Business Objects

BusinessObjects Voyager XI Release 2

Configuring Voyager with Microsoft Analysis Services

Overview

Voyager is a query and analysis tool used to access Online Analytical Processing databases through BusinessObjects InfoView. This document will explain how to setup the BusinessObjects services to be able to authenticate to Microsoft Analysis Services (MSAS) 2000 and 2005.

Contents

INTRODUCTION 1

MICROSOFT ANALYSIS SERVICES ROLE SECURITY 1

Configuring Analysis Services Roles for MSAS 2000 1

Configuring Analysis Services Roles for MSAS 2005 3

OVERVIEW OF VOYAGER AND ANALYSIS SERVICES SECURITY 4

Prerequisites 6

Authenticating to Analysis Services 2005 on a local or remote server 6

Description of deployment scenario 6

Authenticating to Analysis Services 2000 on a local server 7

Description of deployment scenario 8

Authenticating to Analysis Services 2000 on a remote server 8

Description of deployment scenario 9

Authenticating with Single Sign-On to Analysis Services 2000 and 2005 10

Description of deployment scenario 11

Configuring Voyager for SSO to MSAS 2000/2005: 12

CONFIGURING VOYAGER FOR DELEGATION 13

Configuring Active Directory 13

How to determine domain functional level 14

Creating the service account in a Windows 2000 domain 14

Creating the service account in a Windows 2003 domain 16

Configuring computers for delegation 18

Configuring the Service Principal Names 20

Analysis Services SPN required for Kerberos and delegation 20

MDAS Service Account SPN required for Kerberos and delegation 21

Configuring required Local Policies on MDAS server 22

Configuring the Multi-Dimensional Analysis Service account 22

CREATING VOYAGER CONNECTIONS IN THE CENTRAL MANAGEMENT CONSOLE 23

TROUBLESHOOTING 25
Error in the CMC when creating a Voyager connection: "Login Failed. Please check that your username and password are valid" 26
Error "Internal Error: An unknown exception has occurred." 26
"No Cubes Found" when creating a new Voyager connection? 26
Error "An error has occurred propagating the security context between the security server and the client." 26
Error "An error has occurred while attempting to connect to the OLAP server. Failed to initialize…" 27
Error "The authentication provider (secEnterprise) associated with this logon session does not support inter-process Single Sign-On." 27
Error "The authentication provider (secWinAD) associated with this logon session does not support inter-process Single Sign-On." 28
Error "A specified logon session does not exist. It may already have been terminated." or Error "No credentials are available in the security package." 28
Using Event Viewer to view log ons 29
How to determine the patch level of your SQL Server and clients 29

FINDING MORE INFORMATION 30
Useful Microsoft information 30
Kerberos on Windows 2003 30
Troubleshooting Kerberos configuration and errors 30
Enabling Kerberos Event logging for troubleshooting 30
Using SQL Profiler 2005 for tracing logon usernames while troubleshooting 31
How to trace logon usernames for Analysis Services 2000 by enabling AuditEvents 31
Setspn utility download for creating SPNs 31
SQL Server 2005/Analysis Services Service Pack downloads 31
Microsoft Analysis Services 9.0 OLE DB Provider 31

Introduction

Voyager is a powerful, web-based analysis tool used for accessing OLAP data warehouses and allows users to gain insight into business data and make intelligent decisions that impact corporate performance. Voyager can be accessed by end-users through BusinessObjects InfoView by using a web browser. To allow Voyager to connect to MSAS 2000 or 2005, users will have to authenticate using Microsoft Windows credentials. This document guides you through the steps required to connect to your MSAS 2005 OLAP cubes.

Microsoft Analysis Services Role security

SQL Server Analysis Services (SSAS) 2000 and 2005 security architecture is built on Microsoft Windows authentication. In order to access data in SSAS, users must connect with an account that can be authenticated by the Microsoft Windows operating system. SSAS does not recognize user accounts created in the native SQL Server Database (relational) Engine security system, such as the built-in administrator's account "sa". After authenticating the user, SSAS checks the security roles that the user belongs to determine what cubes, dimensions, members and cell values to return.

Although SSAS 2000 and 2005 both support the concept of security roles, there are some minor differences between the two product versions. SSAS 2000 has database and cube roles, while SSAS 2005 has server and database roles. Fundamentally, role security works the same way in both versions. A security role grants Windows users specific read and write access permissions to the cubes on an SSAS server. Windows users who do not belong to a security role on the target SSAS server will not be able to access or view any cubes.

To allow users to view data in an Analysis Services cube from Voyager, you must first define the appropriate security roles on the target cube.

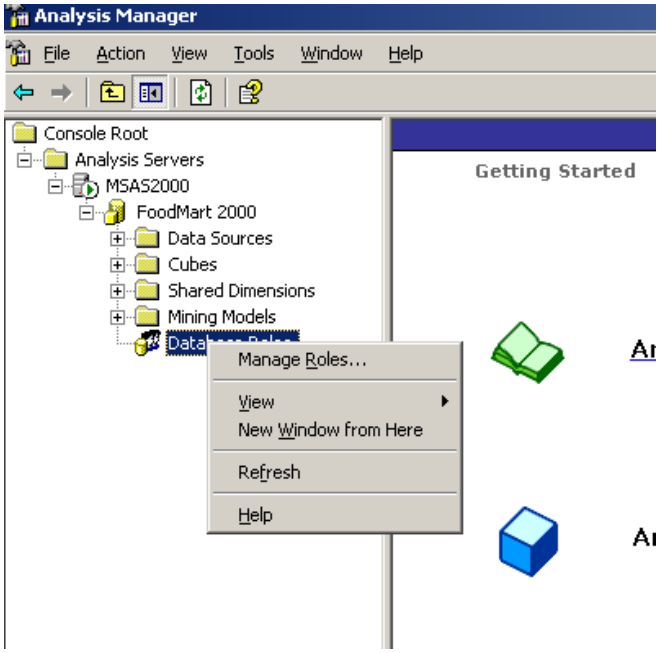
Configuring Analysis Services Roles for MSAS 2000

Follow the directions below to ensure that a role has been defined for the cubes being accessed:

1. Open Microsoft Analysis Manager by clicking **Start > Programs > Microsoft SQL Server > Analysis Services > Analysis Manager**.
2. Expand the folder structure for the data warehouse.

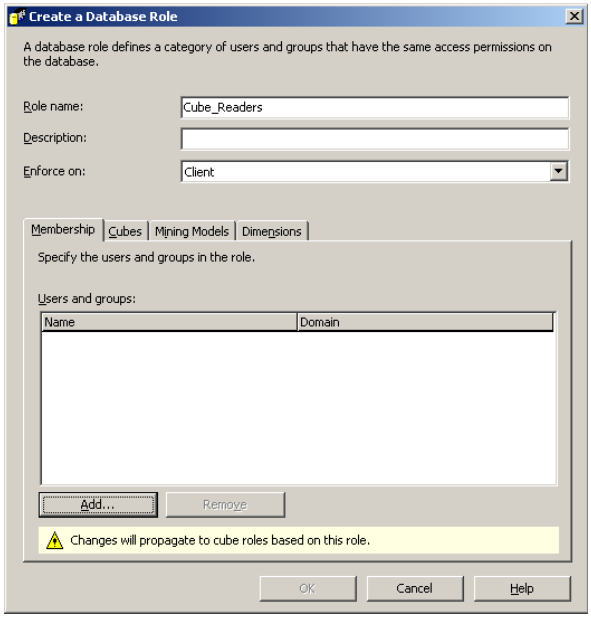
3. Right-click **Database Roles** and select **Manage Roles** from the menu.

Figure 1



4. Click the **New** button in the **Database Role Manager** window.
5. Enter a **Role Name** and **Description** of the new role.

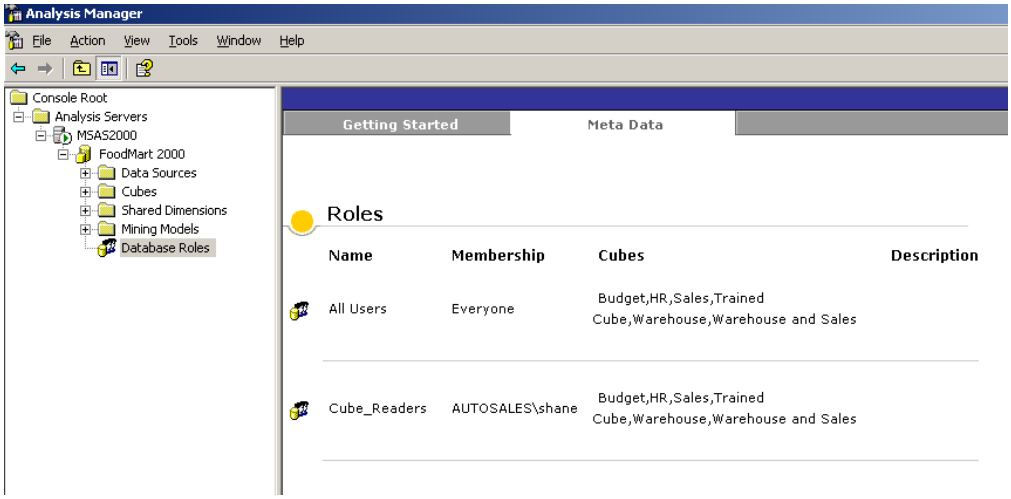
Figure 2



6. Click the **Add** button located to the bottom left and select the users that will have read permissions to the cubes.
7. Select the appropriate permissions using the **Cube**s, **Mining Models** and **Dimensions** tabs.

8. Click **OK** and ensure the role appears under the **Meta Data** tab in Analysis Manager.

Figure 3

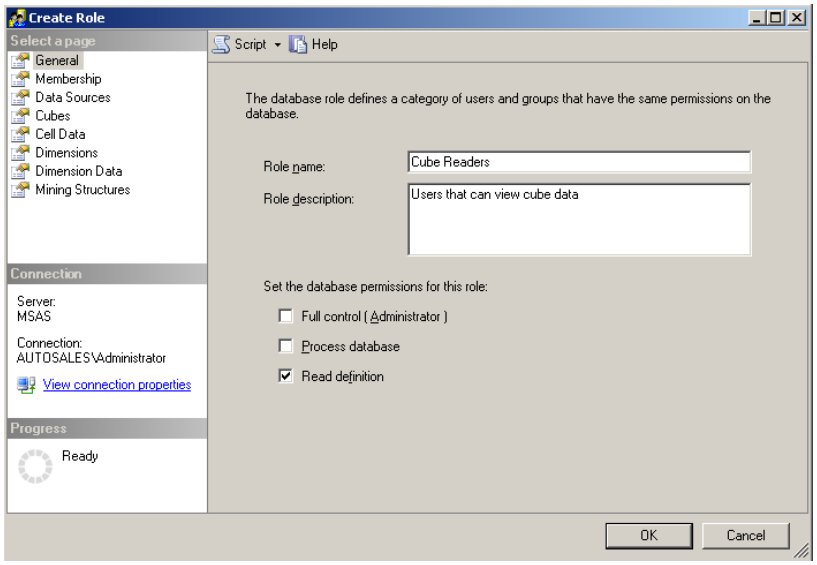


Configuring Analysis Services Roles for MSAS 2005

Follow the directions below to ensure that a role has been defined for the cubes being accessed:

1. Open Microsoft SQL Server Management Studio and connect to the Analysis Services instance.
2. Expand the folder structure for the database.
3. Right-click the **Roles** folder and click **New Role…** in the dropdown menu.
4. Enter a name for the role in the **Role Name** field and select the **Read Definition** checkbox so the users have read rights.

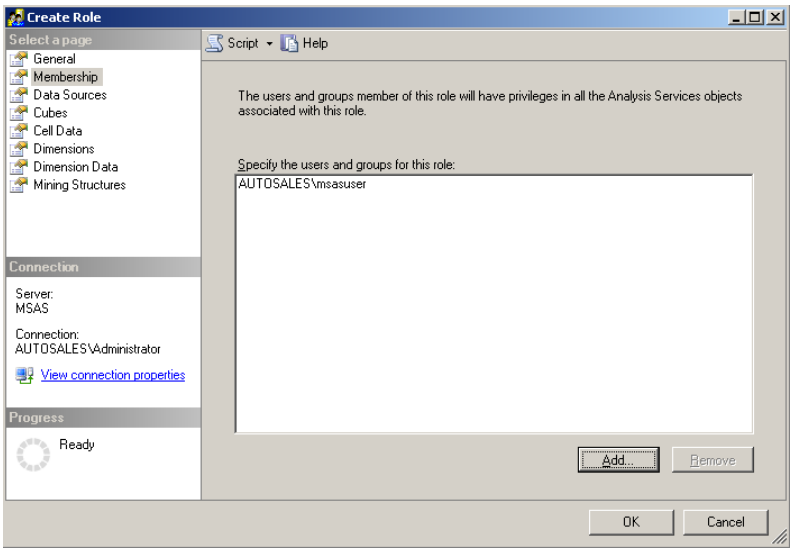
Figure 4



5. Click **Membership** in the left windowpane and click **Add** to add the list of domain users that will be given read access to the database.

NOTE	If there are a large number of users, it may be more efficient to create a group within Active Directory for OLAP access and add all the users to the group, then simply add the group to the list.

Figure 5



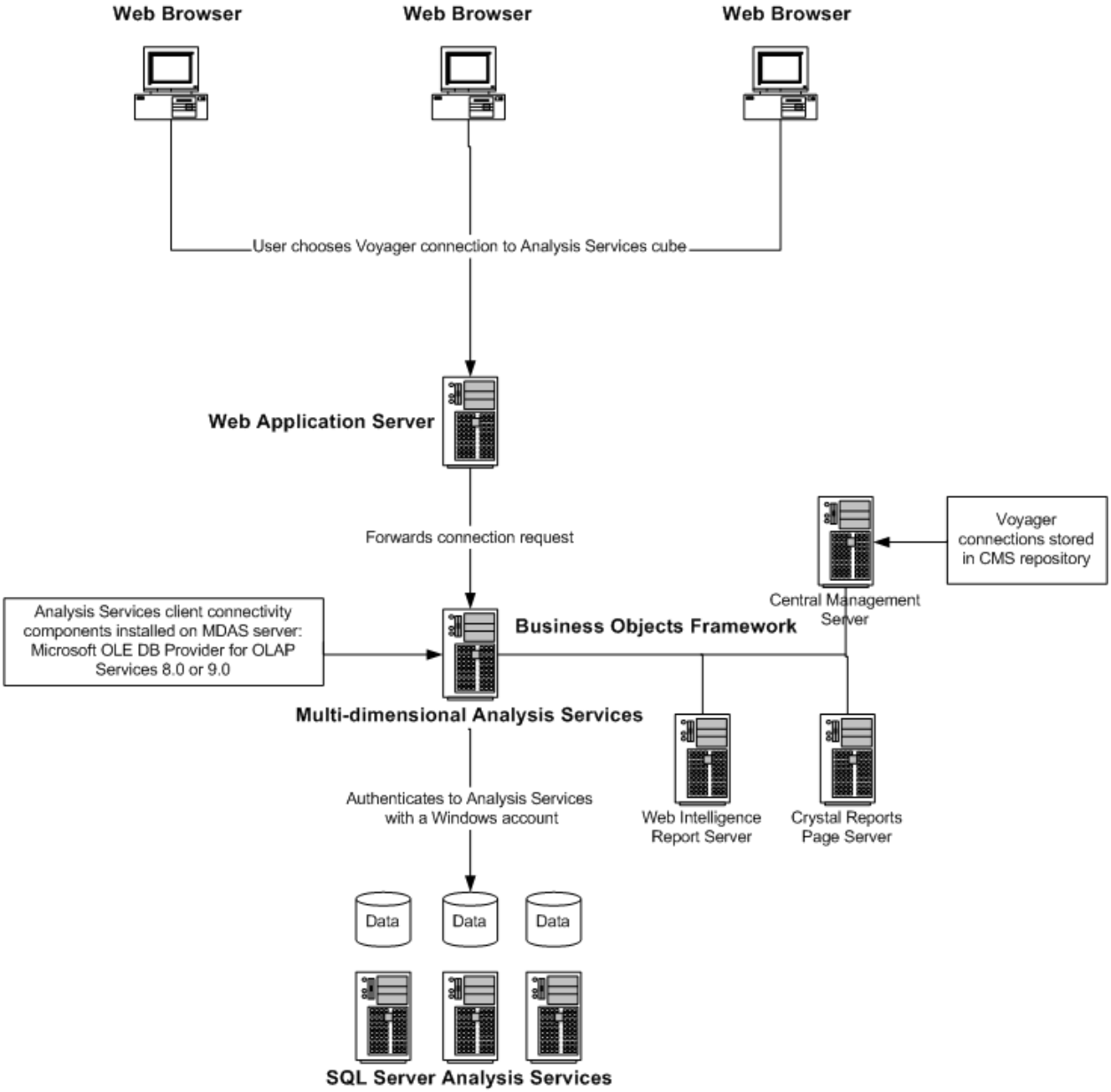
6. Select the appropriate user permissions by clicking **Data Sources**, **Cubes**, **Cell Data**, **Dimensions**, **Dimension Data** and **Mining Structures** to decide what areas the users will have read access to.

NOTE	The extent of how much of the data you want users to have access to is dependent on the reports being created and security within your organization and security should be planned accordingly.

Overview of Voyager and Analysis Services security

The following network diagram illustrates a logical deployment of the Voyager application in a multi-tiered environment. The diagram has been simplified to exclude more complex network factors such as routers, bridges and firewalls.

Figure 6



The BusinessObjects Enterprise server that manages communication between the Voyager application and Microsoft Analysis Services is called Multi-dimensional Analysis Services (MDAS). Figure 6 shows how the MDAS starts a session on the backend Analysis Services by first authenticating with a Windows account. The MDAS performs this authentication in one of the following ways:

- Passing the username and password as property values in a connection string.
- Impersonating the Windows user's security context.
- Passing the security context of the service account.

Prerequisites

The authentication method that is used by the Voyager application depends on the following prerequisites:

- Ensure that BusinessObjects XI R2 is installed and patched to Service Pack 2. BusinessObjects Voyager is installed separately as part of the Productivity Pack.
- Server running the MDAS Service must have SQL Server 2005 Client Components, MDAC 2.8 and OLE DB Providers for OLAP Services 8.0 (Analysis Services 2000) or 9.0 (Analysis Services 2005) installed. The Analysis Services client components must be patched to the same service pack level as the Analysis Services backend.
- At least one security role has been defined and applied to the target cubes on the Analysis Services server.

Authenticating to Analysis Services 2005 on a local or remote server

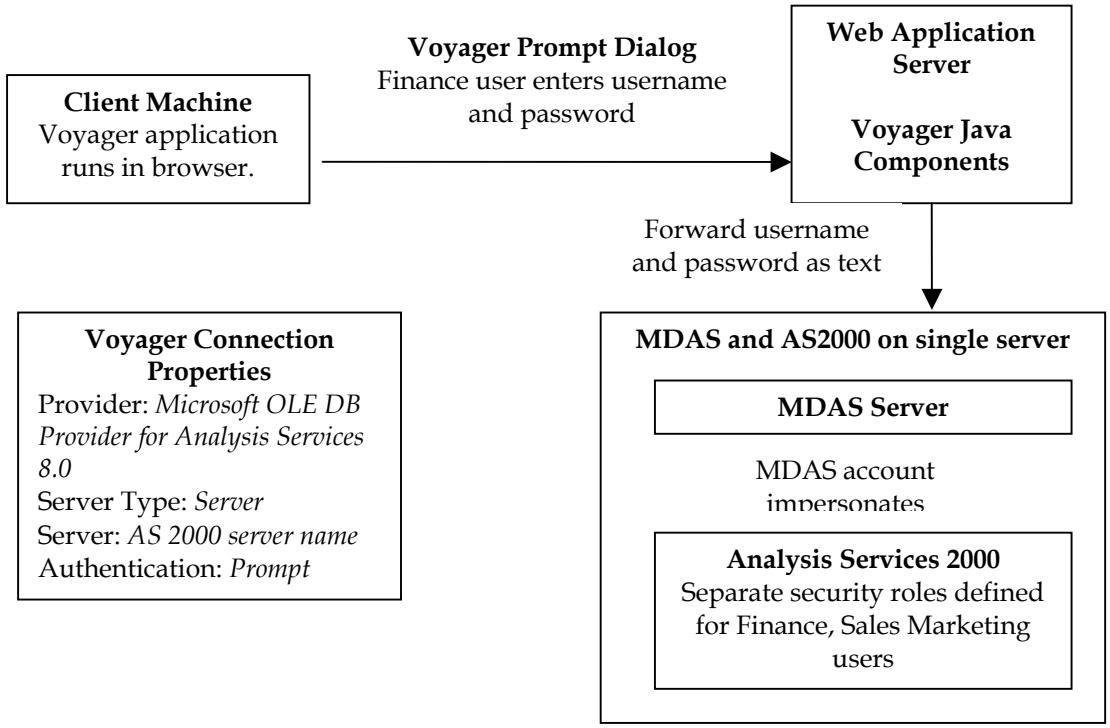
The OLE DB Provider for OLAP Services 9.0 allows you to connect to Analysis Services 2005 by passing user ID and password as property values in a connection string.

The OLE DB Provider for OLAP Services 8.0, however, does not support the user ID and password properties in the connection string. If you are connecting to Analysis Services 2000, you must configure the MDAS server for impersonation. Refer to the following section for the steps to configure MDAS for impersonation.

Description of deployment scenario

- The backend server is Analysis Services 2005.
- MDAS and Analysis Services 2005 are installed on the same machine or on separate machines
- Authentication type of the Voyager connection is set to **Prompt** or **Use specified credentials**
- BusinessObjects Enterprise XI R2 Fix Pack 2.3 is installed on the MDAS server machines.
- Role security model filters cube data based on user identity.

Figure 7



Authenticating to Analysis Services 2000 on a local server

Microsoft documentation defines impersonation as the ability of a thread to execute in a security context that is different from the context of the process that owns the thread. The MDAS service runs as a process under a Windows domain or local account. By default, it runs under the local system account. You can view or change the account that the MDAS launches with by going to **Start > Programs > BusinessObjects XI Release 2 > BusinessObjects Enterprise > Central Configuration Manager** or **Start > Settings > Control Panel > Administrative Tools > Services**.

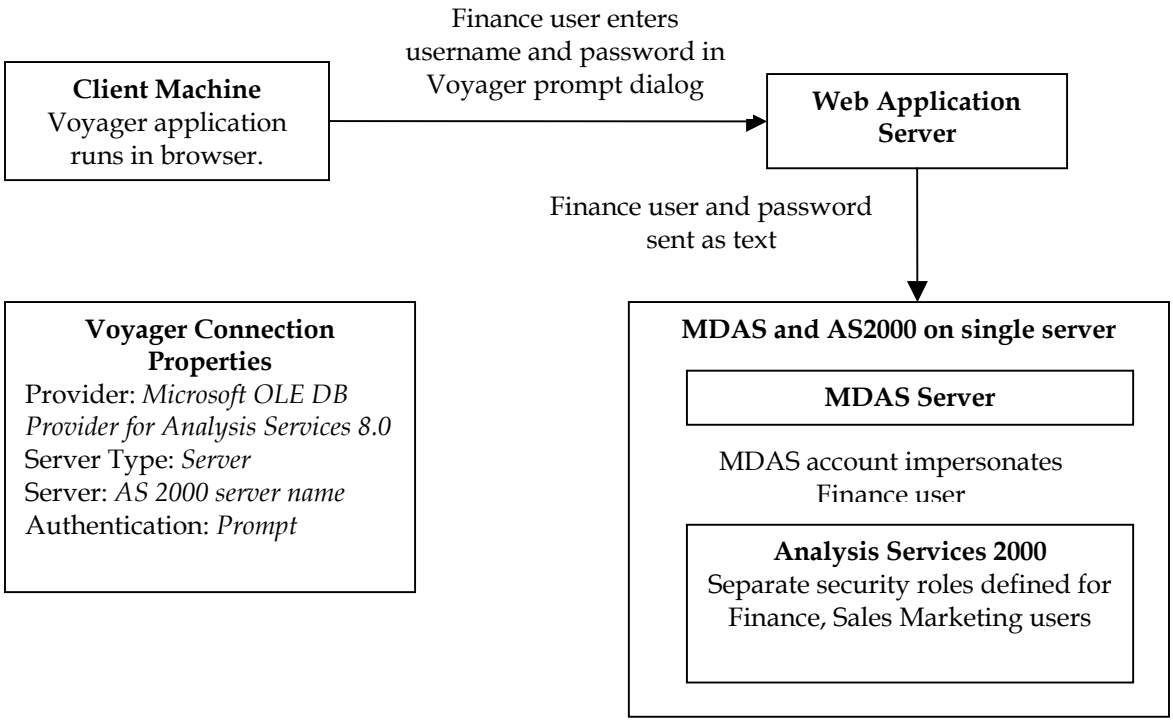
If your security role model restricts access to cube data based on user identity, then you must configure the MDAS service account so that it can impersonate the different Windows users that request data through the front-end Voyager application. If impersonation is successful, the MDAS launches a thread in the security context of the Voyager application user when it connects to the Analysis Services server.

When the MDAS impersonates a client security context to request local resources, the level of impersonation is referred to as impersonate. At this level, no additional configuration is required. In this scenario, the MDAS server can impersonate the client's security context to connect to an instance of Analysis Services server installed on the same physical machine.

Description of deployment scenario

- Backend server is Analysis Services 2000.
- MDAS and Analysis Services 2000 are installed on the same physical machine.
- Authentication type of the Voyager connection is set to **Prompt** or **Use specified credentials**
- Analysis Services role security model filters cube data based on user identity.

Figure 8



Authenticating to Analysis Services 2000 on a remote server

If the MDAS server attempts to connect to a remote Analysis Services server, impersonation will fail. Impersonating a client to access resources on a remote server requires a higher level of impersonation known as delegation. Delegate level impersonation allows the MDAS server to pass the client's security context to an Analysis Services instance running on a remote server. All Windows accounts and servers that are involved in the delegate process must belong to the same Active Directory domain or to trusted domains in the same forest.

Delegate is the most powerful level of impersonation. It requires you to configure the following in your environment:

- The client account being impersonated must not be marked as **Account is sensitive and cannot be delegated** in the Active Directory Service.
- The server account must be marked with the **Trusted for delegation** attribute in the Active Directory Service.
- Service Principal Names have been created for the MDAS and Analysis Services service accounts.

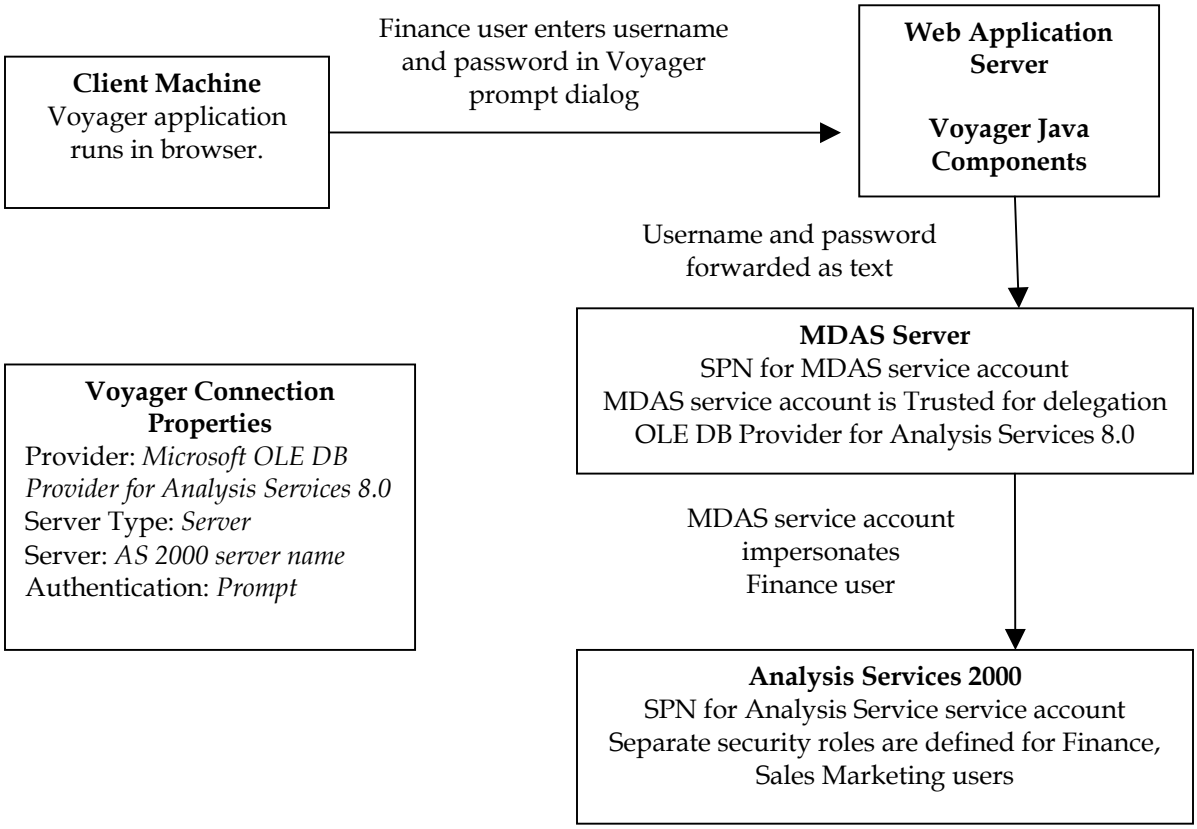
Refer to the section for detailed configuration instructions.

Description of deployment scenario

- Backend server is Analysis Services 2000.
- MDAS and Analysis Services 2000 are installed on separate machines.
- Authentication for Voyager connection is set to **Prompt** or **Use specified credentials**.
- Analysis Services role security model filters cube data based on user identity.
- The computers hosting the client, the server, and any downstream servers must all be running in a Windows 2000 or 2003 domain.

NOTES	
	• If the MDAS or MSAS 2000 reside in separate domains, they must belong to trusted domains in the same forest. • Connectivity fails if either the MDAS server or MSAS 2000 server belongs to a Workgroup. • The MDAS server cannot authenticate to a remote MSAS 2000 server in a Workgroup.

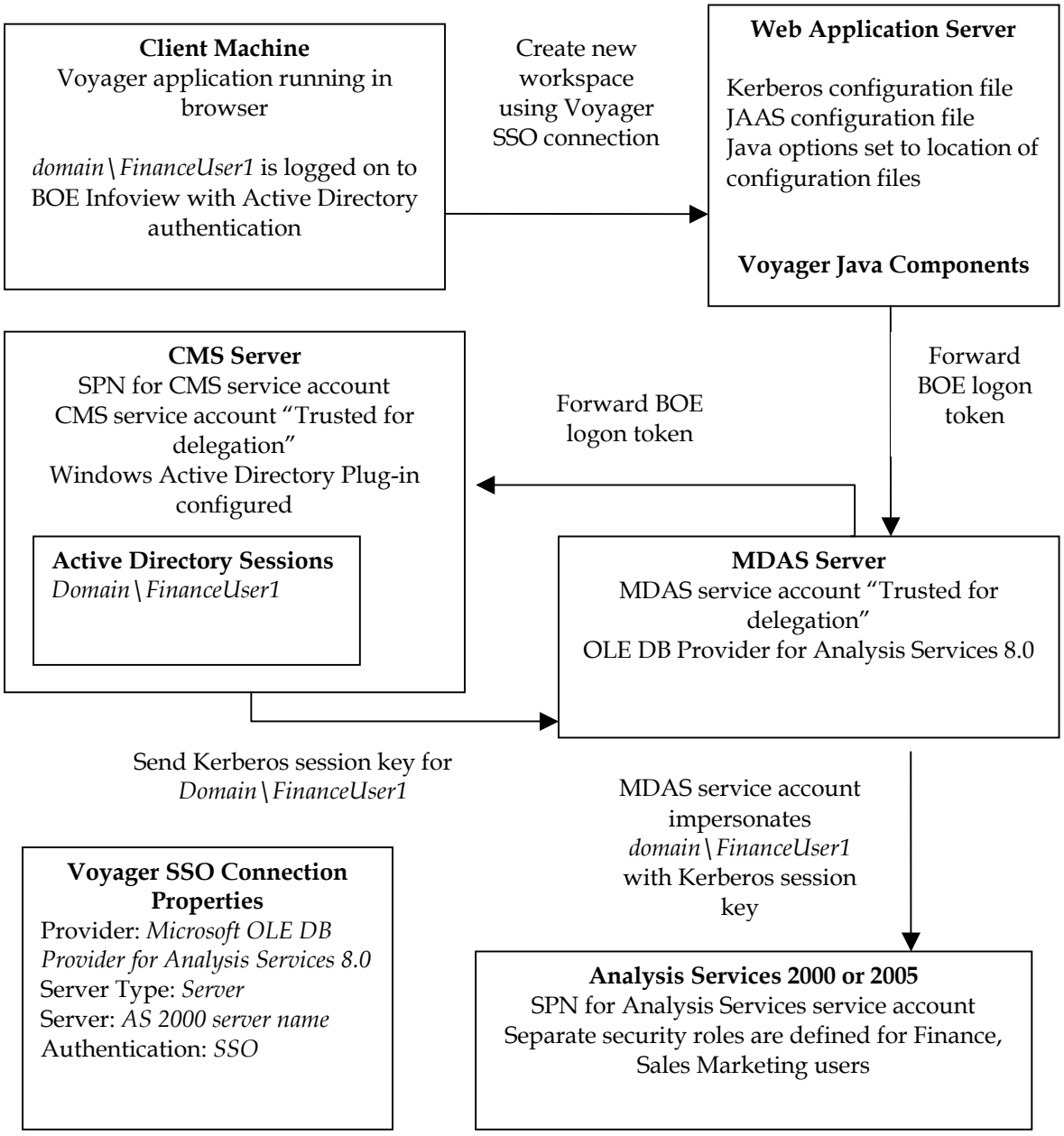
Figure 9



Authenticating with Single Sign-On to Analysis Services 2000 and 2005

Voyager supports end-to-end single sign-on (SSO) to Analysis Services. In this scenario, a user who logs on to BusinessObjects Enterprise InfoView with Active Directory (AD) authentication is not prompted again for credentials when he connects to Analysis Services in a Voyager workspace. Voyager passes the AD credentials of the current InfoView user to the backend Analysis Services server.

Figure 10



Description of deployment scenario

- Backend server is Analysis Services 2000 or 2005.
- MDAS and Analysis Services 2000 or 2005 are installed on separate machines.
- Authentication for Voyager connection is set to SSO.

- Analysis Services role security filters cube data based on user identity.

Configuring Voyager for SSO to MSAS 2000/2005:

- Fix Pack 2.3 must be installed on the BusinessObjects Enterprise Servers. The hot fix can be found at the following link and will be available at the end of July 2007.

  http://support.businessobjects.com/downloads/critical_hot_fixes/default.asp

- You must have Enterprise configured with AD and Kerberos and should be able to login to Infoview using AD credentials. For details on configuring the Java Infoview with AD and SSO, download the BusinessObjects Enterprise XI Release 2 Deployment and Configuration Guide.

- After InfoView has been configured for AD, the krb5.ini file must be modified to include the "forwardable" directive, which ensures that the TGT tickets can be forwarded from the CMS to other servers. This directive is not shown in any of the krb5.ini samples provided in the Deployment and Configuration Guide. Add the following line to the krb5.ini:

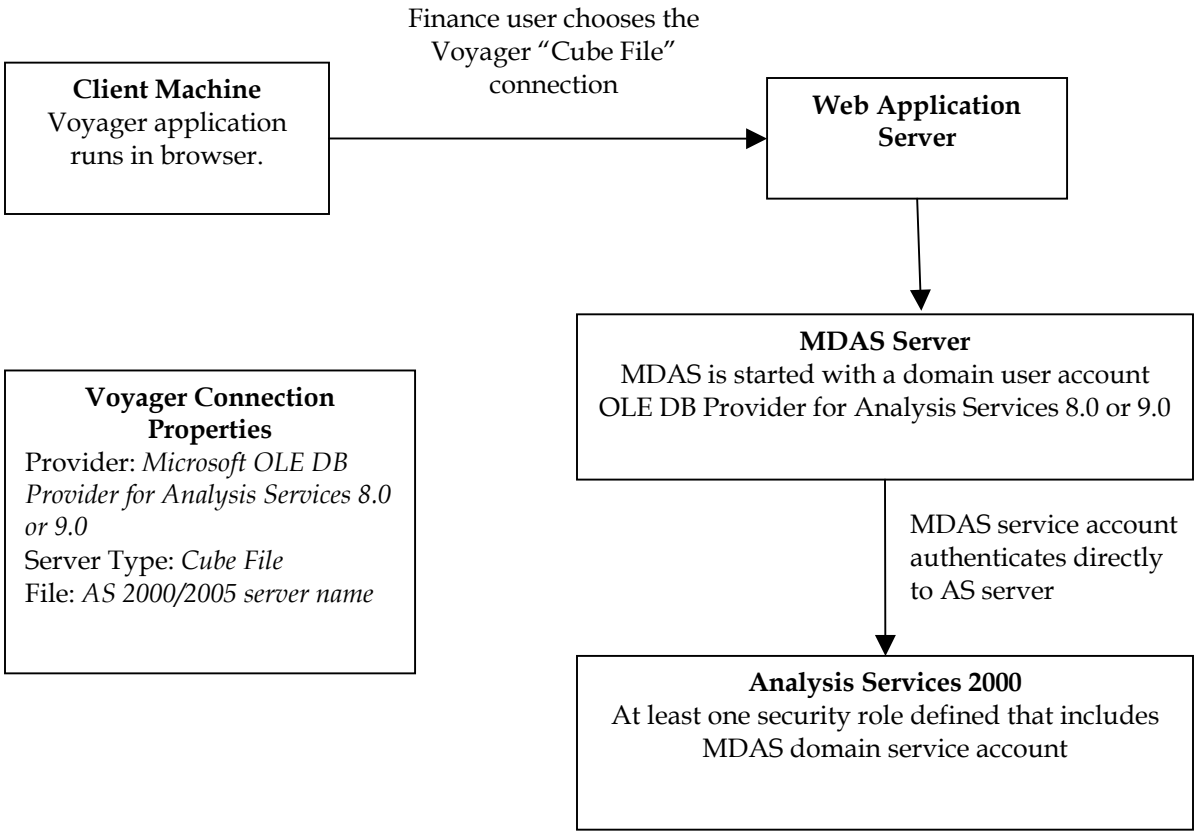
  ```
  forwardable = true
  ```

  This line would be added to the libdefaults section of the krb5.ini file. An example of a simple krb5 configuration can be seen below:

  ```
  [libdefaults]
  default_realm = AUTOSALES.COM
  dns_lookup_kdc = true
  dns_lookup_realm = true
  forwardable = true
  [realms]
  AUTOSALES.COM = {
  kdc = DOMAIN_CONTROLLER.AUTOSALES.COM
  default_domain = AUTOSALES.COM
  }
  ```

- Voyager must be configured for delegation.

Figure 11



Configuring Voyager for delegation

Configuring Active Directory

The MDAS service account will need to have the rights to delegate on the domain. By default, the MDAS service is runs under the LocalSystem account. You can choose to leave the MDAS service running under the LocalSystem account and configure the computer where the MDAS service runs to be trusted for delegation. Refer to the section Configuring Computers for Delegation. This is not recommended; however, as any service running on the server under the LocalSystem account will have the ability to impersonate other users.

The more secure option is to create a separate domain user account to start the MDAS service with and to only trust this specific service account for delegation. The following sections discuss how to create and configure a domain account for delegation on the different Domain Functional Levels.

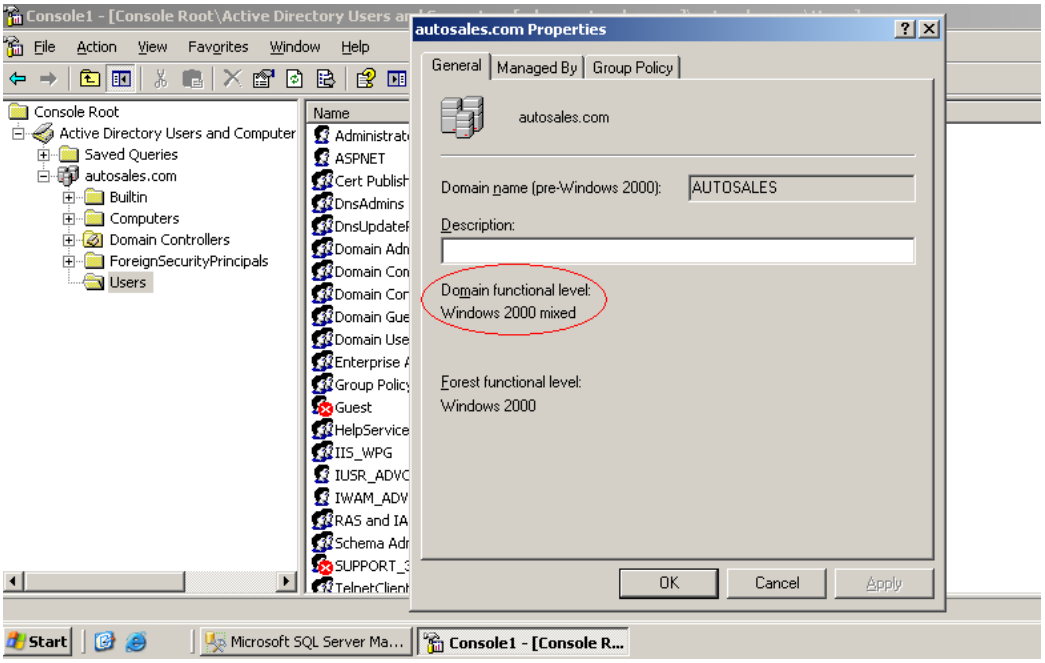
How to determine domain functional level

The current domain functional level can be determined by opening the **Active Directory Users and Computers** snap-in. The tool can be found on the domain controller by clicking **Start > Programs > Administrative Tools > Active Directory Users and Computers**.

If you are performing the check from a server on the domain other than the domain controller, you can access the tool by:

1. Clicking **Start > Run**.
2. Type "mmc" in the text field and click OK.
3. In the Console window, click **File > Add/Remove Snap-In… > Add** button in the Standalone tab of the Add/Remove Snap-In dialogue box.
4. Select **Active Directory Users and Computers** from the list and click the **Add** button and then click **Close**.
5. Click **OK** in the **Add/Remove Snap-in** dialogue box.
6. Right-click on the domain that the BusinessObjects Enterprise Server belongs to and select **Properties**.

Figure 12



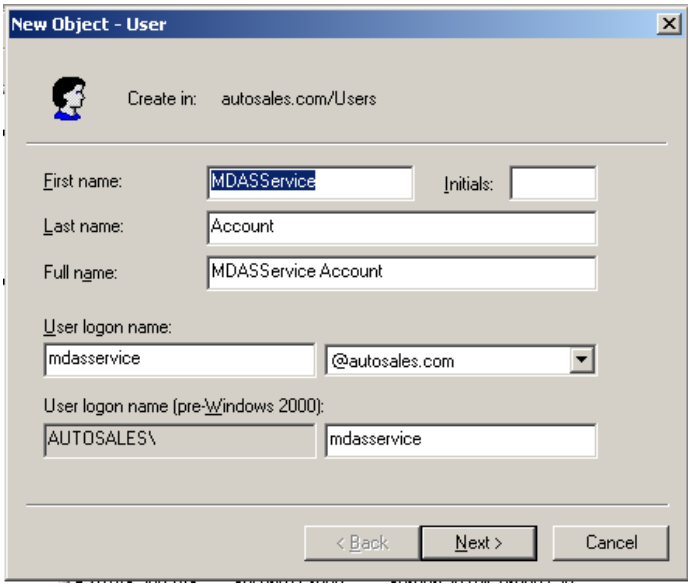
7. Look at the Domain Functional Level property located on the **General** Tab of the properties sheet to determine the mode your domain is running in.

Creating the service account in a Windows 2000 domain

1. Launch the **Active Directory Users and Computers** console.

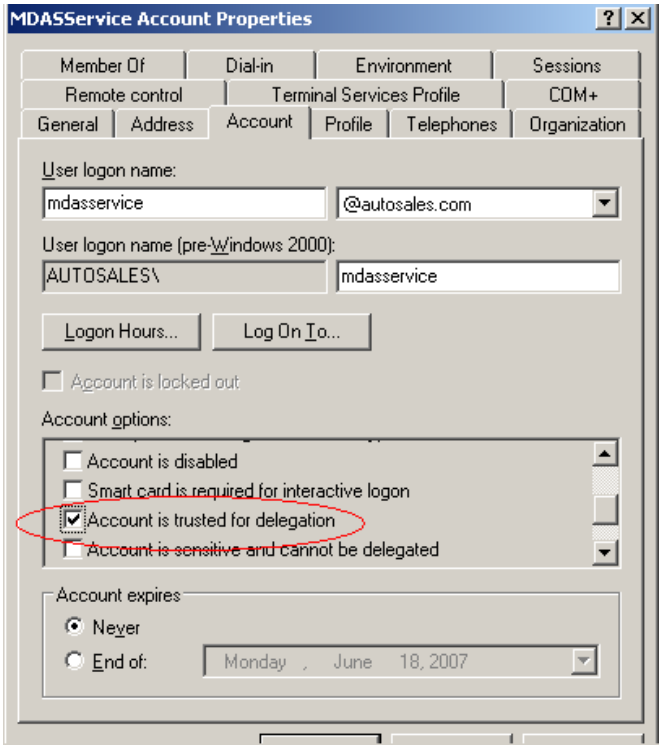
2. Click on the Users container and click the **Create a new user in the current container** button on the toolbar.

Figure 13



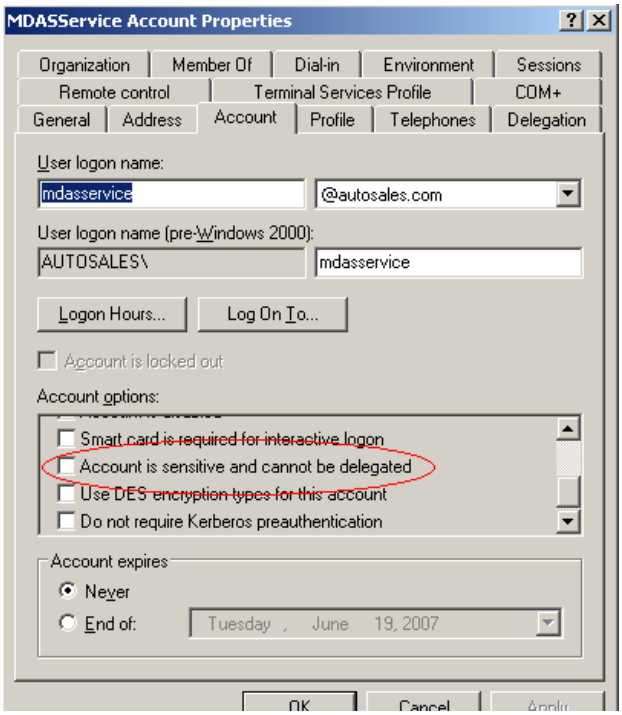
3. Create the service account and click **OK**.
4. Right-click on the user and select **Properties**.
5. Click the **Account** tab, ensure **Account is Trusted for Delegation** option is selected and click **OK**.

Figure 14



6. Ensure that the account has the **Account is Sensitive and cannot be Delegated** option cleared.

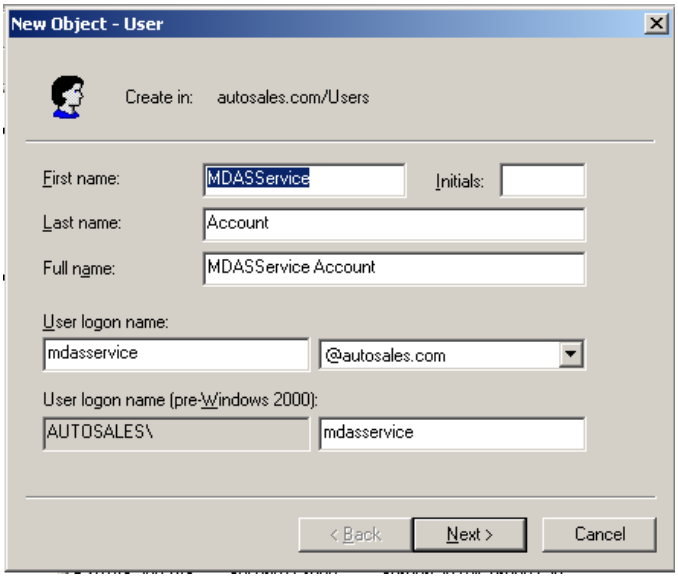
Figure 15



Creating the service account in a Windows 2003 domain

1. Launch the **Active Directory Users and Computers** console.
2. Click the **Users** container and click the **Create a new user in the current container** button on the toolbar.

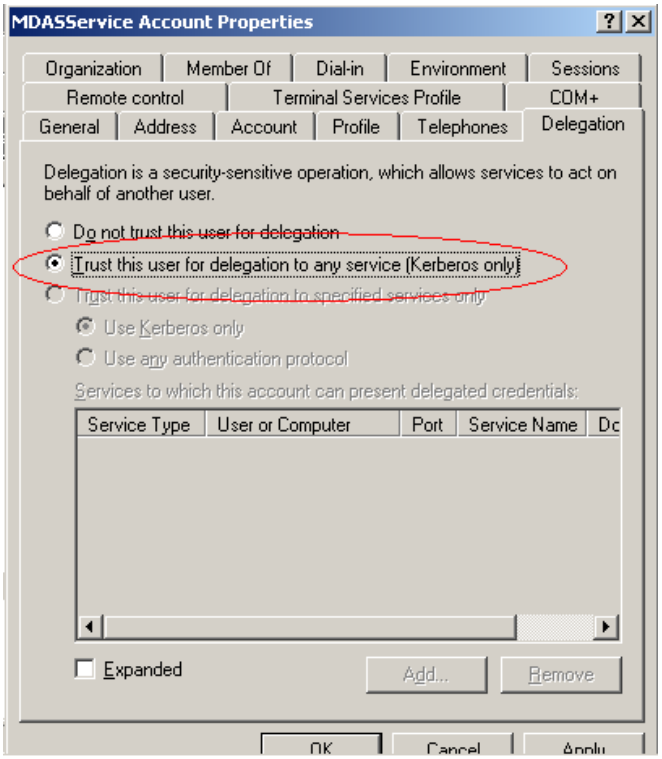
Figure 16



3. Create the service account and click **OK**. Once completed, right click on the user and select **Properties** from the drop down menu.

4. Click the **Delegation** Tab and ensure that **Trust This User for Delegation to Any Service** is selected. Windows 2003 Delegation options differ slightly in that there is no **Account is Trusted for Delegation** option.

Figure 17



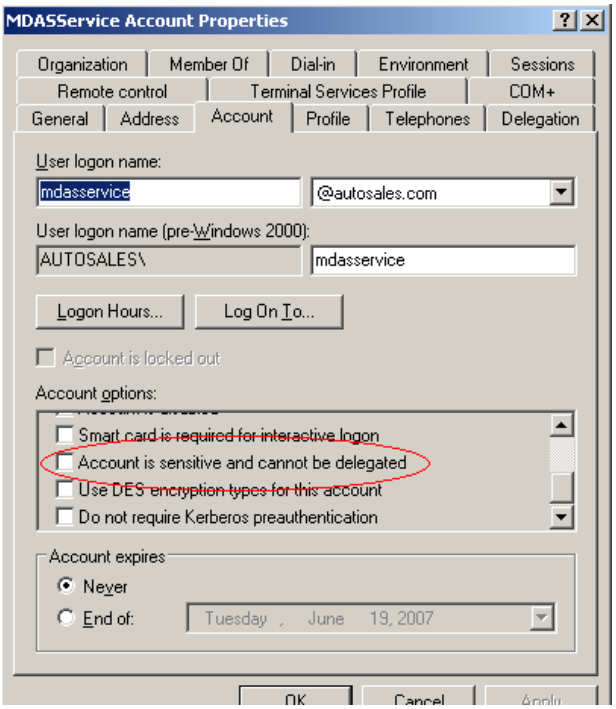
NOTES	If you cannot see the Delegation tab, read the Register a Service Principal Name (SPN) for the computer account using the Setspn utility section.

5. Set the Kerberos option on the **Delegation** tab and then delete the SPN as one is not required for the MDAS Service account.

CAUTION	Delegation is only intended to be used by service accounts, which should have registered SPNs, as opposed to a regular user account, which typically does not have SPNs.

6. Ensure that the account has the **Account is Sensitive and Cannot be Delegated** option cleared.

Figure 18



Configuring computers for delegation

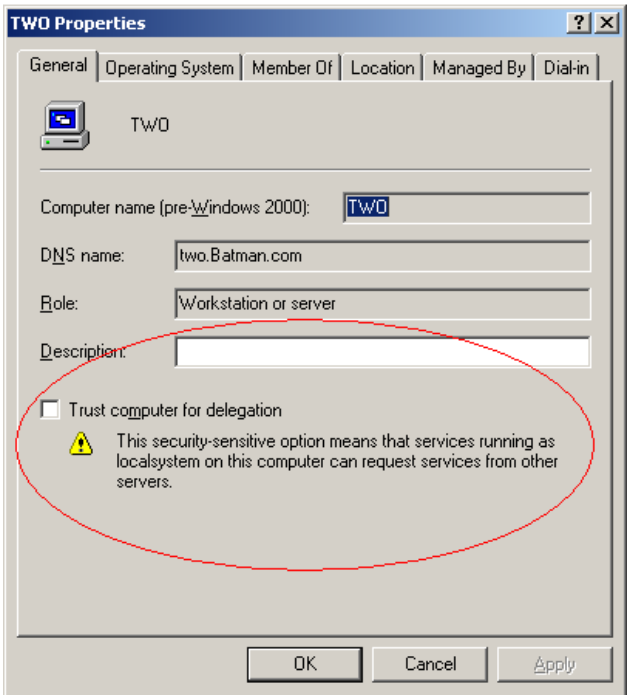
If the MDAS service is configured to start with the LocalSystem account, the server where the MDAS service runs must be trusted for delegation. Delegation allows services running on the trusted server to connect to any resource within the domain with the credentials of another user (impersonation). The middle-tier service in this case would consist of the MDAS server taking credentials from the client and authenticating against Analysis Services using delegation.

In order to trust the server for delegation, perform the following steps:

1. Launch the **Active Directory Users and Computers** console.
2. Click the **Computers** container and locate the server where the MDAS service is located.
3. Right-click on the server name in the right pane and click **Properties**.

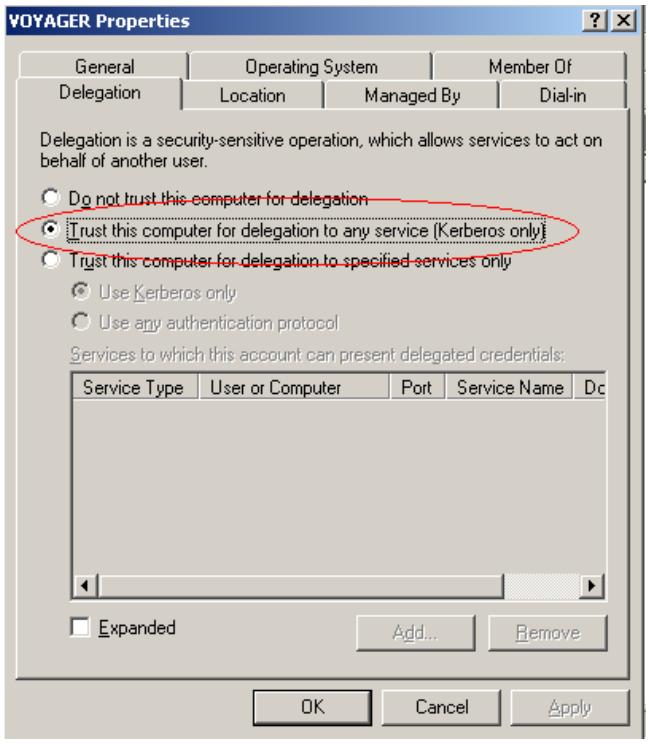
4. For a 2000 Domain Functional Level, select the check box on the **General** tab marked **Trust Computer for Delegation**.

Figure 20



For a 2003 Domain Functional Level, click the **Delegation** tab and select **Trust this Computer for Delegation to Any Service**.

Figure 21



NOTES	To perform all of the procedures on the previous page, you must be a member of the AD Domain Administrators group or Enterprise Administrators group, or you must have been delegated the appropriate rights to perform the tasks.

Configuring the Service Principal Names

Delegation uses Kerberos as the security protocol for authentication. Kerberos identifies network services with Service Principal Names (SPN). An SPN is used by the requesting client to uniquely identify the resources that it needs to access on the network. In this case, the MDAS service must be able to locate the SPN for the Analysis Services hosts that it needs to authenticate to. It does this by first requesting a ticket from the Key Distribution Centre (KDC) on behalf of the Voyager user who wants to connect to Analysis Services. To set the SPN's required for authentication for the MDAS service as well as MSAS 2005, follow the steps below.

Analysis Services SPN required for Kerberos and delegation

1. Ensure the setspn utility is installed on the Analysis Services server. The setspn utility can be downloaded from the following link:

   http://www.microsoft.com/downloads/details.aspx?familyid=5fd831fd-ab77-46a3-9cfe-ff01d29e5c46&displaylang=en

2. Log into the server as a member of the Domain Administrators group in order to create new SPNs with the setspn utility.
3. To create the SPN for the Microsoft Analysis Services Server, run the following commands at a command prompt:

   a. If your Analysis Services Server is running under the LocalSystem account:

      Setspn.exe -A MSOLAPSvc.3/MSAS_Server_Host_Name MSAS_Server_Host_Name

      Setspn.exe -A MSOLAPSvc.3/MSAS_Server_Host_Name.FQDN MSAS_Server_Host_Name.NETBIOS

      For example:

      C:\Setspn.exe MSOLAPSvc.3/MSAS MSAS

      C:\Setspn.exe MSOLAPSvc.3/MSAS.AUTOSALES.COM MSAS

NOTE	The format of the commands above will be: Setspn.exe MSOLAPSvc.3/ServerNameInNetbios ServerNameInNetbios AND Setspn.exe MSOLAPSvc.3/ServerNameInFQDN ServerNameInNetbios

b. If your Analysis Services Server is running under a domain account:

Setspn.exe -A MSOLAPSvc.3/MSAS_**Server_Host_Name**.**Netbios Domain\UserName**

Setspn.exe -A MSOLAPSvc.3/MSAS_**Server_Host_Name**.**FQDN Domain\UserName**

When viewing the results of the SPNs created below using the following command, you should the results below based on the example above:

Setspn.exe –L MSAS

MSOLAPSvc.3/msas

MSOLAPSvc.3/msas.autosales.com

NOTE	Microsoft Analysis Services 2005 supports named instances. If your server is using an instance name then use the setspn to create your SPNs as follows: Setspn.exe –A MSOLAPSvc.3/MSAS_Server_Host_Name.FQDN:Instance_Name Setspn.exe –A MSOLAPSvc.3/MSAS_Server_Host_Name_Netbios:Instance_Name

MDAS Service Account SPN required for Kerberos and delegation

1. Ensure the setspn utility is installed; this step will need to be performed for all servers where a BOE MDAS Server is running. You can download the setspn utility from the following location:

   http://www.microsoft.com/downloads/details.aspx?familyid=5fd831fd-ab77-46a3-9cfe-ff01d29e5c46&displaylang=en

2. Log into the server as a member of the Domain Administrators group in order to create new SPNs with the setspn utility.
3. To create the necessary SPNs needed for delegation enter the following commands at the command prompt:

   a. Setspn.exe –A BOBJMDASServer/HostName.FQDN DOMAIN\MDASServiceAccount

b. Setspn.exe –A BOBJMDASServer/HostName.NETBIOS DOMAIN\MDASServiceAccount

NOTES	• Replace HostName.FQDN with the fully qualified hostname of the server where the MDAS Service is located. • Replace HostName.NETBIOS with the short hostname of the server where the MDAS Service is located. • Replace DOMAIN\MDASServiceAccount with your domain name and service account name that the MDAS Service is running under.

For example, in an environment with a domain name of AUTOSALES.COM, servername of BOEXI, and service account named MDASService see the commands below:

Setspn.exe –A BOBJMDASServer/BOEXI.AUTOSALES.COM AUTOSALES\MDASService

Setspn.exe –A BOBJMDASServer/BOEXI AUTOSALES\MDASService

Configuring required Local Policies on MDAS server

The AD service account that will be used to start and run the MDAS service will need specific privileges on the server it runs. This is in order to get the rights needed to authenticate over the network. Follow the steps below to grant the rights needed:

1. On the server where the MDAS service resides, click **Start > Programs > Administrative Tools > Local Security Policy**.
2. Expand the Local Policies folder.
3. Click **User Rights Assignment**.
4. Ensure the AD MDAS Service account created earlier is added to the user lists for the following rights:
    a. Act as Part of the Operating System
    b. Logon as a Service
    c. Impersonate a Client After Authentication

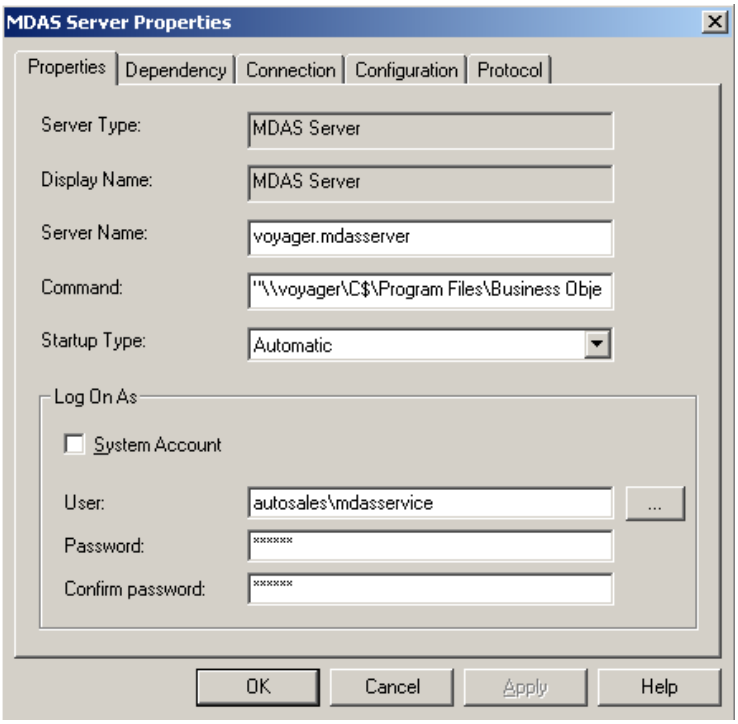
NOTE	The above steps are not required if the MDAS server is running under the LocalSystem account.

Configuring the Multi-Dimensional Analysis Service account

For the MDAS service to be configured to pass client credentials using delegation, the service must be configured to run under a domain account that has been trusted for delegation. The following steps will guide you through this process:

1. Click **Start > Programs > BusinessObjects XI Release 2 > BusinessObjects Enterprise > Central Configuration Manager**.
2. Select the MDAS Service from the list of services and press the **Stop** button located on the toolbar.
3. Double-click the MDAS Service to open its properties sheet.
4. Clear the **System Account** check box.
5. Enter the credentials for the service account into the boxes and click **OK**.
6. Start the MDAS Service.

Figure 22



Creating Voyager connections in the Central Management Console

Before users can begin working with Analysis Services cube data in Voyager, you must create a Voyager connection object that contains the necessary information to connect to the cube: server name or address, catalog name, cube name, etc. The Voyager connection is stored in the Business Objects Enterprise repository.

You create new Voyager connection objects and manage existing connection objects in the Central Management Console (CMC).

Follow the directions below to get started creating Voyager connections:

1. Click **Start > Programs > BusinessObjects Enterprise XI Release 2 > BusinessObjects Enterprise > BusinessObjects Enterprise Java Launchpad > Central Management Console**.

   Alternatively you can enter the URL in a browser, which would look similar to:

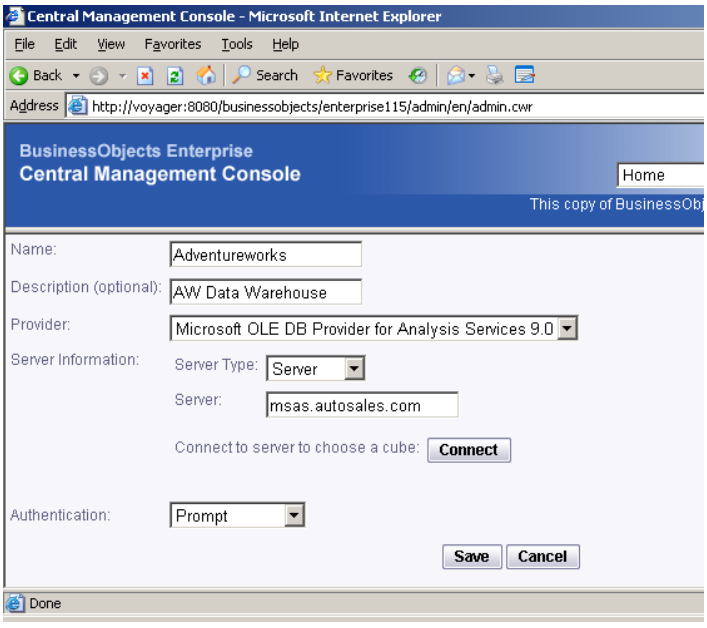
   http://<web_application_server:port>/businessobjects/enterprise115/adminlaunch

NOTE	Replace <web_application_server:port> with the hostname and port that your web application server runs on.

2. Click on **Voyager Connections** located in the **Organize** grouping.
3. Click the **New** button located near the top right of the browser window.
4. Enter the required information to set up the connection:

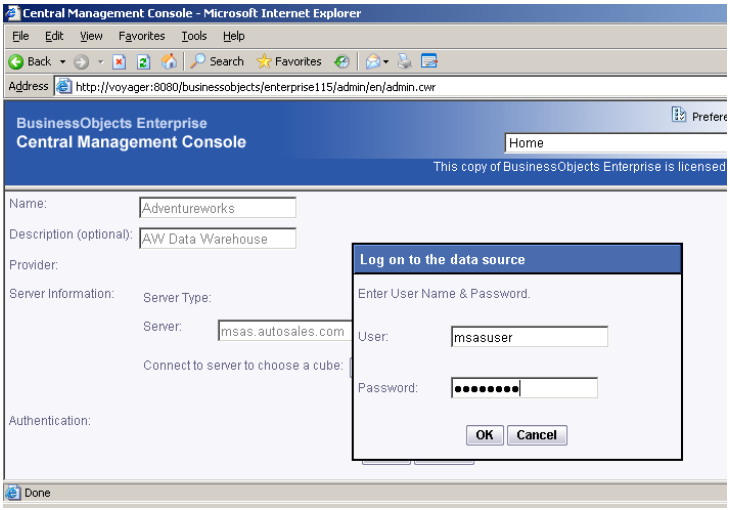
NOTES	Name – Used to reference the connection within InfoView when creating reports off the connection Description – Optional but useful for better organization of the connections as well as for referencing at a later time. Provider – Refers to the driver that will be used to connect to the OLAP datasource. This should read 'Microsoft OLE DB Provider for Analysis Services 9.0' when connecting to MSAS 2005. Server Type - This is the type of datasource; Server, Cube or HTTP URL. In this case we will be using the 'Server' server type to connect to an Analysis Services database on the network. Server Name – The hostname of the server hosting MSAS 2005.

Figure 23



5. Press the **Connect** button to enter the domain credentials required to select a cube that this connection will reference.

Figure 24



NOTES	
	Prompt - Always prompt users for logon credentials. User Specified - With this option selected, the administrator enters a specific username and password which will be stored as part of the connection object. This information will always be used to authenticate to the backend server when this connection object is accessed from a Voyager application. This does not require you to log on in the Voyager application. However, since the same AD credentials are used for every user who accesses the cube through this connection, this option is not always suitable. SSO - With the SSO option selected, you sign on once to the InfoView using your AD credentials and then is able to connect to the backend servers in Voyager without having to enter the username and password again. The Voyager application (through the MDAS server) automatically retrieves the Active Directory credentials from the current InfoView session and passes them to the server.

6. Once you have connected and selected a cube, choose the authentication type that will be used for the connection in the **Authentication** dropdown.

7. Click the **Save** button to save the connection with the properties entered.

Troubleshooting

When you encounter authentication errors in the Voyager application, enable login profiling on your Analysis Services server for troubleshooting. SQL Server Analysis Services 2005 traces login attempts with the SQL Profiler, which can be accessed from the SQL Server Management Studio.

To enable the same tracing for SQL Server Analysis Services 2000, you must modify a registry key and then restart the Analysis Services in the Control Panel. The login attempts are recorded in the Windows Event Viewer. See the section Finding more Information for details.

Error in the CMC when creating a Voyager connection: "Login Failed. Please check that your username and password are valid"

This error is shown if the username and/or password being used to authenticate against AD are incorrect. You will not see a login attempt in SQL profiler when you receive this error in Voyager as the login has failed against the domain controller and not Analysis Services, check that the username and password are correct and then try to login again.

Error "Internal Error: An unknown exception has occurred."

When trying to create a new Voyager Workspace using a connection configured for SSO logon type, you receive an error stating that an unknown exception has occurred. You have logged on to InfoView with your domain credentials so why are you seeing this error?

This error appears when the MDAS Service is still running under the default LocalSystem account or under an account that has not been configured with the proper SPNs and delegation options needed for Kerberos authentication.

To configure the MDAS Service, see the section above called Configuring the Multi-Dimensional Analysis Service Account.

"No Cubes Found" when creating a new Voyager connection?

If you have authenticated against AD and do see your credentials being passed to Analysis Services through SQL Profiler, or see the Success Audit in Event Viewer to indicate your username/password are being passed properly but yet you do not see any cubes. Confirm that you have set up roles in Analysis Services. Check the section above called Configuring Analysis Services Roles for MSAS 2000 or Configuring Analysis Services Roles for MSAS 2005 for further information on how to perform this task.

Error "An error has occurred propagating the security context between the security server and the client."

When attempting to create a new Voyager Workspace in Infoview using a connection that has been configure to use SSO as the logon type, you receive an error stating that an error occurred while propagating the security context. This error will appear if the tickets being requested from the KDC are not forwardable tickets. These tickets then cannot be used by the Krb5 login module to authenticate the user because no other services besides the one that requested the ticket can use it. See the section above on Configuring Voyager for SSO to MSAS 2000/2005 for instructions on adding the proper directives to your KRB5.INI file.

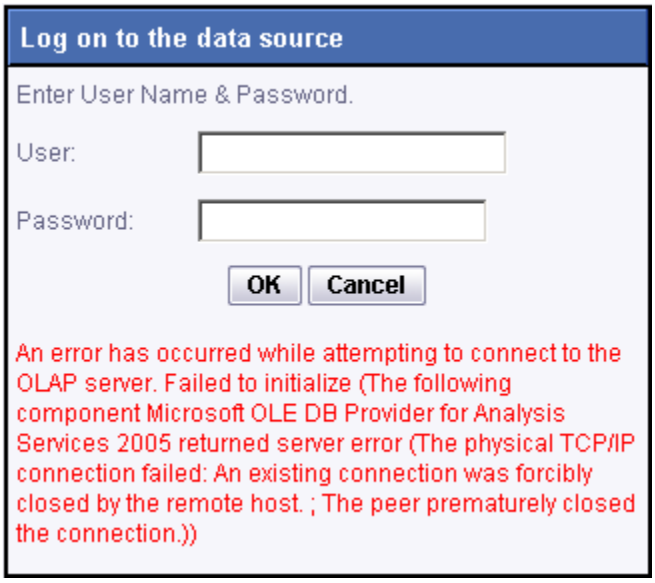
Error "An error has occurred while attempting to connect to the OLAP server. Failed to initialize…"

When attempting to connect to Analysis Services through Voyager, you get an error similar to that shown in the screenshot below. Running SQL profiler reveals that instead of passing the domain credentials, Anonymous is being used in place to authenticate.

You will see this error because the MDAS service cannot forward the domain logon credentials of the user to the Analysis Services server. The error is a result of something commonly referred to as the double hop scenario where a user logs on and is authenticated on one computer but then uses a client application to attempt to connect to a service on another computer through a service running on an intermediary computer, or middle layer. On Microsoft Windows 2000 and 2003, the forwarding of a user's security credentials is not allowed unless Kerberos is configured properly.

An example scenario here would be where the user is passing credentials from their web browser to the MDAS service, which in turn is using delegation to authenticate against AD and then against MSAS 2005. If Kerberos has not been setup properly, the MDAS service will not be able to delegate these credentials and Anonymous will be sent instead of the users credentials. Carefully follow the steps outlined in this guide to ensure that the setup required for authentication is properly configured.

Figure 25



Error "The authentication provider (secEnterprise) associated with this logon session does not support inter-process Single Sign-On."

When attempting to create a new Voyager Workspace in InfoView off a connection that is set to use SSO log on, you receive an error stating that the logon session does not support inter-process SSO. This is because

you have logged into InfoView using Enterprise authentication and Enterprise credentials cannot be used to login to Analysis Services. You must ensure that you are logging into InfoView with your AD domain credentials before attempting to use a connection set for SSO authentication.

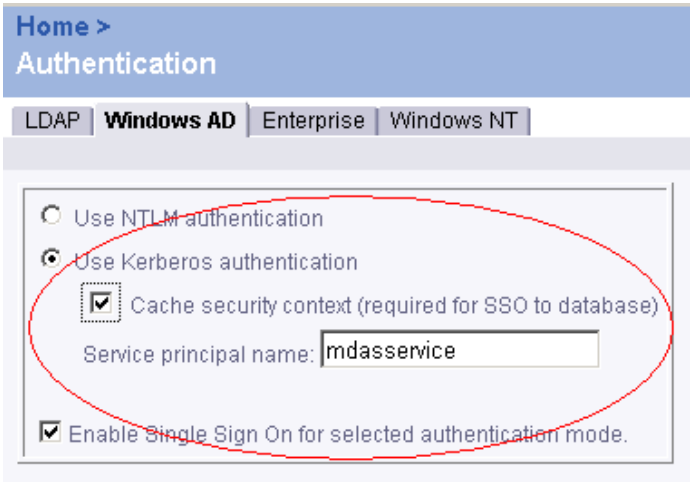
Error "The authentication provider (secWinAD) associated with this logon session does not support inter-process Single Sign-On."

You have logged into Infoview using your AD domain credentials and attempt to create a new Voyager Workspace using a connection that has been set to use SSO as the logon type. Why is the error indicating that Windows AD has not been configured for SSO?

The AD configuration needed to perform SSO to a database has not been completely configured. To ensure that SSO can be accomplished, you will need select the **Cache Security Context** in the **Windows AD** tab. Follow the directions below to make sure this option is secleted:

1. Log on to the CMC.
2. Select **Authentication** from the menu.
3. Click the **Windows AD** tab.
4. Select the **Cache Security Context** check box and enter the account name of the MDAS Service account into the **Service Principal Name** text field.
5. Save settings.

Figure 26



Error "A specified logon session does not exist. It may already have been terminated." or Error "No credentials are available in the security package."

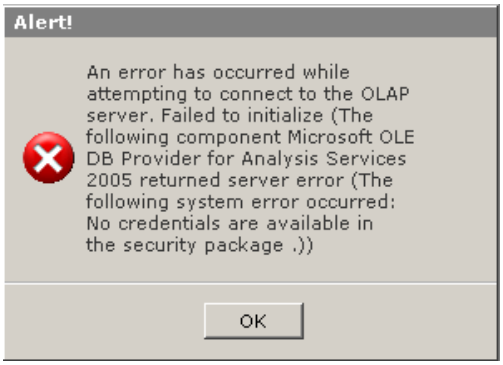
You receive one of the two errors above when creating a Voyager Workspace in Infoview using a connection that is configured to use SSO as the login type. You have followed all of the steps indicated through

this white paper and all configurations are in place yet you cannot seem to complete SSO to the database.

These errors, which can be seen below, have been tracked internally and a fix has been released. You will need to ensure that you have installed Fix Pack 2.3 on the BusinessObjects Enterprise Servers. For further information and to ensure no other requirements are missing, please see the section above on Configuring Voyager for SSO to MSAS 2000/2005.

Figure 27

Figure 28



Using Event Viewer to view log ons

When a user authenticates against MSAS using a client such as Voyager or even Excel, the logon attempt to MSAS is logged in the Event Viewer. If SQL Profiler is not installed, the event viewer can be used to view which username is being passed to authenticate. To view these credentials, open the event viewer on the Analysis Services server by clicking **Start > Programs > Administrative Tooks > Event Viewer > Security** in the left pane. The username, date and time can be viewed in the right pane. Double-click on the event to get more detailed information such as domain and whether the audit was for a success or failed logon attempt.

How to determine the patch level of your SQL Server and clients

To find the patch level of your SQL Server 2005 services, perform the following steps:

1. Launch SQL Server Management Studio.
2. Run the following T-SQL statement:

   SELECT SERVERPROPERTY('productversion'), SERVERPROPERTY ('productlevel'), SERVERPROPERTY ('edition')

3. You will receive output with three columns: Product Version Number, Product Patch Level and Edition.

NOTES	We are interested most in the second column which will indicate whether it is the original product release (RTM), SP1 or SP2. The version number and edition should be noted as well for informational purposes if submitting cases to Business Objects support.

To determine the product version of the SQL Server Client installed on the server running the BusinessObjects MDAS service, perform the following steps:

1. On the server running the MDAS service, click **Start > Run,** type "regedit" and then click **OK**.
2. In Registry Editor, navigate to the following key:

   HKLM\SOFTWARE\Microsoft\Microsoft SQL Native Client\CurrentVersion
3. Look at the Version Key in the right pane and compare the number against the following table:

SQL Client Level	Product Version Number
RTM	9.00.1399.00
SQL Server 2005 Service Pack 1	9.00.2047.00
SQL Server 2005 Service Pack 2	9.00.3042.00

Finding more information

For more information and resources, refer to the product documentation and visit the support area of the web site at http://www.businessobjects.com/

Useful Microsoft information

The next sections are Microsoft web sites that have some useful information on this topic.

Kerberos on Windows 2003

http://www.microsoft.com/windowsserver2003/technologies/security/kerberos/default.mspx

Troubleshooting Kerberos configuration and errors

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/tkerbdel.mspx#E3HAC

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/tkerberr.mspx

Enabling Kerberos Event logging for troubleshooting

http://support.microsoft.com/kb/q262177/

Using SQL Profiler 2005 for tracing logon usernames while troubleshooting

http://msdn2.microsoft.com/en-us/library/ms187929.aspx

How to trace logon usernames for Analysis Services 2000 by enabling AuditEvents

http://msdn2.microsoft.com/en-us/library/aa902654(sql.80).aspx#sql2k_anservregsettings_topic36

Setspn utility download for creating SPNs

http://www.microsoft.com/downloads/details.aspx?familyid=5fd831fd-ab77-46a3-9cfe-ff01d29e5c46&displaylang=en

SQL Server 2005/Analysis Services Service Pack downloads

http://technet.microsoft.com/en-us/sqlserver/bb331754.aspx

Microsoft Analysis Services 9.0 OLE DB Provider

http://www.microsoft.com/downloads/details.aspx?familyid=df0ba5aa-b4bd-4705-aa0a-b477ba72a9cb&displaylang=en

▶ www.businessobjects.com