Cisco TelePresence Management Suite Analytics Extension

Administrator Guide

Software version 1.1

D14668.06

January 2012

Contents

Introduction

This document describes the Cisco TelePresence Management Suite Analytics Extension (Cisco TMSAE).

Cisco TMSAE is an online analytical processing (OLAP) system for Cisco TelePresence Management Suite (Cisco TMS) and provides advanced reporting functionality on your video network. It integrates with Business Intelligence (BI) applications, custom-built applications, and other applications capable of connecting to an OLAP cube, such as Microsoft Excel.

The Cisco TMS Analytics Extension API is described in a separate document, *Cisco TelePresence Management Suite Analytics Extension API Programming Reference Guide*.

Technical overview

The sections provide technical explanations of how Cisco TMSAE components are created and used in ongoing operations, to assist administrators understand system dependencies.

Cisco TMSAE brings business intelligence, customized reporting, and high performance data mining to Cisco TMS. Analysis and data from your visual communications network can be accessed via industry standard tools.

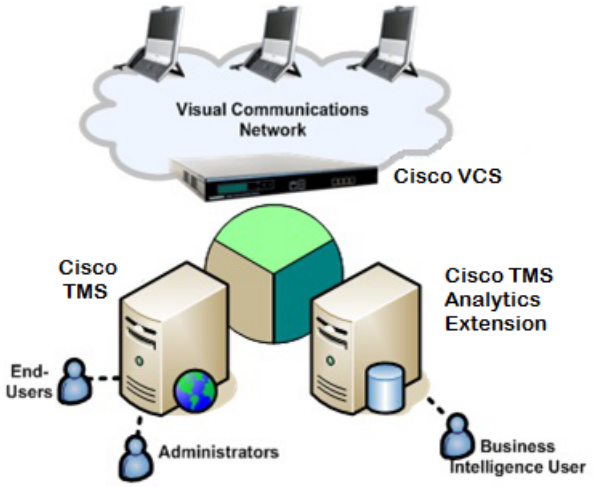


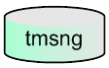
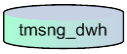
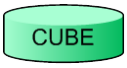
Figure 1 TMS Analytics Platform

Cisco TMSAE makes use of Microsoft's powerful SQL Server Analysis Services to provide business knowledge and customized reporting on your Cisco TMS Server, and integration with Business Intelligence applications. Cisco TMSAE enables the use of standardized, OLAP compatible clients to access a known and supported list of information about the usage of your visual communications network without disrupting ongoing operations.

Cisco TMSAE is installed on an existing Cisco TelePresence Management Suite Server and creates and maintains new information stores. The new information stores enhance the type of data available for Cisco TMS customers, and provides a standardized, supported way of accessing reporting data made available through Cisco TMSAE.

Cisco TMSAE components and roles

The following table and illustration explain the various elements involved with Cisco TMSAE and how they relate to each other.

	**TMS Web Server** – The Windows installation that hosts the TMS web application. The TMS Web Server also requires a TMS SQL Server, which may or may not be the same Windows Server.
	**TMS SQL Server** – The Microsoft SQL Server hosting the TMS Database. In smaller installations, this server is typically hosted on the same physical server that the TMS Web Server is hosted on. In advanced installations, these tasks are usually different physical Windows Servers.
	**TMS Database** – The main database used by TMS itself. This database is hosted by the TMS SQL server role and the default name of the database is tmsng.
	**TMS SQL Login** – The SQL Login used by the TMS Web Server to access the tmsng database. By default, this is the sa account of the TMS SQL server, but can be customized during TMS installation.
	**Data Warehouse Server** – The Microsoft SQL Server that will be hosting the Analytics Databases and SQL Server Analysis Services. This server can be the same SQL server as the TMS SQL Server, but is recommended to be a separate SQL server. This Server installation must be operational before attempting to install the Analytics Extension.
	**Data Warehouse Database** – A new database created by Cisco TMSAE which serves as the long-term data repository for the Analytics Extension. This database is hosted by the Data Warehouse Server
	**Data Warehouse CUBE** – A new specialized multi-dimensional database created by the Analytics Extension which contains the pre-computed data created by the Analytics Extension. This database is hosted by the SQL Server Analysis Services Instance running on the Data Warehouse Server.
	**DWH Service User** – A Windows domain user account used by the Analytics Extension to log into the data warehouse Server for ongoing operations. This account will be given the necessary permissions by the Cisco TMSAE installer.
	**DWH TMS Service User** – A SQL Login for the TMS SQL server used by the Analytics Extension to read data from the TMS Database. This account is a SQL Login, not a Windows Account and must have at least the **`db_datareader`** role. See Appendix 2: Creating User Accounts in Windows Server and Microsoft SQL Server in Cisco TMSAE installation guide for information on how to set up such an account.

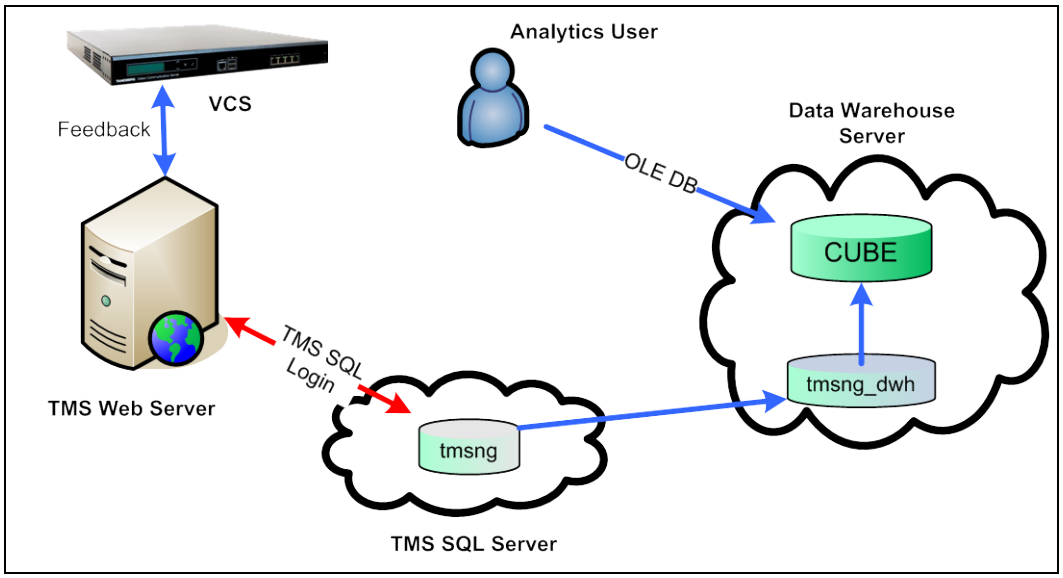


Figure 2 Illustration of roles and Components

Data warehouse server

Cisco TMSAE comprises two major elements - the data warehouse database, and the data warehouse CUBE.

Data warehouse database

The data warehouse database is used for analysis and data mining, and contains information from the Cisco TMS database combined with data computations and analysis.

Using credentials specified by the installing user, the data warehouse database is created in a SQL server instance of the data warehouse server. The default database name is **tmsng_dwh**. The DWH (data warehouse) service user is defined as the owner of the database, and this service account is used by Cisco TMSAE to log into the database for ongoing operations. Ordinary users of the Analytics Extension API do not connect to this database.

The data warehouse database accesses the Cisco TMS database through a linked server, created on the data warehouse server during installation. The linked server is created automatically using the TMS database location and DWH TMS service user credentials supplied during installation. The DWH TMS service user is an SQL login for the Cisco TMS SQL server. This account only needs **db_datareader** role to access the Cisco TMS database, and can reuse any existing login with sufficient SQL access permissions.

Data warehouse CUBE

The data warehouse CUBE is a specialized type of database used in analysis and data mining. Its main advantage is its ability to hold pre-computed aggregates of data across many different dimensions, allowing fast manipulation of queries. The data warehouse CUBE holds different data defined as ‘facts’, each of which has different defined ‘dimensions’, which can be used to manipulate the information stored in the different fact tables. Cisco TMSAE provides sets of facts and dimensions that can be used by programmers and analytics users.

The data warehouse CUBE is created during installation in the Analysis Services instance on the data warehouse server. The default name for the database is **tmsng_dwhAsDb** (its name format must always be <database>AsDb). The DWH service user is configured as the owner of the CUBE and the DWH service user credentials are used by Analytics Extension to connect to the cube for ongoing operations. Ordinary users of the Cisco TMSAE API connect to this CUBE using an OLAP client and their Windows Domain accounts (with *reader role* permissions).

A small IIS web application – an “HTTP pump” – can be installed on the data warehouse Windows server (which may also be the TMS server, depending on the setup) receives requests, authenticates

them, and creates a security context for the requests before forwarding them to Analysis Services. After Analysis Services has executed the request, the pump passes the response back to the client.

The data warehouse CUBE connects to the data warehouse database using a data source defined configured to use the DWH service user credentials.

Data warehouse updates

Data mining and long term analysis of information is done using historical data. The focus is on historical data, instead of real-time data. Because of this, the data warehouse contents are not recorded in real-time as in the traditional reporting information viewed via TMS. Instead the DWH data is refreshed daily by the Windows Service installed on the TMS web server by Cisco TMSAE.

The Windows Service initiates two updates, the ETL task, and the CUBE refresh. The ETL (Extract, Transform, Load) task extracts from the TMS database all new (recorded since the last time the ETL task run) data updates values and computations stored in the data warehouse database. Because only new information is processed, the ETL task is extremely efficient. This task is initiated by the Analytics Extension's Windows Service connecting to the data warehouse server at a scheduled time using the supplied DWH service user credentials. The ETL job executes on the data warehouse server and uses the defined linked server to read information from the TMS database. There is no significant extra load placed the TMS web server. An administrator may also initiate the ETL job to run immediately via the Analytics Extension web interface in Cisco TMS.

The CUBE refresh is performed daily after the data warehouse database has been updated by the ETL task. To initiate this update, the Analytics Extension Windows Service on the TMS Web Server connects to the Analytics Service on the data warehouse server using the DWH service user credentials and tells the CUBE to refresh. The CUBE uses the connection properties defined in the CUBE's Data Source definition to connect to the data warehouse database.

Connecting to an SQL Server on a specific port

To connect to a SQL Server running on a specific port, use the Windows service called SQL Server Browser. For instructions, see the MSDN Library article Using SQL Server Browser. It is responsible for incoming connections to the SQL Server. If SQL Server is set up to use the default instance, SQL Server Browser will (if running) automatically take care of forwarding incoming connections to the port that is used by SQL Server. It will therefore not be necessary to specify the port manually during installation, and a SQL server running on port 1523 on 10.47.26.208 should be referred to only as **10.47.26.208**.

If you are using named instances, each instance will use its own TCP port. However, the port numbers are never used in connection strings. Named instances must be referred to as **10.47.26.208\instancename** when running the installer.

Finding port numbers with SQL Server Analysis Services

The default port for SQL Analysis Services is 2383. Named instances will by default use a dynamic port number. The server can be setup to listen on a specific static port by editing the server property <Port> via SQL Management Studio or the **msmdsrv.ini** file of the instance.

There are two ways of finding the port dynamic port number currently in use by an Analysis Services instance, described below.

Solution 1

1. Start Task Manager on the Server
2. Ensure the PID (Process Identifier) column is visible (View Menu > Select Columns…)
3. Locate the process named msmdsrv.exe and find its PID
4. Start a command prompt, and run the command netstat /aon

5. Find the line with the PID matching your process and the port number will be displayed in the Local Address field

Solution 2

The server will write an informational message to the Windows Application event log during service startup noting how the instance is listening on the network.

1. Start Task Manager on the Server.
2. Open the Application Log in the Event Viewer.

The information will be in an event of type Information with a source of MSSQL$<INSTANCENAME>. It will have a description like in the example below, where the port number is 1072:

```
Server is listening on [ 'any' <ipv4> 1072]
```

Service account permissions and uses

Note that if the account password is changed for either of the below users, the installation must be reconfigured. See the section Reconfiguring Cisco TMSAE for more information.

Data warehouse service user

The data warehouse service user account is used by Cisco TMSAE to log into the data warehouse database and data warehouse CUBE. This user account must be a valid Windows Domain account. It does not need any pre-existing permissions. It is also used by the data warehouse CUBE to connect to the data warehouse database in the Database Engine instance.

DWH TMS service user

The TMS service user account is used by the data warehouse server to pull data from the Cisco TMS database. This account must have an SQL Login capable of connecting to the TMS database **tmsng**. It only needs SQL login access to the TMS and the **db_datareader** role on the TMS database.

Adding and managing users

Cisco TMSAE has two classes of users:

- Administrators who have access to diagnostic information and settings.
- Analytics users who are consumers of the data output.

SQL Server Analysis Services (SSAS) uses a strict security model and only Windows authentication is supported. Any user or client who wishes to be an administrator or analytics user must have a valid Windows Domain account the SSAS instance trusts. Some software clients allow a user to specify which account they will use to authenticate to SSAS; others only support Integrated Authentication where the credentials of your current user identity are used.

Analytics users

Users who wish to read data from Cisco TMSAE must have access to the data warehouse CUBE hosted by the SQL Server Analysis Service (SSAS). An account with SSAS access does not necessarily have the right to read the data warehouse CUBE.

SSAS offers administrators a wide variety of permissions possibilities for users, but to ease configuration the data warehouse CUBE has a custom *reader role* defined during installation. Users who are members of this role will have access to read, but not modify any information in the data warehouse CUBE. Access to the information made available via Cisco TMSAE should be granted by adding users to this *reader role*.

To add a new user to the *reader role*:

1. Open Management Studio, and connect to the relevant SSAS instance.
2. Locate **Databases > tmsng_dwhAsDb > Roles.**
3. Right-click **Reader** and select **Properties**.
4. Go to the **Membership** subpage. Click **Add…** to enter users or groups (Figure 1). To grant read access to domain members, use the **Everyone** group. Use the **Authenticated Users** group to exclude guest accounts and anonymous users.

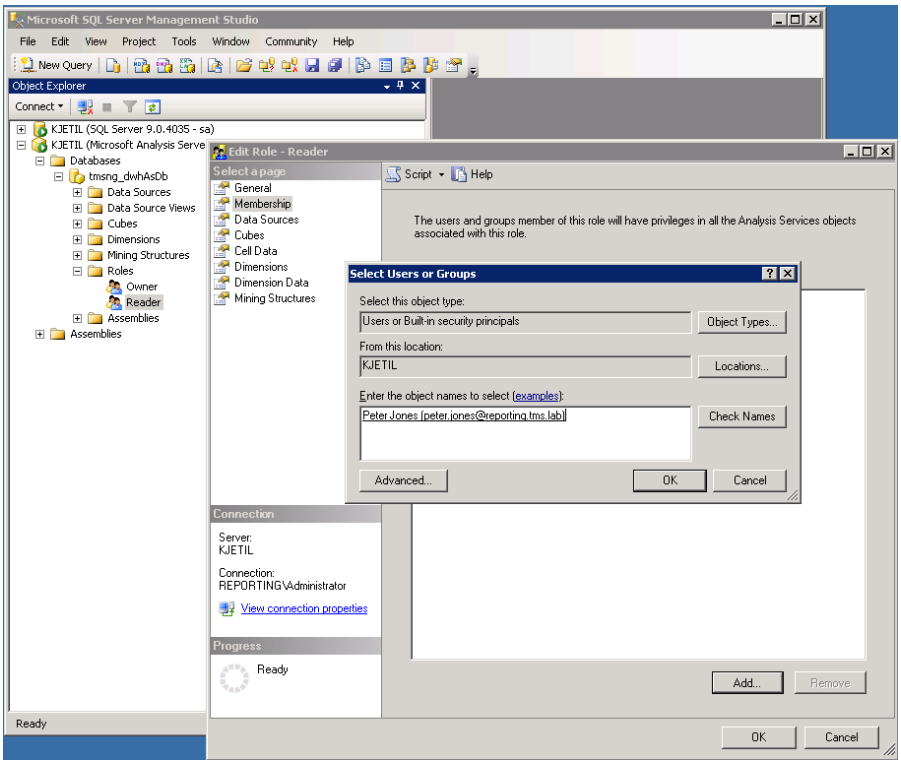


Figure 1: Managing user rights for accessing the cube

To remove a user from the *reader role*:

1. Open Management Studio, and connect to the relevant SSAS instance.
2. Locate **Databases > tmsng_dwhAsDb > Roles.**
3. Right-click **Reader** and select **Properties**.
4. Go to the **Membership** subpage. Select the user to remove and click **Remove**.

Administrator roles

Cisco TMSAE administrators

To view the web interface, you must be a member of a user group in Cisco TMS that has the **Configuration > Read** permission. To run the ETL job, the user must be a member of a user group in TMS that has the **Configuration > Update** permission.

Group membership and group permissions are managed in the User Administration pages of Cisco TMS, located at **Administrative Tools > User Administration**.

Analysis services server administrators

Access to the data warehouse CUBE and data exposed by Cisco TMSAE is controlled via the SSAS *administrator role*. Administrative privileges for the Analysis Services instance are controlled by the *server role* in the Analysis Services server instance.

By default, local administrators of the Windows Server are members of the *server role* and have full access to all features and data in the server instance. Other users can be added to the *server role* to grant them administrator rights. To add another user to the *server role*:

1. In SQL Server Management Studio, connect to the instance of Analysis Services.
2. Right-click the instance name in Object Explorer and then click **Properties**.
3. In the **Select a Page** pane, click **Security**.
4. Click **Add** to add one or more Windows users or groups to the *server role.*

Web interface

The Analytics Extension web interface is accessed via your existing Cisco TMS installation. This section provides further interface information.

Note that if the server name or address used in the URL to access Cisco TMS and the address in the Analytics Extension URL configured in **Administrative Tools** are different, you may be prompted with a username/password dialog when accessing Cisco TMSAE.

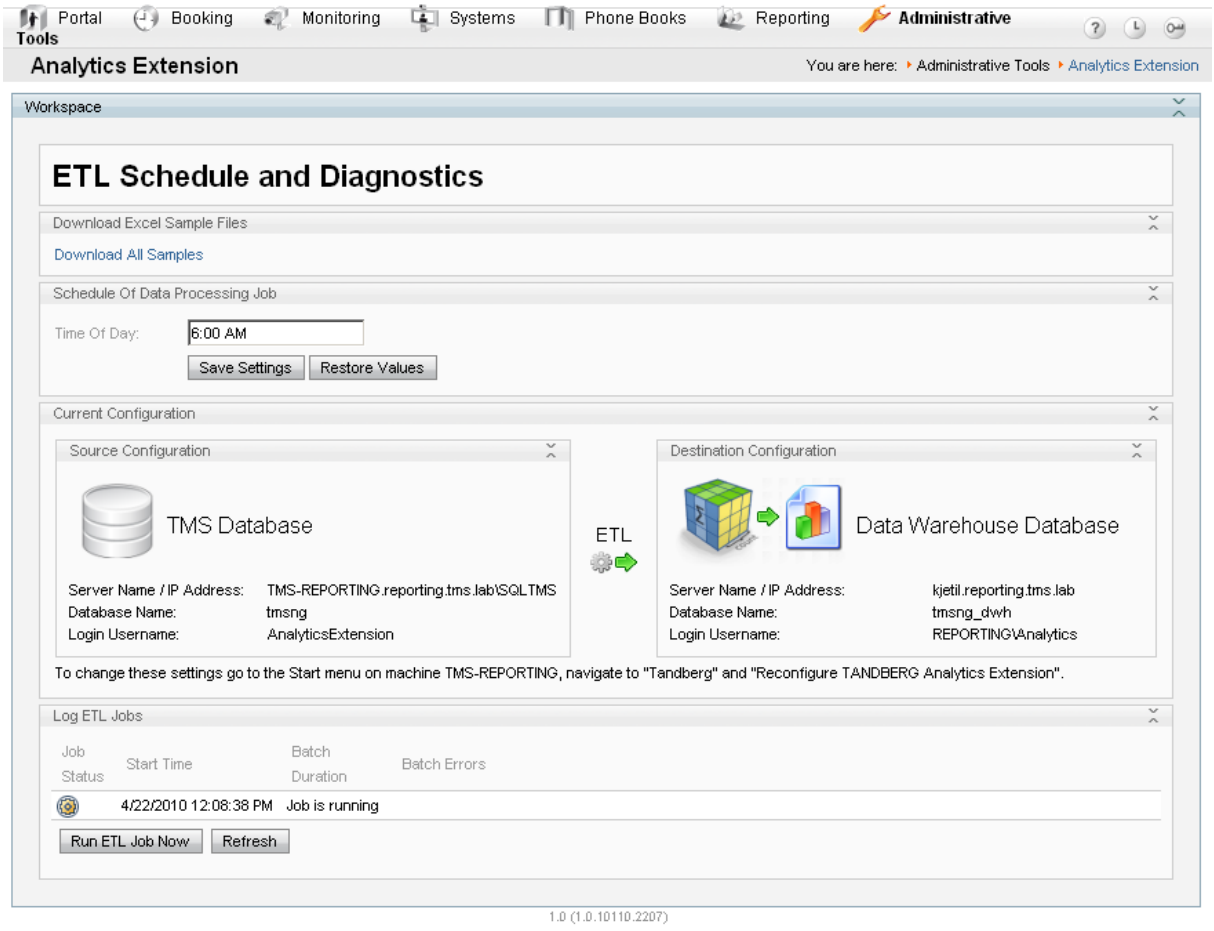


Figure 2: The Analytics Extension web interface

Download Excel sample files

Sample Excel workbooks are included with Cisco TMSAE. See the Cisco TMSAE Installation Guide for more information on installing these example spreadsheets.

Log ETL jobs

The ETL job extracts information from the source TMS database and updates the data warehouse server databases. This panel shows the status and log details for past runs of the ETL job and can be used to verify the job is running, or help diagnose why the data warehouse databases are not updating.

- *Job Status* – Shows a checkmark if the job was complete, a red x if it failed, or a gear icon if it is currently in progress.
- *Start Time* – The start time of the job, in TMS Server time
- *Batch Duration* – How long the job has been running for or how long the job took to complete
- *Batch Errors* – If a job fails, diagnostic information is listed here. Click on the entry to expand the box and see more information.
- *Run ETL Job Now* – Clicking this will manually initiate an immediate ETL job. *Note this task may take a significant amount of time to complete.*

Note: This window does not automatically refresh. Click the **Refresh** button to refresh the list with the latest information.

Reconfiguring Cisco TMSAE

Analytics extension provides a wizard to help you through reconfiguring your setup. Common causes for reconfiguration are to update a server address, an expired password, other account information, or your server configuration or your network changes.

The wizard allows you to update:

- Destination database server name or IP address
- Username and password for the data warehouse service account
- Source TMS database server name or IP address

While the reconfiguration wizard allows you to update the server addresses used by the installation, it cannot move any databases or create new accounts. The wizard can only be used to update your installation with external changes. If you need to change which servers host the TMS or data warehouse databases, those changes must be made by the SQL Administrator manually and then use the reconfigure wizard to update your software.

Note: Cisco TelePresence recommends that the reconfiguration wizard *not* be used to replace the source database with an entirely different Cisco TMS database. The reconfiguration wizard is useful in cases where the underlying data is either the same, or a logical continuation of the current database (such as the current database with more data).

Reconfiguring Cisco TMSAE will temporarily halt other web services on the same IIS, as the *World Wide Web Publishing Service* will be stopped and restarted by the wizard. The expected downtime is a few seconds.

The reconfiguration wizard will summarize your proposed changes and wait for confirmation before making any changes.

1. Open the **Start menu** and select **TANDBERG > Reconfigure TANDBERG Analytics Extension**.
2. Follow the onscreen prompts and instructions.

Troubleshooting

Data quality issues

Repeating or inaccurate data

When using Microsoft Excel to connect to the Cisco TMSAE cube, if the values you get are obviously inaccurate or repeating (as in the figure below, where there apparently are 139 systems in each folder), you may be trying to use a dimension on a measure that the dimension is not applicable to.

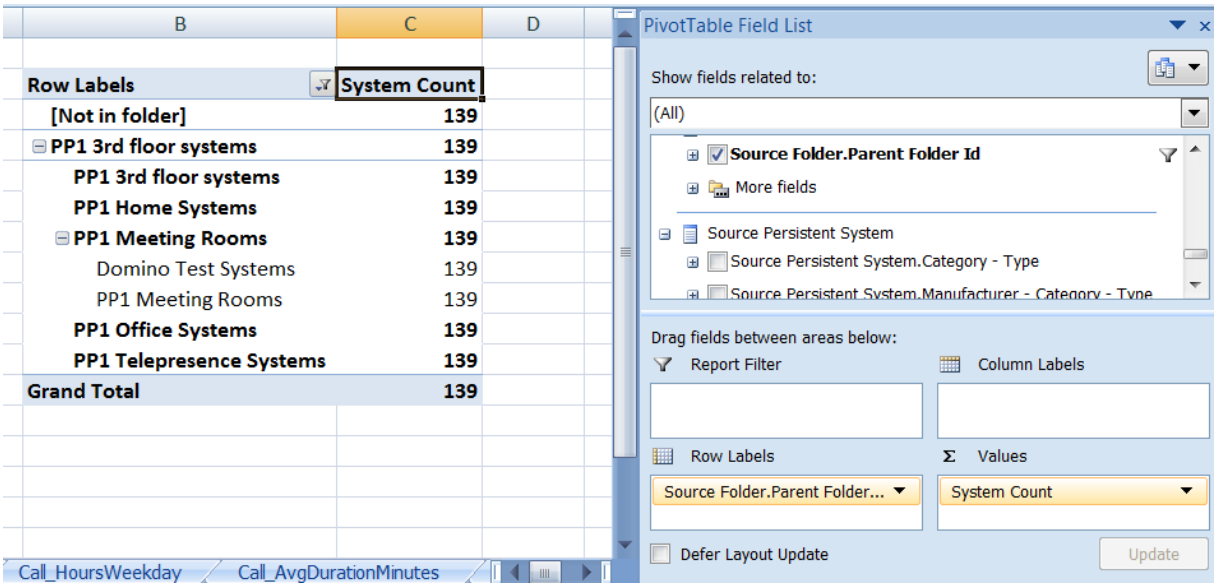


Figure 3 Repeating/inaccurate data

Dimensions named Source […] or Destination […] may only be used on Fact Call. For all other fact tables, you must use dimensions without the Source and Destination prefixes.

For example, when using the System Count measure, applying Source Folder will give you meaningless results. To get correct data, use Folder instead.

As a general rule when working with pivot tables in Excel, always use the Show field related to: drop down at the top of the pivot table field list. If you for example set this drop down to System, Excel will only display dimensions that can be applied to this fact table.

Misleading Fact MCU Utilization data

Specific conditions may cause misleading *Fact MCU Utilization* data, such as *Peak Actual Used Video Ports* or *Peak Audio Port Utilization*, as detailed below.

For example, if you have two MCUs in your video deployment, each with 40 video ports, getting a *Peak Actual Used Video Ports* count of 86 is obviously incorrect. An incorrect Port figure will also slightly skew Utilization calculations.

CDR generation in Cisco TMS 13.0 and 13.1

Prior to Cisco TMS 13.0 and Cisco TelePresence MCU 4.2, call detail records were generated in Cisco TMS based on feedback from the MCU. To improve data quality, CDRs are now generated by and collected from the MCU.

In Cisco TMS version 13.1, duplicate CDR generation may occur, affecting MCU statistics in Cisco TMS and by extension Fact MCU Utilization statistics in Cisco TMSAE.

This issue is addressed in Cisco TMS 13.1.1 and later with Cisco TelePresence MCU version 4.2 or later. Note that the fix will not purge previously created duplicate CDRs.

Reconnected MCU port

In some scenarios, if participants in a multipoint conference lose connection to an MCU and reconnect, the new connection may use a different port on the MCU. If the initial port has not yet been released, the participant can occupy two ports. This results in the MCU reporting a misleading participant count to Cisco TMS.

Port usage imprecision

Depending on port availability, participants may have their connection downgraded (video to audio) or upgraded (audio to video) during a conference.

Any participant that has used a video port at any point during a conference, will be reported as a video participant when the conference ends. This means, for example, that a conference may be reported as having 0 audio participants although multiple audio ports were in use during the conference, skewing video and audio port usage statistics.

Calls appearing in Cisco TMS are missing from the Analytics Extension CUBE

The Endpoint CDR reporting functionality in Cisco TMS relies on CDRs collected directly from the endpoints.

This is different from Cisco TMSAE, which relies on data collected from Cisco VCS. If Cisco TMS receives feedback from the endpoint but not from the Cisco VCS that the endpoint is registered to, calls involving this endpoint will be displayed in the Cisco TMS reporting pages but not in the Cisco TMSAE CUBE.

To verify that the Cisco VCS is sending feedback to Cisco TMS:

1. Locate the VCS in the **System Navigator** in TMS
2. Click the **Logs** tab, and go to the **Call Log**.

All calls shown in the call log will be included in the Cisco TMSAE CUBE the next time the ETL job runs.

If the call log is empty, correct its external manager address:

On the Cisco VCS:

1. Go to **System Configuration > External Manager.**
2. Make sure the **Address** field contains the IP address or host name of the Cisco TMS server.

In Cisco TMS:

1. Go to **Administrative Tools > Configuration > Network Settings**.
2. Make sure that all fields in the **Advanced Network Settings for Systems on Internal LAN** section show the correct IP addresses and host name for your Cisco TMS.
3. Locate the Cisco VCS in **Systems > Navigator**.
4. Go to **Settings > Edit Settings**, and click the **Enforce Management Settings** button.

Using an SSH client

1. Log in to the Cisco VCS as the *admin* user.
2. Type **`xstatus`**. You now see the full configuration of the Cisco VCS, including attributes not visible in the Cisco TMS web interface.
3. Locate the output starting with “Feedback 3”.
4. If the “URL:” value contains either the IP address or host name of Cisco TMS, and the “Status:” value is **On**, the Cisco VCS is correctly set up to send feedback to Cisco TMS.

```
*s Feedback 3:
     Status: On
     URL: "https://10.47.27.81/tms/public/feedback/code.aspx"
     Expression: "/Event/CallDisconnected"
     Expression: "/Event/CallConnected"
     Expression: "/Event/CallFailure"
     Expression: "/Event/RegistrationAdded"
     Expression: "/Event/RegistrationChanged"
     Expression: "/Event/ResourceUsage"
     Expression: "/Event/AuthenticationFailure"
     Expression: "/Status/Warnings"
*s/end
```

Figure 4: Sample Feedback 3 values from running the "xstatus" command on the Cisco VCS.

Web site issues

User does not have sufficient permissions in TMS to view this module

A bug in SQL server can produce this error even when permissions are set correctly. A failed login attempt results in the following message in the web application log file **`log-AdminWeb.txt`**:

System.Data.SqlClient.SqlException: Login failed for user '<domain/account>'. Reason: Server is in script upgrade mode. Only administrator can connect at this time.

This can occur after a fresh installation of Microsoft SQL Server or after installing a SQL server service pack. To resolve this issue reboot the server.

An error has occurred!

This generic error message asks you to look in the logs for further information.

The most common cause is SQL connectivity problems. Look for an **`SQL Network Interfaces: Error Locating Server/Instance Specified`** message in **`log-AdminWeb.txt`**.

Refer to the Cisco TMSAE installation guide for information on troubleshooting connection errors.

Figure 5: The generic "An error has occurred" message

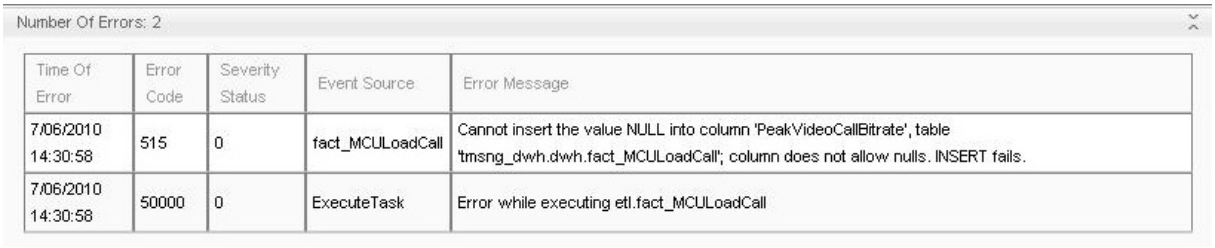
ETL job failures

Cannot insert the value NULL into column…

For some video networks with high MCU activity, the ETL job may fail with an error message:

- Cannot insert the value NULL into column 'PeakAudioCallBitrate'
- Cannot insert the value NULL into column 'PeakVideoCallBitrate'
- Cannot insert the value NULL into column 'PeakActualVideoCalls'

This bug only occurs in Analytics extension version 1.0, and is fixed for version 1.1. A patch for version 1.0 exists. Customers encountering this problem can contact support to obtain the patch.


Number Of Errors: 2

Time Of Error	Error Code	Severity Status	Event Source	Error Message
7/06/2010 14:30:58	515	0	fact_MCULoadCall	Cannot insert the value NULL into column 'PeakVideoCallBitrate', table 'tmsng_dwh.dwh.fact_MCULoadCall'; column does not allow nulls. INSERT fails.
7/06/2010 14:30:58	50000	0	ExecuteTask	Error while executing etl.fact_MCULoadCall

Figure 6: The "Cannot insert the value NULL into column…" bug as seen in the "Log ETL jobs" panel.

Multiple "Error: Internal error: The operation terminated unsuccessfully."

Getting multiple **`Error: Internal error: The operation terminated unsuccessfully.`** messages in the same ETL job indicates that there have been major changes in the TMS database since you last ran the job (Figure 7), and that the Analytics Extension is unable to extract data because of schema changes or changes in constraints.

These errors can occur if you have used the reconfiguration tool to replace the source database with an entirely different TMS database. As described in Analytics Extension Reconfiguration section, the wizard tool should not be used for such changes. To fix the problem, use the reconfiguration tool again to return the source database to the original TMS database.

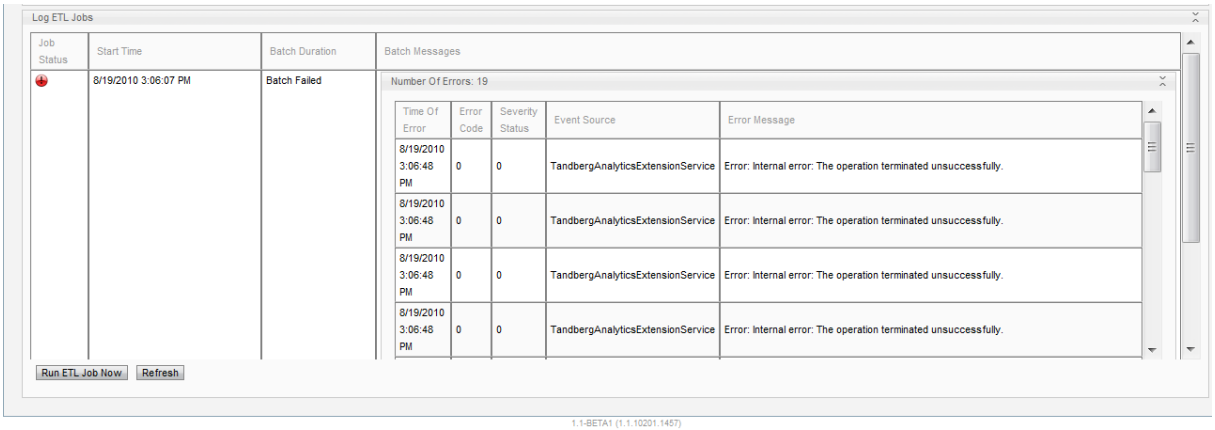


Figure 7: Multiple "Error: Internal error: The operation terminated unsuccessfully." messages from the same failed ETL job.

Client Connectivity Issues

A connection could not be made to the data source

Error: Errors in the high-level relational engine. A connection could not be made to the data source with the DataSourceID of 'TMS DW', Name of 'TMS DW

If your data warehouse server is running SQL Server/Analysis Services 2008, the ETL job may fail logging “Error: Errors in the high-level relational engine. A connection could not be made to the data source with the DataSourceID of 'TMS DW', Name of 'TMS DW'”.

1. Using SQL Server Management Studio, log into Analysis Services
2. Go to Databases -> tmsng_dwhAsDb -> Data Sources and locate the “TMS DW” data source.
3. Right click TMS DW and select **Properties**.
4. Change the **Connection String** from **`Provider=SQLNCLI.1;[…]`** to **`Provider=SQLNCLI10.1;[…]`**
5. Click OK.
6. Rerun the ETL job.

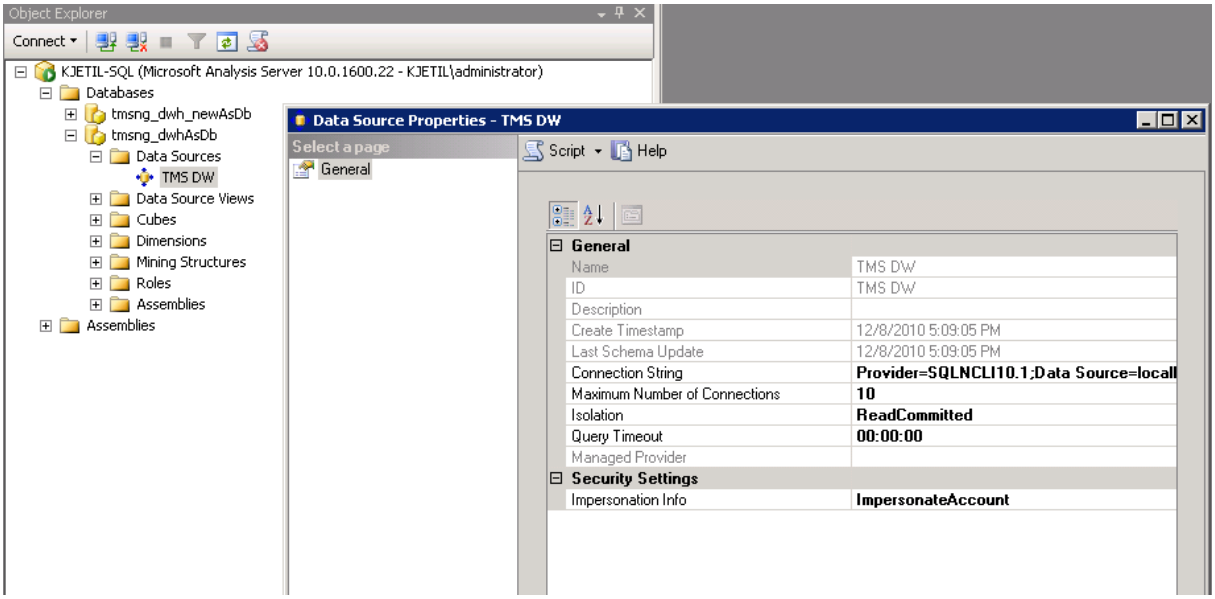


Figure 8: DataSourceID of 'TMS DW'

Encryption not supported on the client

Client unable to establish connection; 08001; Encryption not supported on the client.; 08001

If the ETL job log shows multiple “Internal error: The operation terminated unsuccessfully” errors **and** a “Client unable to establish connection; 08001; Encryption not supported on the client.; 08001” error, your SQL Server Analysis Services instance is unable to connect to the data warehouse SQL relational database.

To correct the issue, reinstall the SQL Native Client on the data warehouse server. The safest way of reinstalling the SQL Native Client is by upgrading your SQL Server instance to the latest service pack. If you already have the latest service pack and still encounter this issue, download the Microsoft SQL Server 2008 Service Pack 2 Feature Pack or the Feature Pack for Microsoft SQL Server 2005, uninstall the current SQL Native Client, and reinstall the SQL Native Client from the downloaded feature pack.

Note: Cisco recommends upgrading the SQL Server instance to the latest service pack rather than reinstalling the SQL Native Client module. If you get a version mismatch between the SQL Native

Client and the other SQL Server components, this can cause issues for other applications relying on the SQL Server. Installing the latest SQL Server service pack is the recommended procedure whenever possible.

Microsoft Excel and Windows Authentication

Initialization of the data source failed

When connecting to a data warehouse Cube in environments where Integrated Authentication is not available or fails, Excel may run into authentication problems. The user will **not** be warned about this when creating the connection to Analysis Services and the connection will apparently be created properly. However, later when the user tries to use the connection in a Pivot Table or Pivot Chart, the user will get an **`Initialization of the data source failed`** error.

A workaround to the problem is appending the connection string manually:

1. In Excel, go to **Data > Existing Connection**.
2. Select the relevant connection, and click **Open**.
3. In the **Import Data** window that follows, click **Properties…**
4. Go to the "**Definition**" tab (Figure 9).
5. Append the text string in the "**connection string**" field with ";password=<your password>". Note the semicolon in front.
   Example: If the user account is named "peter.jones", the connection string might look like this:

   ```
   Provider=MSOLAP.3;Persist Security Info=True;User
   ID=REPORTING\peter.jones;Initial Catalog=tmsng_dwhAsDb;Data
   Source=analytics.reporting.tms.lab;MDX Compatibility=1;Safety Options=2;MDX
   Missing Member Mode=Error
   ```

   If the password of the account is "ENGLAND66", the modified string should look like this:

   ```
   Provider=MSOLAP.3;Persist Security Info=True;User
   ID=REPORTING\peter.jones;Initial Catalog=tmsng_dwhAsDb;Data
   Source=analytics.reporting.tms.lab;MDX Compatibility=1;Safety Options=2;MDX
   Missing Member Mode=Error;password=ENGLAND66
   ```

Checking the "Save password" box will make the changes to the connection string persistent. However, note that the connection string is stored unencrypted in an XML file on the local disk.

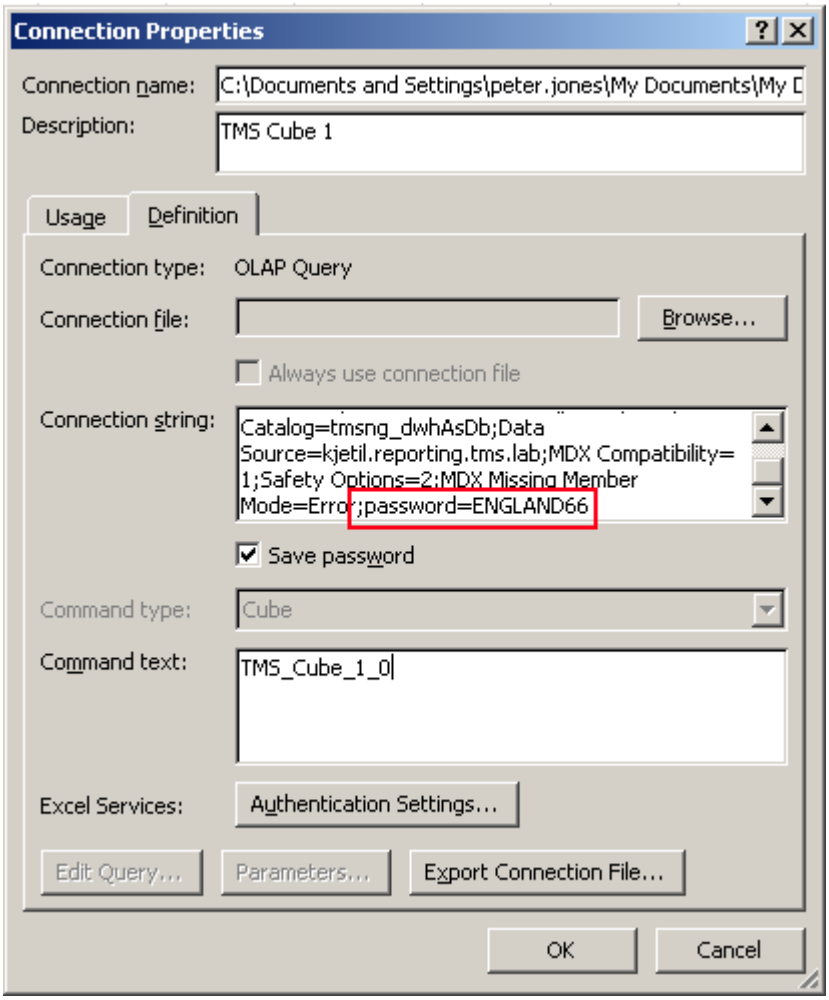


Figure 9: Manually appending the connection string

The LocaleIdentifier property

XML for Analysis parser: The LocaleIdentifier property is not overwritable and cannot be assigned a new value

After creating a connection, the error message **`XML for Analysis parser: The LocaleIdentifier property is not overwritable and cannot be assigned a new value`** may appear when you try to utilize the connection in a pivot table or chart. This issue only applies to certain combinations of old versions of Excel and SSAS. The following Microsoft Connect page describes a workaround Error when creating an Excel Pivot Table from a SSAS project.

1. Right click the connection in the **Select Data Source window** and select ***Open with > Notepad*** (Figure 10) to edit the connection file as described in the Microsoft Connect page.

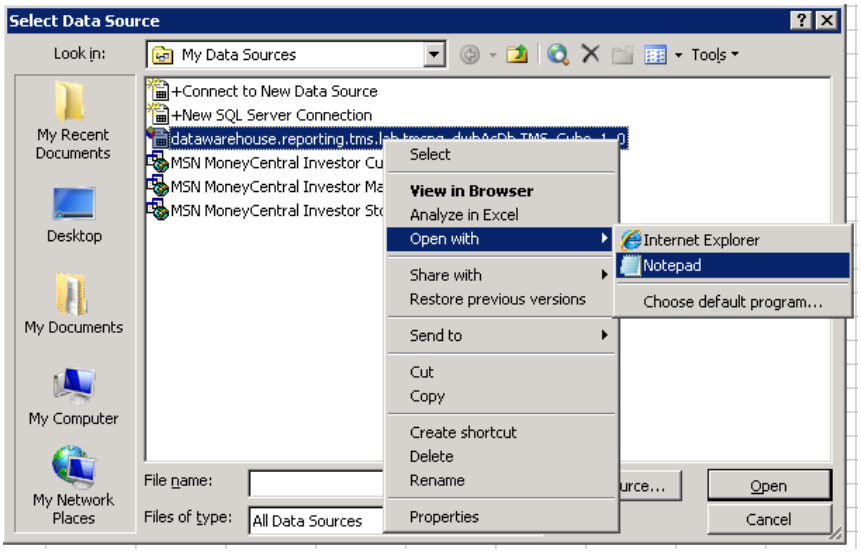


Figure 10: Opening the connection for editing

2. Locate the **`<odc:ConnectionString>`** element, and append **`";Locale Identifier=1033"`** (note the semicolon) to the end of the element's content (Figure 11). Click **Save**.
3. The connection is now updated and ready for use.

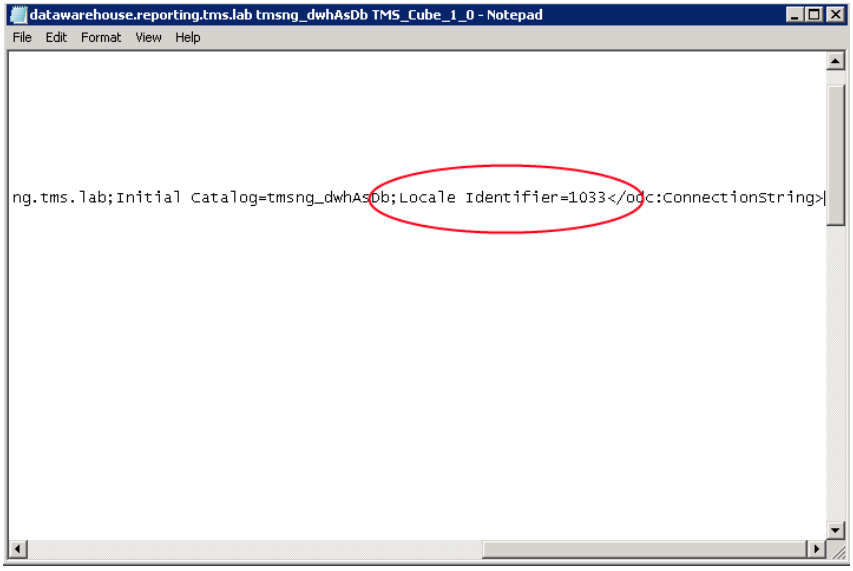


Figure 11: Appending the connection string

Logs

If you experience difficulties with Cisco TMSAE, technical support may ask you to supply log files along with a description of your issue. The follow sections outline the types of logs available. For information on installer logs, see the Installation Guide.

Application Logs

Problems with the Analytics Extension web interface or the Windows Service that initiates the update jobs are logged in files located on the web server where the Analytics Extension was installed. Logged events from the Analytics Extension web interface and the Analytics Extension Service are stored in the following locations:

- <Installation Dir>\TANDBERG\Analytics Extension\ReportingService\Logs
- <Installation Dir>\TANDBERG\Analytics Extension \AdminWeb\App_Data\Logs

These files are plain text but are low level and intended for debugging purposes by support personnel.

Database Logs

The data warehouse itself also keeps logs useful for troubleshooting; these entries are stored in the database itself in the tables

- orc.ExecutionEventLog
- orc.ErrorEventLog
- dwh.AppliedPatch
- dwh.InstallerEventLog

The logs may be browsed using any SQL tool. To save all the entries in these logs to a file:

1. Open **Management Studio** and connect to the database engine instance
2. Expand **Databases**, find your data warehouse database (**tmsng_dwh** by default)
3. Right-click on the database and select “New Query”.
4. Set the Results to save to a file. Right click in the Query Menu, and select **Results to > Results to File.**
5. In the query window, type in the follow four commands

   ```
   SELECT * FROM orc.ExecutionEventLog;
   SELECT * FROM orc.ErrorEventLog;
   SELECT * FROM dwh.AppliedPatch;
   SELECT * FROM dwh.InstallerEventLog;
   ```

6. Click the **Execute** button to run the query. You will be prompted for a file name to save the results to. This will be a CSV file of the output you can share with technical support if requested.

Setting up HTTP access to the CUBE

This section describes how to configure a Windows 2008 Server running SQL Server 2008 so that users may connect to the Analytics Extension CUBE without providing AD credentials. This makes it easier to connect to the CUBE for clients residing in an AD domain beyond the data warehouse server, or clients outside your network.

The solution uses HTTP for data access, taking advantage of IIS 7 as a middleware component to enable access to the CUBE. A small IIS web application – commonly known as an "HTTP pump" – will be set up on the data warehouse Windows server (which may or may not be identical to the TMS server, depending on your setup). This application acts as a "pump" that receives requests, authenticates them, and creates a security context for the requests before forwarding them to Analysis Services. After Analysis Services has executed the request, the pump will in a similar fashion pass the response back to the client.

This approach may also be used in scenarios where IIS and Analysis Services run on different computers. However, Windows does not by default allow AD delegation (remote impersonation by a server of other clients). If using an IIS separate from the Analysis Services server, you must set up Kerberos authentication and configure the domain to allow delegation before proceeding.

Installing IIS

Make sure that IIS is installed on the Windows server you want to set the HTTP pump set up on, normally the data warehouse server.

1. Open **Start > Administrative Tools > Server Manager.**
2. Check whether **Web Server IIS** is mentioned on the **Roles Summary** pane. If IIS is not already installed, click **Add Roles** and follow the installation wizard.

IIS needs the *ISAPI Extensions role* service installed, as well as an Authentication component. This document assumes that Basic authentication is installed. However, this authentication method transmits passwords using an easily decrypted algorithm, and should not be used if you are sending sensitive data over the public internet (unless you are also using SSL). It should however, be sufficient for internal networks.

To check if these components are installed:

1. Use the tree view in Server Manager and go to the **Roles** node.
2. Open the **Web Server (IIS)** pane, and if **ISAPI Extensions** and **Basic Authentication** (or the authentication method of your choice) have their status set to **Installed,** it is not necessary to install them. If they are not installed, install them by clicking **Add Role Services** and follow the installation wizard.

Copying the pump binaries

You must now manually copy binary files from Analysis Services to the directory that you want to use as the basis for your HTTP pump web application.

In a default 32-bit installation of SQL Server 2008, the required files are located in

`C:\Program Files\Microsoft SQL server\MSAS10.MSSQLSERVER\OLAP\bin\isapi`.

Copy all of the files and subdirectories of this folder to a subdirectory of C:\inetpub\wwwroot, for example to **`C:\inetpub\wwwroot\analytics-pump`**.

Do not use a path that contains spaces.

Creating an IIS application pool

1. Open Server Manager
2. Locate the **Server Manager > Roles > Web Server (IIS) > Internet Information Services (IIS) Manager** node.
3. In the "Connections" tree view that opens, right-click **Application Pools** and choose "**Add Application Pool…"**

4. Give the new application pool a suitable name (for example “Analytics-pump”), and set **Managed pipeline mode** to **Classic** (Figure 12).

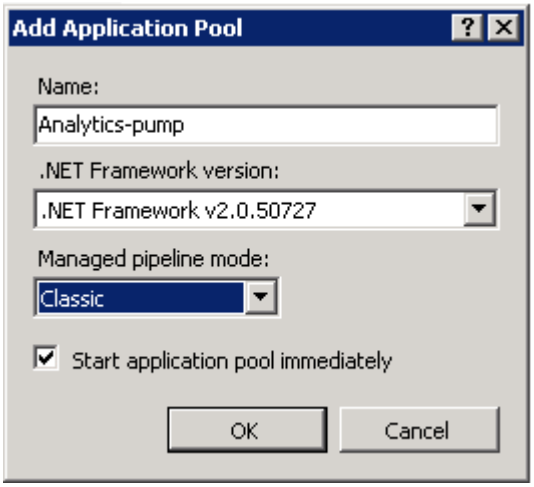


Figure 12

Locate **Default Web Site** in the tree view. Right-click **Default Web Site**, and choose **Add Application…** (Figure 13).

1. Give the application an alias (for example “Analytics-pump”)
2. Click **Select…** and choose the application pool you created above
3. Set the **Physical path** field to the location of the pump binaries (for example `C:\inetpub\wwwroot\analytics-pump`, see above)
4. Click **OK** to close the **Add Application** dialog.

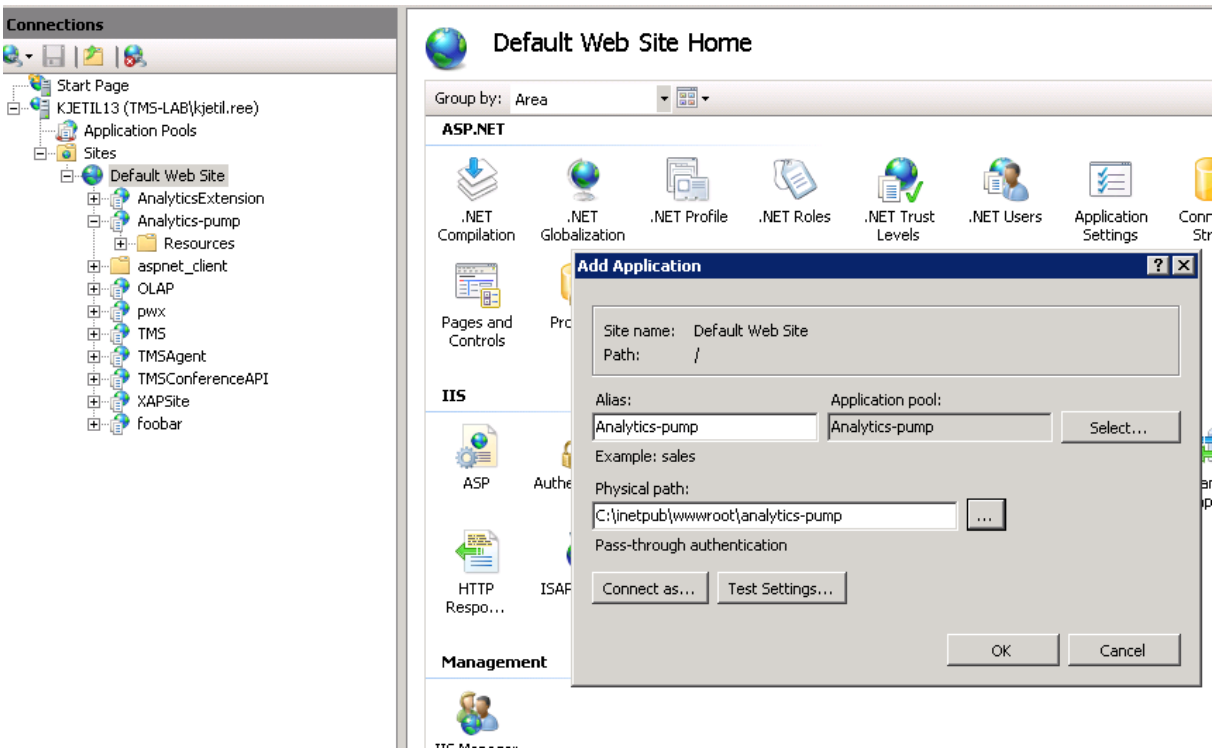


Figure 13

Setting up handler mappings

1. Open the Internet Information Services (IIS) Manager tree view, and select the newly created web application.
2. Select **Handler Mappings** from the menu.
3. Click **Edit Feature Permissions…** in the Actions list to the far right.

4. Make sure that both **Read** and **Script** are selected. Click **OK**.
5. Click **Add Script Map…** in the Actions list. A new dialog window now opens (Figure 14).
6. In the **Request path:** filed, type *.dll
7. Click **…**, and locate the folder that you copied the binaries to. Select **`msmdpump.dll`** and click **Open**.
8. Give a suitable name in the **Name**: field, for example Analytics-pump.
9. Click **OK**. You are now asked if you want to allow this ISAPI extension. Click **Yes**.

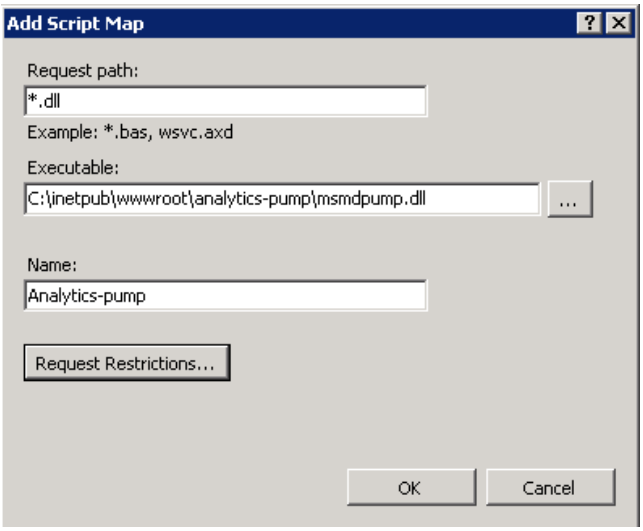


Figure 14

Name extension

1. Go to the Internet Information Services (IIS) Manager tree view and select the server node.
2. Click the **ISAPI and CGI Restrictions** icon from the IIS group (Figure 15).

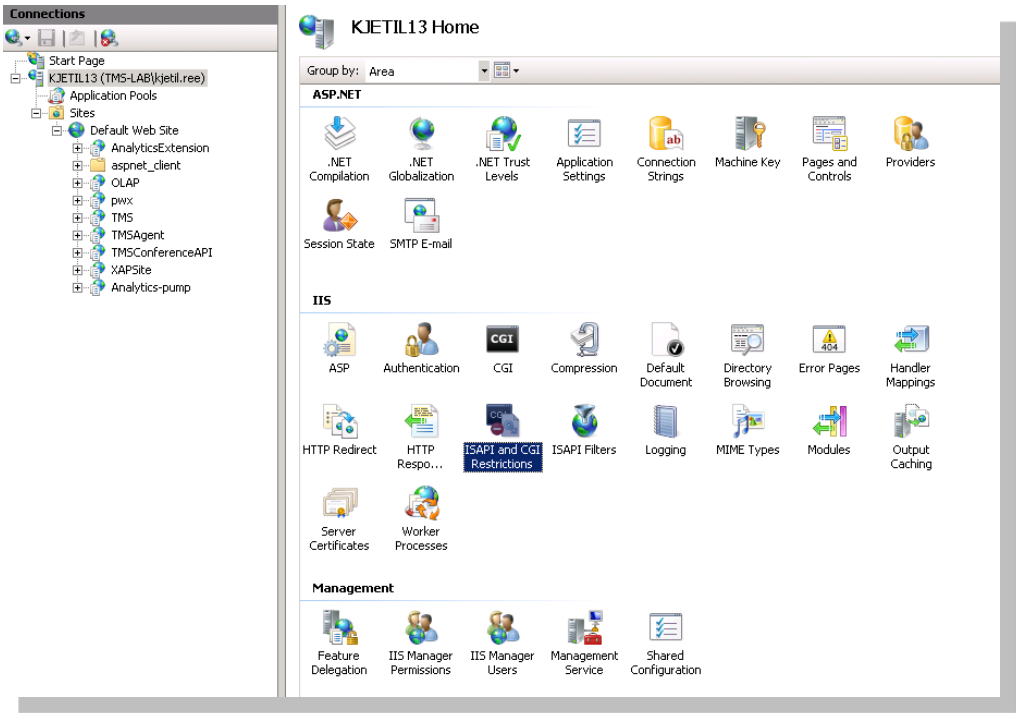


Figure 15

3. A list of extensions appears. Find the extension you just created, select it, and click **Edit…**.
4. Give the extension a descriptive name (Figure 16), and click **OK**.

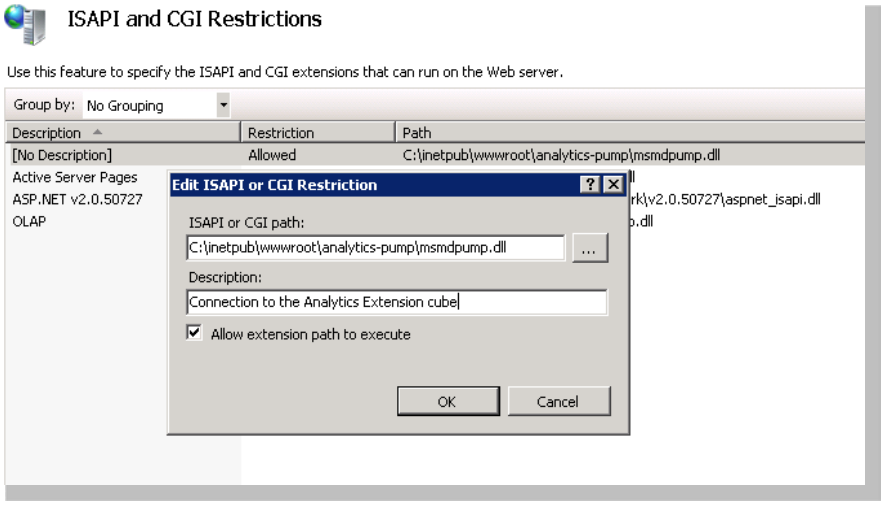


Figure 16 Descriptive extension name

Choosing an authentication mode

Select the Analytics-pump node from the tree view, and click **Authentication**. You will now get a list of all authentication methods installed on your IIS server.

1. Right-click **Anonymous Authentication** and click **Disable**.
2. Right-click **Basic Authentication** and click **Enable**.
3. Right-click **Basic Authentication** and click **Edit…** An **Edit Basic Authentication Settings** window opens (Figure 17).
4. Enter the Windows domain of the data warehouse server in both the **Default domain** and **Realm** fields. Click **OK**.

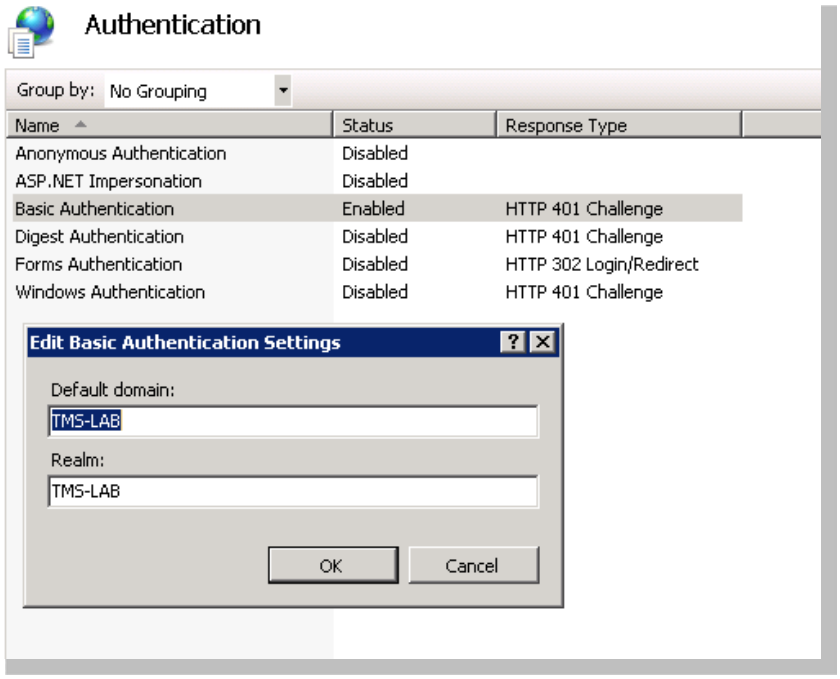


Figure 17 Edit Basic Authentication Settings window

Setting msmdpump.dll as the default document

1. Open the Internet Information Services (IIS) Manager tree view and select the Analytics-pump node
2. Click **Default Document**.
3. Click **Add…** in the **Actions** list.

4. In the dialog box, type *msmdpump.dll* and click **OK**.

Setting the target Analysis Services server

1. Open the folder containing the binary files (C:\inetpub\wwwroot\analytics-pump, if you used the example values above).
2. Open the **`msmdpump.ini`** file in a text editor.
3. Locate the **`<ServerName>localhost</ServerName>`** line in the .ini file.
4. If you installed Analysis Services using the default instance, leave the setting unchanged. If you use a named instance of Analysis Services, change the setting accordingly. For example, if the instance is named “myinstance”, the line should be changed to **`<ServerName>localhost\myinstance</ServerName>.`**
5. If you installed the HTTP pump on another server than your data warehouse server, replace **`localhost`** with the data warehouse machine name.

Creating a domain service account and giving it read access to the cube

You will need to create a domain account that is allowed to read the cube. This may be any domain account, as long as it is member of the *Reader role* defined in the **tmsng_dwhAsDB** Analysis Services database. See the Cisco TMSAE Installation Guide for instructions on adding accounts to this role.

This account will be used by all clients that access the HTTP pump. Cisco TelePresence recommends setting up this account so that users are not allowed to change its password.

Verifying that the connection works

The HTTP pump is now set up and ready to use.

You should verify your setup by connecting to it from a computer that is not in the same domain as the data warehouse server. It is assumed in this section that you are using Microsoft Excel to test the connection, but any client that can connect to an OLAP cube may be used.

Open a new workbook, and create a new workbook connection to Microsoft SQL Server Analysis Services by going through Excel’s Data Connection Wizard. See the Cisco TMSAE Installation Guide for a guide to creating connections.

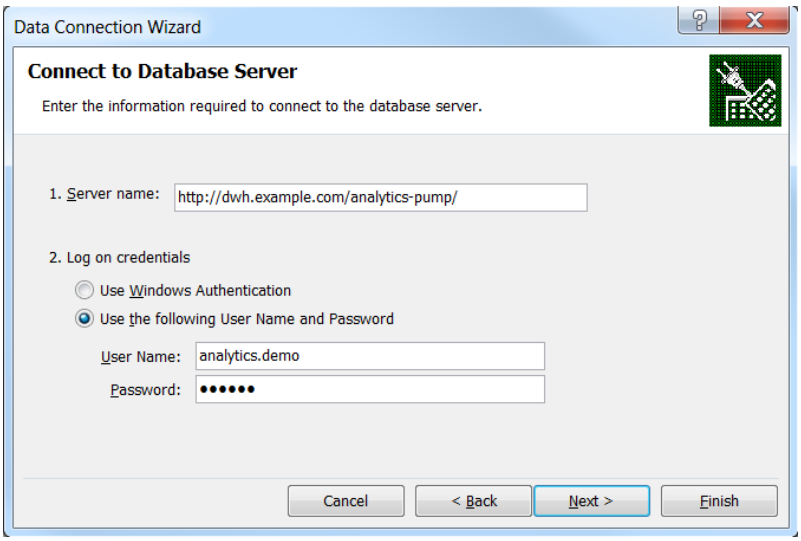


Figure 18 The HTTP pump URL

In the step where you normally enter the server name, enter the url to the HTTP pump instead (Figure 18). For example, if your IIS resides on dwh.example.com, the full url to the HTTP pump will be **`http://dwh.example.com/analytics-pump/`** (note the trailing slash). Use the username and password of the service account you just created.

When saving the data connection file, make sure to select **Save password in file** (Figure 19).

When the connection has been created, it can be used in pivot tables and pivot charts just like any other connection to Analysis Services.

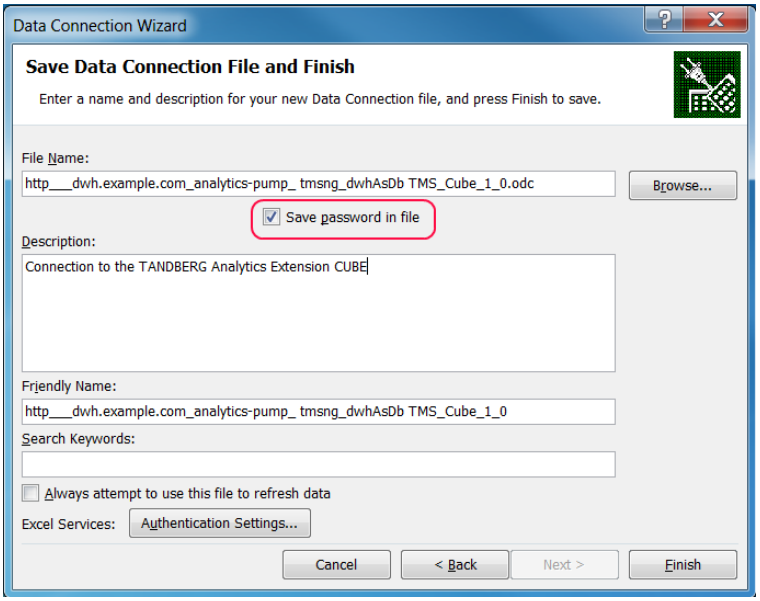


Figure 19 Save password in file

Bibliography

The following table lists documents and websites referenced in this document.

Title	Reference	Link
Cisco TelePresence Management Suite Analytics Extension Installation Guide	D14657	http://cisco.com
Cisco TelePresence Management Suite Analytics Extension API Programming Reference Guide	D14701	http://cisco.com
Using SQL Server Browser		http://msdn.microsoft.com

Licenses

TANDBERG Analytics Extension © NOTICE

TANDBERG Analytics Extension PRODUCT

This product has been developed using software that is protected under copyright and other laws. Such software can be used under the following terms and conditions:

Apache License, Version 2.0:

Software released under the Apache License, Version 2.0: log4net.

The license can be found at http://www.apache.org/licenses/LICENSE-2.0.html

Microsoft End-User License Agreement:

Software released under the Microsoft End-User License Agreement: MICROSOFT SQL SERVER 2008 ADOMD.NET.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2008 ADOMD.NET

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE.

If you comply with these license terms, you have the rights below.

1. INSTALLATION AND USE RIGHTS. You may install and use any number of copies of the software on your devices for your use solely with Microsoft SQL Server 2008 software.

2. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

a. Distributable Code. The software is “Distributable Code” that you are permitted to distribute in programs you develop if you comply with the terms below.

i. Right to Use and Distribute.

· Distributable Code. You may copy and distribute the object code form of the Distributable Code. You may not modify the Distributable Code and your programs must include a complete copy of the Distributable Code, including set-up.

· Third Party Distribution. You may permit distributors of your programs to copy and distribute the Distributable Code as part of those programs.

ii. Distribution Requirements. For any Distributable Code you distribute, you must

· add significant primary functionality to it in your programs;

· require distributors and external end users to agree to terms that protect it at least as much as this agreement;

· display your valid copyright notice on your programs; and

· indemnify, defend, and hold harmless Microsoft from any claims, including attorneys' fees, related to the distribution or use of your programs.

iii. Distribution Restrictions. You may not

· alter any copyright, trademark or patent notice in the Distributable Code;

· use Microsoft's trademarks in your programs' names or in a way that suggests your programs come from or are endorsed by Microsoft;

· distribute Distributable Code to run with a software program other than Microsoft SQL Server 2008 software;

· include Distributable Code in malicious, deceptive or unlawful programs; or

· modify or distribute the source code of any Distributable Code so that any part of it becomes subject to an Excluded License. An Excluded License is one that requires, as a condition of use, modification or distribution, that

· the code be disclosed or distributed in source code form; or

· others have the right to modify it.

3. Scope of License. The software is licensed, not sold. This agreement only gives you some rights to use the software. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. You may not

· work around any technical limitations in the software;

· reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;

· make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;

· publish the software for others to copy;

· rent, lease or lend the software; or

· use the software for commercial software hosting services.

4. BACKUP COPY. You may make one backup copy of the software. You may use it only to reinstall the software.

5. DOCUMENTATION. Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.

6. TRANSFER TO A THIRD PARTY. The first user of the software may transfer it and this agreement directly to a third party. Before the transfer, that party must agree that this agreement applies to the transfer and use of the software. The first user must uninstall the software before transferring it separately from the device. The first user may not retain any copies.

7. Export Restrictions. The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.

8. SUPPORT SERVICES. Because this software is "as is," we may not provide support services for it.

9. Entire Agreement. This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.

10. Applicable Law.

a. United States. If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

b. Outside the United States. If you acquired the software in any other country, the laws of that country apply.

11. Legal Effect. This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.

12. Disclaimer of Warranty. The software is licensed “as-is.” You bear the risk of using it. Microsoft gives no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this agreement cannot change. To the extent permitted under your local laws, Microsoft excludes the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

13. Limitation on and Exclusion of Remedies and Damages. You can recover from Microsoft and its suppliers only direct damages up to U.S. $5.00. You cannot recover any other damages, including consequential, lost profits, special, indirect or incidental damages.

This limitation applies to

· anything related to the software, services, content (including code) on third party Internet sites, or third party programs; and

· claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.