for Microsoft Dynamics GP. In the basic configuration, Windows Communication Foundation (WCF) and the Web Services for Microsoft Dynamics GP are installed on the same server that is hosting SQL Server and managing Microsoft Dynamics GP data. This is shown in the following illustration:

SQL Server with Dynamics GP Data
+
WCF, eConnect runtime, and
Web Services
for Microsoft Dynamics GP

The following illustration shows the second common configuration for the Web Services for Microsoft Dynamics GP. In this configuration, the web services are installed on a separate server, and access the SQL Server that manages Microsoft Dynamics GP data over the local network.



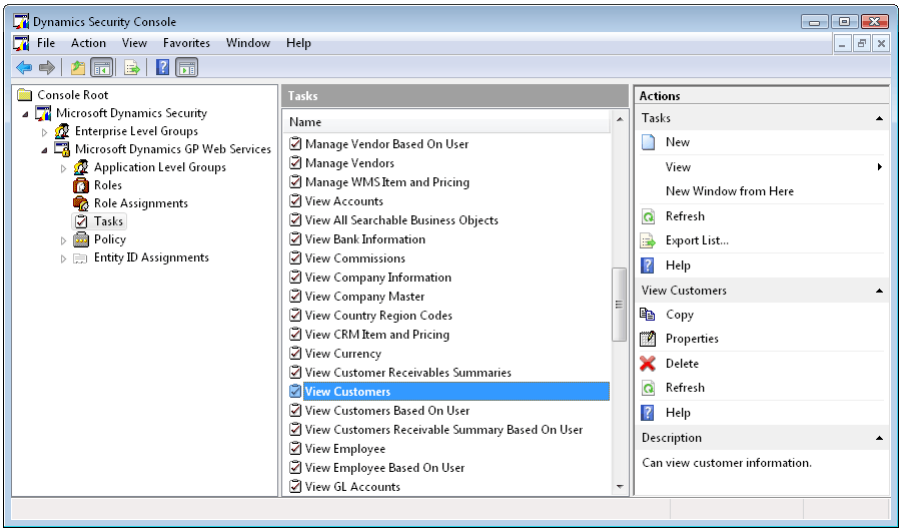
Which configuration you choose will depend on how extensively you will be using the Web Services for Microsoft Dynamics GP, and what server resources you have available. The two-server configuration will provide better performance if the web service will be heavily used.

Security

Refer to Chapter 6, "Web Services Security" for details about managing web service security.

Security for the Dynamics GP service is controlled by the Dynamics Security service. The Dynamics Security service is installed on the same server as the Dynamics GP service.

Through the Dynamics Security service, the web service administrator will configure which users and groups are able to execute the methods (operations) provided by the Dynamics GP service. If an application attempts to run a method for which the current user doesn't have access, a security exception will be raised and the action will be prevented. Security is controlled through the Dynamics Security Administration console, which is a snap-in for Microsoft Management Console (MMC). The console is shown in the following illustration.



Policy

Refer to Chapter 7, "Policy," for details about configuring policy for the Dynamics GP service.

Policy is another security-related feature for the Dynamics GP service. The policy system allows the web service administrator to control how business objects are created, updated, or deleted through the Dynamics GP service.

Each create, update, and delete or void method has a *policy* object that is passed with the operation. This policy object specifies the set of *behaviors* for the operation. Each behavior controls one characteristic for the operation being performed. For instance, the policy for the **CreateCustomer** method has the behavior named "Create Active Behavior". This behavior controls whether the customer being created is set to the active or inactive state.

Behaviors are classified as internal or external. An *internal behavior* is one that can be specified by only the web service administrator. An *external behavior* is one that can be specified by the application that is calling the method and passing in the policy object. Policy is configured using the Dynamics Security console.

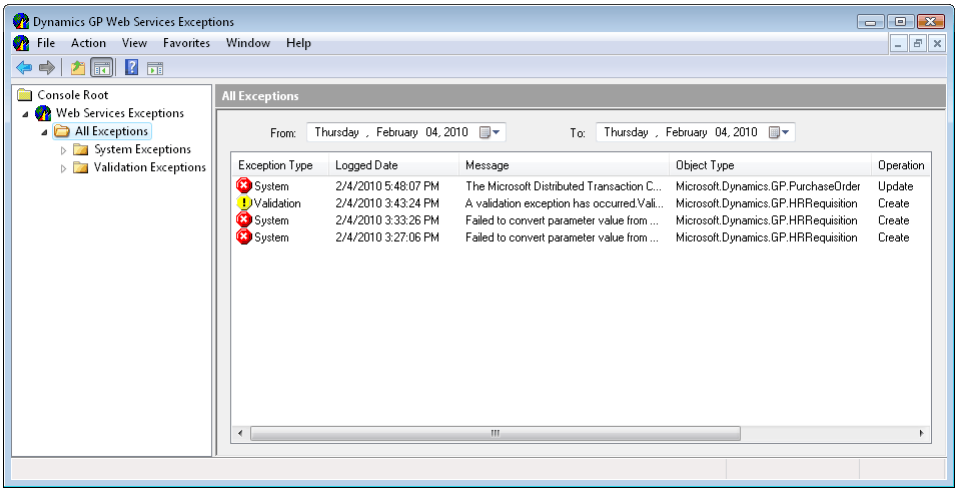
Exception logging

Refer to Chapter 9, "Troubleshooting," for more information about using the exception log to troubleshoot the web service.

The Dynamics GP service maintains a record of all exceptions (errors) that occur for web service operations. The web service administrator will use this information to help diagnose and resolve any issues for applications that use the web service.

You can use the Dynamics GP Web Services Exceptions console to view the exception information. This is a snap-in for Microsoft Management Console (MMC) that retrieves and displays the exceptions logged by the Dynamics GP service.

The console is shown in the following illustration.



The exception information can also be queried by applications that access the Dynamics GP service. Retrieving exception information allows the client applications to display helpful error messages for the user, or to respond appropriately to exceptions that occur.

PART 2: INSTALLATION

Part 2: Installation

This portion of the documentation explains how to install the Web Services for Microsoft Dynamics GP. The following information is discussed:

- Chapter 3, "Prerequisites," describes the software required and the actions you must perform before you install the Web Services for Microsoft Dynamics GP.
- Chapter 4, "Web Services Installation," describes the steps needed to install the web services.
- Chapter 5, "Management Tools Installation," explains how to install the management tools available for the services.

Chapter 3: Prerequisites

Before installing Web Services for Microsoft Dynamics GP, there are several prerequisites needed. This portion of the documentation describes the software required and the additional steps that must be performed before installing the web services. The following topics are discussed:

Operating system

We recommend that you install Web Services for Microsoft Dynamics GP on a server that is running the one of the following operating systems:

- Windows Server 2003 Standard or Enterprise edition
- Windows Server 2008 Standard or Enterprise edition

For development purposes, you can install Web Services for Microsoft Dynamics GP on the following operating systems:

- Windows Vista
- Windows 7

Microsoft .NET 3.5 Framework

To use Web Services for Microsoft Dynamics GP, the Microsoft .NET 3.5 Framework is required. This version of the .NET Framework is installed by the Microsoft Dynamics GP setup utility. You can also download and install this framework by going to the Microsoft Update site:

http://update.microsoft.com

Active Directory Lightweight Directory Services role

If you installing on Windows Server 2008 and will be storing security information in ADAM (Active Directory Application Mode), the Active Directory Lightweight Directory Services (ADLDS) role is required. To install this role, complete the following steps:

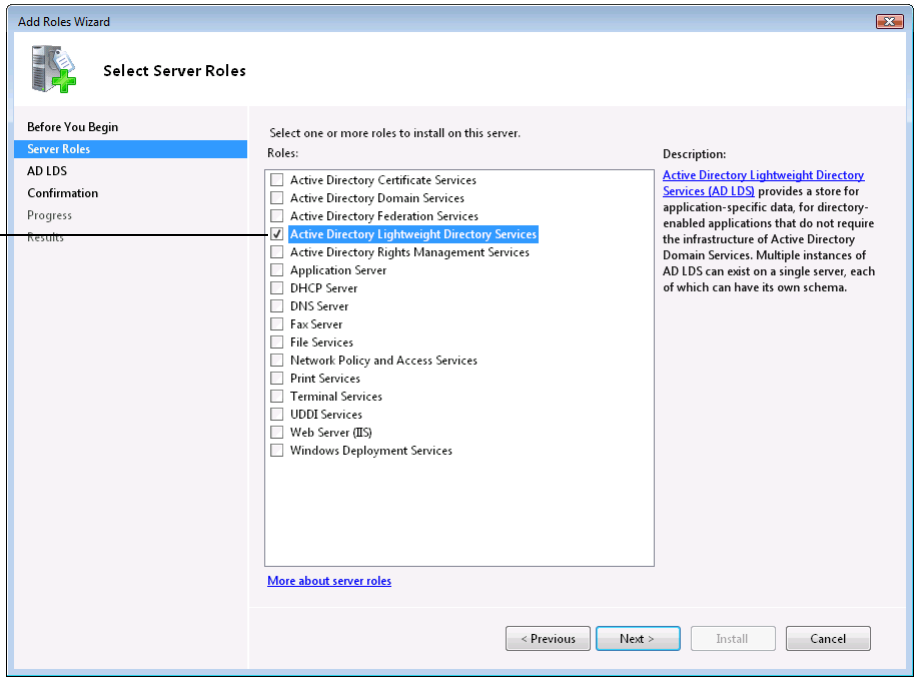
1. **Open the Server Manager.**
   Roles are added in the Server Manager. Choose Start >> Administrative Tools >> Server Manager.

2. **Select the Roles node in the Server Manager.**
   The roles currently installed will be displayed.

3. **Add a new role.**
   In the Action menu, choose Add Roles. The Add Roles Wizard will be displayed. Click Next to continue.

4. **Mark the Active Directory Lightweight Directory Services role.**
   In the list of available roles, mark the Active Directory Lightweight Directory Services role. Click Next to continue.

Mark the Active Directory Lightweight Directory Services role.



5. **Review the information about the directory services.**
   Click Next to continue.

6. **Confirm the installation.**
   Review the installation messages, and then click Install.

7. **Review the installation results.**
   After you have viewed the installation results, click Close.

Microsoft Management Console (MMC) 3.0

Version 3.0 of the Microsoft Management Console (MMC) is required to use the Security Console and Exception Management console that will be installed with Web Services for Microsoft Dynamics GP. If you have Windows Server 2003 R2, Windows Server 2008, Windows Vista, or Windows 7, you already have MMC 3.0 installed. If you do not, there are two ways to get this version of the MMC:

- Install the upgrade for Windows Server 2003 R2.
- Go to www.microsoft.com and search for Knowledge Base article KB907265. This article explains how to download and install the MMC 3.0 update.

Service user account

The Microsoft Dynamics GP Service Host is the Windows service that hosts the various services that are part of Web Services for Microsoft Dynamics GP. The Microsoft Dynamics GP Service Host service must run under a user account To make the service more secure, a specific "service user account" should be created and used only for this purpose.

Which type of user (local or domain) you need to create depends on the configuration you plan to use for Web Services for Microsoft Dynamics GP.

- If you will be installing the web services on the same computer that is running the SQL Server and managing data for Microsoft Dynamics GP, you can create a local user account.
- If you will be installing the web services on a different computer than the one running SQL Server and managing data for Microsoft Dynamics GP, you must create a domain account.

For improved security, this new user should be given minimal privileges.

When you install Web Services for Microsoft Dynamics GP, you will need to supply the credentials for this new account.

Microsoft Dynamics GP 2010

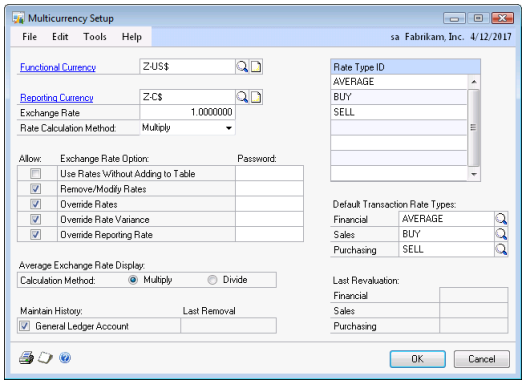
To use this release of Web Services for Microsoft Dynamics GP, you must be using Microsoft Dynamics GP 2010. Be sure the Microsoft Dynamics GP installation is working properly, and that you have made a complete backup before installing the Web Services for Microsoft Dynamics GP.

You must be using Microsoft SQL Server 2005 or 2008 to manage the data for Microsoft Dynamics GP. The databases cannot be running in SQL Server 2000 compatibility mode.

Functional currency

Web Services for Microsoft Dynamics GP relies on eConnect for data access. eConnect requires a functional currency to be set up for Microsoft Dynamics GP, even if multicurrency is not being used. To set up a functional currency, complete the following procedure:

1. **Open the Multicurrency Setup window in Microsoft Dynamics GP.** Choose Tools >> Setup >> Financial >> Multicurrency from the Microsoft Dynamics GP menu. Set the Functional Currency.



Refer to the Microsoft Dynamics GP documentation for additional information about currency setup and multicurrency access.

2. **Complete check links when needed.**
   If a message prompts you to run check links for the multicurrency table, you should do so. To run checklinks, open the Microsoft Dynamics GP menu. Point to Maintenance and then choose Check Links. Select the series and tables to check. Click OK.

ISO currency codes

The Dynamics GP service uses ISO codes to identify currencies in Microsoft Dynamics GP. These ISO codes were not previously required for the currencies defined in the system, so the currencies may not have them. If they do not, you must add the appropriate ISO code for each currency.

Web Services for Microsoft Dynamics GP does not support using the same ISO code for more than one currency.

To add ISO codes, complete the following procedure:

1. **Open the Currency Setup window in Microsoft Dynamics GP.**
   Choose Microsoft Dynamics GP menu >> Tools >> Setup >> System >> Currency and enter the system password to display this window.

2. **Display each currency.**
   Use the Currencies lookup to display each currency.

3. **Enter the ISO value and save the currency.**
   The following table lists the ISO values for the currencies commonly defined in Microsoft Dynamics GP:

ISO Code	Country/Region	Currency
AUD	Australia	Dollars
CAD	Canada	Dollars
EUR	European Union	Euros
JPY	Japan	Yen
MXN	Mexico	Pesos
NZD	New Zealand	Dollars
PLN	Poland	Zlotych
SGD	Singapore	Dollars
ZAR	South Africa	Rand
GBP	United Kingdom	Pounds
USD	United States	Dollars

Chapter 4: Web Services Installation

This portion of the documentation describes how to perform the installation of Web Services for Microsoft Dynamics GP. The following items are discussed:

Installing web services

If you're upgrading an existing installation of web services, refer to Upgrading an earlier installation on page 25.

To install Web Services for Microsoft Dynamics GP, complete this procedure.

1. **Verify the user you are logged in as.**
   This user will become the initial Security Administrator for the Dynamics Security Service. This user will also be added to the Superuser role for the Dynamics GP web service, allowing access to all web service operations. On Windows Server 2003, the user you are currently logged in as must be in the Administrator role for the computer on which you are installing.

2. **Determine which installer to use.**
   The installers for Web Services for Microsoft Dynamics GP are found in the \AdProd\WebServices\ folder of the Microsoft Dynamics GP installation media. Choose the appropriate installer, based on whether you are installing on a 32-bit or 64-bit version of Windows.

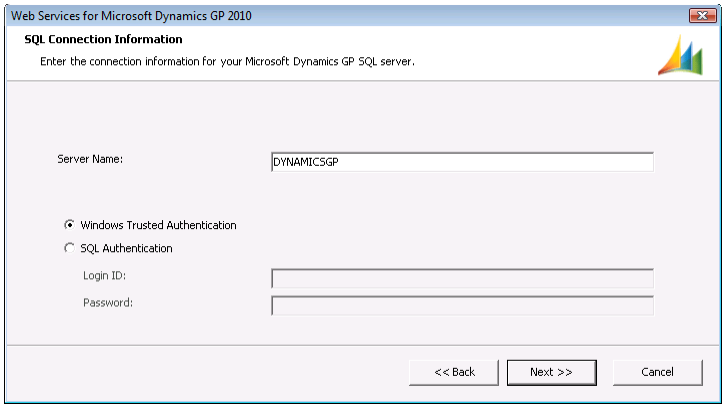
Version	Installer
32-bit	Microsoft_DynamicsGP11_WebServices_x86_en-us.msi
64-bit	Microsoft_DynamicsGP11_WebServices_x64_en-us.msi

If you choose to install the Web Services Runtime from the main Microsoft Dynamics GP setup, the correct installer is selected automatically.

3. **Start the Web Services for Microsoft Dynamics GP installer.**
   Run **Setup.exe** to start the installer. If required, you will be prompted for administrator credentials. The Welcome page of the installer will be displayed. Click Next to continue.

4. **Review the license agreement.**
   After reviewing the license agreement, mark the option to accept the terms, and then click Next to continue.

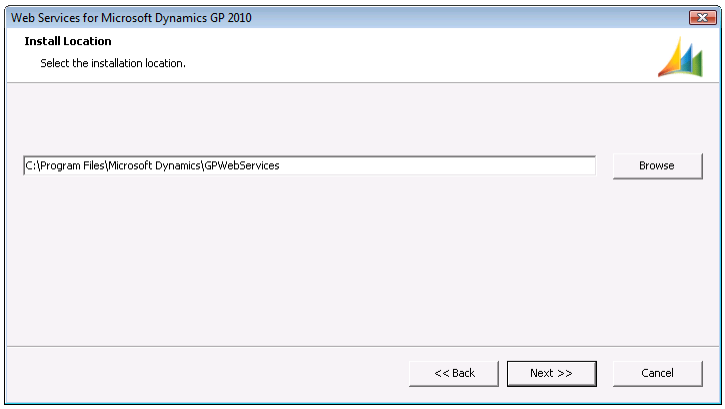
5. **Specify the location of the Microsoft Dynamics GP data.**
   In the Server Name field, supply the name of the machine that is running SQL Server and managing the data for Microsoft Dynamics GP. The installation program must connect to this database to complete the installation. You must use Windows Trusted Authentication to connect to the SQL Server.



Click Next to continue. If the database connection cannot be made, an error will be displayed. Correct the issue and continue.

6. Select the installation location.

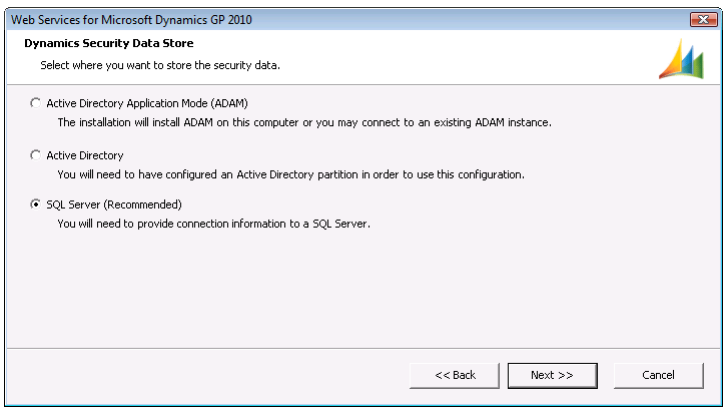
Select the location where the files for the Web Services for Microsoft Dynamics GP will be installed. You can use the default location, or click Browse to specify a different location.



When you have made your selections, click Next to continue.

7. Specify where the security data will be stored.

The Dynamics Security Service that is used to manage security must have a location to store the security data. The options available will depend on the operating system on which you are installing.



Choose one of the following options:

Active Directory Application Mode (ADAM) The security data will be stored in ADAM (for Windows Server 2003) or ADLDS (for Windows Server 2008).

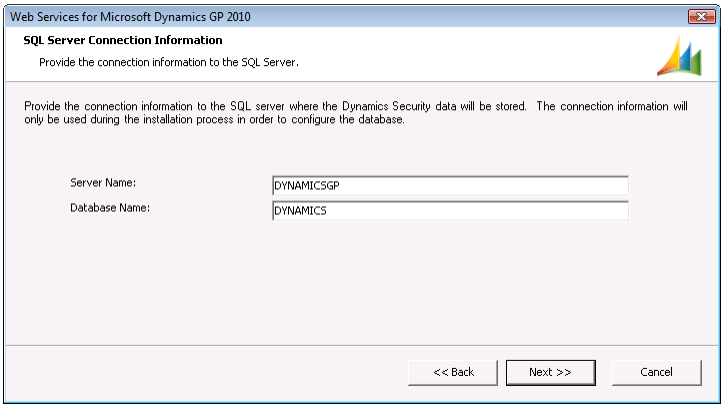
If you choose this option for the 64-bit version of Windows Server 2003, you may encounter an error indicating that the AZRoles.dll is not in the global assembly cache. Refer to Knowledge Base article KB 937292 for details about how to resolve this problem.

Active Directory The security data will be stored in Active Directory. The user installing Web Services for Microsoft Dynamics GP must have sufficient privileges to add the security data to Active Directory. The partition to store the security data must already exist. Refer to Appendix B, "Creating an Active Directory Partition," for information about creating a partition.

SQL Server The security data will be stored in a SQL Server database. It is the preferred way to store the security data. This option is not available on Windows Server 2003.

Click Next to continue.

8. **Specify the SQL database for security data (if required).**
If you chose to store security data in SQL Server, specify the server and database where the security data will be stored.



Be aware of the following requirements for this database:

- The SQL Server you specify must be running on Windows Server 2008 or later.
- The database you specify must use a case-insensitive sorting order.
- The database owner must be a Windows user account. It cannot be a SQL Server account.
- If the database you specify does not exist, a message will be displayed indicating that it will be created.

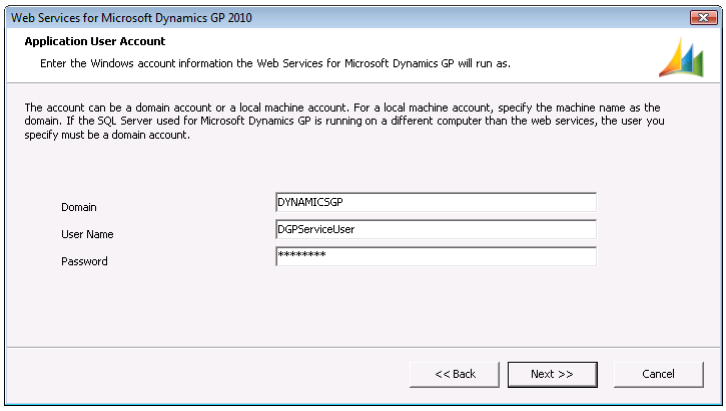
Click Next to continue.

9. Specify the application account.

This account will be used for the following:

- User for the Microsoft Dynamics GP Service Host
- User for the eConnect Service Host (if eConnect is not already installed)
- Reader of ADAM (if ADAM or ADLDS is being used)
- Reader of AzMan
- User for SQL Server and the databases used for Microsoft Dynamics GP

Typically, you will enter the account that you created while performing the prerequisites for the installation. If you are installing Web Services for Microsoft Dynamics GP on a different machine than the SQL Server used to manage Microsoft Dynamics GP data, this must be a domain user account. If you are installing on the same machine as the SQL Server, it can be a local machine account. This case is shown in the following illustration:



If the account you specified has already been added as a user for Microsoft SQL Server, be sure the case for the Domain and User Name match those of the user ID in SQL.

Click Next to continue.

10. Start the installation.

Click Install to begin the installation process. The following additional installations may occur if they have not already been performed:

- eConnect Runtime Installation
- ADAM or ADLDS instance - This component is required by the Dynamics Security Service. The current user is added as an ADAM or ADLDS administrator.

You may want to add other users as ADAM or ADLDS administrators so they can perform repair or upgrade procedures for the Web Services for Microsoft Dynamics GP. Refer to Appendix A, "ADAM or ADLDS Administrators," for details about adding other users as administrators.

11. Complete the installation.

After a few minutes, the installation will finish. You must now perform the initial configuration of Web Services for Microsoft Dynamics GP. To do this, you can mark the Run Configuration Wizard option, and then click Exit.

Initial configuration for web services

After Web Services for Microsoft Dynamics GP has been installed, you must run the Web Services for Microsoft Dynamics GP Configuration Wizard to complete the initial configuration. To do this, complete this procedure.

1. **Start the configuration wizard.**
   In the Start menu, locate the Microsoft Dynamics group. Point to Web Services for Microsoft Dynamics GP 2010, and then choose GP Web Services Configuration Wizard. The Welcome page for the wizard will be displayed.

   Click Next to continue.

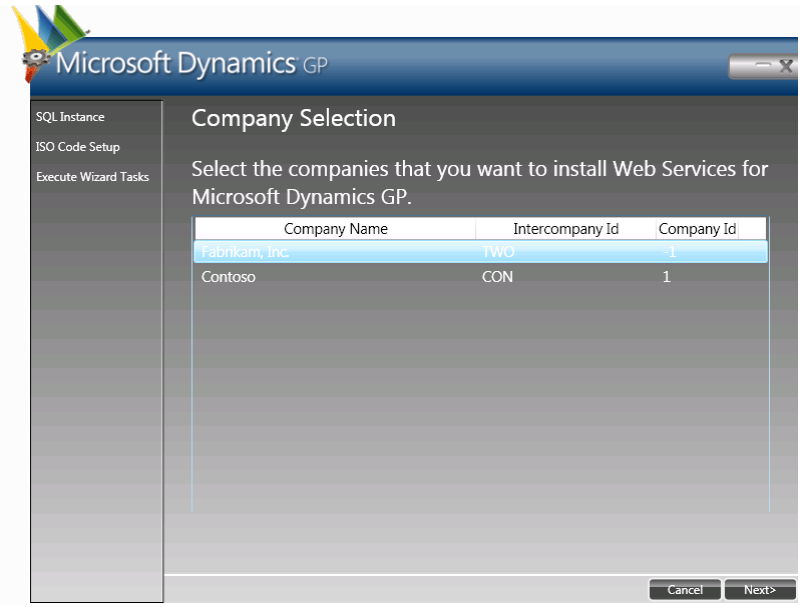
2. **Enter the connection information for Microsoft Dynamics GP.**
   The SQL Server Name field will contain the name of the SQL Server that is managing the data for Microsoft Dynamics GP. The configuration wizard must connect to this server to perform the setup operations. You must use Windows Trusted Authentication to connect to the SQL Server. Click Next to continue.

3. **Verify system check results.**
   The configuration wizard will verify the following:

   - ISO currency codes have been defined for each currency
   - Functional currencies have been set up for each company

   If either of the system checks do not pass, make the appropriate corrections in Microsoft Dynamics GP. Then re-run the configuration wizard. When the checks pass, click Next to continue.

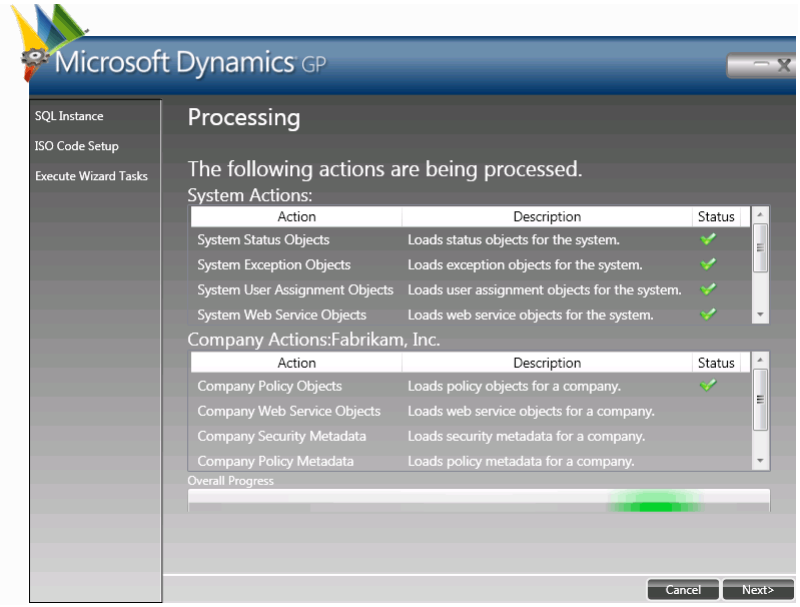
4. **Select the companies for which to install web services.**
In the list of available companies, select the companies for which you want to install web services. Hold down the CTRL key to select multiple companies.



Click Next to continue.

5. **View the summary of actions to be performed.**
A list of the actions to be performed will be displayed. Click Next to continue. A dialog will be displayed, asking whether to continue with the installation. Click Yes to start the installation process.

6. **Verify progress for the configuration tasks.**
The configuration tasks for the system and for each company will be performed. The overall progress shown at the bottom of the window. A green check will be displayed as each task is processed.



7. **Complete the configuration.**
   Click Complete to close the GP Web Services Configuration Wizard.

8. **Restart the Microsoft Dynamics GP Service Host.**
   The configuration wizard will ask whether to restart the Microsoft Dynamics GP Service Host. This is the Windows service that manages the various services in Web Services for Microsoft Dynamics GP. Click Yes to restart the service.

9. **Verify the service has restarted.**
   After a few moments, verify that the service has restarted. Do this by choosing Start > Administrative Tools > Services. Locate the entry for Microsoft Dynamics GP Service Host, and verify that it is running.

Upgrading an earlier installation

If you have a web services installation from an earlier release of Microsoft Dynamics GP, you can upgrade it to the current version. The same upgrade method is used whether you are upgrading to a new major version or just applying a service pack. Use the Microsoft Dynamics GP installer to update the Dynamics system and company databases to the new release before you update web services.

Before you start the upgrade, be sure that your current Web Services for Microsoft Dynamics GP installation is working properly. Do not perform other maintenance activities as part of the upgrade process. Perform these other maintenance activities before starting the upgrade or after the upgrade has been successfully finished.

Among the various upgrade tasks, the web service upgrade does the following:

- Adds additional objects for the Dynamics GP service
- Adds additional policy objects
- Updates the Dynamics Security Console
- Adds new security objects, such as roles and tasks. The roles and tasks that have changed, but were part of the earlier version of web services *will not be updated*. The update will try to preserve the changes you have made to the security data.
- Re-creates the Superuser role so that it will include access to all of the web service objects.
- Updates the BusinessObjectFile.config, to add registrations for any new events for the Dynamics GP service. This file is located in the "ServiceConfigs" folder, typically found in this location:

  C:\Program Files\Microsoft Dynamics\GPWebServices\ServiceConfigs\

If you have manually added any event registrations to the BusinessObjectFile.config, be sure to make a copy of this file before you perform the upgrade. You may need to manually re-add the additional registrations after the web service upgrade is complete.

Complete the following procedure to upgrade the web service installation.

1. **Verify that the Dynamics databases have been updated.**
   You must have used the Microsoft Dynamics GP installer to update the databases to the new release.

2. Verify the user you are logged in as.
The user you are currently logged in as must be the following:

- For Windows Server 2003, you must be in the Administrator role for the computer on which you are upgrading the installation.
- An ADAM or ADLDS administrator. The user who installed the earlier version of web services will be an ADAM administrator. Refer to Appendix A, "ADAM or ADLDS Administrators," for information about adding other users as administrators.

This user will become a Security Administrator for the Dynamics Security Service. This user will also be added to the Superuser role for the Dynamics GP service, allowing access to all service operations.

3. Determine which installer to use.
The installers for Web Services for Microsoft Dynamics GP are found in the \AdProd\WebServices\ folder of the Microsoft Dynamics GP installation media. Choose the appropriate installer, based on whether you are upgrading on a 32-bit or 64-bit version of Windows.

Version	Installer
32-bit	Microsoft_DynamicsGP11_WebServices_x86_en-us.msi
64-bit	Microsoft_DynamicsGP11_WebServices_x64_en-us.msi

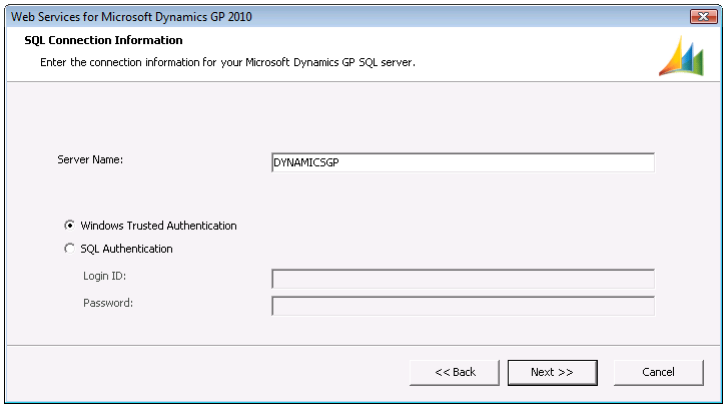
If you choose to install the Web Services Runtime from the main Microsoft Dynamics GP setup, the correct installer is selected automatically.

4. Start the Web Services for Microsoft Dynamics GP installer.
Run **Setup.exe** to start the installer.

5. Review the license agreement.
After reviewing the license agreement, mark the option to accept the terms and click Next to continue.

6. Specify the location of the Microsoft Dynamics GP data.
In the Server Name field, supply the name of the machine that is running SQL Server and managing the data for Microsoft Dynamics GP.

The installation program must connect to this database to complete the installation. You can use Windows Trusted Authentication or SQL Authentication (supplying the Administrator login ID and password).

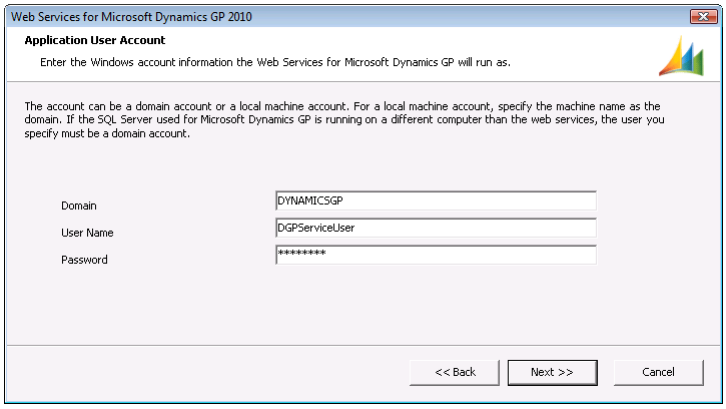


Click Next to continue. If the database connection cannot be made, an error will be displayed. Correct the issue and continue.

7. **Specify the application account.**
This account will be used for the following:

- User for the Microsoft Dynamics GP Service Host
- User for the eConnect Service Host (if eConnect is not already installed)
- Reader of ADAM (if ADAM or ADLDS is being used)
- Reader of AzMan
- User for SQL Server and the databases used for Microsoft Dynamics GP

Typically, you will use the same account that you created when you installed the previous version of web services. If you are installing Web Services for Microsoft Dynamics GP on a different machine than the SQL Server used to manage Microsoft Dynamics GP data, this must be a domain user account. If you are installing on the same machine as the SQL Server, it can be a local machine account. This case is shown in the following illustration:



If the account you specified has already been added as a user for Microsoft SQL Server, be sure the case for the Domain and User Name match those of the user ID in SQL.

Click Next to continue.

8. **Start the installation.**
Click Upgrade to begin the process of upgrading the installed instance of the web services.

9. **Complete the installation.**
After a few minutes, the installation will finish. You must now perform the initial configuration of Web Services for Microsoft Dynamics GP. To do this, mark the Run Configuration Wizard option, and then click Exit.

10. **View the configuration wizard.**
After a few moments, the Web Services for Microsoft Dynamics GP Configuration Wizard will be displayed. Click Next to continue.

11. **View the connection information for Microsoft Dynamics GP.**
The SQL Server Name field will contain the name of the SQL Server that is managing the data for Microsoft Dynamics GP. The configuration wizard must connect to this server to perform the setup operations. You must use Windows Trusted Authentication to connect to the SQL Server. Click Next to continue.

12. **Verify system check results.**
The configuration wizard will verify the following:

    - ISO currency codes have been defined for each currency
    - Functional currencies have been set up for each company

    If either of the system checks do not pass, make the appropriate corrections in Microsoft Dynamics GP. Then re-run the configuration wizard. When the checks pass, click Next to continue.

13. **Choose the action to perform.**
Select the Upgrade Companies action to upgrade companies to work with the new version of Web Services for Microsoft Dynamics GP. Click Next to continue.

14. **Select the companies to upgrade.**
In the list of available companies, select the companies that you want to upgrade to the new version of web services. Hold down the CTRL key to select multiple companies. Click Next to continue.

15. **View the summary of actions to be performed.**
A list of the actions to be performed will be displayed. Click Next to continue. A dialog will be displayed, asking whether to continue with the update. Click Yes to continue the update process.

16. **Verify progress for the upgrade tasks.**
The upgrade tasks for the companies you chose will be performed. The overall progress is shown at the bottom of the window. A green check will be displayed as each task is processed.

17. **Complete the upgrade.**
Click Complete to close the GP Web Services Configuration Wizard.

18. **Restart the Microsoft Dynamics GP Service Host.**
The configuration wizard will ask whether to restart the Microsoft Dynamics GP Service Host. Click Yes to restart the service.

Verifying the web service installation

After the web service installation is complete, you should verify that the services for Microsoft Dynamics GP are operational.

Dynamics GP service

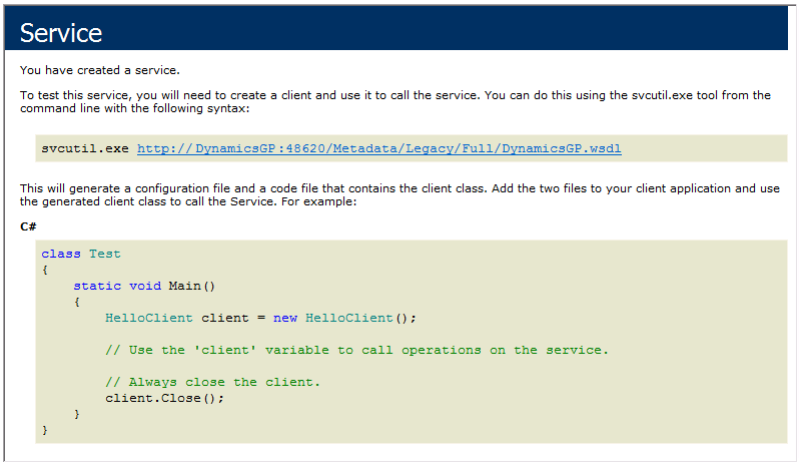
To verify the Dynamics GP service is operational, complete the following steps while logged in to the server:

1. **Open a web browser.**
The web browser will be used to display information about the endpoint that applications use to interact with the service.

2. **Verify the Dynamics GP service legacy endpoint.**
In the web browser, enter the URL to display the legacy endpoint of the Dynamics GP service. The URL for the legacy endpoint will have the form:

    http://*machine_name: port*/DynamicsGPWebServices

Replace *machine_name* with the name of the server onto which you installed Web Services for Microsoft Dynamics GP. The port value is typically 48620.



3. **Verify the Dynamics GP service native endpoint.**
   In the web browser, enter the URL to display the native endpoint of the Dynamics GP service. The URL for the native endpoint will have the form:

   http://*machine_name: port*/Dynamics/GPService

   Replace *machine_name* with the name of the server onto which you installed Web Services for Microsoft Dynamics GP. The port value is typically 48620.

   Close the browser when you have finished.

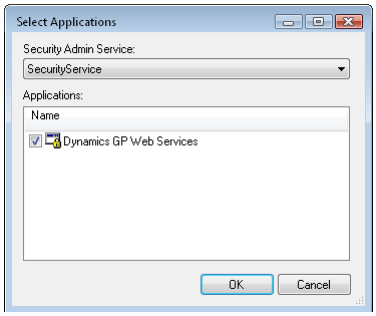
Dynamics Security Service

To verify the Dynamics Security service, complete the following steps:

1. **Open the Dynamics Security Console.**
   Choose the Dynamics Security Console from the Administrative Tools group, accessed through the Start menu. After a few moments, the Dynamics Security Console will be displayed.

2. **Select the application to manage.**
   Select the Microsoft Dynamics Security node in the left pane of the console. In the Action menu, choose Select Applications. The Select Applications window will appear.

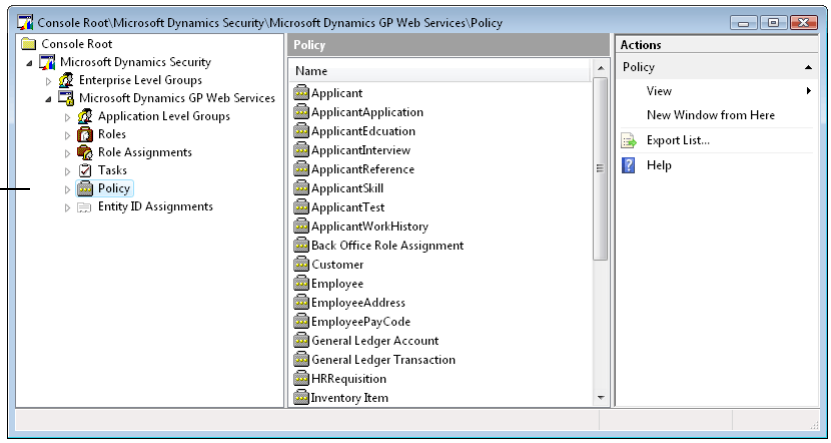
3. **Choose the Dynamics GP Web Services application.**
   In the Select Applications window, choose SecurityService in the drop-down list, and then mark the Dynamics GP Web Services application.



Click OK to close the window. Additional nodes will be added in the left pane of the Dynamics Security Console.

4. **Select the Policy node.**
Expand the Microsoft Dynamics Security node, and then expand the DynamicsGPWebServices node. Select the Policy node. A list of policy categories should be displayed. If it is, the Dynamics Security Service and its interaction with the Dynamics GP service are operating properly.

Select the Policy node. A list of policy categories should be displayed.



When you have finished, close the Dynamics Security Console.

User account summary

Two user accounts are used for a Web Services for Microsoft Dynamics GP installation. These user accounts are:

- The account the installer for Web Services for Microsoft Dynamics GP is run as. (Referred to as the **installation account**)
- The account supplied during the installation that the Microsoft Dynamics GP Service Host will run as. (Referred to as the **application account**)

Installation account

This is the account under which the installer for Web Services for Microsoft Dynamics GP is run. Typically, the initial configuration performed with the Web Services for Microsoft Dynamics GP Configuration Wizard is also done under this user account. In addition to being an administrator on the system on which web services is being installed, this account is used for the following:

- Added to the Superuser role for the Dynamics GP web service
- Added as a Security Administrator for the Dynamics Security service
- An ADAM administrator (Windows Server 2003) or ADLDS administrator (Windows Server 2008) if security data is being stored in ADAM
- Owner of the SQL database that contains the security data used for Web Services for Microsoft Dynamics GP (if you chose to store security data in SQL Server, and the installer created the database)

Application account

This is the account supplied during the Web Services for Microsoft Dynamics GP installation. It is used for the following:

- Account for the Microsoft Dynamics GP Service Host
- Reader of ADAM if security data is being stored in ADAM
- Reader of AzMan
- User for SQL Server and the databases used for Microsoft Dynamics GP

What to do next

After the Web Services for Microsoft Dynamics GP have been installed and verified, consider taking the following steps:

- Set up the security for the Dynamics GP web service. Refer to Part 3, **Security**, for details about security configuration.
- Learn about actions you will need to take in the day-to-day operation of the web services. Details are found in Part 4, **Running the Web Service**.
- To learn about developing applications that use the Web Services for Microsoft Dynamics GP, install the Web Services for Microsoft Dynamics GP Software Development Kit (SDK).

Removing web services

If you need to remove Web Services for Microsoft Dynamics GP from your server, be aware that the removal is done in two places. If you want to remove web services completely, do the following:

1. **Remove the system and company objects.**
   Use the Web Services for Microsoft Dynamics GP Configuration Wizard to remove the system and company objects.

2. **Remove the Web Services for Microsoft Dynamics GP installation.**
   Use the Web Services for Microsoft Dynamics GP installer to remove files and infrastructure that was placed by the installer.

If you want to move the Web Services for Microsoft Dynamics GP to a different server, you can leave the system and company objects in place. Use the remove option for the Web Services for Microsoft Dynamics GP installer. Then re-install the Web Services for Microsoft Dynamics GP onto the new server. When asked by the installer, point to your existing Microsoft Dynamics GP data that already has the system and company objects for web services.

Chapter 5: Management Tools Installation

The Management Tools for Microsoft Dynamics GP Web Services consist of the Microsoft Dynamics Security console and the Microsoft Dynamics GP Web Service Exception Management console. These tools are automatically installed on the computer that is running the Web Services for Microsoft Dynamics GP. The Management Tools Installer allows these tools to be installed on other computers. The following topics are discussed:

Prerequisites

To use the Management Tools for Microsoft Dynamics GP Web Services, your system must have the following:

- Microsoft .NET Framework 2.0
- Microsoft Management Console (MMC) 3.0

If you are using Windows XP or Windows Server 2003 you may need to add these components. Later versions of Windows will already have them. The Microsoft .NET Framework 2.0 can be downloaded from the web site update.microsoft.com. The MMC 3.0 is available for download from www.microsoft.com. Search for Knowledge Base article KB907265.

In the situation where the Web Services for Microsoft Dynamics GP have been installed for a network that does not have a domain controller, you cannot use the Management Tools for Microsoft Dynamics GP. The services must be administered from the server where they were installed.

Installing the management tools

Complete the following steps to install the Microsoft Dynamics GP Web Services Management Tools.

1. **Start the installer.**
   Choose the appropriate installer, based on whether you are using a 32-bit or 64-bit version of Windows.

Version	Installer
32-bit	Microsoft_DynamicsGP11_WebServicesMgmtTools_x86_en-us.msi
64-bit	Microsoft_DynamicsGP11_WebServicesMgmtTools_x64_en-us.msi

2. **Acknowledge the welcome screen.**
   Click Next to continue.

3. **Read and acknowledge the license agreement.**
   After reading and accepting the terms of the license agreement, click Next to continue.

4. **Enter the URL for the Dynamics GP service.**
   The typical URL for the Dynamics GP service is:

   http://*machine*:*port*/DynamicsGPWebServices/DynamicsGPService.asmx

   Notice this URL contains a port number. The port value **48620** is the default value that will be used when the Dynamics GP service is installed. Use this value when entering the URL.

   For example if the machine running the Dynamics GP service was named GPServer, the URL would be:

   http://GPServer:48620/DynamicsGPWebServices/DynamicsGPService.asmx

   If this port value doesn't work to access the service, you will need to contact your administrator to find what port the Dynamics GP service is running on.

5. **Enter the URL for the Dynamics Security Administration service.**
   The typical URL for the Microsoft Dynamics Security Administration service is:

   http://*machine*:*port*/DynamicsAdminService.asmx

   Notice this URL contains a port number. The port value **48621** is the default value that will be used when the Microsoft Dynamics Security Administration service is installed. Use this value when entering the URL.

   For example if the machine running the Microsoft Dynamics Security Administration service was named GPWebService, the URL would be:

   http://GPWebService:48621/DynamicsAdminService.asmx

   If this port value doesn't work to access the service, you will need to contact your administrator to find what port the Microsoft Dynamics Security Administration service is running on.

   Press the TAB key to accept the URL values entered, and then click Next to continue.

6. **Begin the installation.**
   Click Install to begin installing the management tools.

7. **Finish the installation.**
   After the management tools are installed, click Finish to complete the installation.

Required roles and permission

Refer to Chapter 6, "Web Services Security," for detailed information about assigning roles.

To use the Microsoft Dynamics Security console and the Microsoft Dynamics GP Web Service Exception Management console, a user must be assigned to the required roles and permission.

Dynamics Security console

To access the Microsoft Dynamics Security console, a user must be assigned to be a **Security Administrator** for the service. To access the Policy node displayed in the Microsoft Dynamics Security console, a user must also be assigned to the Policy **Administrator** role, or to the **Superuser** role.

Exception Management console

To access the Microsoft Dynamics GP Web Service Exception Management console, the user must be assigned to the **Error Viewer** role for all companies.

Accessing the management tools

The Management Tools Installer creates shortcuts in the Administrative Tools program group for the two consoles that it installs. Choose the item from the group to display the corresponding console.

The Dynamics Security console and the Exception Management console have a significant amount of data to retrieve. They can take a few moments to open and display.

Part 3: Security

This portion of the documentation provides detailed information about managing security for the Web Services for Microsoft Dynamics GP. The following items are discussed:

- Chapter 6, "Web Services Security," explains how to configure and control security access for the Dynamics GP service.
- Chapter 7, "Policy," describes how policy is used to control service operations.
- Chapter 8, "Authentication and Encryption," describes how to control what authentication method is used for the services.

Chapter 6: Web Services Security

Because the Web Services for Microsoft Dynamics GP can access sensitive data, it's important that proper security is applied for the Dynamics GP service. Information about web service security is divided into the following sections:

Overview

The Microsoft Dynamics Security Service provides security features for various Microsoft Dynamics applications and features, such as Web Services for Microsoft Dynamics GP. The Microsoft Dynamics Security Service controls access to the operations that can be performed by users of the Dynamics GP service.

Security Administrator

The Security Administrator uses the Microsoft Dynamics Security Console to configure which users have access to service operations. A user must be designated as a Security Administrator in order to access the Microsoft Dynamics Security Console and configure security settings.

The user who initially installed Web Services for Microsoft Dynamics GP is automatically a Security Administrator.

To designate which users will be Security Administrators for the Microsoft Dynamics Security Service, complete the following steps:

1. **Select the Microsoft Dynamics Security node.**
   In the left pane of the Dynamics Security Console, select the Microsoft Dynamics Security node.

2. **Choose to define Security Administrators.**
   In the Action menu, choose Define Security Administrators. The Security Administrators window will appear.

3. **Add or remove users.**
   Click Add to select additional users to become Security Administrators. To remove current users, select them in the list and click Remove.

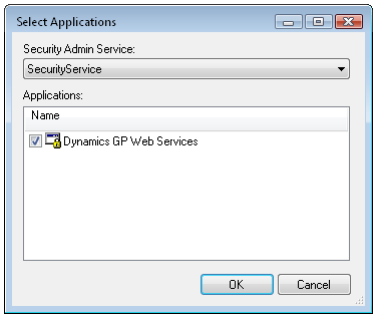
4. **Close the Security Administrators window.**
   Click OK to close the window and save your changes.

Selecting applications

Before you can control security settings, you must select the applications that you want to administer security for. To select applications, complete the following steps:

1. **Select the Microsoft Dynamics Security node in the left pane of the Dynamics Security Console.**

2. **Choose to select applications to administer.**
   In the Action menu, choose Select Applications. The Select Applications window will appear.



3. **Select the Security Administration Service.**
   This is the service that controls administration for the Microsoft Dynamics Security Service.

4. **Mark the applications to administer security for.**
   The available applications for the selected security administration service will be listed. For example, mark the Dynamics GP Web Services application to configure security settings for it.

5. **Close the Select Applications window.**
   Click OK to close the window and save your changes.

Administering security

As you configure security settings with the Dynamics Security Console, it's important to understand when those changes will become effective.

To improve the performance of the Microsoft Dynamics Security Service, the various security settings for each application are cached. This cache is refreshed by default every 20 minutes. When you make changes to the security settings, the changes will not become effective until the cache is refreshed. This could be **up to 20 minutes** from the time the changes are made.

The web services administrator can change the cache refresh interval to a lower value (with a minimum of 5 minutes) by editing the configuration for the application. For example, to change the cache timeout for the Dynamics GP service, you would edit the **DynamicsSecurity.config** file for this application, typically found at the location:

C:\Program Files\Microsoft Dynamics\GPWebServices\ServiceConfigs\DynamicsSecurity.config

The following key would be added to the <appSettings> section of this configuration file:

<add key= "AzManCacheRefreshInterval" value="300000"/>

The interval is specified in milliseconds, so divide by 60,000 to see the time in minutes. The previous setting will set the interval to the minimum 5 minutes.

Tasks

Operations are the individual actions that can be performed by the application for which security is being configured. For instance, the operations that can be performed by the Dynamics GP service are displayed as operations in the Dynamics Security console.

Tasks provide a way to group related operations together. A task can contain the following:

- Individual operations
- Other tasks

Predefined tasks

Applications typically have several tasks already defined for them. For instance, the Dynamics GP Web Services application has the **View Commissions** task defined. This task contains the **Query Salesperson Commissions** and **View Salesperson Commissions** operations.

One predefined task has special importance. The **View Company Information** task contains all of the operations needed to interact with the Dynamics GP service. This task is automatically assigned to every role that is created. It's important that you don't remove any operations from the View Company Information task. Doing so could prevent users from accessing the Dynamics GP service.

Creating tasks

You can create additional tasks to manage security access within an application. To create a new task, complete the following steps:

1. **Select the Tasks node in the left pane of the Dynamics Security Console.**

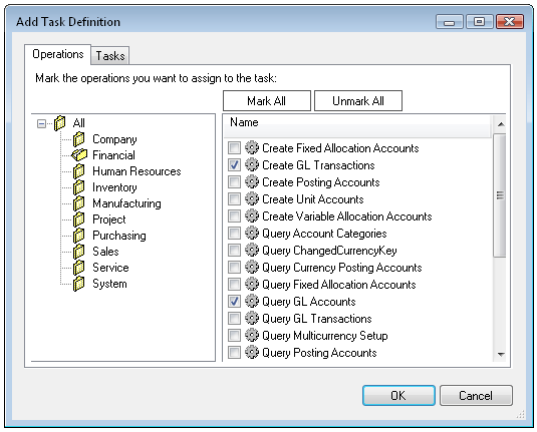
2. **Choose to create a new task.**
   In the Action menu, choose New. The New Task window will appear.

3. **Name the task.**

4. **Provide a task description.**
   The description will be displayed in the Actions pane when you select the task in the Dynamics Security Console.

5. **Select the keyword for the new task (optional).**
   The keyword indicates in what area of Microsoft Dynamics the task applies.

6. **Add operations or other tasks to the new task.**
   Click the Add button to display the Add Task Definition window. Use this window to select the individual operations and other tasks you want to include in the new task. Click OK to add the operations and tasks.



7. **Save the task definition.**
   Click OK to save the new task definition.

Modifying tasks

You can modify tasks that have already been created for an application. To modify a task, complete the following steps:

1. **Select the Tasks node in the left pane of the Dynamics Security Console.**

2. **Select the task you want to modify.**

3. **Choose to modify the task.**
   In the Action menu, choose Properties. The properties for the task will be displayed. Make the necessary changes to the task and click OK to save them.

Copying tasks

You can create a new task by starting with a copy of an existing task. This is useful when the new task has many characteristics that are the same as those of an existing task. To copy a task, complete the following steps:

1. **Select the Tasks node in the left pane of the Dynamics Security Console.**

2. **Select the task you want to copy.**

3. **Choose to copy the task.**
   In the Action menu, choose Copy. The Copy Task window will be displayed. Make the necessary changes to the new task and click OK to save them.

Deleting tasks

To delete a task, complete the following steps:

1. **Select the Tasks node in the left pane of the Dynamics Security Console.**

2. **Select the task you want to delete.**

3. **Choose to delete the task.**
   In the Action menu, choose Delete. A dialog will be displayed, asking you whether you want to delete the task. Click Yes to delete the task, or No to cancel the delete operation.

Roles

A role contains a set of operations, tasks, or other roles. Roles are used to group together the actions that can be performed by users who will be assigned to the role.

Predefined roles

Applications typically have several roles already defined for them. For instance, the Dynamics GP Web Services application has the **Sales Representative** role defined. This role contains tasks that would be performed by somebody assigned to this role, such as **Manage All Sales Transactions** and **Manage Customers**.

Special predefined roles

The following is a list of the special predefined roles that are included with the Dynamics Security Service:

Error Viewer Users assigned to this role will be able to view error information that is logged by the Dynamics GP service. Typically, this information is viewed through the Dynamics GP Web Service Exception Management Console.

Entity Id Assignment Administrator Users assigned to this role will be able to manage entity ID assignments for the Dynamics GP service.

Policy Administrator Users assigned to this role will be able to configure policies that are used to configure Dynamics GP service operations.

Superuser Users assigned to this role will have access to all operations that have been defined, without any restrictions.

Do not assign the Superuser role widely. Doing so makes the system less secure.

Creating roles

You can create additional roles to manage security access within an application. To create a new role, complete the following steps:

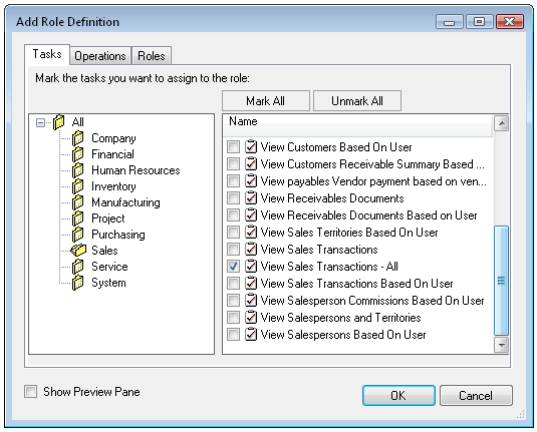
1. **Select the Roles node in the left pane of the Dynamics Security Console.**

2. **Choose to create a new role.**
   In the Action menu, choose New. The New Role window will appear.

3. **Name the role.**

4. **Provide a role description.**
   The description will be displayed in the Actions pane when you select the role in the Dynamics Security Console.

5. **Add tasks, operations, or other roles to the new role.**
   Click the Add button to display the Add Role Definition window. Use this window to select the individual tasks, operations, and other roles you want to include in the new role. Click OK to add the selected items.



Every role created will automatically include the View Company Information task. The operations in this task are required for users assigned to the role to use the Dynamics GP service. Don't delete operations from this task.

6. **Save the role definition.**
   Click OK to save the new role definition.

Modifying roles

You can modify roles that have already been created for an application. To modify a role, complete the following steps:

1. **Select the Roles node in the left pane of the Dynamics Security Console.**

2. **Select the role you want to modify.**

3. **Choose to modify the role.**
   In the Action menu, choose Properties. The properties for the role will be displayed. Make the necessary changes to the role and click OK to save them.

Copying roles

You can create a new role by starting with a copy of an existing role. This is useful when the new role has many characteristics that are the same as those of an existing role. To copy a role, complete the following steps:

1. **Select the Roles node in the left pane of the Dynamics Security Console.**

2. **Select the role you want to copy.**

3. **Choose to copy the role.**
   In the Action menu, choose Copy. The Copy Role window will be displayed. Make the necessary changes to the new role and click OK to save them.

Deleting roles

To delete a role, complete the following steps:

1. **Select the Roles node in the left pane of the Dynamics Security Console.**

2. **Select the role you want to delete.**

3. **Choose to delete the role.**
   In the Action menu, choose Delete. A dialog will be displayed, asking you whether you want to delete the role. Click Yes to delete the role, or No to cancel the delete operation.

Enterprise level groups

Groups are used to create collections of Windows users for whom security access is being controlled. Enterprise Level groups are available to use in all of the applications for which the Microsoft Dynamics Security Service is controlling access.

Enterprise level groups are used when you're managing security for several applications. Since the same group can be used within multiple applications, adding or removing a user from an enterprise level group will add or remove their access to multiple applications in one step.

Creating an enterprise level group

To create a new enterprise level group, complete the following steps:

1. **Select the Enterprise Level Groups node in the left pane of the Dynamics Security Console.**

2. **Choose to create a new enterprise level group.**
   In the Action menu, choose New. The New Enterprise Level Group window will appear.

3. **Name the group.**

4. **Provide a group description.**
   The description will be displayed in the Actions pane when you select the enterprise level group in the Dynamics Security Console.

5. **Add members to the group.**
   Display the User Members or Group Members tabs to add individual users or other groups to the group being created.

6. **Save the enterprise level group definition.**
   Click OK to save the new enterprise level group definition.

Modifying enterprise level groups

You can modify enterprise level groups that have already been created. To modify an enterprise level group, complete the following steps:

1. **Select the Enterprise Level Groups node in the left pane of the Dynamics Security Console.**

2. **Select the group you want to modify.**

3. **Choose to modify the group.**
   In the Action menu, choose Properties. The properties for the enterprise level group will be displayed. Make the necessary changes to the group and click OK to save them.

Copying enterprise level groups

You can create a new enterprise level group by starting with a copy of an existing group. This is useful when the new group has many characteristics that are the same as those of an existing enterprise level group. To copy a group, complete the following steps:

1. **Select the Enterprise Level Groups node in the left pane of the Dynamics Security Console.**

2. **Select the enterprise level group you want to copy.**

3. **Choose to copy the enterprise level group.**
   In the Action menu, choose Copy. The Copy Enterprise Level Group window will be displayed. Make the necessary changes to the new group and click OK to save them.

Deleting enterprise level groups

To delete an enterprise level group, complete the following steps:

1. **Select the Enterprise Level Groups node in the left pane of the Dynamics Security Console.**

2. **Select the group you want to delete.**

3. **Choose to delete the group.**
   In the Action menu, choose Delete. A dialog will be displayed, asking you whether you want to delete the enterprise level group. Click Yes to delete the group, or No to cancel the delete operation.

Application level groups

Groups are used to create collections of Windows users for whom security access is being controlled. Application Level groups are available to use only within the application for which they are defined. For example, any application level groups defined for the Dynamics GP Web Services application will be available to use only within that application.

Creating an application level group

To create a new application level group, complete the following steps:

1. **Select the Application Level Groups node in the left pane of the Dynamics Security Console.**

2. **Choose to create a new application level group.**
   In the Action menu, choose New. The New Application Level Group window will appear.

3. **Name the group.**

4. **Provide a group description.**
   The description will be displayed in the Actions pane when you select the application level group in the Dynamics Security Console.

5. **Add members to the group.**
   Display the User Members or Group Members tabs to add individual users or other groups to the group being created.

6. **Save the application level group definition.**
   Click OK to save the new application level group definition.

Modifying application level groups

You can modify application level groups that have already been created for an application. To modify an application level group, complete the following steps:

1. **Select the Application Level Groups node in the left pane of the Dynamics Security Console.**

2. **Select the group you want to modify.**

3. **Choose to modify the group.**
   In the Action menu, choose Properties. The properties for the application level group will be displayed. Make the necessary changes to the group and click OK to save them.

Copying application level groups

You can create a new application level group by starting with a copy of an existing group. This is useful when the new group has many characteristics that are the same as those of an existing application level group. To copy a group, complete the following steps:

1. **Select the Application Level Groups node in the left pane of the Dynamics Security Console.**

2. **Select the application level group you want to copy.**

3. **Choose to copy the application level group.**
   In the Action menu, choose Copy. The Copy Application Level Group window will be displayed. Make the necessary changes to the new group and click OK to save them.

Deleting application level groups

To delete an application level group, complete the following steps:

1. **Select the Application Level Groups node in the left pane of the Dynamics Security Console.**

2. **Select the group you want to delete.**

3. **Choose to delete the group.**
   In the Action menu, choose Delete. A dialog will be displayed, asking you whether you want to delete the application level group. Click Yes to delete the group, or No to cancel the delete operation.

Role assignments

A role assignment consists of the following:

- A role (with its associated tasks and operations)
- A company or companies
- A user or group for which access is being granted

When the role assignment is created, the users or groups of users will have access to the items in the role for the specified company or companies.

Adding a role assignment

To add a new role assignment, complete the following steps:

1. **Select the Role Assignments node in the left pane of the Dynamics Security Console.**

2. **Choose to add a new role assignment.**
   In the Action menu, choose Add. The Add Role Assignments window will appear.

3. **Select the role.**
   In the Role drop-down list, select the role that you want to assign users or groups to.

4. **Add the users and groups.**
   Click the Add Windows Users button to add individual windows users to the role assignment. Click the Add Groups button to add application level groups or enterprise level groups to the role assignment.

5. **Specify the company access.**
   Indicate which company or companies for which the access applies. You can choose All Companies, or you can choose Select Individual Companies. If you choose individual companies, mark the appropriate companies in the list.

6. **Save the new role assignment.**
   Click OK to save the new role assignment.

Deleting a role assignment

To delete a role assignment, complete the following steps:

1. **Select the Role Assignments node in the left pane of the Dynamics Security Console.**

2. **Select the role assignment you want to delete.**
   When you remove the role assignment, the users or groups will no longer have access to the items specified in the role.

3. **Choose to delete the role assignment.**
   In the Action menu, choose Delete. A dialog will be displayed, asking you whether you want to delete the role assignment. Click Yes to delete the role assignment, or No to cancel the delete operation.

Entity ID assignments

Windows User IDs can be associated with the following objects in Microsoft Dynamics GP:

- Back Office User
- Customer
- Employee
- Salesperson
- Sales Territory
- Vendor

These objects are referred to as *user-assignable business objects*. An entity ID assignment allows assigning a Windows User ID to one of these objects in Microsoft Dynamics GP. An entity ID assignment consists of the following:

- A Windows user ID
- The type of entity in Microsoft Dynamics GP
- A company or companies
- The back office ID to which the Windows user ID will be associated

This assignment is used by web service applications to display data that is specific to the user currently accessing the Dynamics GP web service. For instance, a Windows user assigned to a specifc salesperson ID could be restricted to see only their own salesperson commission information.

A Windows User ID can be assigned to more than one type of entity ID in Microsoft Dynamics GP. A Windows User ID should not be assigned to more than one entity ID of the same type. For example, a single Windows User ID should not be assigned to several different salesperson IDs.

Security for entity ID filtering

Additional security roles, operations, and tasks are defined for the Dynamics GP web service to support entity ID filtering. These roles, operations, and tasks indicate whether entity ID filtering will be applied for the current web service user.

For example, granting access to a role that contains the operation **Query Sales Orders** allows the user to retrieve any sales orders. Granting access to a role that contains the operation **Query Sales Orders Based On User** allows the user to retrieve only those sales orders that have an ID (such as the Salesperson ID) mapped to the current Windows User.

Roles that contain the tasks and operations that implement entity ID filtering have the word "Self" in their name. Users assigned to these roles will be able to see only objects that are associated to them based on the entity ID assignments. For example, the **Salesperson - Self** role provides access to customer, salesperson, and sales transaction information for the salesperson assigned to the current user.

Adding an entity ID assignment

To add a new entity ID assignment, complete the following steps:

1. **Select the Entity ID Assignments node in the left pane of the Dynamics Security Console.**

2. **Choose to add a new entity ID assignment.**
   In the Action menu, choose Add. The Add Entity ID Assignments window will appear.

3. **Select the Windows user.**
   Click Select Windows User to display the dialog used to select a Windows user. Specify the user for whom you are creating the entity ID assignment.

4. **Select the entity type.**
   This specifies the type of ID in Microsoft Dynamics GP to which you are assigning the Window ID. Choose one of the following:

   - Back Office User
   - Customer
   - Employee
   - Sales Territory
   - Salesperson
   - Vendor

5. **Specify the company access.**
   Indicate the company in Microsoft Dynamics GP for which the entity ID is defined. After a few moments, the IDs of the specified type will be listed.

6. **Filter the list of entity IDs (optional).**
   The list of available entitiy IDs can be quite large for some types, such as customers. The total number of IDs listed is limited to 250 at one time. If more entities are available, you must specify filter criteria to limit the number of IDs displayed. Type the filter text and click the Apply Filter button. For example, to list only those entities with IDs that begin with "G", enter that value and click Apply Filter. After a few moments, the list of IDs matching the filter criteria will be displayed.

The filter applied uses SQL criteria syntax. The value you enter will automatically be enclosed by % wildcard characters. If you entered ***Erin*** *as the filter text, the IDs matching the criteria* ***%Erin%*** *will be displayed.*

   To remove the filte criteria, clear the text from Filter by ID and click the Apply Filter button.

7. **Select the back office entity ID.**
   In the list of available entity IDs, select the ID to assign to the selected Windows User ID.

8. **Save the new entity ID assignment.**
   Click OK to save the new entity ID assignment and close the window. Click Apply to save the entity ID assignment, leaving the window open to add another.

Deleting an entity ID assignment

To delete an entity ID assignment, complete the following steps:

1. **Select the Entity ID Assignments node in the left pane of the Dynamics Security Console.**

2. **Select the Entity ID assignment you want to delete.**
   When you remove the entity ID assignment, the Windows user will no longer be associate with the specified ID in Microsoft Dynamics GP.

3. **Choose to delete the entity ID assignment.**
   In the Action menu, choose Delete. A dialog will be displayed, asking you whether you want to delete the entity ID assignment. Click Yes to delete the entity assignment, or No to cancel the delete operation.

Chapter 7: Policy

The policy system for the Dynamics GP service allows the web service administrator and the application using the service to control how business objects are created, updated, or deleted. The following items are discussed:

Overview

Each create, update, and delete operation has a policy object that is passed with the operation. This policy object specifies the set of behaviors for the operation. Each behavior controls one characteristic for the operation being performed. For instance, the policy for the CreateCustomer web method has the behavior named "Create Active Behavior". This behavior controls whether the customer being created is set to the active or inactive state.

Behaviors are classified as internal or external. An *internal behavior* is one that can be specified only through the Dynamics Security Console. An *external behavior* is one that can be specified by the application that is calling the service method and passing in the policy object.

Policy administrator

The policy administrator uses the Microsoft Dynamics Security Console to configure the various policies for the Dynamics GP service. To manage polices with the Microsoft Dynamics Security Console, a user must be designated as a Security Administrator. The user must also be assigned to the **Policy Administrator** role. When you assign a user to the Policy Administrator role, the user will be able to manage policies for all companies. Refer to *Role assignments* on page 48 for details about assigning roles.

The user who initially installed Web Services for Microsoft Dynamics GP is automatically a Security Administrator. That user is also assigned to the Superuser role, which has access to the Manage Policies task.

Policy instances

Each company has a set of default policies that are available. There is one default policy for each web service operation that requires a policy. Within a company, additional versions of the policy (with different behavior settings) can be created for each role defined in the Dynamics Security Service. Each of these is called a *policy instance*. When a web service application retrieves a policy to use, the Dynamics GP service applies logic to ensure the appropriate policy instance is returned.

Applications that call the Dynamics GP service can specify the role to use for the service call. If a policy instance exists for that role, it will be used. Developers creating applications that use the Dynamics GP service are encouraged to not explicitly set the role. Instead, they should let the Dynamics GP service find what role the user of the application is assigned to, so the correct policy instance can be used.

Be aware that the Dynamics GP service will set the role for a user only if the user is assigned to a **single** role. If the user is assigned to more than one role, the role won't be set, and the default policy instance will be used. For this reason, it's a good idea to limit the number of roles you assign a user to.

Editing a policy instance

When you edit a policy instance, you are configuring the set of behaviors for that policy. To do this, complete the following steps in the Dynamics Security Console:

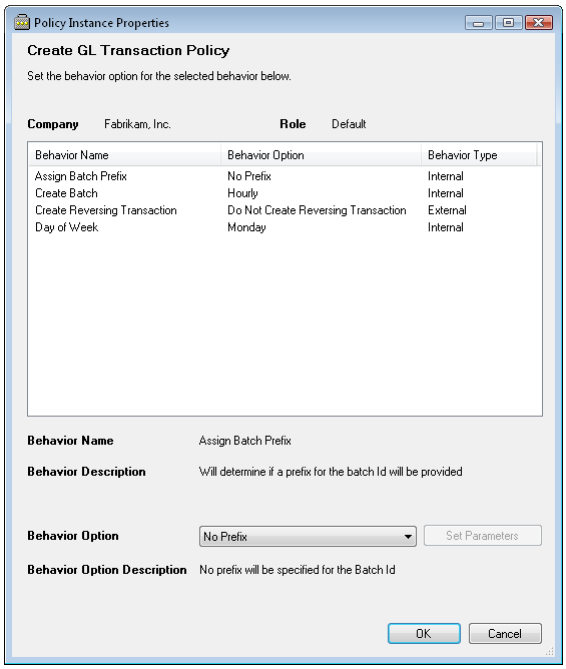
1. **Select and expand the Policy node in the left pane of the Dynamics Security Console.**

2. **Locate the policy that you want to edit.**
   Select the policy in the expanded tree view in the left pane of the Dynamics Security Console. It may take a few moments for the information about the policy to load.

3. **Select the company for which the policy instance applies.**

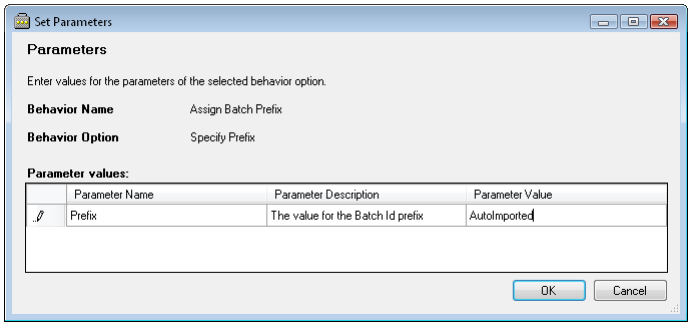
4. **Select the role for the policy instance you want to edit.**
   Choose Default to edit the policy instance that is used when no role is associated with the user.

5. **Edit the policy instance properties.**
   Click the Properties link in the Actions pane to display the Policy Instance Properties window. Within this window, you will edit the individual behaviors that are included in the policy. This window is shown in the following illustration:



6. **Edit the individual behaviors.**
   Select a behavior in the list. The details of the behavior will be displayed. Use the Behavior Option drop-down list to specify the behavior option that you want to use.

Some behavior options allow you to supply a specific value that will be used, such as a transaction date. If you select one of these behavior options, the Set Parameters button will become active. Click this button to open the Set Parameters window. In the Parameter Value column, supply the value to use for the parameter and click OK.



7. **Save the changes.**
   When you have finished making changes to the behaviors, click OK to save the policy instance.

Creating a new policy instance

To create a new policy instance, complete the following steps in the Dynamics Security Console:

1. **Select and expand the Policy node in the left pane of the Dynamics Security Console.**

2. **Locate the policy for which you want to create a new instance.**
   Select the policy in the expanded tree view in the left pane of the Dynamics Security Console. It may take a few moments for the information about the policy to load.

3. **Choose to create a new policy instance.**
   In the Action menu, choose New. The New Policy Instance window will appear.

4. **Select the company for which the new policy instance applies.**

5. **Select the role for which the new policy instance applies.**

6. **Edit the individual behaviors.**
   Select a behavior in the list. The details of the behavior will be displayed. Use the Behavior Option drop-down list to specify the behavior option that you want to use. Refer to the previous procedure, *Editing a policy instance* on page 52, for details about editing the new policy instance.

7. **Save the changes.**
   When you have finished making changes to the behaviors, click OK to save the new policy instance.

Deleting a policy instance

To delete a policy instance, complete the following steps in the Dynamics Security Console:

1. **Select and expand the Policy node in the left pane of the Dynamics Security Console.**

2. **Locate the policy for which you want to delete a policy instance.**
   Select the policy in the expanded tree view in the left pane of the Dynamics Security Console. It may take a few moments for the information about the policy to load.

3. **Select the company for which the policy instance applies.**

4. **Select the role for the policy instance you want to delete.**

5. **Delete the policy instance.**
   Click the Delete link in the Actions pane. A dialog will be displayed, asking you whether you want to delete the policy instance. Click Yes to delete the policy instance, or No to cancel the delete operation.

Chapter 8: Authentication and Encryption

As the administrator of the Web Services for Microsoft Dynamics GP, we encourage you to take the steps to fully secure them. You should understand the authentication mode used when accessing the services. You should also understand the encryption options available for the service messages. The following items are discussed:

Supported authentication methods

Two methods of authentication are supported when connecting to the Web Services for Microsoft Dynamics GP:

NTLM This the challenge/response authentication protocol used in Windows NT 4.0 and earlier.

Windows This method attempts to use Kerberos, the more secure authentication protocol used in Windows 2000 and later. If it cannot authenticate using Kerberos, it will fall back to NTLM authentication.

For the default installation of Web Services for Microsoft Dynamics GP, the following authentication methods are used for the Dynamics GP service:

- The legacy endpoint is configured to use NTLM authentication.
- The native endpoint is configured to use Windows authentication.

Registering the SPN

If you have chosen to use Kerberos authentication, you must register the SPN (Service Principal Name) under the following circumstances:

- Kerberos authentication mode is used.
- The user under which the Microsoft Dynamics GP Service Host is running is a domain user. You must also include this fully-qualified domain name of this user in the <userPrincipalName> attribute for the configuration file of your web service application.

If these conditions are true, you must have the Domain Administrator register the SPN for the domain account. To do this, complete the following steps:

1. **Obtain the SetSPN.exe command-line tool.**
   To obtain this tool, go to the following location to download the Windows Server 2003 Service Pack 2 32-bit Support Tools:

   http://go.microsoft.com/fwlink/?LinkId=100114

2. **Open a command prompt.**
   In the Start menu, choose Run. Type **cmd** and click OK.

3. **Use the SetSPN.exe tool to register the machine name and user.**
   To do this, enter the following command:

   ```
   setspn -A HTTP/ServerName Domain\UserName
   ```

   Replace *ServerName* with the machine name on which web services are being run. Replace *Domain* and *UserName* with the domain and name for the user account under which the Microsoft Dynamics GP Service Host is being run.

4. **Use the SetSPN.exe tool to register the fully-qualified machine name.**
   To do this, enter the following command:

   ```
   setspn -A HTTP/ServerName Domain\UserName
   ```

   Replace *ServerName* with the fully-qualified domain name (FQDN) of the machine on which the Microsoft Dynamics GP Service Host is being run. (You can find this name in the properties for My Computer.) Replace *Domain* and *UserName* with the domain and name for the user account under which the Microsoft Dynamics GP Service Host is being run.

Encryption

Because the data being accessed from Microsoft Dynamics GP through the Dynamics GP service may be sensitive, encryption can be used to help secure the data. The encryption options available depend in which endpoint is being used. The *mode* attribute of the <security> node in the WSBindings.config controls what type of encryption is used for the endpoint.

Legacy endpoint

With the default settings, the legacy endpoint uses no encryption for the SOAP messages that are exchanges with the Dynamics GP service. There are two common ways to encrypt the data exchanged with the Dynamics GP service:

- You can set the *mode* attribute of the <security> node of the WSBindings.config to "Message". This implements message security, and causes the SOAP messages to be encrypted. The following sample shows this setting in the configuration file.

```
<basicHttpBinding>
    <binding name="BasicHttpBindingTarget">
        <security mode="Message">
            <transport clientCredentialType="Ntlm"/>
        </security>
    </binding>
</basicHttpBinding>
```

Be aware that some applications that support the BasicHttpBinding used for the legacy endpoint do not support encrypted SOAP messages.

- You can set the *mode* attribute of the <security> node of the WSBindings.config to "Transport". This indicates that the transport layer will be responsible for encrypting the SOAP message data. You must then set up the WCF endpoint to use transport security. Search for "HTTP Transport Security" on MSDN (msdn.microsoft.com) for details about how to implement this.

Native endpoint

With the default settings, the native endpoint uses message security. This mean that the SOAP messages that are exchanged with the Dynamics GP service are encrypted. This provides better default security than the legacy endpoint.

You may see improved performance by switching from message security to transport security. This indicates that the transport layer will be responsible for encrypting the SOAP message data. You must then set up the WCF endpoint to use transport security. Search for "HTTP Transport Security" on MSDN (msdn.microsoft.com) for details about how to implement this.

PART 4: RUNNING THE WEB SERVICE

Part 4: Running the Web Service

This portion of the documentation provides information about the day-to-day operation of the Web Services for Microsoft Dynamics GP. The following items are discussed:

- Chapter 9, "Troubleshooting," discusses how to troubleshoot issues that occur with the services and the applications that use them.
- Chapter 10, "Logging and Auditing," describes how to log the events that occur for the services.
- Chapter 11, "Making Backups," explains how to include the web services in the backup strategy for the Microsoft Dynamics GP installation.
- Chapter 12, "Adding Additional Companies," describes how to add web service support to additional companies added to Microsoft Dynamics GP.
- Chapter 13, "Repairing Web Services," explains how to perform repair operations on a Web Services for Microsoft Dynamics GP installation.

Chapter 9: Troubleshooting

If you encounter problems with the Web Services for Microsoft Dynamics GP, the following sections may be helpful. They describe some of the most common situations that can occur while running the web services. The following items are discussed:

Exceptions

The following are common exceptions that may occur when applications are working with the Dynamics GP service:

An unhandled system exception occurs

A system exception occurs when an unexpected event prevents the normal completion of a method for the Dynamics GP Service. A system exception returns the following message:

"The application encountered an unhandled system exception. Contact your system administrator for details."

The Dynamics GP Web Service Exceptions console displays the details for each system exception. If you are logged into the server on which Web Services for Microsoft Dynamics GP is installed, or you have installed the Management Tools for Microsoft Dynamics GP Web Services, you can access the Exceptions console. It is found in the Administrative Tools group accessed through the Start menu. The additional information the console provides may help identify the source of the system exception.

Another source of exception information is the system's event logs. Use the system event viewer to open and review the system logs. Relevant errors, warnings and informational updates for the Dynamics GP service may be found in the Application log.

Insufficient authorization to perform this action

When attempting to use the Dynamics GP service, an exception may return the message:

"Insufficient authorization to perform this action."

This exception indicates the current user does not have sufficient security authorization to perform the requested operation. Logging on as a user with the necessary security authorization should resolve the exception. Another option is to assign the current user to a role that includes the required security authorization.

This error may also occur when an application is using the "working on behalf of another user" option. This option allows the user and role performing the operation to be different from the logged-on user. The user that is running the application may not be assigned to the "Work On Behalf Of" task, or the user the application is working on behalf of may not have security access to the operations the application is performing. Use the Security console to view the role or roles assigned to the user.

Entity ID filtering is another possible source of this error. If the application is requesting filtered results, users can receive this error if they don't have access to the restricted operation used for the entity ID filtering. They may also receive this error if the entity ID assignment that maps a Windows User ID to a back office object ID cannot be found.

Service does not respond

The following issues can cause the Dynamics GP service to stop responding:

Service host not running

If the Microsoft Dynamics GP Service Host service is not running, the Dynamics GP service will not respond. Use the Services window to verify that the service host is running. This window is found in the Administrative Tools group accessed through the Start menu.

If the Microsoft Dynamics GP Service Host will not stay running, there is likely a configuration problem for the service. Use the system event viewer to open and review the system logs. Relevant errors, warnings and informational updates for the Microsoft Dynamics GP Service Host can be found in the Application log. Correct the error and then restart the service host.

Extensions

Applications that access the Dynamics GP service may have extensions that you needed to install. These extensions require changes to the BusinessObjectsFile.config (in the ServiceConfigs folder of the Dynamics GP web service installation) to register the extension for a service event. If the edit creates an error in the contents of the configuration file, the Dynamics GP service may no longer respond.

Always make a backup copy of the BusinessObjectsFile.config prior to editing the file. Store the copy to a safe location. Use the backup copy to restore the Dynamics GP service if problems occur.

If changes to the BusinessObjectsFile.config prevent a method from responding, open the Exception Management Console to identify the source of the error. Edit the BusinessObjectsFile.config to correct the specified error. Restart the Microsoft Dynamics GP Service Host to ensure the changed BusinessObjectsFile.config is used.

Configuration file changes

Changes made to the configuration files for the Microsoft Dynamics GP Service Host or for the service endpoints can cause the Dynamics GP service to stop responding.

It's a good idea to make a backup copy of a configuration file prior to editing it. Store the copy to a safe location. Use the backup copy to restore the configuration file if problems occur.

Security

The following is a list of issues associated with the Dynamics Security Administration service:

A security authorization change is not used

A change occurs to a user's security authorization to add or restrict access to a service operation. Testing by that user reveals the ability to perform the specified operation remains unchanged.

To optimize the responsiveness of services, a memory cache stores the security settings. The security service reloads the cache at 20 minute intervals. Changes to security authorization will not take effect until they are loaded into the security cache.

If testing of a new security authorization change does not immediately show the expected result, re-test the operation after 20 minutes. The delay allows the security service to update its security cache with your change. Restarting the Microsoft Dynamics GP Service Host can force an immediate reload of the security cache. This should be performed only after careful consideration of the impact it will have on current users of the Dynamics GP service.

The security service is not working

The Dynamics Security Administration service uses two system logs to record error and warning messages. The Dynamics and ADAM (DynamicsSecurityService) logs contain error and warning messages associated with the Dynamics Security Administration service. If the security service is not running or is producing error messages, use the system event viewer to find detailed errors or warnings messages that specify the source of the problem.

Policy

The following is an issue that occurs when using policies with the Dynamics GP service:

The expected policy is not used

Various Dynamics GP service operations can use a policy to control the characteristics of an operation. The user role determines the specific policy instance used by the operation. If an operation does not use the expected policy, view the user's role assignments in the Dynamics Security console. A user that has more than one role will always use the default policy for the operation. To ensure a specific policy is used with an operation, assign the user to a single role.

Timeout issues

When a web service application processes large numbers of documents or documents that contain large amounts of data, it may encounter timeout errors. It is possible to adjust the timeout behavior of the Dynamics GP service.

Applications that access the Dynamics GP Service can control the timeout length for the service requests they make. Refer to the information about creating proxy instances in the Web Service Programmer's Guide for details about setting timeout values for applications that access the Dynamics GP service.

Chapter 10: Logging and Auditing

When adminstering Web Services for Microsoft Dynamics GP, It can also be helpful to log actions performed by the services. Information about logging and auditing is divided into the following sections:

Dynamics GP service logging

The Dynamics GP service can log the security response for actions users are attempting to perform. For instance, the log could be used to show a user who was trying to access information for which they were not authorized.

Types of events

The Dynamics GP service can log the following events:

Success These are requests to perform operations in Dynamics GP service that were allowed by the current security settings. It's most useful to log these events when you're trying to assess the level of activity for the Dynamics GP service.

Fail These are requests to perform operations in the Dynamics GP service that were denied by the current security settings. It's most useful to log these events when your trying to track unauthorized activity for the Dynamics GP service.

Configuring logging

To enable logging, you must adjust some settings in the **DynamicsSecurity.config** file for the Microsoft Dynamics GP Service Host. This file is typically found at this location:

C:\Program Files\Microsoft Dynamics\GPWebServices\ServiceConfigs\

Using a text editor, open the DynamicsSecurity.config file. In the <appSettings> section of the file, you will see the keys that control logging.

Turning logging on or off

To turn on logging, set the following key to true:

<add key ="SecurityRuntimeAuditingIsActive" value="true"/>

Events to log

To specify which types of events to log, set the following key:

<add key ="SecurityRuntimeAuditLogType" value="SuccessFail"/>

The following table shows the possible values for this key:

Value	Description
Success	Log only successful access attempts.
Fail	Log only failed access attempts.
SuccessFail	Log both successful and failed access attempts.

Log location

To specify the location of the log, set the following key:

<add key ="SecurityRuntimeAuditLogFolder" value="C:\Program Files\Microsoft Dynamics\GPWebServices\Logs"/>

The user that the Microsoft Dynamics GP Service Host is being run as must have write access to the location that you specify.

Enabling logging for the endpoint

You must also enable security logging in the configuration file for each endpoint that you want to track. The configuration file for the native endpoint is **DynamicsGP.config**, while the configuration file for the legacy endpoint is **DynamicsGPLegacy.config**. These files are typically found at this location:

C:\Program Files\Microsoft Dynamics\GPWebServices\ServiceConfigs\

To turn on logging, set the following key in the configuration file to true:

<add key ="SecurityRuntimeAuditingIsActive" value="true"/>

Example log

The following shows a portion of a security audit log that was logging both successful and failed access attempts.

```
<!-------------------------------------------------------------------------------------------->
<!-- SecurityRuntimeService: created on 2010-02-21 16:45:53Z -->
<log action='CheckAccess' operation='View Customers' member='HORIZON\kberg' result='Success'
datetime='2010-02-21 16:45:55Z'>
    <context user='HORIZON\kberg' type='Scope'>
        <application name='Dynamics GP Web Services' key='25cc1a21-2cc4-4b13-a1c8-eea186fb688a' />
        <scope name='TWO' key='-1' />
    </context>
</log>
<log action='CheckAccess' operation='View Vendors' member='HORIZON\mallen' result='Fail'
datetime='2010-02-21 16:48:28Z'>
    <context user='HORIZON\mallen' type='Scope'>
        <application name='Dynamics GP Web Services' key='25cc1a21-2cc4-4b13-a1c8-eea186fb688a' />
        <scope name='TWO' key='-1' />
    </context>
</log>
<!-------------------------------------------------------------------------------------------->
```

Dynamics Security Admin web service logging

The Dynamics Security Admin web service can log the security configuration changes that were made to the web service installation.

Configuring logging

By default, the logging for te Dynamics Security Admin web service is enabled. To configure the logging, you must adjust some settings in the **DynamicsSecurityAdmin.config** file. This file is typically found at this location:

C:\Program Files\Microsoft Dynamics\GPWebServices\ServiceConfigs\

Using a text editor, open the DynamicsSecurityAdmin.config file. In the <appSettings> section of the file, you will see the keys that control logging.

Turning logging on or off

To turn on logging, set the following key to true:

<add key="SecuritySetupAuditingIsActive" value="true" />

Log location

To specify the location of the log, set the following key:

<add key="SecuritySetupAuditLogFile" value="C:\Program Files\Microsoft Dynamics\GPWebServices\SecuritySetupAudit.log" />

Example log

The following shows a portion of a security setup audit log that shows a security change that was made to assign a user to a role.

```
<log action='Create' type='RoleAssignment' name='Sales Representative' datetime='2010-03-01
18:22:33Z'>
    <context user='HORIZON\kberg' type='Application'>
        <application name='Dynamics GP Web Services' key='25cc1a21-2cc4-4b13-a1c8-eea186fb688a' />
    </context>
    <values>
        <fieldValues key='aaeb72e0-77f9-4925-ab9a-73012417fb37' />
        <members>
            <member value='HORIZON\mallen' />
        </members>
    </values>
</log>
```

Chapter 11: Making Backups

Web Services for Microsoft Dynamics GP is an important component of the Microsoft Dynamics GP installation. It should be included in the standard backup strategy you use to create backups for the accounting system. The following sections describe the specific areas you should consider:

SQL tables

Web Services for Microsoft Dynamics GP stores data in several tables managed by the SQL Server. Several tables are found in the system (DYNAMICS) database, while other tables are found in each company's database. When you create backups of these databases, the information in these tables should be included. They contain setup information for the services, policy configurations, and exception information.

SQL security database

If you chose to store security settings for Web Services for Microsoft Dynamics GP in a SQL database, then you should be sure to include this additional database in your backup strategy.

ADAM database

If you chose to store security settings in ADAM or ADLSD, then the ADAM database used by the Dynamics Security Services stores most of the security settings for the web services installation. You should create a backup for this database, to avoid having to re-create the security settings you have made.

The ADAM database file, Adamntds.dit, and the associated log files are found in Program Files\Microsoft ADAM\DynamicsSecurityService\Data. These files should be included as part of the regular backup plan of your organization. You can back up the directory stores using any standard backup program, such as the Backup Utility for Windows.

Restoring ADAM

When you restore a database to an existing ADAM instance, you must stop the ADAM instance before you run the restore operation. In addition, it is recommended that you move (or delete) the existing database and log files from the ADAM instance before beginning the restore operation.

Refer to the ADAM online help for details about performing these management tasks.

Authoritative Restore

If objects in the directory are inadvertently deleted or modified, and if those objects are replicated in a configuration set, you must authoritatively restore those objects so that the correct version of the objects is replicated. To authoritatively restore directory data, run the dsdbutil.exe utility (an ADAM command-line utility) after you have restored the data but before you restart the ADAM instance. With dsdbutil, you can mark directory objects for authoritative restore. When an object is marked for authoritative restore, its metadata version number is changed so that the number is higher than any other metadata version number in the configuration set. This ensures that any data you restore is properly replicated throughout the configuration set.

Configuration files

The various services installed with Web Services for Microsoft Dynamics GP can be included in a system-wide backup for the server. You might also want to create backups for the configuration files used for the services, especially if you have made changes to them. Most of these configuration files are found in the ServiceConfigs folder of the Web Services for Microsoft Dynamics GP installation. One exception is the following configuration file, which can be found in the main folder of the Web Services for Microsoft Dynamics GP installation:

- Microsoft.Dynamics.GP.ServiceHost.exe.config

Another exception is the following configuration file, which can be found in the SecurityAdminService folder of the Web Services for Microsoft Dynamics GP installation:

- Dynamics.SecurityAdmin.config

Chapter 12: Adding Additional Companies

If you add a new company to Microsoft Dynamics GP after Web Services for Microsoft Dynamics GP has been installed, you must perform the following procedure for the new company to be accessible through the Dynamics GP service.

1. **Start the configuration wizard.**
   In the Start menu, locate the Microsoft Dynamics group. Point to Web Services for Microsoft Dynamics GP 2010, and then choose GP Web Services Configuration Wizard. The Welcome page for the wizard will be displayed.

   Click Next to continue.

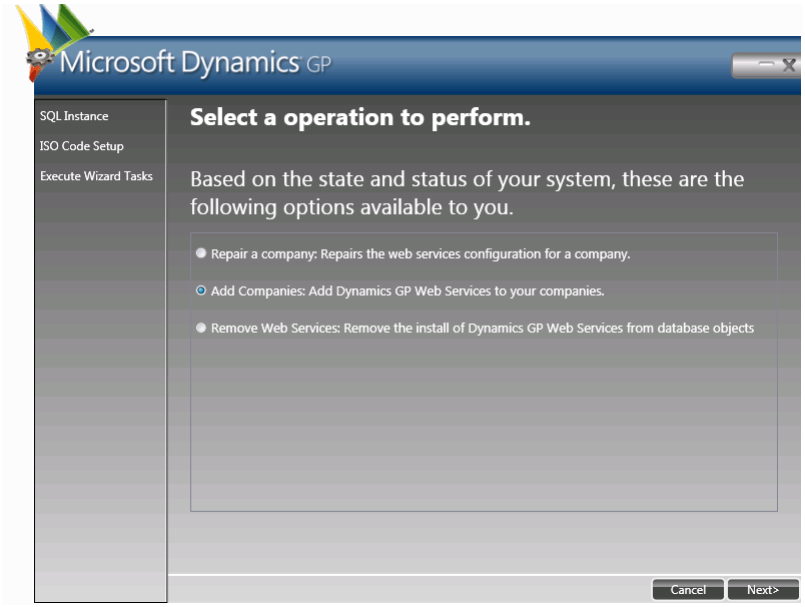
2. **Enter the connection information for Microsoft Dynamics GP.**
   The SQL Server Name field will contain the name of the SQL Server that is managing the data for Microsoft Dynamics GP. The configuration wizard must connect to this server to perform the setup operations. You must use Windows Trusted Authentication to connect to the SQL Server. Click Next to continue.

3. **Verify system check results.**
   The configuration wizard will verify the following:

   - ISO currency codes have been defined for each currency
   - Functional currencies have been set up for each company

   If either of the system checks do not pass, make the appropriate corrections in Microsoft Dynamics GP. Then re-run the configuration wizard. When the checks pass, click Next to continue.

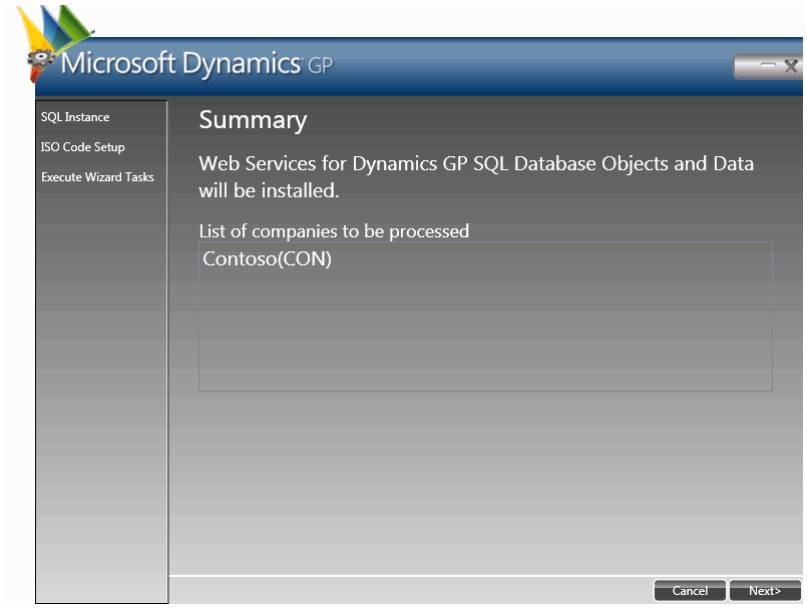
4. **Choose the action to perform.**
   Select the Add Companies action to add web service support to the new company.



   Click Next to continue.

5. **Select the companies for which to install web services.**
   In the list of available companies, select the companies for which you want to install web services. Hold down the CTRL key to select multiple companies. Click Next to continue.

6. **View the summary of actions to be performed.**
   A list of the actions to be performed will be displayed. Click Next to continue. A dialog will be displayed, asking whether to continue with the installation. Click Yes to start the installation process.



7. **Verify progress for the configuration tasks.**
   The configuration tasks for the system and for each company will be performed. The overall progress shown at the bottom of the window. A green check will be displayed as each task is processed.

8. **Complete the configuration.**
   Click Complete to close the GP Web Services Configuration Wizard.

9. **Restart the Microsoft Dynamics GP Service Host.**
   The configuration wizard will ask whether to restart the Microsoft Dynamics GP Service Host. This is the Windows service that manages the various services in Web Services for Microsoft Dynamics GP. Click Yes to restart the service.

Chapter 13: Repairing Web Services

If the Web Services for Microsoft Dynamics GP installation becomes damaged, the repair operations available may help resolve the issues. Information about repairing is divided into the following sections:

Repair options

Repair operations for Web Services for Microsoft Dynamics GP can be performed in two ways:

- The Web Services for Microsoft Dynamics GP installer can repair the files and infrastructure that was placed by the installer.
- The Dynamics GP Web Service Configuration Wizard can repair the system, company, policy, and security objects for the Microsoft Dynamics GP system and for individual companies.

Which repair option you need will depend on what components need to be repaired.

Repairing with the installer

The following actions are performed when using the repair functionality of the Web Services for Microsoft Dynamics GP installer:

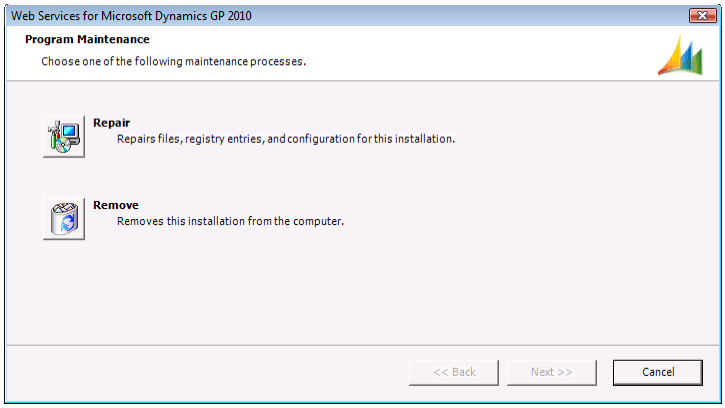
- The Microsoft Dynamics GP Service Host service is re-installed.
- All assemblies, XSLT files, and executable files are replaced.
- All configuration files are replaced or re-built. The installer will try to save any custom settings or additions you may have made to the configuration files.

If you want a configuration file to be replaced with an original copy, delete the configuration file before performing the repair.

- The Dynamics Security Console is re-installed. Any additional security administrators you had defined will need to be redefined.
- The Microsoft Dynamics GP Web Service Exception console is re-installed. This will delete any previous exception information that was logged by the Dynamics GP service.

To repair the Web Services for Microsoft Dynamics GP installation, complete the following steps:

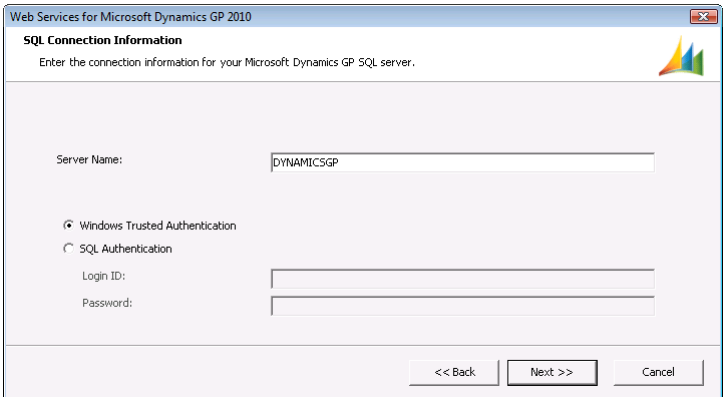
1. **Modify the Web Services for Microsoft Dynamics GP installation.** For Windows Server 2003, go to Add or Remove Programs. For Windows Server 2008, go to Programs and Features. Choose Web Services for Microsoft Dynamics GP, and then click Change. The program maintenance options will be displayed.



2. **Repair the installation.**
   Click Repair.

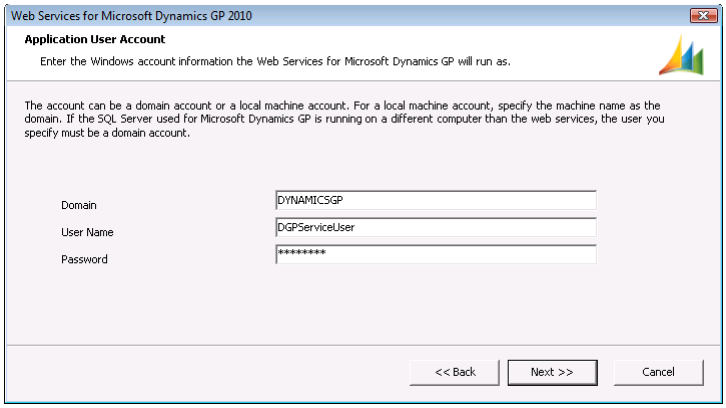
3. **Specify the location of the Microsoft Dynamics GP data.**
   In the Server Name field, supply the name of the machine that is running SQL Server and managing the data for Microsoft Dynamics GP.

   The installation program must connect to this database to complete the repair operation. You can use Windows Trusted Authentication or SQL Authentication (supplying the Administrator login ID and password).



   Click Next to continue. If the database connection cannot be made, an error will be displayed. Correct the issue and continue.

4. **Specify the application account.**
   Typically, you will enter the account that you created while performing the initial installation of Web Services for Microsoft Dynamics GP. If the installation of Web Services for Microsoft Dynamics GP is on a different machine than the SQL Server used to manage Microsoft Dynamics GP data, this must be a domain user account. If you are repairing an installation on the same machine as the SQL Server, it can be a local machine account. This case is shown in the following illustration:



If the account you specified has already been added as a user for Microsoft SQL Server, be sure the case for the Domain and User Name match those of the user ID in SQL.

Click Next to continue.

5. **Start the repair process.**
   Click Repair to start the repair process.

6. **Complete the repair process.**
   Click Finish to complete the repair process.

Repairing with the configuration wizard

The actions that are performed when using the repair option of the Dynamics GP Web Services Configuration Wizard will depend on the condition of the installation, and which repair options you choose. You can choose to perform all of the repair actions, or you can use the advanced mode to perform only selected repair actions.

If you use the configuration wizard to repair system or company security metadata, all of your existing security settings for the Dynamics GP service will be lost. Use this option only if you are certain you want to rebuild security data.

To use the configuration wizard to repair Web Services for Microsoft Dynamics GP, complete the following procedure.

1. **Start the configuration wizard.**
   In the Start menu, locate the Microsoft Dynamics group. Point to Web Services for Microsoft Dynamics GP 2010, and then choose GP Web Services Configuration Wizard. The Welcome page for the wizard will be displayed. Click Next to continue.

2. **Enter the connection information for Microsoft Dynamics GP.**
   The SQL Server Name field will contain the name of the SQL Server that is managing the data for Microsoft Dynamics GP. The configuration wizard must connect to this server to perform the setup operations. You must use Windows Trusted Authentication to connect to the SQL Server. Click Next to continue.

3. **Verify system check results.**
   The configuration wizard will verify the following:

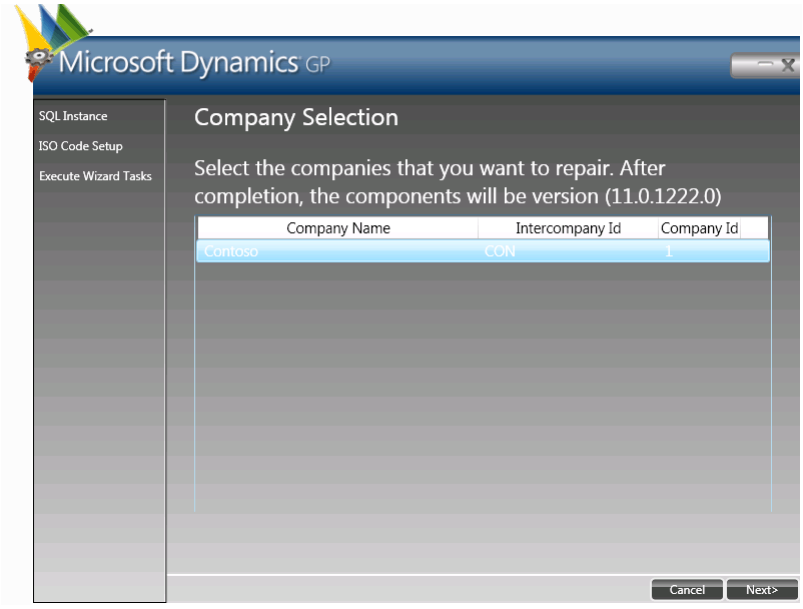
   - ISO currency codes have been defined for each currency
   - Functional currencies have been set up for each company

   If either of the system checks do not pass, make any needed corrections in Microsoft Dynamics GP. Then re-run the configuration wizard. When the checks pass, click Next to continue.

4. **Choose the action to perform.**
   Select the Repair a Company action to repair a company. Click Next to continue.

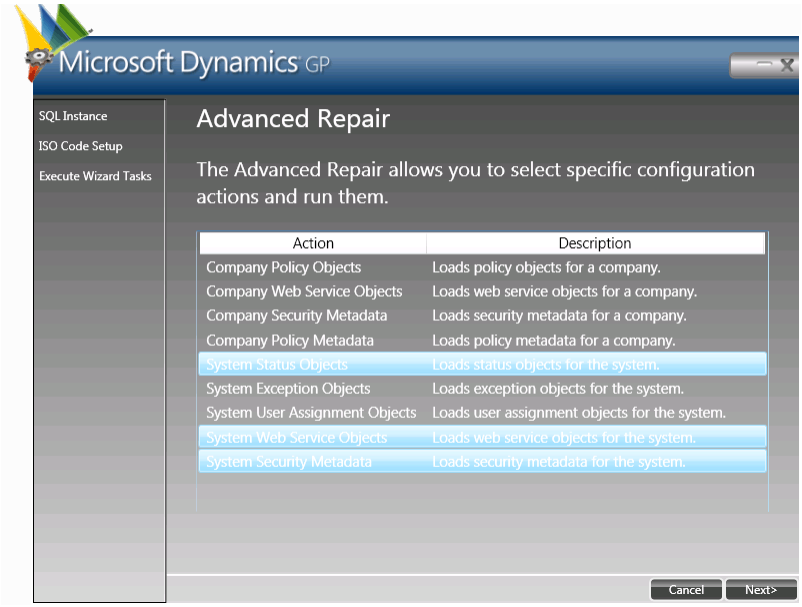
5. **Indicate the type of repair to perform.**
   If you want to individually select the components to repair, mark the Use Advanced Repair check box. If you don't choose this option, all items in the selected companies will be repaired.

6. **Select the companies to repair.**
   In the list of available companies, select the companies for which you want to reapir web services. Hold down the CTRL key to select multiple companies.



Click Next to continue.

7. **Choose the advanced repair options (if required).**
This step is necessary only if you chose to perform and advanced repair. In the list of available actions to perform, select the repair actions you want to run for the selected companies. Hold down the CTRL key to select multiple actions.



The following actions can be performed:

- Company Policy Objects
- Company Web Service Objects
- Company Security Metadata
- Company Policy Metadata
- System Status Objects
- System Exception Objects
- System User Assignment Objects
- System Web Service Objects
- System Security Metadata

The list of actions available may be different depending on the current state of the Web Services for Microsoft Dynamics GP installation.

Click Next to continue.

8. **View the summary of actions to be performed.**
A list of the actions to be performed will be displayed. Click Next to continue. A dialog will be displayed, asking whether to continue with the repair. Click Yes to continue the repair process.

9. **Verify progress for the repair tasks.**
The repair tasks chosen will be performed. The overall progress is shown at the bottom of the window. A green check will be displayed as each task is processed.

10. **Complete the configuration.**
Click Complete to close the GP Web Services Configuration Wizard.

11. **Restart the Microsoft Dynamics GP Service Host.**
    The configuration wizard will ask whether to restart the Microsoft Dynamics GP Service Host. Click Yes to restart the service.

APPENDIX

Appendix

The following appendices are included for this documentation:

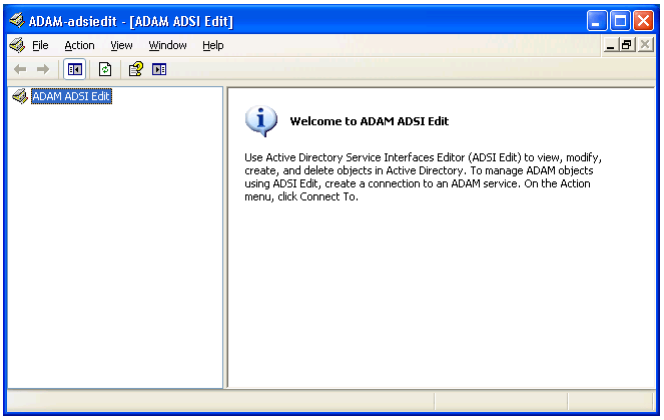
- Appendix A, "ADAM or ADLDS Administrators," describes the procedure of adding additional users to be administrators for ADAM.
- Appendix B, "Creating an Active Directory Partition," provides a basic procedure for creating an Active Directory partition.

Appendix A: ADAM or ADLDS Administrators

By default, the user who installed ADAM (Windows Server 2003) or Active Directory Lightweight Directory Services (Windows Server 2008) will be an ADAM or ADLDS administrator. You may want to add additional users to be administrators so that several different users could perform an install, repair, or upgrade of Web Services for Microsoft Dynamics GP. To add an administrator, complete the following procedure:

1. **Verify the current login.**
   You must be an ADAM or ADLDS administrator to add other users as administrators.

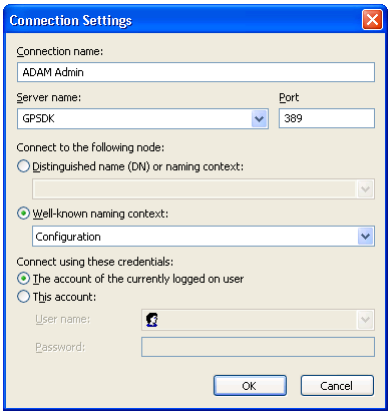
2. **Launch ADAM ADSI Edit or ADSI Edit.**
   For Windows Server 2003, this is in the ADAM program group, and is typically found in All Programs >> ADAM. For Windows Server 2008, this is in Administrative Tools. The editing window will be displayed.



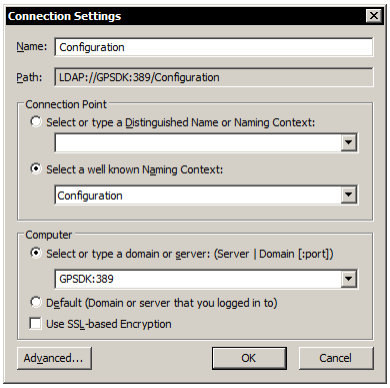
3. **Create a connection.**
   In the Action menu, choose Connect to. The Connection Settings window will be displayed.

4. **Specify the connection settings.**
   You can supply a name for the connection or use the default name. Specify the server name onto which ADAM or ADLDS was installed. If the Web Services for Microsoft Dynamics GP installer has installed ADAM or the ADLDS instance, it will use the default port 389. If you've used a different port, specify that port value. Choose Configuration as the well-known naming context.

The following illustration shows the connection settings for Windows Server 2003:



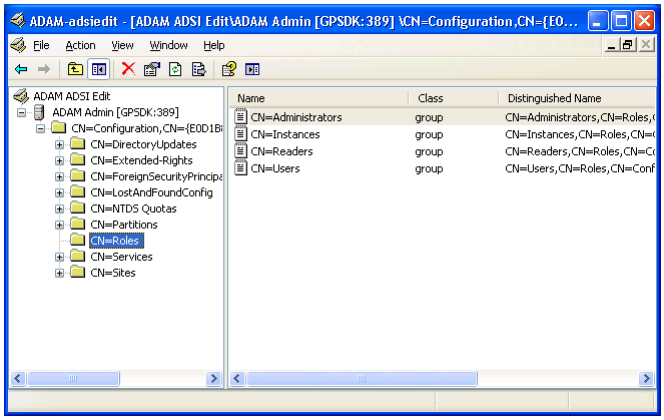
The following illustration shows the connection settings for Windows Server 2008:



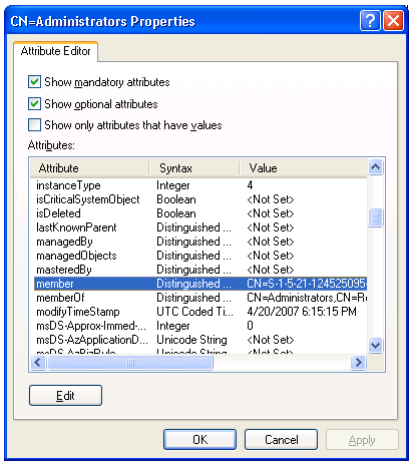
Click OK to create the connection.

5. Locate the roles for the ADAM installation.

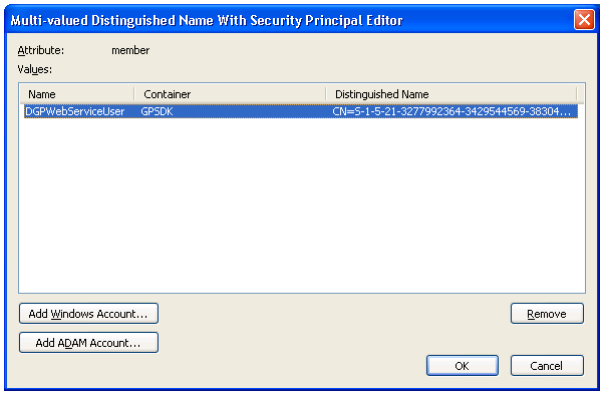
The details of the ADAM installation will appear in the tree view on the left side of the window. Expand the tree and select the CN=Roles node.



6. **Display the properties for the Administrators role.**
   In the list of roles, select Administrators. Choose Properties from the Action menu to display the properties for the Administrators role.



7. **Select and edit the "member" attribute.**
   In the list of attributes for the Administrators role, locate and select "member". Click Edit. The Multi-valued Distinguished Name With Security Principal Editor window will be displayed.



8. **Add the user.**
   Click Add Windows Account to specify the user to add as an administrator. Click OK to save your changes.

9. **Close the properties window.**
   Click OK to close the Administrator role properties window.

10. **Close the ADSI Editor.**

Appendix B: Creating an Active Directory Partition

If you want to store the Web Services for Microsoft Dynamics GP security data in Active Directory, you must create a partition in Active Directory first. When you install Web Services for Microsoft Dynamics GP, you will indicate that the security data will be stored in this partition.

For detailed information about using Active Directory, refer to the technical information available at http://technet.microsoft.com and the developer information available at http://msdn.microsoft.com.

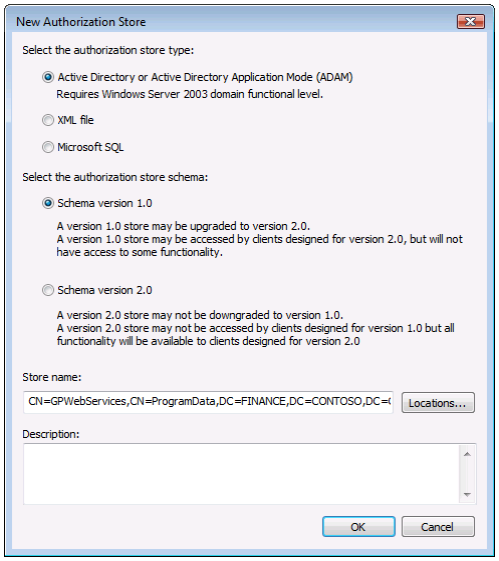
The following basic procedure describes how to create an Active Directory partition.

1. **Verify the current login.**
   You must have appropriate permissions to create the partition.

2. **Launch Authorization Manager.**
   From the Start menu, choose Run. Enter AzMan.msc and press Enter.

3. **Switch to Developer mode.**
   In the Action menu, choose Options. In the Options window, click Developer mode and then click OK.

4. **Create a new authorization store.**
   In the Action menu, choose New Authorization Store.



In the New Authorization Store window, make the following selections:

Authorization Store Type Active Directory

Schema Either schema version can be used

Store name The store name has the following format:

```
CN=<STORENAME>,CN=<PARTITION>,DC=<FQDN1>,DC=<FQDN2>,DC=<FQDN3>
```

The FQDN entries are the portions of the fully-qualified domain name. It's also a good practice to put the new store in the Program Data partition. For example, if the GPWebServices store was being created for the finance.contoso.com domain, the store name string would be:

```
CN=GPWebServices,CN=Program Data,DC=FINANCE,DC=CONTOSO,DC=COM
```

Description A description is optional.

Click OK to create the store.

5. **Set permissions on the store (optional).**
You can now connect to and manage the store. You may want to give permissions to a different user who will be installing Web Services for Microsoft Dynamics GP. Use a connection string with the following format, replacing the the names appropriately for the store you created:

```
msldap://<DOMAINCONTROLLER>:389/CN=<STORENAME>,CN=<PARTITION>,DC=<FQDN1>,
DC=<FQDN2>,DC=<FQDN3>
```

6. **Use the store when installing Web Services for Microsoft Dynamics GP.**
When you install Web Services for Microsoft Dynamics GP, you will specify the following location for security data to use the Active Directory store you created:

Server Your domain controller machine

Port 389

Partition Use the following syntax, replacing the store name and domain name with the values you had used earlier:

```
CN=<STORENAME>,CN=<PARTITION>,DC=<FQDN1>,DC=<FQDN2>,DC=<FQDN3>
```

For the previous example, this would be:

```
CN=GPWebServices,CN=Program Data,DC=FINANCE,DC=CONTOSO,DC=COM
```

Glossary

ADAM
Active Directory Application Mode. A special stand-alone version of Active Directory that is used by the Dynamics Security service on Windows Server 2003 to store and manage security information.

ADLDS
Active Directory Lightweight Directory Services. The stand-alone version of Activie Directory that is used by the Dynamics Security service on Windows Server 2008 to store and manage security information.

Authorization Manager (AzMan)
A security framework available in Windows Server 2003 that can be used to control access to application resources. The Dynamics Security Service uses Authorization Manager.

Dynamics Security Service
A service used to control access to various Dynamics applications, such as Web Services for Microsoft Dynamics GP.

eConnect
A set of SQL stored procedures and supporting code used by integrating applications to acccess data in Microsoft Dynamics GP.

Entity ID assignments
For the Dynamics GP service, the things that assign Windows User IDs to specific objects in Microsoft Dynamics GP that have identity information. See also *User-assignable business objects*.

Legacy endpoint
An endpoint for the Microsoft Dynamics GP Service Host. It uses the BasicHTTPBinding, which has the characteristics of a standard ASMX-based web service. The legacy endpoint provides functionality that is equivalent to the web service from earlier versions of Microsoft Dynamics GP.

Microsoft Dynamics GP Service Host
A Windows service built with Windows Communication Foundation. It hosts the various services that are made available for Microsoft Dynamics GP.

Native endpoint
An endpoint for the Microsoft Dynamics GP Service Host. It uses the WSHTTPBinding, which has better performance and default security than te legacy endpoint.

SOAP
Simple Object Access Protocol. The XML-based protocol used to communicate with a web service.

User-assignable business objects
Those objects in Microsoft Dynamics GP that have identity information and can be associated with a Windows User ID. Examples include customers or salespeople.

Web reference
A URL that points to service that supports ASMX-compatible operations.

Web service
A software system that provides data and services to other applications. Web services use standard Internet transport protocols such as Hypertext Transfer Protocol (HTTP) and standard XML-based document formats such as Simple Object Access Protocol (SOAP) to exchange information.

WCF
Windows Communication Foundation. This is a framework included in the .NET Framework that can be used to build services that allow applications to exchange data. WCF supports several standard protocols and authentication methods.

WSDL
Web Service Description Language. The XML-based language used to describe web services.

Index

Numerics

A

B

C

D

E

F