Microsoft Dynamics® AX 2009

Configuring Kerberos Authentication with Role Center Pages

White Paper

This document describes how to configure Kerberos authentication so that reports created by Microsoft® SQL Server® Reporting Services and Microsoft SQL Server Analysis Services display in Microsoft Dynamics AX 2009 Enterprise Portal Role Center pages.

UPDATED: February 2010

Microsoft Dynamics®

Table of Contents

Introduction

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

Enterprise Portal can be configured to display role-tailored home pages called *Role Centers*. Role Centers provide an overview of information that pertains to a user's job function in the business or organization, including reports generated by SQL Server Reporting Services and SQL Server Analysis Services.

This document describes how to configure Kerberos authentication for Role Center pages in Microsoft Dynamics AX 2009. You must configure Kerberos authentication if SQL Server Analysis Services and SQL Server Reporting Services are on a separate server from the Enterprise Portal server. If you do not configure Kerberos authentication, as described in this document, users will not be able to view Analysis Services reports and/or Reporting Services reports in Role Center pages.

About Kerberos authentication

Kerberos is an industry-standard ticketing authentication method that is implemented in Active Directory. A Kerberos authentication server grants a ticket in response to a client computer authentication request, assuming that the request contains valid user credentials and a valid service principal name (SPN). The client computer then uses the ticket to access network resources. To enable Kerberos authentication, the client and server computers must have a trusted connection to the domain Key Distribution Center (KDC). The KDC distributes shared secret keys to enable encryption. The client and server computers must also be able to access Active Directory directory services.

Server configurations

Microsoft Dynamics AX requires the following applications to run Enterprise Portal:

- Internet Information Services (IIS)
- Windows SharePoint Services or Office SharePoint Server

If you configure Enterprise Portal for Role Centers and you want to use the business intelligence and reporting capabilities of Role Centers, then you must also run the following:

- SQL Server Analysis Services
- SQL Server Reporting Services

If all of these applications are running on the same server, then you do not need to configure Kerberos authentication. If the SQL Server applications are running on a separate server (or multiple servers), then you must configure Kerberos authentication as described in this document.

Before you begin

You must install the following applications and features before you configure Kerberos authentication.

Application/Feature	Where to find installation instructions
Dynamics AX 2009 (full installation)	See the Microsoft Dynamics AX Installation Guide.
Microsoft SQL Server 2005 or SQL Server 2008 Reporting Services	See the SQL Server online Help.
Microsoft SQL Server 2005 or SQL Server 2008 Analysis Services	See the SQL Server online Help.
Reporting Extensions in Dynamics AX 2009	See **Install required components > Reporting extensions** in the Microsoft Dynamics AX Installation Guide.
Analysis Extensions in Dynamics AX 2009	See **Install required components > Analysis extensions** in the Microsoft Dynamics AX Installation Guide.
Enterprise Portal and Role Centers	See the "Configuring Enterprise Portal and Role Centers with SQL Server Reporting" whitepaper on PartnerSource and on the Using Microsoft Dynamics AX 2009 Web site.

Install relevant hotfixes

Review the details for the following hotfixes and apply those that are relevant to your computer environment:

- If you plan to use Windows SharePoint Services or Microsoft Office SharePoint Server on Windows Server 2008 R2, you must upgrade and deploy these applications according to Knowledge Base article 962935.
- If you host Microsoft Dynamics AX Enterprise Portal and Microsoft SQL Server report server on computers running Microsoft Windows Server 2008, apply the Kerberos authentication hotfix documented in Knowledge Base article 969083. This hotfix does not apply to Microsoft Windows Server 2003 R2 or Windows Server 2008 R2. You can also view this blog post for more information.

Configure the domain controller

Your Microsoft Windows domain controller must be running in Windows 2003 or Windows 2008 mode to accommodate Kerberos authentication between report servers and the Enterprise Portal server. Use the following procedure to raise the domain functional level. To perform this procedure, you must be a member of the domain administrators group in the domain for which you want to raise functionality or the enterprise administrators group in Active Directory, or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.

Important: Due to a known issue, if SQL Server Analysis Services and SQL Server Reporting Services are running on separate servers, you must configure your domain controllers to run using the Windows Server 2003 domain functional level. This applies to Windows Server 2003 and 2008 computers. If you do not configure the domain controller to run the Windows Server 2003 domain functional level, Kerberos authentication fails.

Windows Server 2003 domain controller

1. On the Windows domain controller, in **Active Directory Users and Computers**, click **Raise Domain Functional Level**.
2. Click **Windows Server 2003**, and then click **Raise**.
3. Click **OK**.

Windows Server 2008 domain controller

1. To open the Active Directory Domains and Trusts snap-in, click **Start**, click **Administrative Tools**, and then click **Active Directory Domains and Trusts**.
2. In the console tree, right-click the domain for which you want to raise functional level, and then click **Raise Domain Functional Level**.
3. In **Select an available domain functional level**, do one of the following:
   - To raise the domain functional level to Windows Server 2003, click **Windows Server 2003**, and then click **Raise**.
   - To raise the domain functional level to Windows Server 2008, click **Windows Server 2008**, and then click **Raise**.

Enable Kerberos authentication in SharePoint Services

Use the following procedure to enable Kerberos authentication in Windows SharePoint Services. If you are running Microsoft Office SharePoint Server, see "Enable Kerberos authentication in Office SharePoint Server" later in this document.

1. Click **Start**, click **Administrative Tools**, and click **SharePoint 3.0 Central Administration**.
2. Click the **Application Management** tab.
3. Under **Application Security**, click **Authentication Providers**.
4. Select the Web application you want to configure with Kerberos authentication from the **Web Application** list.
5. Under **Zone**, click **Default**.
6. Under **IIS Authentication Settings**, click **Negotiate (Kerberos)**, and then click **Save**.
7. Close **SharePoint 3.0 Central Administration**.
8. Click **Start**, and then click **Run**.
9. In the **Run** dialog box, enter **iisreset** and then press **Enter**.

To continue configuring Kerberos authentication, please see "Verify that Kerberos authentication is set for the Report Server and Report Manager virtual directories" later in this document.

Enable Kerberos authentication in Office SharePoint Server

Use the following procedure to enable Kerberos authentication in Office SharePoint Server.

1. Click **Start**, click **Administrative Tools**, and click **SharePoint Central Administration**.
2. Click the **Application Management** tab.
3. Under **Application Security**, click **Authentication Providers**.
4. Select the Web application that you want to configure with Kerberos authentication from the **Web Application** list.

5. Under **Zone**, click **Default**.
6. Under **IIS Authentication Settings**, click **Negotiate (Kerberos)**, and then click **Save**.
7. Repeat steps 4-6 until you have specified **Negotiate (Kerberos)** authentication for, at a minimum, the content application and the Shared Service Provider (SSP) application.
8. Close **SharePoint Central Administration**.
9. Click **Start**, and then click **Run**.
10. In the **Run** dialog box, enter **iisreset**, and then press **Enter**.

Verify that Kerberos authentication is set for the Report Server and Report Manager virtual directories

The following procedure applies to SQL Server 2005 Reporting Services. If you are using SQL Server 2008, you can skip to the next section, "Configure service principal names".

By default, the SQL Server Reporting Services Report Server and Report Manager virtual directories are configured for Kerberos authentication. If your organization or business deployed an SQL Reporting Services server, use the following procedure to verify the authentication mode on these directories. This procedure also includes the commands to set Kerberos authentication for the virtual directories, if necessary.

1. Click **Start**, click **Administrative tools**, then click **Internet Information Services (IIS) Manager**.
2. In the left pane, click the **Web sites** directory and locate the **Reports a**nd **Report Server** applications.
3. Locate the **Identifier** column and write down the identifier for each application.
4. Enter the following command in a command prompt and press Enter:
   cd \inetpub\adminscripts
5. Use the following command to determine if Negotiate,NTLM (Kerberos) authentication is set for the Report Manager and Report Server applications. In the command, replace <*identifier*> with the identifier for the Report Manager and Report Server applications, respectively. Then enter the commands in the command prompt and press Enter:
   - **cscript adsutil.vbs get w3svc/**<*identifier*>**/root/reports/NTAuthenticationProviders**
   - **cscript adsutil.vbs get w3svc/**<*identifier*>**/root/reportserver/NTAuthenticationProviders**
6. If Negotiate,NTLM (Kerberos) authentication is not set, use the following commands to set it:
   - **cscript adsutil.vbs set w3svc/**<*identifier*>**/root/reports/NTAuthenticationProviders "Negotiate,NTLM"**
   - **cscript adsutil.vbs set w3svc/**<*identifier*>**/root/reportserver/NTAuthenticationProviders "Negotiate,NTLM"**
7. In the command prompt, type **iisreset** and then press Enter.

Configure service principal names

Kerberos authentication requires that you specify certain properties in Active Directory about how and where a service should run. In the context of Active Directory, this is called configuring a service principal name (SPN). Using the following procedure, you will specify the server name, domain name, and application pool account for the HTTP service and the SQL Server Analysis Services service (if applicable) in Active Directory using the SetSPN.exe command-line tool. Setspn.exe is included with Windows Server 2003 Service Pack 1 and Service Pack 2. This command-line tool enables you to read, modify, and delete SPN properties for an Active Directory service account like the HTTP service. To perform this procedure, you must be a member of the domain administrator group in Active Directory, or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.

Before you begin, confirm that Windows Server 2003 Service Pack 1 or Service Pack 2 is installed on each Enterprise Portal and SQL Server computer. If you do not install one or more of these service packs, you will not be able to locate the Setspn.exe tool.

Important: If your Web servers use Microsoft Network Load Balancing (NLB), please see the following whitepaper for information about configuring Kerberos with NLB: Kerberos authentication for load balanced web sites

Configure the HTTP service principal name

Use this procedure to create an HTTP SPN for each Enterprise Portal and SQL Server Report Server computer. You can perform this procedure from one computer. It is not necessary to perform this procedure locally on each server.

Important: SQL Server 2008 Reporting Services does not use an application pool. Service principal names for SQL Server 2008 Reporting Services must be set on the Reporting Services service account. If you are running SQL Server 2008 Reporting Services, substitute the service account details for all instances of {application pool account} in the following procedure.

1. Open the Windows Support Tools command prompt (**Start** > **All Programs** > **Windows Support Tools** > **Command prompt**).
2. At a command prompt, type the following command and press Enter:

   Setspn.exe -A HTTP/{*server name*} {*application pool account*}

   For this command, remove the braces {}, replace *server name* with the name of the server computer, and replace *application pool account* with the *domain**name* used for the IIS application pool. Here is an example of this command using a fictitious domain "contoso":

   Setspn.exe -A HTTP/EnterprisePortal1 contoso\WebAccount
3. Type the following command and press Enter:

   Setspn.exe -A HTTP/{*the server fully-qualified domain name*} {*application pool account*}

   For this command, remove the braces {}, replace *the server fully-qualified domain name* with the FQDN of the server computer, and replace *application pool account* with the *domain**name* used for the IIS application pool. Here is an example of this command:

   Setspn.exe -A HTTP/EnterprisePortal1.contoso.corp.contoso.com contoso\WebAccount
4. Repeat this procedure to create an HTTP SPN for each Enterprise Portal and SQL Server Report Server computer.

Configure the SQL Server Analysis Services service principal name

Use this procedure to create a SQL Server Analysis Services SPN for each SQL Server Analysis Services computer. You can perform this procedure from one computer. It is not necessary to perform this procedure locally on each server.

Important: If Analysis Services is running as a named instance, please refer to the following knowledge base articles for information about how to set up service principal names for SQL Server Analysis Services and for the SQL Server browser.

- How to configure SQL Server 2005 Analysis Services to use Kerberos authentication
- An SPN for the SQL Server Browser service is required when you establish a connection to a named instance of SQL Server 2005 Analysis Services or of SQL Server 2005

1. At a command prompt, type the following command and press Enter:

   Setspn.exe -A MSOLAPSvc.3/{*server name*} {*SSAS account*}

   For this command, remove the braces {}, replace *server name* with the name of the SQL Server Analysis Services computer, and replace *SSAS account* with either the *domain**name* (for a domain account) or with the computer name (if Analysis Services is running under the NetworkService account). Here is an example of this command:

   Setspn.exe -A MSOLAPSvc.3/SSAS_Server1 contoso\SSASAccount

2. Type the following command and press Enter:

   Setspn.exe -A MSOLAPSvc.3/{*the server fully-qualified domain name*} {*SSAS account*}

   For this command, remove the braces {}, replace *the server fully-qualified domain name* with the FQDN of the server computer, and replace *SSAS account* with either the *domain**name* (for a domain account) or with the computer name (if Analysis Services is running under the NetworkService account). Here is an example of this command:

   Setspn.exe -A MSOLAPSvc.3/SSAS_Server1.contoso.corp.contoso.com contoso\SSASAccount

3. Repeat this procedure to create an SPN for each SQL Server Analysis Services computer.

Configure the service principal name for the SQL Server service

If the SQL Server service is running on a separate server (not on the Enterprise Portal server or the SQL Server Reporting Services server) then you must set up a service principal name for the SQL Server service account. Please refer to Scenario 4 in the following knowledge base article for information about how to set up the service principal name for the SQL Server service account.

- How to use SPNs when you configure Web applications that are hosted on IIS 6.0

Additionally, if your SQL server is running in a clustered environment, see the following article on MSDN: How to: Enable Kerberos Authentication on a SQL Server Failover Cluster

Verify your SPN setup

You can view information about service principal names, including duplicate SPNs which might cause problems for Kerberos authentication, using the Setspn tool with the **–x** switch. In Windows Server 2008, you can run the Setspn tool from a command prompt, though you must open the command prompt with elevated privileges (Run as administrator). For Windows Server 2003, you can download the Setspn tool here. For more information about

identifying and removing duplicate SPNs with the Setspn tool, see Event ID 11 — Service Principal Name Configuration.

Configure accounts in Active Directory

Use the procedures in this section to further configure user accounts and application pool accounts for Kerberos authentication. You must be a domain administrator with **Enable computer and user accounts to be trusted for delegation** permissions in Active Directory to perform the following procedures.

Disable delegated authentication for user accounts

Delegated authentication occurs when a network service accepts a request from a user and assumes that user's identity in order to initiate a new connection to a second network service. By default, user accounts are not configured for delegated authentication, but you must verify that no user accounts that will use Kerberos authentication in Enterprise Portal are currently configured for delegated authentication.

1. In **Active Directory Users and Computers**, right-click a user account and select **Properties**.
2. On the **Delegation** tab, under **Account Options**, clear the **Account is sensitive and cannot be delegated** check box (if applicable), and click **OK**.

Note: If you do not see the **Delegation** tab, verify that your domain account is running at the Windows Server 2003 or Windows Server 2008 functional level. In the case of the Windows Server 2003 functional level, you will only see the **Delegation** tab if there is a service principal name registered for the account.

Enable delegated authentication for IIS application pool accounts

Use this procedure to enable delegated authentication for the IIS application pool account.

1. In **Active Directory Users and Computers**, right-click the name of the IIS application pool account and select **Properties**.
2. Click the **Delegation** tab, select **the Account is trusted for delegation** check box, and then click **OK**.

NOTE: If you do not see the Delegation tab, verify that your domain account is running as Windows Server 2003 or Windows Server 2008 functional level. In the case of Windows Server 2003 functional level, you will only see the **Delegation** tab if there is a service principal name registered for the account.

Enable delegation on domain controllers

1. In **Active Directory Users and Computers**, under **Computers Organizational Unit**, right-click the name of the IIS server and click **Properties**.
2. On the **General** tab, click **Trust Computer for Delegation**, and then click **Apply**.

NOTE: Enabling your IIS server for delegation raises a security concern, as noted in the warning on the **General** tab. This delegation permits services that run in the context of the system account to request information from remote services. This is enabled because Kerberos is a mutual authentication protocol, that is, it verifies both client and server credentials.

Deploy ODC files and configure for Kerberos authentication

Use the procedure in this section to deploy Office Data Connection (ODC) files to Enterprise Portal and then configure those files for Kerberos authentication. An ODC file enables reports in Enterprise Portal to connect to the OLAP cube from which they retrieve data. ODC files contain a data source type, connection string, and credential information.

1. Open the Microsoft Dynamics AX client.
2. Open the **OLAP Administration** form (**Administration** > **Setup** > **Business analysis** > **OLAP** > **OLAP Administration**).
3. Click the **Deploy ODC Files** button.

   The following eleven ODC files are deployed. An ODC file is deployed for the Dynamics AX OLAP database. In addition, an ODC file is deployed for each of the ten Microsoft Dynamics AX cubes.

   - Dynamics AX
   - Dynamics AX Accounts Payable Cube
   - Dynamics AX Accounts Receivable Cube
   - Dynamics AX Customer Relationship Cube
   - Dynamics AX Expense Management Cube
   - Dynamics AX General Ledger Cube
   - Dynamics AX Human Resources Management Cube
   - Dynamics AX Production Cube
   - Dynamics AX Project Accounting Cube
   - Dynamics AX Purchase Cube
   - Dynamics AX Sales Cube

The ODC files are deployed to the Data Connections page on the Enterprise Portal site. By default, the Data Connections page is located at:

http://*ServerName*/sites/DynamicsAx/Data%20Connections/Forms/AllItems.aspx

Edit the connection string for each ODC file

Use this procedure to specify Kerberos authentication in the connection string for each ODC file.

1. View the Enterprise Portal site in a Web browser.
2. From the **Site Actions** menu, click **Site Settings**.
3. Under **Galleries**, click **Master Pages**.
4. In the left corner of the page, click **View All Site Content**.
5. Under **Document Libraries**, click **Data Connections**.
6. Edit the connection string for each ODC file and append the following:

```
;SSPI=Kerberos
```

Configure Component Services

Use this procedure to configure **Component Services** on the Enterprise Portal Web server.

1. On the Enterprise Portal Web server, open Component Services (**Start** > **Administrative Tools** > **Component Services**).
2. Locate the **IIS WAMREG admin Service** (**Component Services** > **Computers** > **My Computer** > **DCOM Config** > **IIS WAMREG admin Service**).
3. Right-click this service and click **Properties**.
4. Click the **Security** tab.
5. In the **Launch and Activation Permissions** section, click **Edit**.
6. In the **Launch Permission** dialog box, click **Add**.
7. In the **Select Users, Computers, or Groups** dialog box, type the domain user account that you specified as the IIS application pool service account, click **Check Names**, and then click **OK**.
8. In the **Permissions for** *UserName* list, select the **Allow** check box that is next to **Local Activation**, and then click **OK**.

Configure Windows Server 2008

For Kerberos authentication to work with Windows Server 2008, you must either configure IIS 7.0 kernel-mode authentication to work with Kerberos authentication, or you must disable IIS 7.0 kernel-mode authentication. Both options are described here. For more information about kernel-mode authentication, see the IIS 7.0 documentation.

Configure IIS 7.0 kernel-mode authentication to work with Kerberos authentication

Perform the following procedure if you want IIS 7.0 kernel-mode authentication to work with Kerberos authentication.

1. On the Enterprise Portal Web server, open Windows Explorer and navigate to the following directory: \Windows\System32\inetsrv\config
2. Locate the applicationHost.config file.
3. Make a copy of this file for backup purposes.
4. Open the file in a text editor such as Notepad.
5. Locate the properties section for your Enterprise Portal site. By default, this section begins at the following tag: <location path="SharePoint - 80">.
6. In the <security> section, locate the following tag: <windowsAuthentication enabled="true">
7. Add the following information to the tag:

```
<windowsAuthentication enabled="true" useKernelMode="true"
useAppPoolCredentials="true">
```

8. Save your changes.

If you are running Microsoft SQL Server 2005 Reporting Services, you must repeat this procedure for the Reports and ReportServer sites. By default, the properties sections for these sites are:

<location path="Default Web Site/ReportServer">

<location path="Default Web Site/Reports">

If you are running Microsoft SQL Server 2008, configure the RsReportServer.config file as described in the next section.

Disable IIS 7.0 kernel-mode authentication

If you chose not to configure IIS 7.0 kernel-mode authentication to work with Kerberos authentication as described in the previous procedure, then you must disable kernel-mode authentication.

1. In Internet Information Services (IIS) Manager, expand the local computer node, expand **Sites**, and click the Enterprise Portal Web site.
2. In the center pane, under **IIS**, double-click **Authentication**.
3. Click **Windows Authentication**.
4. In the right pane, under **Actions**, click **Advanced Settings**.
5. Clear the **Enable Kernel-mode authentication** checkbox.
6. Click **OK**.
7. Repeat these steps for your Report Server and Report Manager sites, if applicable.

Configure SQL Server Reporting Services 2008

For Kerberos authentication to work with SQL Server Reporting Services 2008, you must configure the RsReportServer.config file. For information about Reporting Services configuration files, see Configuration Files (Reporting Services).

1. Open the configuration file in a text editor such as Notepad. By default the file is located here: <Installation directory>\Reporting Services\ReportServer\
2. Under <AuthenticationTypes> remove the NTLM entry and add the following types:
   - <RSWindowsKerberos />
   - <RSWindowsNegotiate />
3. Save your changes and close the file.

Enterprise Portal Role Center pages with Key Performance Indicators

If you experience problems configuring Kerberos authentication with Enterprise Portal Role Center pages that use Key Performance Indicators (KPI), read this blog post.

Verify that Kerberos authentication is configured correctly

If you configured Kerberos authentication correctly, you should be able to view SQL Server Analysis Services reports and/or SQL Server Reporting Services reports in Role Center pages from a Web browser on a computer other than the Enterprise Portal server.

You can also verify the configuration using the KerbTray.exe and Klist.exe utilities, which are included in the Windows Server 2003 Resource Kit Tools. If you run these tools on Windows Server 2008 or Windows Server 2008 R2, you must run them with elevated privileges (**Run as administrator**). When using KerbTray.exe tool, browse the Enterprise Portal site and verify that you see the HTTP/Enterprise Portal server ticket in the utility. Then browse the SQL Server Reporting Services Web site and verify that you see the HTTP/SQL Server Reporting Services ticket. If you see both tickets, then Kerberos is configured correctly. Use the Klist.exe tool to view and delete Kerberos tickets.

If you are not able to view reports in Role Center pages after completing the procedures in this document, verify that you have followed all of the Kerberos configuration procedures in this document and verify that you have correctly set up and configured Enterprise Portal and Role Centers with SQL Server reporting. See the "Configuring Enterprise Portal and Role Centers with SQL Server Reporting" white paper on PartnerSource and on the Using Microsoft Dynamics AX 2009 Web site.

Advanced configuration

After you have configured and verified Kerberos authentication in your intranet environment, you can configure your domain controller for Kerberos and allow internal users to view Role Center pages from a remote location. For more information, see this blog post for more information about configuring Kerberos clients to access Role Centers from outside the intranet.

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

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

Worldwide +1-701-281-6500

www.microsoft.com/dynamics

Microsoft