crystal decisions™

Crystal Analysis

Crystal Analysis Professional Security and the Crystal Enterprise Environment

---

Overview

Crystal Analysis (CA) allows you to connect to and design custom applications against Online Analytic Processing (OLAP) data sources. When connecting to Microsoft Analysis Server, Microsoft's OLAP solution, CA and its web components use Microsoft's security system to determine which data a given user has access to.

The information in this document applies to CA and CE versions 8.5 and 9.

Contents

Introduction

This document focuses on configuring the operating systems hosting the Domain controller, the Microsoft Analysis server, and the Crystal Enterprise (CE) CA components server to use Microsoft security.

This document contains information on the following topics:

- Basic OLAP Security
- Secondary Logon
- Differences between Windows NT LAN Manager (NTLM) and Kerberos security with regards to CA
- Configuration of CE to use Kerberos or NTLM to access OLAP data

Required Software and System Assumptions

For the topics discussed in this document, the following system attributes are assumed:

- A full installation of:

  Crystal Enterprise 8.5 including the Crystal Analysis Professional 8.5 Web Components

  - OR -

  Crystal Enterprise 9.0 including the Crystal Analysis Professional 9.0 Web Components
- Microsoft Windows 2000 Server with Service Pack 3 applied
- Microsoft PivotTable Service included with the Microsoft Analysis Server service pack 3.
- If you are implementing version 8.5 then you will need the newest CAP 8.5 and CE 8.5 hot fixes.

CE 8.5 APS Hot Fix -
ftp://ftp.crystaldecisions.com/outgoing/ehf/ce85apswin_en.zip

CE 8.5 Common Hot Fix -
ftp://ftp.crystaldecisions.com/outgoing/ehf/ce85comwin_en.zip

CE 8.5 SDK Hot Fix -
ftp://ftp.crystaldecisions.com/outgoing/ehf/ce85sdkwin_en.zip

CE 8.5 WCS Hot Fix -
ftp://ftp.crystaldecisions.com/outgoing/ehf/ce85wcswin_en.zip

CE 8.5 Servers Hot Fix -
ftp://ftp.crystaldecisions.com/outgoing/ehf/ce85servwin_en.zip

CAP 8.5 ActiveX Viewer -
ftp://ftp.crystaldecisions.com/outgoing/EHF/CAP85actxwin_en.zip

CAP 8.5 Hot Fix –

ftp://ftp.crystaldecisions.com/outgoing/EHF/CAP85win_en.zip

- The following Microsoft patch:

Microsoft Analysis Server Service Pack 3 -
http://www.microsoft.com/sql/downloads/default.asp

OLAP Security

This section discusses the security considerations for each of the components involved in authenticating a user to an OLAP data source.

OLAP Services is Microsoft's OLAP solution for Microsoft SQL Server 7. Microsoft Analysis Server (Analysis Server) is the OLAP solution for SQL Server 2000. Since version 7, Microsoft's OLAP solution has been included with Microsoft SQL Server but is not installed by default. Microsoft SQL Server and Microsoft Analysis Server are two separate servers, are managed separately, and should not be confused.

Analysis Server supports the following authentication:

- NTLM
- Kerberos
- Negotiate

"When an end user attempts to connect directly to an Analysis server, Microsoft® SQL Server™ 2000 Analysis Services attempts to authenticate the end user based on the credentials the end user was granted in the operating system when the end user logged on to the domain. Analysis Services automatically detects a connecting end user's credentials. If, in the connection string, the end user specifies a user name and password that is different from his or her logon user name and password, the specified user name and password are ignored. If the end user's credentials allow the end user to access the Analysis server computer from the network, authentication on the Analysis server is successful, and the end user is allowed to connect to the Analysis server. If the end user's credentials do not allow the end user to access the Analysis server computer from the network, authentication on the Analysis server is unsuccessful, and the end user is not allowed to connect to the Analysis server."[1]

Microsoft Analysis Server allows an OLAP Administrator to restrict access to certain dimensions or cells based on the logon information supplied by the process attempting to access the data.

For example, when a user logs onto a Windows 2000 computer and attempts to access OLAP data with the CAP thick client, the credentials supplied are sent to the Analysis Server for authentication. If the user supplies a username and password when attempting to connect to the Analysis Server, that information is ignored. That is, the credentials used to run the process will be used for authentication.

NOTE	Windows 2000 Feature Windows 2000 provides a new feature that allows a user to specify which

	credentials are used to run a process. For example, if the CAP thick client is opened by User A with User B's credentials, the OLAP server will receive User B's credentials rather than User A's. To try this, create a shortcut to cap.exe on Windows 2000 and configure it to 'Run as different user'. When you double-click on the shortcut you will be prompted for credentials, fill in the information to proceed. The application is now running with the supplied credentials, not the logon credentials.

The only tool used to create, manage, and maintain the cubes provided by Microsoft Analysis Server is Analysis Manager. The SQL Books Online covers this tool thoroughly. Most of its functionality is outside of the scope of this document. Please refer to the SQL Books Online for more information.

Managing Cube Roles

1. Open Analysis Manager on the Analysis Server by going to **Start** > **Programs** > **Microsoft SQL Server** > **Analysis Services** > **Analysis Manager**.
2. Expand the Server name, the database name, the cubes sub-section, and then find the cube you'd like to review. This is shown in Figure 1.

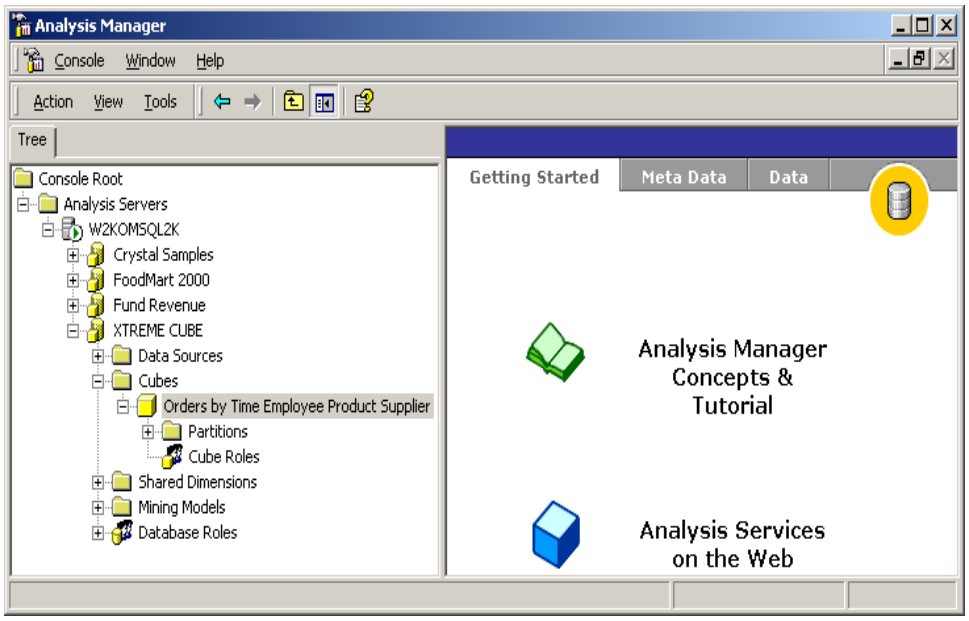


Figure 1

3. Right-click the cube name and click **Manage Roles**. The following screen appears:

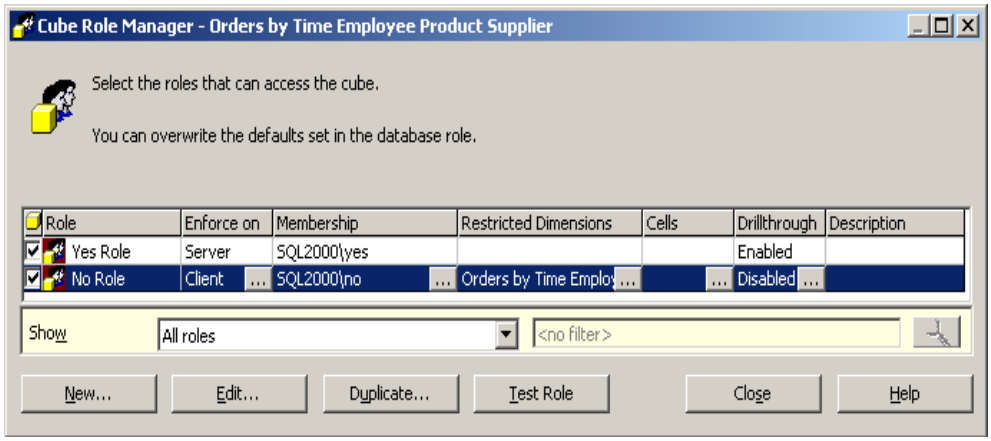


Figure 2

By default, a new cube has no roles defined. An Administrator must define them. If no roles have been defined for a cube then it is completely accessible to everyone. Once a role has been defined, the most important feature on this dialog box is the **Test Role** button. If you highlight a role and click the **Test Role** button, the resulting dialog box displays the data that this role's membership will be allowed to access.

Verifying Cube Roles

Once you have ensured that the cube role is implemented correctly on the server, it is often necessary to verify that the role is being enforced on the client machine as well. To verify client connectivity you must install the following two tools:

- **PivotTable Service** – "PivotTable® Service, which is included with Analysis Services, is an OLE DB provider that supports the optional OLE DB for OLAP extensions. It functions as a connection interface with cache management functionality to Analysis Services to support client application access to OLAP data."[2] In other words, PivotTable Service is the portion of MDAC that allows clients to connect to the Analysis Server. This component must be installed on each machine that connects to the Analysis Server. Typically this includes: clients using the ActiveX viewer, the WCS (WCS), and computers running the CAP thick client.

The two most important PivotTable Service DLLs to consider are msolap.dll and msolap80.dll. When troubleshooting client issues, always make sure that the proper versions of these files are present. Use the following information as a guide:

MSOLAP.DLL – Microsoft OLE DB Provider for OLAP Services. The major versions of this DLL are:

msolap.dll 7.0.1295.428 - Access 2000 SR1, Office 2000 SR1, Small Business Server 2000

msolap.dll 7.0.1073.1114 - Office 2000 Premium or any component (Access, Excel, FrontPage, Outlook, PhotoDraw, PowerPoint, Word)

MSOLAP80.DLL – Microsoft OLE DB Provider for Analysis Services 8.0. The major versions of this DLL are:

msolap80.dll 8.0.760.0 – SQL Server 2000 SP3

msolap80.dll 8.0.534.0 – SQL Server 2000 SP2

msolap80.dll 8.0.384.0 – SQL Server 2000 SP1

msolap80.dll 8.0.3.23 – Office XP Professional, Project 2002 Professional

msolap80.dll 8.0.1.94 – Small Business Server, All version of SQL Server 2000 (Standard, Personal, Professional and Enterprise)

NOTE	There are two different versions of Microsoft OLEDB Provider for OLAP Services: Microsoft OLE Provider for OLAP Services – This driver supports Analysis Server 7.0 cubes. (msolap.dll) Microsoft OLE Provider for OLAP Services 8.0 – This driver supports Analysis Services 2000 cubes and lower. (msolap80.dll) Ensure that you choose the correct driver when connecting to Analysis Services.

NOTE	**Microsoft PivotTable Service** Microsoft Analysis Server service packs often include a newer version of PivotTable Service. When a service pack is applied to an Analysis Server, all computers running either the CAP thick client or CE WCS must have the PivotTable Service updated from the Analysis Server service pack installation directory.

- **Microsoft Excel** – Microsoft Excel 2000 and XP have the ability to create "PivotTable reports". Excel **OLAP source data** gives Excel the ability to connect to an Analysis Server and access the cubes stored there. This is the best tool for verifying that the Analysis Server is returning the appropriate data to the client.

Excel installs a version of PivotTable Service for Excel to use only. The version of PivotTable Service installed by Microsoft Office is insufficient for CAP to connect to a Microsoft Analysis Server. You must install PivotTable Service included with the Analysis Server.

CAP includes a Microsoft Excel add-in that allows users to access Microsoft Analysis data with CAP through Excel.

NOTE	When using PivotTable Service on the Analysis Server, PivotTable Service accesses the Analysis Server's shared cache. No network communication occurs.

Additional References regarding Analysis Server

Like most Microsoft products, Analysis Server can be configured using certain registry values. Information about these entries can be found in the following Microsoft documentation.

Registry Entries for Microsoft SQL Server 2000 Analysis Services

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsql2k/html/sql2k_anservregsettings.asp

Most of these values will have no bearing on your work, but one key is especially important. The following key can be configured to log information in the event viewer that describes which credentials are used to access the data. When initially configuring Secondary Logon this registry key should be enabled.

AuditEvents Registry key

http://msdn.microsoft.com/library/en-us/dnsql2k/html/sql2k_anservregsettings.asp?frame=true - sql2k_anservregsettings_topic05

Analysis Services Component Tools

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/olapdmpr/printro_6oab.asp

Microsoft Office Comparison Chart

http://www.microsoft.com/office/evaluation/indepth/compare.asp

Authentication Methods

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/olapdmad/agsecurity_5ucz.asp

CE Configuration

Now that we have discussed security types, it is time to focus on configuring CE for OLAP security.

CAP Report Viewer

This section discussed what happens when OLAP data is viewed from a CAP report viewer.

ActiveX Viewer

When a client attempts to view a cube using the ActiveX viewer, the ActiveX viewer uses PivotTable services on the local computer to connect to the OLE DB data. The user credentials of the user who is currently logged on will be presented to the Analysis Server for authentication. For information on how to choose which credentials are used to connect to the Analysis Server, please contact Crystal Decisions Technical Support.

DHTML Viewer

When a client attempts to view a cube using the DHTML viewer, the DHTML viewer requests the data from the WCS through the web server. The WCS uses its local PivotTable services to connect to the Analysis Server. By default, the WCS attempts to connect to the Analysis Server with the credentials used to start it. Depending on its configuration, the WCS can present the Analysis Server with a different set of credentials. This is in effect a second log on and therefore known as Secondary Logon in the CE environment. The Secondary Logon functionality is only available when using the DHTML viewer.

Web Component Server

The WCS has one configuration option for the CAP plug-in. By default, the WCS uses NTLM security to connect to the Analysis Server.

To configure the WCS to use Kerberos security, the following registry key must be added to the WCS machine:

For version 8.5:

HKLM\Software\Crystal Decisions\8.5\OCCA(o)\SOFA\ODBO\MSOLAP

For version 9:

HKLM\Software\Crystal Decisions\9.0\OCCA(o)\SOFA\ODBO\MSOLAP

The following value (of type REG_SZ or string) should be added to the new key: SecurityPackage

The SecurityPackage value can contain one of the following text strings:

Value	Meaning
NTLM	Uses the NTLM security protocol. This is the default and is used when the registry key is not present.
Kerberos	Uses the Kerberos security protocol.
Negotiate	Kerberos if supported otherwise NTLM.

Figure 3

This key is not present by default and must be added manually to the registry. If it is not present, NTLM will be used by default.

NTLM vs. Kerberos Security

All Microsoft Windows operating systems use either the NTLM or the Kerberos security package. Sometimes both are used. The major difference between the two as far as CE is concerned, is that NLTM security does not support delegation. The following two sections are crucial for understanding the

differences between NTLM and Kerberos security. You must understand these concepts in order to configure Secondary Logon properly.

NTLM Security

Windows NT operating systems use the Windows NT LAN Manager (NTLM) challenge/response security package by default. The following diagram depicts the challenge/response process:

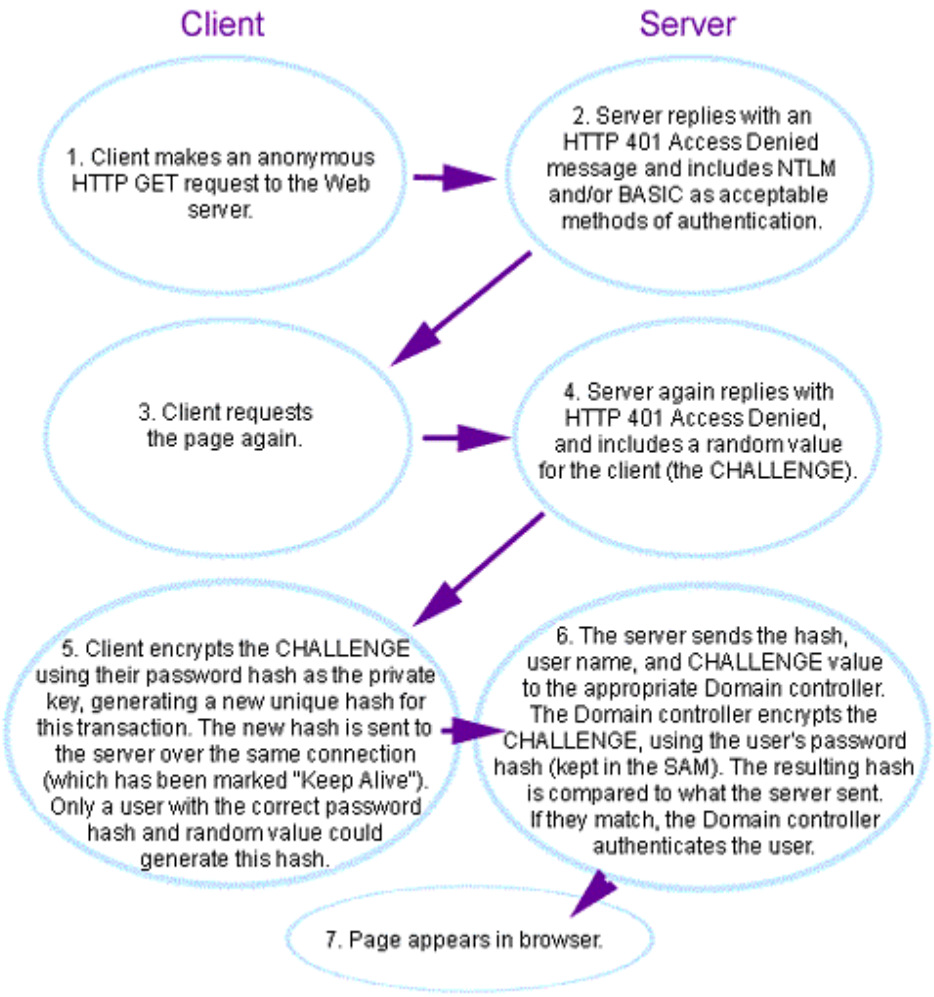


Figure 4

The most important thing to note here is that the server never receives the user's password hash. Because the server does not have the user's password hash, it cannot impersonate that user. This behavior means that for CAP Professional Secondary Logon to work using NTLM security, the CE WCS and the Analysis Server must be on the same computer. This is a limitation of NTLM, not CE.

In Figure 5, User A has logged onto Computer 1 and opened a session with the web server and the CE WCS running on Computer 2. User A requests to view a published CAP application that has been configured to use Secondary Logon. This request is serviced by the WCS running as User B, where User B acts as User C's delegate and requests the data for the application from the OLAP server running on Computer 2. The data returned will be restricted to what User C has access to.

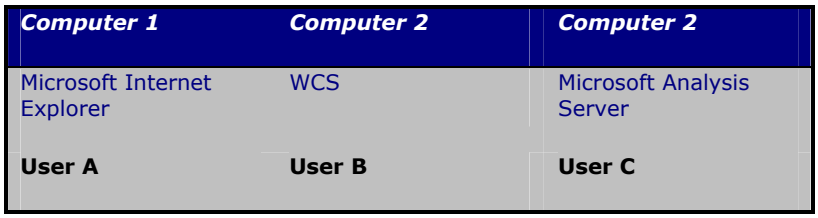


Figure 5

Additional References regarding NTLM Security

IIS Authentication

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vsent7/html/vxconIISAuthentication.asp

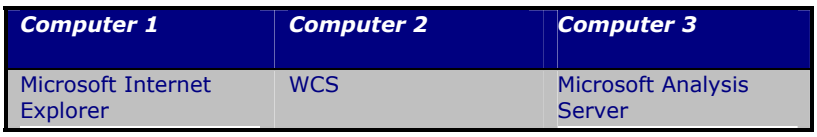
Authentication and Security for Internet Developers

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnauth/html/dnauth_security.asp

Kerberos Security

Active Directory uses Kerberos security and introduces some new security concepts that are leveraged by Crystal Decisions products. Delegation is a feature that allows a server, while impersonating a client, to access remote resources on behalf of the client. Delegation is new to Active Directory and is intended to overcome shortcomings of the Windows NT NTLM security system; therefore you can only take advantage of delegation when using Kerberos security.

In the following diagram, User A has logged into Computer 1 and opened a session with the web server and the CE WCS running on Computer 2. User A requests to view a published CAP application that has been configured to use Secondary Logon. This request is serviced by the WCS running as User B, where User B acts as User C's delegate and requests the data for the application from the OLAP server running on Computer 3. The data returned will be restricted to what User C has access to.



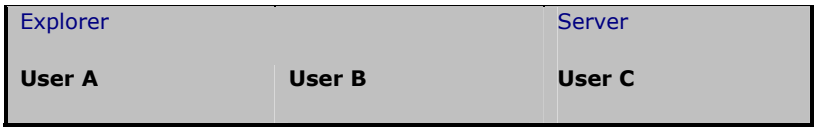


Figure 6

Requirements

When a server impersonates a client, Kerberos authentication generates a delegate-level token, capable of being used to respond to network authentication challenges from remote computers, if the following conditions are met:

- The client account that is being impersonated is not marked as **sensitive** and cannot be delegated in Microsoft Active Directory directory service.
- The server process account (the user account under which the server process is running or the computer account if the process is running under the local SYSTEM account) is marked as **trusted** for delegation in Active Directory.
- The **Enable Computer** and **user accounts to be trusted for delegation** rights must be granted to each user that will set the **Trusted for delegation** flag. This is User A in Figure 6.

Additional References regarding Kerberos Security

Exploring Kerberos, the Protocol for Distributed Security in Windows 2000

http://www.microsoft.com/msj/defaultframe.asp?page=/msj/0899/kerberos/kerberos.htm

Understanding Kerberos Credential Delegation in Windows 2000 Using the TktView Utility

http://msdn.microsoft.com/msdnmag/issues/0500/Security/default.aspx

How To: Implement Kerberos Delegation for Windows 2000

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/SecNetHT05.asp

How To: Set a computer account as 'Trusted for Delegation'

http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/iisbook/c09_trusted_for_delegation.asp

How To: Enable computer and user accounts to be trusted for delegation - http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/538.asp

How To: Use Delegation in Windows 2000 with COM+

http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B283201

DCOM

NOTE	Distributed Common Object Model (DCOM) has been replaced by COM+. This is only important when reading on the subject as DCOM and COM+ are used interchangeably.

When the WCS receives a request for data from a remote Analysis Server, the WCS service launches a process named OlapSessions. OlapSessions is a COM object that connects to the remote OLAP data source and retrieves the required information. When the WCS creates the OlapSessions process, it uses delegation to impersonate the credentials supplied by the client. This configuration does not need to be edited to allow CE to function properly.

Figure 7 is a screen shot of the DCOMCFNG.exe utility. To check the configuration of OlapSessions, complete the following steps:

1. Run DCOMCFNG.exe
2. Click OlapSessions as shown in Figure 7.

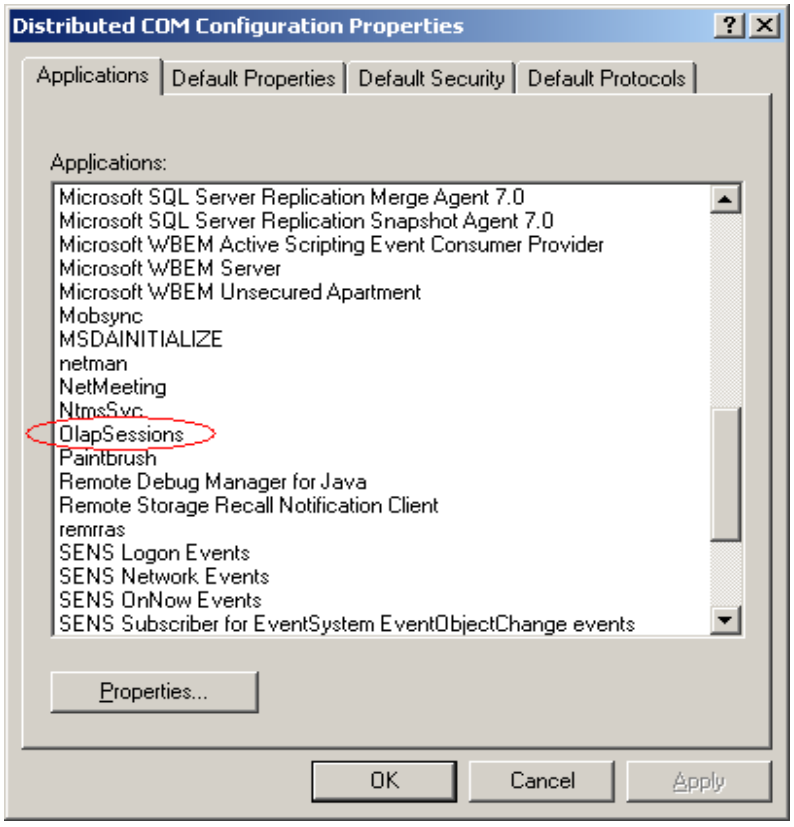


Figure 7

3. Click the **Properties** button once the dialog box appears and then click the **Identity** tab. The screen shown in Figure 8 appears.

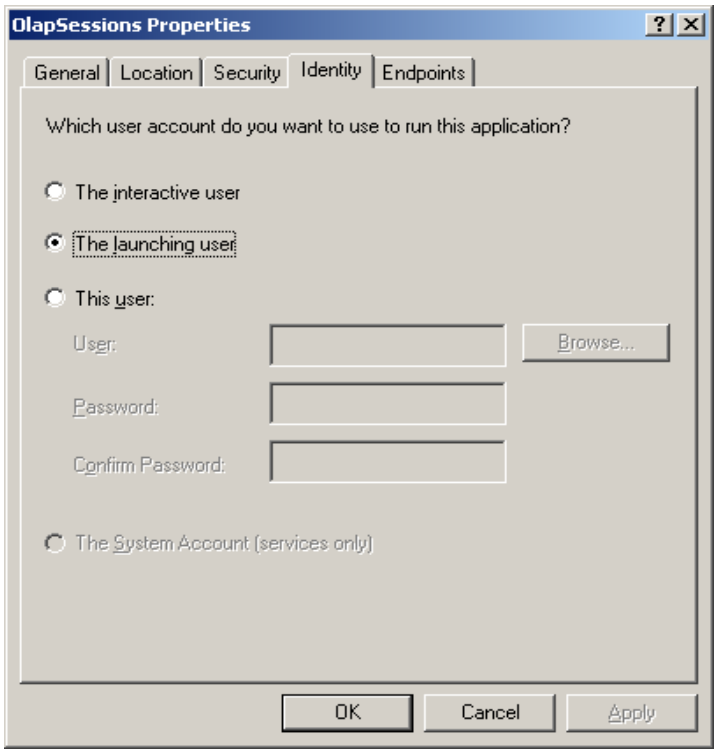


Figure 8

Additional References regarding DCOM

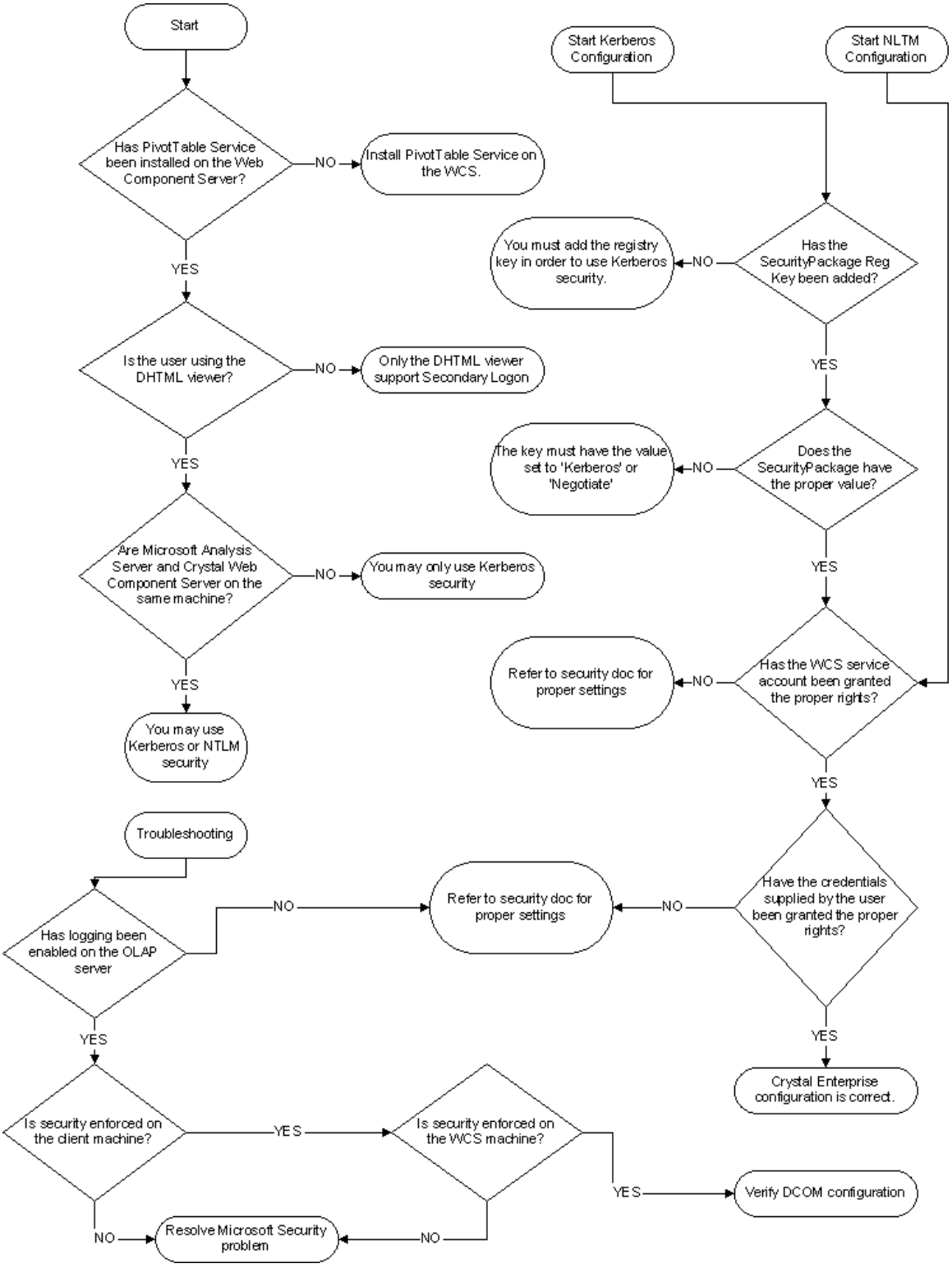
DCOMCNFG Explained.

http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/adsecureconcepts_38vn.htm

INFO: Using DCOM Config (DCOMCNFG.EXE) on Windows NT

http://support.microsoft.com/default.aspx?scid=kb;EN-US;176799

Troubleshooting Flowchart



Footnotes

1. MSDN Library, "Authentication of Direct Connections", <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/olapdmad/agsecurity_7g6m.asp> (March 31, 2003).

2. MSDN Library, "Connected to Analysis Services", <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/olapdmpr/pt_keyco_6bzn.asp> (March 31, 2003).

Contacting Crystal Decisions for Technical Support

We recommend that you refer to the product documentation and that you visit our Technical Support web site for more resources.

Self-serve Support:

http://support.crystaldecisions.com/

Email Support:

http://support.crystaldecisions.com/support/answers.asp

Telephone Support:

http://www.crystaldecisions.com/contact/support.asp