Telescope
Installation and Configuration Guide
for Windows Server Edition

northplains™

Connecting your world. Visually.

Northplains http://www.northplains.com/contact/ help@northplains.com

Version 9.4.0.17 (February, 2019)

Contents

Core Installation 9

1 Overview 10

1.1 Introduction 11
1.1.1 About Telescope 11
1.1.2 Telescope Server Architecture Overview 11
1.1.3 Prerequisites Of Note 12
1.2 Overview of Installation Steps 14
1.2.1 Enterprise Considerations 14

2 Get Started 17

2.1 Set an ODBC Connection for the Telescope Database 18
2.2 Prepare for Installation 20
2.2.1 Unzip the Telescope Release Files 20
2.2.2 Copy the License File to the Hub Server 20
2.2.3 Verify the Machine Names 20

3 Edit the Installation Configuration File 23

3.1 Edit the installConfig.xml Configuration File 24
3.1.1 For Installing on One Machine 24
3.1.2 For Installing across Multiple Machines 24
3.2 Hub Server Configuration 25
3.2.1 Configure the InstallConfig.xml File on the Hub Server 25
3.2.2 Run LightsoutInstaller on the Hub Server 29
3.3 Web Application Server Configuration 30
3.3.1 Configure the InstallConfig.xml File on the Web Application Server 30
3.3.2 Run LightsoutInstaller on the Web Application Server 31
3.4 Web Server Configuration 32
3.4.1 Configure the InstallConfig.xml File on the Web Server 32
3.4.2 Run LightsoutInstaller on the Web Server 33
3.5 InstallConfig Properties 34
3.5.1 Essential InstallConfig Properties 34

4 Install Telescope 37

4.1 Run the lightsoutInstall.exe Installer ... 38
4.1.1 Before You Continue: Checklist ... 38
4.1.2 Run the Lights Out Installation ... 38
4.1.3 Ensure the Correct Java Version is Being Used ... 39
4.2 LightsoutInstall Options ... 41

5 Install Telescope Database Server 43

5.1 Create a Microsoft SQL Database ... 44
5.2 Create an Oracle Database ... 50
5.2.1 Notes on Using Oracle Databases with Telescope ... 50
5.2.2 Create an Oracle Database ... 50
5.3 Mirroring the Database (Optional) ... 56
5.3.1 Prepare the Environment for Mirroring ... 56
5.3.2 Prepare the Principal and Mirror Database for Mirroring (Backup and Restore) 56

6 Configure Telescope over the Web 59

6.1 Configure for Launching the WebObjects Monitor ... 60
6.1.1 Include WebObjects in ISAPI and CGI restrictions ... 60
6.1.2 Configure IIS Application Pools for 32-Bit ... 62
6.1.3 Create a Scripts Virtual Directory ... 63
6.1.4 Configure Handler Mappings for the IIS Folders ... 64
6.1.5 Enable Anonymous Authentication ... 68
6.1.6 Restart the World Wide Web Publishing Service ... 68
6.1.7 Browser Considerations ... 69
6.1.8 Firewall Configuration ... 69
6.1.9 Test the WebObjects Monitor ... 70
6.1.10 Next Steps ... 71
6.2 Define an Encryption Passphrase ... 72
6.2.1 Change the Encryption Passphrase Later ... 74
6.3 Next Steps ... 75

7 Additional Configuration 77

7.1 Install/Configure Telescope Brokers ... 78
7.1.1 Introduction to Telescope Brokers ... 78
7.2 Install Solr Search ... 80
7.2.1 Install Solr on a Clean Machine (on the C: drive) ... 80
7.2.2 Install Solr on a Clean Machine on Drives other than C: ... 80
7.2.3 Next Steps ... 81
7.3 Enable Telescope Video Support ... 82

7.3.1 Install the Appropriate Media Players 82
7.3.2 Additional Configuration for IIS 7 82
7.3.3 Configure the VideoPlayersConfig.xml File 83
7.3.4 Video Download Performance Considerations 84
7.4 Configure I-Pieces and C-Pieces 86
7.5 Configure for Multiple File Brokers 87
7.5.1 88
7.6 Install the Xinet File Broker 89
7.6.1 Install and Configure a Xinet File Broker 89
7.6.2 Configure the Xinet File Broker 91
7.6.3 Starting the Xinet File Broker 92
7.6.4 Stopping the Xinet File Broker 92
7.7 Install and Configure the Queue Broker 93
7.7.1 Install the Queue Broker 93
7.7.2 To Remove the Queue Broker 93
7.8 Customize your Sites 95
7.8.1 Additional Site Customization 95

8 Apply Product Upgrades 97

8.1 Upgrade the Telescope Release 98
8.1.1 Before You Start 98
8.1.2 Install the Upgrade 99
8.1.3 Ensure the Correct Java Version is Being Used 100
8.1.4 Notes on Reinstalling Solr Search 102
8.1.5 Verify the Upgrade 102
8.1.6 Upgrade the Telescope Database 104
8.1.7 Apply Configurations and Customizations from Backups 105
8.2 Upgrade the Telescope Database 106
8.2.1 Upgrade the Telescope Database 106
8.2.2 Update Telescope Database Credentials 109
8.2.3 Back up and Restore from Oracle 11g to Oracle 12C 110

9 Troubleshooting 113

9.1 Cannot Access Telescope on the Web 114
9.1.1 Initial Troubleshooting Steps 114
9.1.2 Troubleshooting Steps for Multiple Server Machines 116
9.2 Miscellaneous Troubleshooting 121
9.2.1 404 Errors for Telescope Uploader or Other Web Applications 121
9.2.2 Content Search does not work with WHERE clause (Oracle) 121

9.2.3 Server names with special characters not supported 121
9.2.4 Client gets "Session expired" when routing through Blue Coat Proxy 121
9.2.5 Video assets do not play in Preview (QuickTime) using Firefox 122
9.2.6 “Trust anchor missing” error in TSWeb logs 122
9.3 Add License Keys 123
9.4 Update the Master License Key 124
9.5 Contact Customer Service 127

Security Considerations 129

10 Configure SSL for Downloads 130

10.1 Configure SSL for Downloads 131
10.1.1 Prerequisites 131
10.1.2 Install the Certificate on the Web Server 131
10.1.3 Add the Site Binding 134
10.1.4 Configure plist Files 136
10.1.5 Restart and Verify 138
10.2 Set Up Reverse Proxy for Downloads (Using Microsoft ARR) 139
10.2.1 What is Reverse Proxy? 139
10.2.2 Set Up Microsoft ARR (Overview) 139
10.2.3 Determine the Embedded Port Number 139
10.2.4 Configure IIS to Route All Requests Through ARR 140
10.2.5 Configure DLManager for ARR 145
10.2.6 Troubleshooting Microsoft ARR 147

11 Configure Web Security Features 149

11.1 What are XSS Security Attacks? 150
11.1.1 Types of XSS Security Attacks 150
11.1.2 Telescope Security Features 150
11.2 Change XSS Configuration 152
11.2.1 Default XSS Code Example 152
11.2.2 Interpret and Change the Configuration File for Blacklisted Strings 154
11.2.3 Change the Configuration File to Allow Search for Special Characters 155
11.2.4 Change the Secure Session ID 156
11.2.5 Change the Password Policy 156
11.2.6 Regular Expression Syntax 157
11.2.7 Grouping Expressions 158
11.2.8 For More Information 158

Enterprise Considerations 159

12 Configure LDAP 160

12.1 Set up LDAP to Work with Telescope ... 161
12.1.1 Before You Start 161
12.1.2 Configure the LDAP Plugin ... 161
12.2 Set Up LDAPS (LDAP over SSL, Secure LDAP) ... 165
12.2.1 Before You Start 165
12.2.2 Set up LDAP Plugin for LDAP over SSL ... 165
12.3 Identify Base Authentication Using the LDAP Browser Tool ... 167
12.4 LDAP Troubleshooting Tips ... 172

13 Install Telescope in a Clustered Environment 173

13.1 Overview ... 174
13.2 Create a Cluster ... 175
13.2.1 Install a Failover Cluster ... 175
13.2.2 Validate the Cluster Configuration ... 175
13.3 Create a Failover Cluster ... 178
13.4 Set Up the Cluster ... 179
13.4.1 Set up the Generic Server ... 179
13.4.2 Set up the NPS Name Service ... 180
13.4.3 Set Up All the Services ... 180
13.4.4 Set Up the Broker Service Dependencies ... 180
13.4.5 Notes on Clustering ... 182

Appendixes 183

14 Telescope Configuration Parameters 184

14.1 Telescope Administrator Configuration Parameters ... 185
14.1.1 Info.plist (TSAdmin) ... 185
14.1.2 config.plist (TSAdmin) ... 186
14.2 Download Manager Configuration Parameters ... 188
14.2.1 Info.plist (Download Manager) ... 188
14.2.2 config.plist (Download Manager) ... 190
14.3 Site Manager Configuration Parameters ... 191
14.3.1 Info.plist (Site Manager) ... 191
14.3.2 Config.plist (Site Manager) ... 192
14.4 TSWeb Configuration Parameters ... 193

14.4.1 Info.plist (TSWeb) 193
14.4.2 config.plist (TSWeb) 195
14.5 Other Settings 198
14.5.1 DBUtils 198
14.5.2 Annotation Stroke Width Configuration 198
14.5.3 Update Maximum Number of Assets Viewable in Filmstrip and Side-by-Side Views 198
14.6 Java Applets 200

15 Telescope Registry Keys 201

15.1 Authentication Broker 202
15.2 Connection Broker 204
15.3 Distribution Broker Configuration 205
15.4 File Broker 208
15.5 Graphics Broker 212
15.6 InDesign Server 216
15.7 Indexing Broker and Child Indexing Brokers 217
15.8 Ingest Broker 218
15.9 Lookup Broker Configuration 222
15.10 Message Broker 224
15.11 Multi-Hub Settings 226
15.12 Queue Broker Registry Keys 227
15.13 Session Broker 229
15.14 State Broker 231
15.15 Zoom Broker Configuration 233
15.16 Zoom Builder Configuration 234
15.16.1 Add a New Field to the EDITORIAL Table 236
15.16.2 Create a Folder to Store Zoom Images 236

16 Third-Party License Acknowledgements 237

16.1 MediaInfo(Lib) License Acknowledgement 238
16.2 ZenLib License Acknowledgement 239
16.3 zlib Data Compression Library 240
16.4 MD5 (from RSA Data Security, Inc.) 242

Core Installation

Chapter 1: Overview

The Installation and Configuration Guide for Telescope contains the information required for a complete and successful installation of Telescope 9.1 using the Windows Server 2008 R2 or 2012 operating system.

After installing Telescope, refer to the *Telescope Administrator's Reference Manual* for administrative tasks, and the *Telescope User Guides* for end-user tasks.

In this Chapter:

- Section 1.1, "Introduction," on page 11

1.1 Introduction

NOTE: The Telescope interface can look slightly different depending on which browser you are using. Fonts, buttons, links, and other interface elements can appear slightly different than the screen examples in this guide, but the location of the functionality should be the same. The screen examples in this guide are from Telescope running on Mozilla Firefox on Windows.

1.1.1 About Telescope

Telescope Enterprise is North Plains' modular, award-winning digital asset management platform. It enables the secure access, management and distribution of all digital and rich media content in virtually any file format, across any size organization in any industry.

1.1.2 Telescope Server Architecture Overview

NOTE: For a detailed introduction to the Telescope server architecture, see the *Telescope Systems Requirements* guide.

Typically, enterprises install Telescope servers on multiple machines for increased web security and/or improved load balancing. Configuration is required for the following servers, which can reside on one, two, or multiple machines.

- **A Telescope server**—this server includes all Telescope brokers. It includes the **hub server**, which contains the core set of brokers necessary to run Telescope: the authentication, connection, state, session, and name service brokers. It also includes other brokers, which are typically installed on the same machine, but can be installed on remote server storage in distributed environments. For example, the **file server**, where File Broker and Graphics brokers are installed.

  (Provide this machine's name, IP address, or domain name when examples in this guide show "<your_hub_server>".)

- **A web application server**—this server runs the WebObjects software, which includes web applications such as TSAdmin, TSWeb, DLManager, and Site Manager. These applications can be installed on separate servers if required. They are accessible from the WebObjects Monitor.

  (Provide this machine's name, IP address, or domain name wherever examples in this guide show "[WEB_APPLICATION_SERVER_HOST]" or "<your_web_app_server>".)

- **A web server**—this server is the interface between Telescope and the web. It stores images and runs WebObjects adaptors, IIS is required on Windows (Apache on UNIX).

  (Provide this machine's name, IP address, or domain name wherever examples in this guide show "[WEB_SERVER_HOST]" or "<your_web_server>".)

- **A database server**—this server runs the database that stores all metadata and other information required by the Telescope server.

  (Provide this machine's name, IP address, or domain name wherever examples in this guide show "<your_database_server>".)

- **File Store**—assets themselves are stored in a network-accessible repository. These assets can include images, digital print and multimedia files, including video and music.

- **Solr Search platform**—the Solr search platform and its brokers should also run on its own servers. For details on setting up Solr, see the *Telescope Administrator's Guide*.

Third-Party Software Used By Telescope

A variety of third-party executables and libraries are installed as part of the Telescope installation. For a detailed list, go to the *Telescope System Requirements* guide.

1.1.3 Prerequisites Of Note

NOTE: This section provides a small subset of key requirements. For a full list of system requirements (including server and database size considerations and supported browsers), go to the *Telescope System Requirements* guide.

System Requirements

A basic Telescope installation requires one or more server machines with the following software installed. For details on choosing your server configuration, see the *System Requirements Guide*.

- Windows Server 2008 SP2 or 2012 operating system.
- Internet Information Services (IIS) 7 and required components (on the web server). See the next section.
- Microsoft .NET Framework 3.5.1 components (on the Graphics Broker).

Notes:

- Red Hat Enterprise Linux (RHEL) 6.4 (64-bit) is also supported for some hub server functionality. Documentation is available from North Plains.
- For Windows systems, you must have QuickTime 7.7.3 installed. (There are certain limitations that North Plains cannot overcome for later versions.) For Macintosh systems, you should use the QuickTime version installed with the operating system (QuickTime 10.2 for OS X 10.8; QuickTime 10.3 for OS X 10.9, QuickTime 10.4 for OS X 10.10)
- If the Telescope server is installed on a machine with a name that includes an underscore (_) or other special characters, the server may not be accessible from Internet Explorer browsers. In some situations, it may also be unavailable for SSL configurations.

Obtain a North Plains license key file

You need a North Plains Systems license key file to install and use this software. Consult your North Plains Systems representative.

Verify Internet Information Services (IIS) is installed

Before you begin, Internet Information Services (IIS) and required components must be installed on the web server.

1. Open the *Windows Control Panel > Programs and Features*.
2. Select the *Turn Windows features on or off* link.

NOTE: If you are using Windows 2012, you will need to use the Add Roles and Features wizard to get to the following Server Roles step.

3 Enable Web Server (IIS), then enable Application Development under it, and then make sure the following options are enabled under that:

- .NET Extensibility 3.5
- ASP
- CGI
- ISAPI Extensions
- ISAPI Filters

Verify 8dot3 (Windows Server 2012)

For Windows Server 2012, the NTFS feature known as "8dot3 name creation" must be enabled on the file system running Telescope. By default this feature is disabled on the Windows Server 2012 operating system.

To verify this feature is enabled:

1 From a command prompt, run the following command:

```
fsutil 8dot3name query C:
```

where "C:" is the drive letter for the Telescope installation.

2 If the command reports the 8dot3name feature is disabled, issue the following command to enable it for all volumes:

```
fsutil behavior set disable8dot3 0
```

3 Repeat this procedure for all servers where you plan to install Telescope and any third-party dependencies (for example, Image Magick or Adobe InDesign Server).

Details on the 8dot3name feature are available in Microsoft's KnowledgeBase.

Install Adobe Software

- If you plan to use the Adobe InDesign server, you must install this Adobe software before you install Telescope, on the same server machine running the Graphics Broker. If you plan to use the Adobe InDesign Conversion Piece, you must also install the Telescope File Broker on this same server.
- If Adobe DNGConverter has been manually pre-installed on the Telescope server, confirm that the System Environment Path variable has been updated with the DNGConverter install path: `C:\Program Files (x86)\Adobe`. This update must be made on every machine that will run the Graphics Broker.

  System variables are configured in *Start > Control Panel > System and Security > System > Advanced System Settings*.

1.2 Overview of Installation Steps

NOTE: If you are upgrading your Telescope release, go to Section Chapter 8:, "Apply Product Upgrades," on page 97.

The following lists the high-level installation steps for a new installation.

1. Decide on the Telescope architecture appropriate to your organization (number of servers, server configuration, and so on).

   See the *System Requirements* guide.

2. Verify you have all the system requirements in place (including IIS on Windows).

   See Section 1.1.3, "Prerequisites Of Note," on page 12 and the *System Requirements* guide.

3. Configure an ODBC connection for the Telescope database.

   See Section 2.1, "Set an ODBC Connection for the Telescope Database," on page 18 to get started.

4. Unzip the installation package on each server machine.

   See Section 2.2, "Prepare for Installation," on page 20

5. Modify the `InstallConfig.xml` file on each server machine.

   See Section 3.1, "Edit the Installation Configuration File," on page 23.

6. Run the `lightsoutInstall.exe` file.

   See Section 4.1, "Install Telescope," on page 37

7. Install the Telescope database. Choose from either:

   Section 5.1, "Create a Microsoft SQL Database," on page 44
   Section 5.2, "Create an Oracle Database," on page 50

8. Configure for web access to the Telescope administrator's interface, WebObjects.

   See Section 6.1, "Configure for Launching the WebObjects Monitor," on page 60

9. Add a database connection encryption passphrase.

   See Section 6.2, "Define an Encryption Passphrase," on page 72.

10. Perform TSAdmin tasks to provide access permissions to users and groups.

    See Section 6.3, "Next Steps," on page 75.

11. Install and configure the Solr search platform.

    See Section 7.2, "Install Solr Search," on page 80.

12. Perform additional configuration as required.

    See Section 7.1, "Additional Configuration," on page 77.

1.2.1 Enterprise Considerations

The following sections are also available for further optional customization of Telescope installations:

Security considerations:

- Section 10.1, "Configure SSL for Downloads," on page 130
- Section 11.1, "Set Up Reverse Proxy for Downloads," on page 123
- Section 11.1, "Configure Web Security Features," on page 149

Enterprise considerations:

- Section 12.1, "Configure LDAP," on page 160
- Section 13.1, "Install Telescope in a Clustered Environment," on page 173

Linux:

- Red Hat Enterprise Linux (RHEL) installations are available for the web server, web application server, and some hub server functionality. Contact North Plains for more information.

Apache Tomcat:

- It is possible to enable TSWeb, DLManager, and TSAdmin to run under a Apache Tomcat application framework (as opposed to a Web Objects Application framework). This is offered on a limited availability basis. Contact North Plains for more information.

Chapter 2: Get Started

This chapter provides several initial steps you need to take to get started. Before you start, be sure to

Before You Start

Review the overview chapter, especially:

- Section 1.2, "Overview of Installation Steps," on page 14

In this Chapter:

- Section 2.1, "Set an ODBC Connection for the Telescope Database," on page 18
- Section 2.2, "Prepare for Installation," on page 20

2.1 Set an ODBC Connection for the Telescope Database

An ODBC connection to the database must be configured before proceeding with any Telescope installation. The settings you define in these steps will be used during Telescope installation to configure the database settings.

NOTE: If you are creating an Oracle database, you first must install a 32-bit Oracle client (not 64-bit) on the hub server before proceeding with these steps.

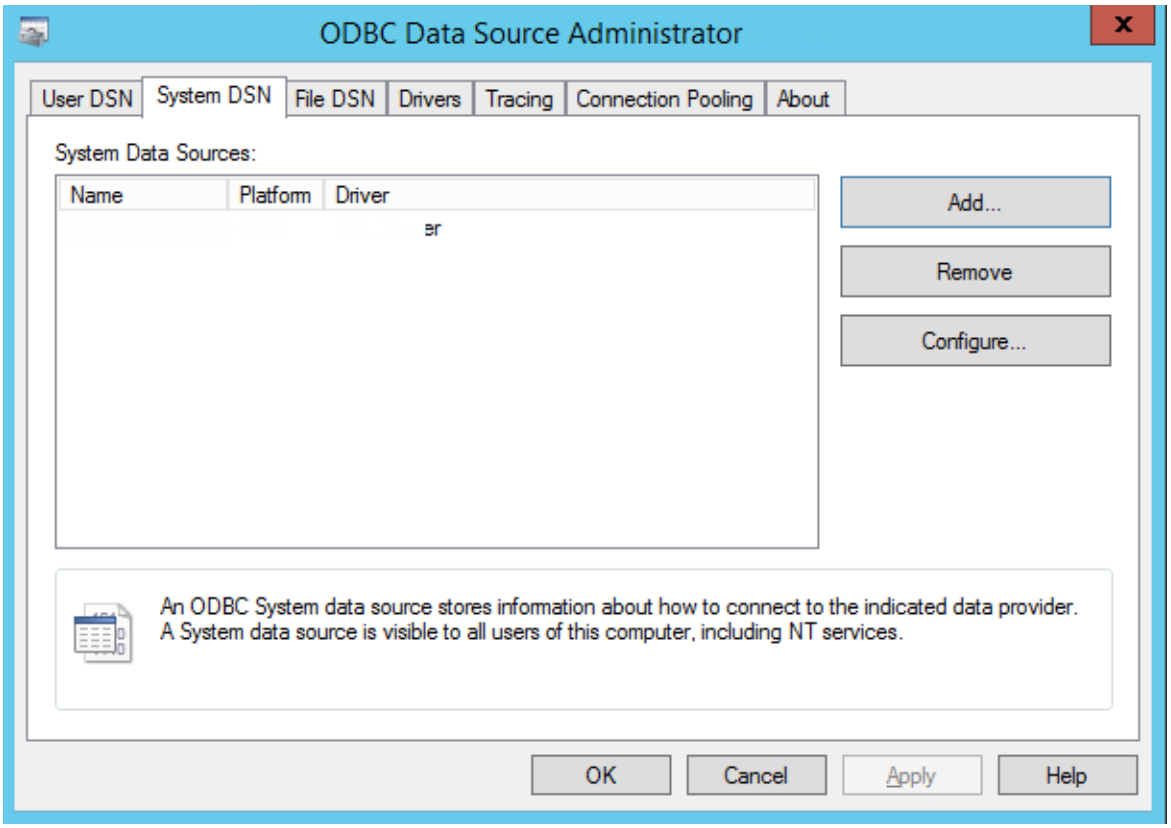
To set an ODBC connection:

1. From the command line of the hub server, open the following executable:

   `C:\WINDOWS\SysWOW64\odbcad32.exe`

2. Click the *System DSN* tab.

Figure 2.1 *Add an ODBC Data Source*

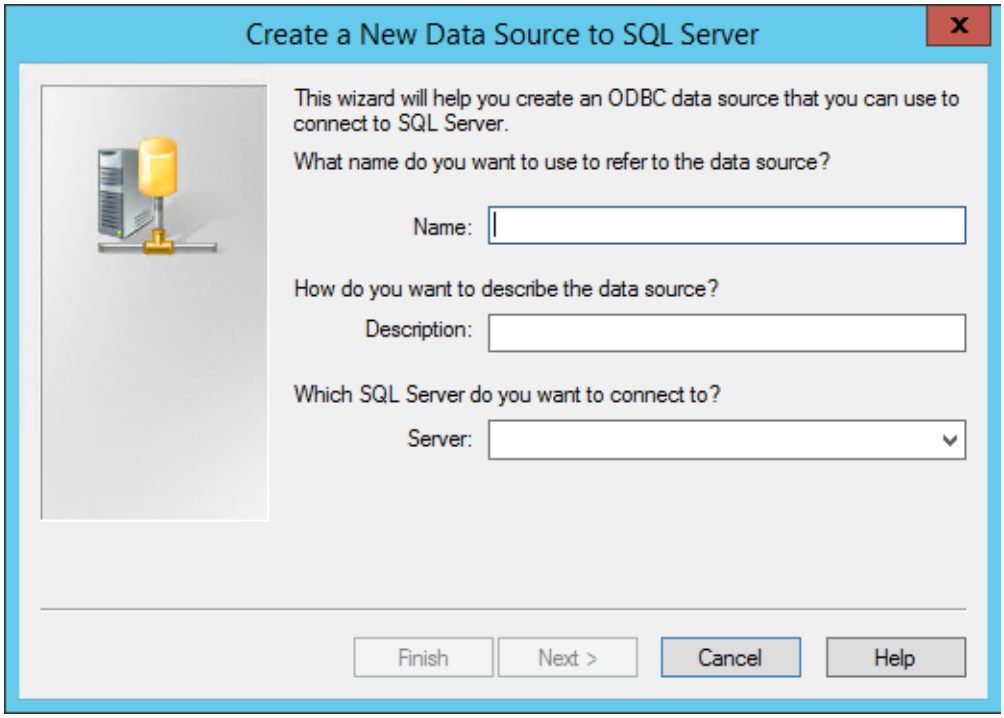


3. Click *Add* and complete the wizard as directed to add a new data source.
4. You are asked to select a driver. Depending on your database server, select either:
   - SQL server
   - Microsoft ODBC for Oracle

Then click Finish.

5 For SQL servers, you will see the following screen. The settings will vary depending on your organization.

Figure 2.2 *Add an ODBC Data Source (Settings)*



Take note of the following settings, which will be needed for configuration in the next chapter:

Value in this window	Description	installConfig property	Your value
Name	Data source name	N/A	
Description	Database description	N/A	
Server	The SQL server you are using (select from the pulldown).	TS_DBServer	

2.2 Prepare for Installation

2.2.1 Unzip the Telescope Release Files

On each server machine:

1. Copy the zipped release file from North Plains to the machine(s) you are going to use as your Telescope server(s).
2. Unzip the release file.
   - Do not store or unzip this file to a directory whose path includes a space. For example, do not store it in `C:\My Documents\`.
   - Do not change the folder structure of the unzipped files or move any files out of the folder.
   - Ensure the folder containing the unzipped files is writable.
3. Go to the top directory of the unzipped files. Verify it contains the files `installConfig.xml` and `lightsoutInstall.exe`.

   Do not run the lightsoutInstall.exe file yet! First, proceed to the next section to modify the configuration file.

2.2.2 Copy the License File to the Hub Server

Copy the license file you obtained from North Plains to the top directory of the unzipped release files on the hub server. Place it in the same directory that contains the files `installConfig.xml` and `lightsoutInstall.exe`. It will be required later during the installation.

2.2.3 Verify the Machine Names

The installation process will require you to use the fully-qualified machine name for each server. (IP addresses can also be used.)

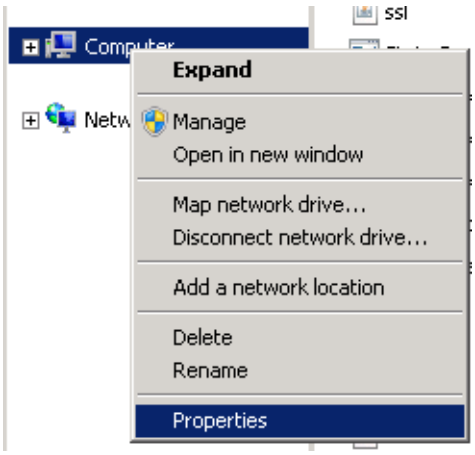
To find the machine name:

NOTE: These steps are for Windows Server 2008. They vary slightly for Windows Server 2012 R2.

---

1. Select *Start* > *Computer*.
2. In the left column of the file browser, right-click over *Computer* and select *Properties* from the menu:

Figure 2.3 *Computer Properties*



3 From the Systems window that appears, look for the *Full Computer Name*.

NOTE: To avoid possible limitations, it is recommended that computer names contain no special characters (such as underscores or hyphens). If this is the case with one of the machines you plan to use, check with your system administrator to see if you can change the machine name or use a different machine.

Chapter 3: Edit the Installation Configuration File

The installation process requires you to modify the `InstallConfig.xml` configuration file before you run the Lights Out installation for each server installation. This chapter provides details on how to edit this file for a successful installation.

Prerequisites:

- Section 2.1, "Set an ODBC Connection for the Telescope Database," on page 18
- Section 2.2, "Prepare for Installation," on page 20

In this Chapter:

- Section 3.1, "Edit the installConfig.xml Configuration File," on page 24
- Section 3.2, "Hub Server Configuration," on page 25
- Section 3.3, "Web Application Server Configuration," on page 30
- Section 3.4, "Web Server Configuration," on page 32
- Section 3.5, "InstallConfig Properties," on page 34

3.1 Edit the installConfig.xml Configuration File

Use a text editor to modify the Telescope installation configuration file `installConfig.xml`, found at the top folder of the installation package you created in Section 2.2, "Prepare for Installation," on page 20.

You must edit this file using a text editor that will not add line breaks or other extra characters. For example, use Notepad (with wordwrap disabled) or a source code editor. DO NOT USE WordPad or Microsoft Word.

3.1.1 For Installing on One Machine

If you are installing all Telescope servers on one machine, set `install="Yes"` for all MSIs you have purchased. Review the information in Section 3.5.1, "Essential InstallConfig Properties," on page 34.

NOTE: For improved performance, most Telescope installations are installed across multiple machines. In particular, to avoid severe performance issues, it is not recommended that you install web components (such as the web server, web application server, Indexing Broker, or Child Indexing Brokers) on the same machine as the hub MSIs.

3.1.2 For Installing across Multiple Machines

If you are installing Telescope across multiple machines, you must edit this file differently before installing Telescope on each machine. We have provided a typical 3-server installation scenario in the following sections:

- A Telescope server (a “hub” server)

  See Section 3.2, "Hub Server Configuration," on page 25

- A web application server

  See Section 3.3, "Web Application Server Configuration," on page 30

- A web server.

  See Section 3.4, "Web Server Configuration," on page 32

NOTE: This is only one server scenario. In some cases, you will want to install brokers across multiple servers, and typically you will install the Solr Multicore server on a separate machine. In each case, check carefully the `install` value for each MSI, and set it to `Yes` if the MSI should be installed on the machine, or `No` if it should not be installed.

3.2 Hub Server Configuration

NOTE: You need to first copy and unzip the release files to the machine you want to use as the hub server. For details, see Section 2.2, "Prepare for Installation," on page 20.

3.2.1 Configure the InstallConfig.xml File on the Hub Server

1 Navigate to the InstallConfig.xml file, located in the Telescope installation folder you unzipped on the hub server. Open it with a text editor.

2 Scroll down to find **TeleScopeHub.msi** and set its install value to "Yes", as shown here:

```
<msi installorder="1" name="TeleScopeHub.msi" install="Yes">
```

For the `TeleScopeHub.msi`, edit the following parameters:

a Update the database configuration information. These settings will install the configuration for the database needed to handle the Telescope installation. Some of these settings depend on settings determined in Section 2.1, "Set an ODBC Connection for the Telescope Database," on page 18.

TS_DBType—the database type (SQLServer or Oracle)

TS_CONNECTION—the connection name (an arbitrary name you can choose to name the Telescope database connection. Use the same value throughout for all the InstallConfig.xml files on all servers.)

TS_DBName—the database source name you assigned when creating the ODBC connection

TS_DBServer—the server name you used when creating the ODBC connection.

TS_DBPort—the ODBC settings set for the port name (typically, 1433 for Microsoft SQL Server, 1521 for Oracle)

Example:

```
<property name="TS_DBType" value="SQLServer"/>
<property name="TS_CONNECTION" value="your_database_connection>"/>
<property name="TS_DBName" value="<your_database_name>"/>
<property name="TS_DBServer" value="<your_database_server>"/>
<property name="TS_DBPort" value="1433"/>
```

b Update the value of the TS_MASTER_KEY property tag to your Telescope Master Key, found in your license file supplied by North Plains:

```
<property name="TS_MASTER_KEY" value="masterkey"/>
```

c Configure the value of the TS_OMNIORB_HOST property within the TeleScopeHub.msi with the Hub Server's full computer name (with domain), or IP address, as follows:

```
<property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>
```

NOTE: To find the full computer name on Windows 2008 R2, select *Start* > *Computer*. In the left column of the file browser, right-click over *Computer* and select *Properties* from the menu. From the Systems window that appears, look for the *Full Computer Name*. Computer names with special characters such as hyphens or underscores are not recommended.

3 Ensure the 'install' value for **TeleScopeWebApp.msi** is set to "No" as shown here:

```
<msi name="TeleScopeWebApp.msi" install="No">
```

4 Ensure the 'install' value for **TeleScopeWeb.msi** is set to "No" as shown here:

```
<msi name="TeleScopeWeb.msi" install="No">
```

5 Only set the 'install' value to "Yes" for each of the following msi components if you hold a valid license for them, and if they are intended to be installed on the hub server. Set the 'install' value to "No" within each .msi section if it does not need to be installed.

- Depending on your configuration, set the 'install' value for **ChildIndexBroker.msi** to "Yes" as shown here:

```
<msi name="ChildIndexBroker.msi" install="Yes">
```

NOTE: It is recommended that you install Child Indexing Brokers on separate machines, for optimal performance. For more information on Solr Search configuration, see the *Telescope Administrator's Guide*.

Configure the value of the TS_OMNIORB_HOST property within the ChildIndexBroker.msi with the IP address, domain name or machine name of the Hub Server, as follows:

```
<property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>
```

Configure the value of TS_CONNECTION_NAME property to the value you specified for the TeleScopeHub.msi , as follows:

```
<property name="TS_CONNECTION_NAME" value="your_database_connection"/>
```

- Set the 'install' value for **DBManager.msi** to "Yes" as shown here:

```
<msi name="DBManager.msi" install="Yes">
```

- Set the 'install' value for **DistributionBroker.msi** to "Yes" as shown here:

```
<msi name="DistributionBroker.msi" install="Yes">
```

Configure the value of the TS_OMNIORB_HOST property within the DistributionBroker.msi with the IP address, domain name or machine name of the Hub Server, as follows:

```
<property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>
```

- Set the 'install' value for **FileBroker.msi** to "Yes" as shown here:

```
<msi name="FileBroker.msi" install="Yes">
```

  - (Applicable only for use with Equilibrium) Configure the value of the TS_EQ_MapSysPath property within the FileBroker.msi with the IP Address or Machine Name of the Hub Server, as follows:

    ```
    <property name="TS_EQ_MapSysPath" value="file:////<your_hub_server>/Archive/"/>
    ```

  - Configure the value of the TS_OMNIORB_HOST property within the FileBroker.msi with the IP Address or Machine Name of the Hub Server, as follows:

    ```
    <property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>
    ```

  - (Optional) You can set the path to the File Broker's archive directory through the TS_ARCHIVE_DIR property tag found within the FileBroker.msi. This will determine where your assets will get archived in future. The default path is:

    ```
    <property name="TS_ARCHIVE_DIR" value="C:\Archive"/>
    ```

  - (Optional) After setting the path to the File Broker's archive directory, ensure that the value within the TS_SHARE_NAME property tag of the FileBroker.msi is the same as the directory or file name used in the previous step. The default value is "Archive".

    Example: `<property name="TS_SHARE_NAME" value="Archive"/>`

- Set the 'install' value for **GraphicsBroker.msi** to "Yes" as shown here:

  ```
  <msi name="GraphicsBroker.msi" install="Yes">
  ```

  - Update the value of the TS_CONNECTION property tag for the GraphicsBroker.msi with the Connection Name as shown here:

    ```
    <property name="TS_CONNECTION" value="conn_name">
    ```

  - (Applicable only for use with Equilibrium) Configure the value of the TS_EQ_MapSysPath property within the GraphicsBroker.msi with the IP Address or Machine Name of the Hub Server, as follows:

    ```
    <property name="TS_EQ_MapSysPath" value="file:////your_hub_server>/Archive/"/>
    ```

  - Configure the value of the TS_OMNIORB_HOST property within the GraphicsBroker.msi with the IP Address or Machine Name of the Hub Server, as follows:

    ```
    <property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>
    ```

- Set the 'install' value for **InDesignBroker.msi** to "Yes" as shown here:

  ```
  <msi name="InDesignBroker.msi" install="Yes">
  ```

  - Configure the value of the TS_OMNIORB_HOST property within the InDesignBroker.msi with the IP Address or Machine Name of the Hub Server, as follows:

    ```
    <property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>
    ```

  - Update the value of the TS_CONNECTION property tag for the InDesignBroker.msi with the Connection Name as shown here:

    ```
    <property name="TS_CONNECTION" value="conn_name">
    ```

- Set the 'install' value for **IndexBroker.msi** to "Yes" as shown here:

  ```
  <msi name="IndexBroker.msi" install="Yes">
  ```

NOTE: You may prefer to install the Indexing Broker on a separate machine, for optimal performance. For more information on Solr Search configuration, see the *Telescope Administrator's Guide*.

  - Configure the value of the TS_OMNIORB_HOST property within the IndexBroker.msi with the IP address, domain name or machine name of the Hub Server, as follows:

    ```
    <property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>
    ```

  - Update the value of the TS_CONNECTION_NAME" property tag with the Connection Name as shown here:

    ```
    <property name="TS_CONNECTION_NAME"" value="conn_name">
    ```

- Set the 'install' value for **IngestBroker.msi** to "Yes" as shown here:

  ```
  <msi name="IngestBroker.msi" install="Yes">
  ```

  - Update the value of the TS_CONNECTION property tag for the IngestBroker.msi with the Connection Name as shown here:

    ```
    <property name="TS_CONNECTION" value="conn_name">
    ```

  - Configure the value of the TS_OMNIORB_HOST property within the IngestBroker.msi with the IP Address or Machine Name of the Hub Server, as follows:

    ```
    <property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>
    ```

- (Optional) The path to the Ingest Broker's auto ingest directory can be set through the TS_AUTOINGEST_DROPBOX_DIR property tag found within the `IngestBroker.msi`. This will determine the path to all assets stored within your TeleScope Dropbox folder. The default path is:

  ```
  <property name="TS_AUTOINGEST_DROPBOX_DIR" value="C:\TeleScope\Dropbox"/>
  ```

- Set the 'install' value for **InteropBroker.msi** to "No" as shown here:

  ```
  <msi name="InteropBroker.msi" install="No">
  ```

  - The Interoperability Broker is for internal use only. If you are requested by North Plains staff to use it, configure the value of the TS_OMNIORB_HOST property with the IP Address or Machine Name of the Hub Server, as follows:

    ```
    <property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>
    ```

- Set the 'install' value for **LookupBroker.msi** to "Yes" as shown here:

  ```
  <msi name="LookupBroker.msi" install="Yes">
  ```

  - Configure the value of the TS_OMNIORB_HOST property within the LookupBroker.msi with the IP Address or Machine Name of the Hub Server, as follows:

    ```
    <property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>
    ```

- Set the 'install' value for **MessageBroker.msi** to "Yes" as shown here:

  ```
  <msi name="MessageBroker.msi" install="Yes">
  ```

  - Configure the value of the TS_OMNIORB_HOST property within the MessageBroker.msi with the IP Address or Machine Name of the Hub Server, as follows:

    ```
    <property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>
    ```

- Set the 'install' value for **QuickFindSkin.msi** to "No" as shown here:

  <msi name="QuickFindSkin.msi" install="no">

- Set the 'install' value for **SolrMulticore.msi** to "Yes" as shown here (if the Solr search engine will be installed on the same hub machine):

  ```
  <msi name="SolrMulticore.msi" install="Yes">
  ```

- Set the 'install' value for **TeleScopeDocs-Standalone.msi** to "Yes" as shown here (or "No", if you would prefer not to install the documentation):

  ```
  <msi name="TeleScopeDocs-Standalone.msi" install="Yes">
  ```

- Set the 'install' value for **ZoomBroker.msi** to "Yes" as shown here:

  ```
  <msi name="ZoomBroker.msi" install="Yes">
  ```

  - Update the value of the TS_CONNECTION property tag for the ZoomBroker.msi with the Connection Name as shown here:

    ```
    <property name="TS_CONNECTION" value="conn_name">
    ```

  - Configure the value of the TS_OMNIORB_HOST property within the ZoomBroker.msi with the IP Address or Machine Name of the Hub Server, as follows:

    ```
    <property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>
    ```

- Set the 'install' value for **ZoomBuilder.msi** to "Yes" as shown here:

  ```
  <msi name="ZoomBuilder.msi" install="Yes">
  ```

  - Update the value of the TS_CONNECTION property tag for the ZoomBuilder.msi with the Connection Name as shown here:

```
<property name="TS_CONNECTION" value="conn_name">
```

- Configure the value of the TS_OMNIORB_HOST property within the ZoomBuilder.msi with the IP Address or Machine Name of the Hub Server, as follows:

  ```
  <property name="TS_OMNIORB_HOST" value="your_hub_server>"/>
  ```

- Within the ZoomBuilder.msi, configure the value of the TS_ZOOM_SERVER_URL property with the IP Address or Machine Name of the server in which ZoomBuilder is installed (not necessarily the Hub Server):

  ```
  <property name="TS_ZOOM_SERVER_URL" value="http://<zoom_builder_server>/iipmooviewer-
  1.0/iipmooviewer.html"/>
  ```

- Configure other properties and features as required. For example, set the 'install' value of each of the I-Pieces and/or C-Pieces you have purchased and wish to install to "Yes", under each of the various MSIs.

3.2.2 Run LightsoutInstaller on the Hub Server

1. After you have concluded all configuration steps listed in the previous section, run *lightsoutInstall.exe* from the command line on the Hub Server. Be sure to use the -l option to ensure your licenses are also installed.

   See Section 4.1, "Run the lightsoutInstall.exe Installer," on page 38 for details.

3.3 Web Application Server Configuration

NOTE: You need to first copy and unzip the release files to the machine you want to use as the web application server. For details, see Section 2.2, "Prepare for Installation," on page 20.

3.3.1 Configure the InstallConfig.xml File on the Web Application Server

1. Navigate to the `InstallConfig.xml` file, located in the Telescope installation folder you unzipped on the web app server machine. Open it with a text editor.
2. Set the 'install' values for **TeleScopeHub.msi** and **TeleScopeWeb.msi** to "No":

```
<msi installorder="1" name="TeleScopeHub.msi" install="no">
<msi installorder="11" name="TeleScopeWeb.msi" install="no">
```

3. Ensure the 'install' value for **TeleScopeWebApp.msi** is set to "Yes" as shown here:

```
<msi installorder="21" name="TeleScopeWebApp.msi" install="yes">
```

4. Update the value of the following property tags under TeleScopeWebApp.msi with the full machine names of the appropriate servers, as follows:

NOTE: DLAgent is deprecated for Version 9.3. Any DLAgent properties will be ignored.

```
<property name="TS_INETPUB_DIR" value="C:\inetpub"/>   (TYPICALLY, LEAVE AS IS)
<property name="TS_COMVERSION_TIMEOUT" value="3600"/>   (TYPICALLY, LEAVE AS IS)
<property name="TS_DL_AGENT_HOST" value="<your_web_server>"/> (TYPICALLY, LEAVE AS IS)
<property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>
<property name="TS_WEBSERVERHOST" value="<your_web_server>"/>
<property name="TS_WEBSITE_NAME" value="default"/>   (LEAVE AS IS)
<property name="TS_APPSERVERHOST" value="<your_web_app_server>"/>
<property name="TS_CONNECTION" value="<your_database_connection>"/>
<property name="TS_DL_AGENT_PORT" value="8080"/>   (TYPICALLY, LEAVE AS IS)
<property name="TS_DL_USE_AGENT" value="false"/>   (TYPICALLY, LEAVE AS IS)
<property name="TS_OMNIORB_PORT" value="12345"/>   (TYPICALLY, LEAVE AS IS)
```

5. Leave **QuickFindSkin.msi** set to “No”:

```
<msi name="QuickFindSkin.msi" install="no">
```

NOTE: As of Version 9.4.0, QuickFind is no longer supported.

6. Set **every other MSI** to “No” (whether or not you have a license for it):

```
<msi name="DBManager.msi" install="No">
<msi name="DistributionBroker.msi" install="No">
<msi name="ChildIndexBroker.msi" install="No">
```

```
<msi name="FileBroker.msi" install="No">
<msi name="GraphicsBroker.msi" install="No">
<msi name="InDesignBroker.msi" install="No">
<msi name="IndexBroker.msi" install="No">
<msi name="IngestBroker.msi" install="No">
<msi name="InteropBroker.msi" install="No">
<msi name="LookupBroker.msi" install="No">
<msi name="MessageBroker.msi" install="No">
<msi name="SolrMulticore.msi" install="No">
<msi name="TeleScopeDocs-Standalone.msi" install="No">
```
(set this to "Yes", if you would prefer to install the documentation on this server)
```
<msi name="ZoomBroker.msi" install="No">
<msi name="ZoomBuilder.msi" install="No">
```

7 Configure other properties and features as required.

NOTE: Installing WebObjects on a drive other than the C: drive can only be done when doing a clean install.

3.3.2 Run LightsoutInstaller on the Web Application Server

1 After you have concluded all configuration steps listed in the previous section, run *lightsoutInstall.exe* from the command line on the Web Application Server.

The -l option is **not required** for the Web or Web Application Servers (only the hub server).

See Section 4.1, "Run the lightsoutInstall.exe Installer," on page 38 for details.

3.4 Web Server Configuration

NOTE: You need to first copy and unzip the release files to the machine you want to use as the web application server. For details, see Section 2.2, "Prepare for Installation," on page 20.

3.4.1 Configure the InstallConfig.xml File on the Web Server

1. Navigate to the `InstallConfig.xml` file, located in the Telescope installation folder you unzipped on the web server machine. Open it with a text editor.
2. Set the 'install' values for **TeleScopeHub.msi** and **TeleScopeWebApp.msi** to "No":

```
<msi installorder="1" name="TeleScopeHub.msi" install="no">
<msi installorder="21" name="TeleScopeWebApp.msi" install="no">
```

3. Ensure the 'install' value for **TeleScopeWeb.msi** is set to "Yes" as shown here:

```
<msi installorder="11" name="TeleScopeWeb.msi" install="yes">
```

4. Update the value of the following property tags under TeleScopeWeb.msi with the full machine names of the appropriate servers, as follows:

```
<property name="TS_INETPUB_DIR" value="C:\inetpub"/>   (TYPICALLY, LEAVE AS IS)
<property name="TS_WO_CONF_URL" value="http://<your_web_app_server>:1085"/>
<property name="TS_IIS_SCRIPTS_DIR" value="C:\inetpub\Scripts"/>   (TYPICALLY, LEAVE AS
IS)
<property name="TS_OMNIORB_PORT" value="12345"/>   (TYPICALLY, LEAVE AS IS)
<property name="TS_COMVERSION_TIMEOUT" value="3600"/>   (TYPICALLY, LEAVE AS IS)
<property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>
<property name="TS_WEBSERVERHOST" value="<your_web_server>"/>
<property name="TS_WEBSITE_NAME" value="default"/>   (LEAVE AS IS)
<property name="TS_WO_CONF_INTERVAL" value="10"/>   (TYPICALLY, LEAVE AS IS)
<property name="TS_APPSERVERHOST" value="<your_web_app_server>"/>
<property name="TS_CONNECTION" value="<your_connection_name>"/>
```

5. Leave **QuickFindSkin.msi** set to “No”:

```
<msi name="QuickFindSkin.msi" install="no">
```

NOTE: As of Version 9.4.0, QuickFind is no longer supported.

6. Set **every other MSI** to “No” (whether or not you have a license for it):

```
<msi name="DBManager.msi" install="No">
<msi name="ChildIndexBroker.msi" install="No">
<msi name="DistributionBroker.msi" install="No">
<msi name="FileBroker.msi" install="No">
<msi name="GraphicsBroker.msi" install="No">
```

```
<msi name="InDesignBroker.msi" install="No">
<msi name="IndexBroker.msi" install="No">
<msi name="IngestBroker.msi" install="No">
<msi name="InteropBroker.msi" install="No">
<msi name="LookupBroker.msi" install="No">
<msi name="MessageBroker.msi" install="No">
<msi name="SolrMulticore.msi" install="No">
<msi name="TeleScopeDocs-Standalone.msi" install="No">
```
(set this to "Yes", if you would prefer to install the documentation on this server)

```
<msi name="ZoomBroker.msi" install="No">
<msi name="ZoomBuilder.msi" install="No">
```

7 Configure other properties and features as required.

3.4.2 Run LightsoutInstaller on the Web Server

1 After you have concluded all configuration steps listed in the previous section, run *lightsoutInstall.exe* from the command line on the Web Server.

The -l option is **not required** for the Web or Web Application Servers (only the Hub server).

See Section 4.1, "Run the lightsoutInstall.exe Installer," on page 38 for details.

3.5 InstallConfig Properties

3.5.1 Essential InstallConfig Properties

At a minimum, you need to make the following updates to the `installConfig.xml` file. See the other sections in this chapter for more details on how these updates apply to various servers.

installConfig.xml Property	Update to:

All IP addresses or domain names or machine names	For a single-machine installation, update all IP addresses or domain names in the file to match those of the target computer. Full machine names (with domains) are recommended.
	For multiple-machine installations, these values need to reflect the IP address or domain name or machine name for the applicable server machine. For details, see the other sections in this chapter.
	TS_OMNIORB_HOST—The machine hosting the Telescope hub server.
	TS_WEBSERVERHOST—The machine hosting the Telescope web server.
	TS_APPSERVERHOST—The machine hosting the Telescope web application server.
	TS_DBServer—The machine hosting the Telescope database
	TS_DL_AGENT_HOST—The machine hosting the Download Agent (typically, the web server machine). Note that DLAgent was deprecated for Version 9.3.
	Examples:
	`<property name="TS_OMNIORB_HOST" value="<your_hub_server>"/>`
	`<property name="TS_WEBSERVERHOST" value="<your_web_server>"/>`

`install=`	For every component you are installing, set the msi install parameter to “yes”. (If you do not have the license to install the component, set it to “no”.) For multiple-machine installations, these values need to reflect the components being installed on the particular server machine. For details, see the other sections in this chapter. Example: `<msi name="TeleScopeHub.msi" install="yes">`
`TS_MASTER_KEY`	This key is located in the TelescopeHub.msi property tag, and is contained in the license file obtained from North Plains. Contact North Plains technical support to obtain your license file. Example: `<property name="TS_MASTER_KEY" value="5g15e8523bb910ae33273601e02fb614233340d91a382ad4"/>`

installConfig.xml Property	Update to:
TS_DBType	The database type (“SQLServer” or “Oracle”). Example: <property name="TS_DBType" value="SQLServer"/>
TS_CONNECTION	The database connection name (an arbitrary name you can choose to name the Telescope database) Example: <property name="TS_CONNECTION" value="conn_name"/>
TS_DBName	The Telescope database name (or schema name). See Section 2.1, "Set an ODBC Connection for the Telescope Database," on page 18. Example: <property name="TS_DBName" value="TS913"/>
TS_DBServer	The ODBC settings set for the database server name. See Section 2.1, "Set an ODBC Connection for the Telescope Database," on page 18. Example: <property name="TS_DBServer" value="127.0.0.1"/>
TS_DBPort	The ODBC settings set for the databse port number (typically, 1433 for Microsoft SQL Server, 1521 for Oracle) Example: <property name="TS_DBPort" value="1433"/>
TS_ARCHIVE_DIR	Points to the File Broker’s archive directory, the directory used to store assets. This key is located in the FileBroker.msi property tag. Example: <property name="TS_ARCHIVE_DIR" value="C:\Archive"/>
TS_AUTOINGEST_DROPBOX_DIR	Points to the Ingest Broker’s auto ingest directory. To configure auto-ingestion, see the *Administrator’s Guide*. Example: <property name="TS_AUTOINGEST_DROPBOX_DIR" value="C:\TeleScope\Dropbox"/>

NOTE: To install using an alternative configuration file, use the -f command-line option with the LightsoutInstall.exe command.

‘

Chapter 4: Install Telescope

Telescope must be installed from the command line, rather than from the user interface. This process is called a “Lights Out” installation.

Prerequisites:

- Section 2.1, "Set an ODBC Connection for the Telescope Database," on page 18
- Section 2.2, "Prepare for Installation," on page 20
- Section 3.1, "Edit the Installation Configuration File," on page 23 (on all server machines)

In this Chapter:

- Section 4.1, "Run the lightsoutInstall.exe Installer," on page 38
- Section 4.2, "LightsoutInstall Options," on page 41

4.1 Run the lightsoutInstall.exe Installer

4.1.1 Before You Continue: Checklist

Before you run the install command, make sure you have:

- Copied your North Plains Systems license file to the hub machine. It is recommended you copy it to the same level of the unzipped release package where the `installConfig.xml` file is located.
- Copied the unzipped files to every Telescope server machine.
- Edited the default `InstallConfig.xml` file on each server machine to ensure the appropriate MSI components are installed. To find out which components are installed on which servers, see Section 3.1, "Edit the installConfig.xml Configuration File," on page 24.
- Ensured the date and time are synchronized on all servers. This will prevent potential failure of processes that need to run from one server to the next. (This may be an issue if you are using virtual environments that do not reflect your local time.)
- Ensured that your firewall does not prevent communication between all required servers running Telescope components.

4.1.2 Run the Lights Out Installation

The Lights Out Installation is an executable designed to install Telescope in the background, with minimal interaction required. The installation is based on the settings in the `installConfig.xml` file.

Important Tips:

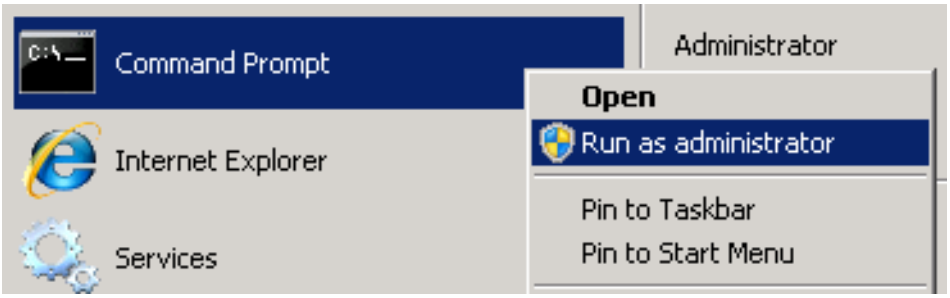
- Review the lightsoutInstall options in Section 4.2, "LightsoutInstall Options," on page 41.
- You need to run the lights out installation on every machine you plan to run Telescope on. (Hub server, brokers, Web server, Web Application server, Solr server, and so on.) Each of these will need a uniquely customized `installConfig.xml` file.
- The -l option is strongly recommended (for the hub server only), so you will not need to add licenses manually later. (The -l option is applicable to the Hub server, not the Web or Web App servers.)
- Use the -i option if the installation is on a drive other than C:
- The installation program does NOT automatically create a single installation log file. To create a log file (which is extremely helpful in troubleshooting potential issues resulting from an installation procedure), either copy and paste the command prompt output immediately after running the command, or redirect output from the Telescope installation program to a file by adding the redirect "`>LOG_FILE_NAME.txt`" to the end of the command. Include the path if you want to store it to another location; for example, "`>E:\logs\LOG_FILE_NAME.txt`"

Run the Lights Out Installation:

Repeat the following on each server you plan to use

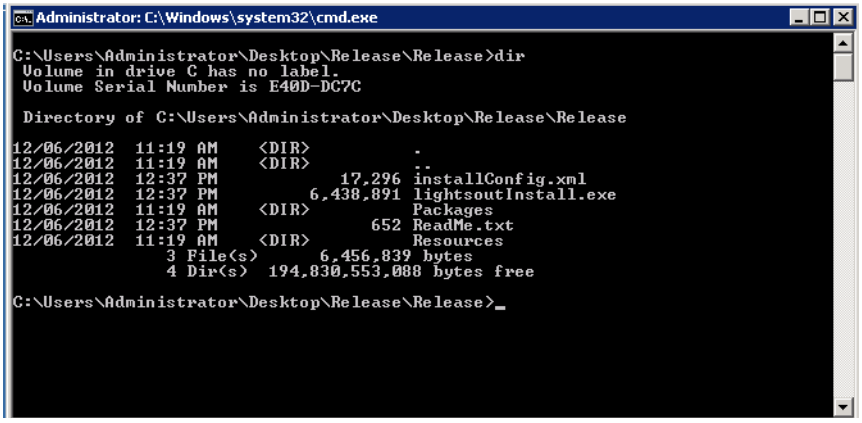
1. Log in to the Telescope server machine as administrator.
2. Right-click over the Command Prompt option and choose "Run as administrator," as shown in the following image:

Figure 4.1 *Run as Administrator*



3 Enter the path to lightsoutInstall.exe, or change to the directory that contains lightsoutInstall.exe.

Figure 4.2 *lightsoutInstall*



4 Run the lightsoutInstall command with appropriate options. For example:

```
lightsoutInstall -l <LicenseKeysfile> [OPTIONS] [> [LOG FILE PATH]]
```

For a complete list of options, see Section 4.2, "LightsoutInstall Options," on page 41.

NOTE: If you get a warning that a file does not exist, just press OK to continue the installation.

4.1.3 Ensure the Correct Java Version is Being Used

For version 9.3, you must follow the steps in this section to ensure Java 8 is going to be used by Telescope. Follow these steps after you have installed all components on all servers in the previous section.

1 Verify that Java 1.8 is installed and run all Telescope 9.3 applications. In particular, ensure:

- WebObjects is re-installed pointing to Java 1.8. (From Server Manager, go to Services, select Apple WebObjects Taskd, and choose Properties from the right-click menu. Ensure you see `jre1.8.0_40` in the path to executable.)
- Jetty-Service no longer appears in the list of Services. Instead, you should see NPS Jetty-Service.
- NPS Brokers and web applications will be running under Java 1.8. (From Resource Monitor, select a Telescope executable such as cdx.exe. Ensure you see `jdk1.8.0_40` in the Handle name.)

2 Manually stop all NPS services (as applicable to your installation), in the following order. You must stop all NPS brokers on all computers. (The following list represents all brokers; if they are not installed, they won't appear.)

   a NPS Interoperability Broker

   b NPS Zoom Builder

   c NPS Zoom Broker

   d NPS Distribution Broker

   e NPS Ingest Broker

   f NPS Graphics Broker

   g NPS Lookup Broker

   h NPS Child Indexing Broker

   i NPS Indexing Broker

   j NPS Jetty-Service

   k NPS Message Broker

   l NPS NTFS File Broker

   m NPS Authentication Broker

   n NPS Connection Broker

   o NPS State Broker

   p NPS Session Broker

   q NPS Name Server

3 Stop the Apple Webobjects Taskd Service on the web application machine.

4 Back up the following files on your hub and web application server machines

```
C:\Program Files (x86)\Java\jdk1.8.0_40\jre\lib\security\local_policy.jar
C:\Program Files (x86)\Java\jdk1.8.0_40\jre\lib\security\US_export_policy.jar
C:\Program Files (x86)\Java\jre1.8.0_40\lib\security\local_policy.jar
C:\Program Files (x86)\Java\jre1.8.0_40\lib\security\US_export_policy.jar
```

5 After your backups are complete, replace the above files with the files with the same names found in the 9.3 release package:

```
\Release\Resources
```

Next Step:

1 Install the Telescope database. See Section Chapter 5:, "Install Telescope Database Server," on page 43

4.2 LightsoutInstall Options

Highlights

- All of the following options are optional.
- To see all options for this command, use the -h option (or --help): `lightsoutInstall.exe -h`
- To display the release version, use the -a parameter.
- The -l option is recommended for hub server installations so you will not need to add licenses manually later. (The -l option is applicable for the Hub server, not the Web or Web App servers.)
- The default Telescope installation location is `C:\Telescope`. To change the installation location (drive and/or directory), use the -i command-line option.
- When upgrading an existing installation of Telescope, use -b to back up the configuration files. Then use -r to restore the backed up configuration files.

All Options

Table 4.1 *lightsoutinstall options*

Option and usage	Description
-h, --help	Shows the latest list of options, then exits. Use this option to list all options, and verify their syntax.
-f CONF, --configfile CONF	Lets you specify an alternative configuration file. (The default is installConfig.xml.)
-m MASTER_KEY, --master_key MASTER_KEY	Lets you define the master key (and over-rides values defined in the installConfig.xml or in the -l option below). Use this option to install with a new master key, while using a pre-configured installConfig.xml file. (This option is overriden by the -l option, if both are present.)
-l LICENSE_FILE, --license_file LICENSE_FILE	Lets you define the path to the license file (and over-ride any values defined in the installConfig.xml). The full path is required. **Recommended option** to avoid the need to license individual components later. (The -l option is applicable to the Hub server only, not the Web server or Web Application server.) (This option overrides the -m option, if both are present.)
-u, --uninstall	Forces the uninstall of all TeleScope components.
-v, --verbose	Increases the amount of information outputted from this program.
-i INSTALLDIR, --install_location INSTALLDIR	Lets you specify an alternative install location [The default is C:\TeleScope]. Spaces in the path are not supported. With the –i option, Telescope also installs third party applications to specified drives, except for Adobe products such as DNG Converter or InDesign, which are always installed on the C drive.

Table 4.1 *lightsoutinstall options*

Option and usage	Description
-d INSTALLDRIVE	Lets you specify an alternative install drive [default: C]. The ":" is optional). The default install directory remains "Telescope", but is placed on a different drive. This option over-rides any drive specified in -i.
-a, --about	Display details about this product release, then exits. **Recommended option** to confirm you are going to install the correct release.
-b BACKUPZIP, --backup BACKUPZIP	Specify backup zip file [default: ./Utilities/backupData.zip]. Spaces in the path are not supported.
-r RESTOREZIP, --restore RESTOREZIP	Specify restore zip file [default: ./Utilities/restoreData.zip]. Spaces in the path are not supported.

Examples:

NOTE: These examples, and the example above, show the -l licensing option, and are intended to be run on the hub server. The web or web application servers do not require the licensing option.

```
C:\Users\Administrator\Release\Release> lightsoutInstall.exe
-l C:\Users\Administrator\Release\Release\LicenseKeys.txt
```

- In this example, the release was unzipped into a "Release" directory, and the user has navigated to where the lightsoutInstall.exe file is located. The license key file was copied to this same location. Telescope will be installed into the default location (`C:\Telescope`).

```
C:\Users\Administrator>
C:\Users\Administrator\Desktop\Release\Release\lightsoutInstall.exe
-l C:\Users\Administrator\Licenses\TelescopeLicenseKeys.txt -i E:\apps\telescope >
install_log.txt
```

- In this example, Telescope is installed from a path in the C: drive to a particular path in the E: drive (`E:\apps`).The license keys file, `TelescopeLicenseKeys.txt`, is located at `C:\Users\Administrator\Licenses`. Log output will be redirected to a file, `install_log.txt` and placed in the current directory, `C:\Users\Administrator`.

Chapter 5: Install Telescope Database Server

Prerequisites:

Make sure you have completed these sections:

- Section 2.1, "Set an ODBC Connection for the Telescope Database," on page 18
- Section 4.1, "Run the lightsoutInstall.exe Installer," on page 38

In this Chapter:

- Section 5.1, "Create a Microsoft SQL Database," on page 44
- Section 5.2, "Create an Oracle Database," on page 50
- Section 5.3, "Mirroring the Database (Optional)," on page 56

5.1 Create a Microsoft SQL Database

NOTE: Complete these steps after you have installed Telescope in Section Chapter 4:, "Install Telescope," on page 37

Use the database manager application, DBManager, to create a Microsoft SQL database to serve as the Telescope database server:

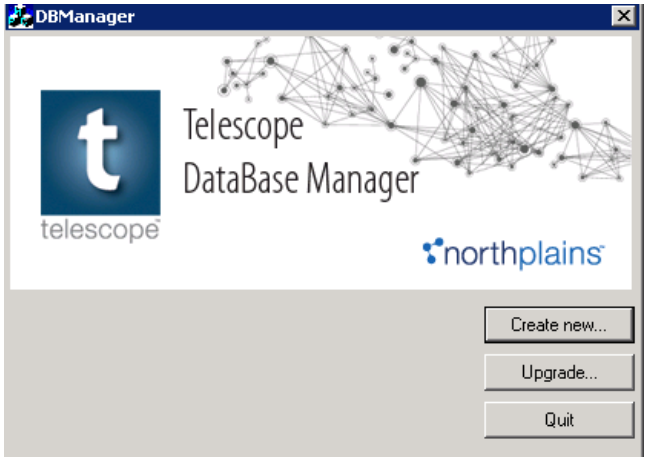
1. Go to the Registry Editor (`regedit` from a command line) and delete the following key (if it exists)
   `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\North Plains Systems\Telescope\Installer\DBManager`

   (This will ensure that the database updates occur from the beginning of the 9.4.0 release, ensuring that all database changes for the latest release are properly applied.)

2. On the hub server, start the Telescope Database Manager:

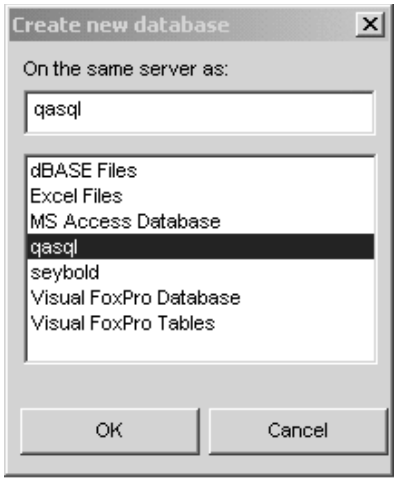
   Double-click the DBManager.exe file in the DBManager directory in the Telescope installation directory (typically, `C:/TeleScope/DBManager/DBManager.exe`).

Figure 5.1 *DB Manager*



3. Click *Create New.*

Figure 5.2 *Create New Database*



4 Select the data source you configured for the target database server in Section 2.1, "Set an ODBC Connection for the Telescope Database," on page 18.

5 Click *OK*.

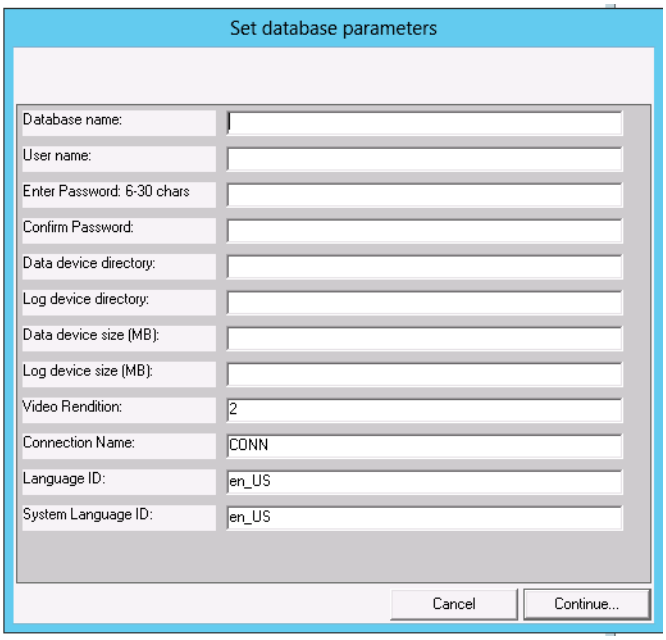
6 You may be prompted to enter database credentials. In this case, enter the database account user name and password, then click *OK*.

NOTE: Please refer to the SQL Server documentation for password requirements.

---

7 Complete the *Create New Database* dialog as follows. **Be sure to record this information**; you will need it later.

Figure 5.3 *Create New Database*



Field	**Comment**	**Example**	**Your Site: (Write it down here to remember it later)**
Database name	Name of database being created. It must be unique to this installation of SQL Server. No spaces are allowed.	database_name	
User name	Must be unique for this installation of SQL Server as DBManager sets the required Database access permissions on creation.	database_admin	
Password	A password of at least six characters with alphanumeric characters and mixed case letters is recommended. Refer to the SQL Server documentation for detailed password requirements.	AStrongPassword12!	
Confirm Password	This field must match the Password.	AStrongPassword12!	

Field	Comment	Example	Your Site: (Write it down here to remember it later)

Data device directory	The full path where the data files for the table spaces are created. It must end with a backslash (\).
	The path is relative to the machine where the database is installed, and must already exist. (Ask your system administrator if you are not familiar with this path.)
		For SQL Server 2008 R2:
		`c:\Program Files\Microsoft SQL Server\ MSSQL10_50.MSSQLSERVER\MSSQL\data\`
		For SQL Server 2012:
		`C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\ MSSQL\DATA\`	

Log device directory	The full path where SQL Server logs are stored on the database server. It must end with a backslash (\).
	The path is relative to the machine where the database is installed, and must already exist. (Ask your system administrator if you are not familiar with this path.)
		For SQL Server 2008 R2:
		`c:\Program Files\Microsoft SQL Server\ MSSQL10_50.MSSQLSERVER\MSSQL\log\`
		For SQL Server 2012:
		`C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\ MSSQL\Log\`	

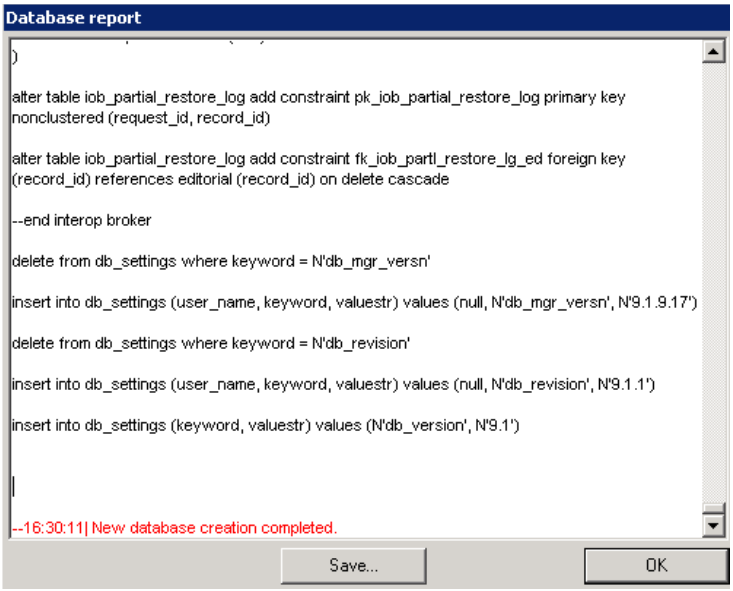
Data device size	The approximate size of the database. The default is 50 megabytes.	50	
Log device size	The approximate size of the log file. It should be sized as 20% of the data device size. The default is 10 megabytes.	10	
Video Rendition	The rendition number assigned to the QuickTime version of your video files. If you do not know which rendition is used, leave the default value (2). This value can be changed in the database.	2	
Connection Name	The connection name for this database; the name you chose as the `TS_CONNECTION` value in the InstallConfig file.	`TelescopeDAM`	

Field	Comment	Example	Your Site: (Write it down here to remember it later)
Language ID	The default system language, presented to users of that system. Default is U.S. English (en_US) The language specified must exist in the file DBManager\files\extras\mssql\langlocale	en_US * It is strongly recommended you leave this default.	
System Language ID	The list of languages handled by the system (that is, the number of different languages supported for asset metadata and other descriptive information). For multiple languages, separate them by commas. Default is U.S. English (en_US). All languages specified must exist in the file DBManager\files\extras\mssql\langlocale	en_US * It is strongly recommended you leave this default.	

8 Click *Continue*.

9 The Database Report dialog is displayed. Error messages may appear in the report indicating that indexes have been dropped. This is normal and does not impact the database creation.

Figure 5.4 *Database Report*



10 When the database is created (or when a major error is encountered), it is recommended to save the database report by clicking the *Save* button. This information may be required later for debugging.

11 Click *OK* to close the report. The database created will have a default Telescope administrator account created with the user name *admin* with no password. The *create new database SQL* script is stored in plain text format at the file system level, under `<DBManagerRoot>\FILES\new\mssql\8.0.sql`.

5.2 Create an Oracle Database

NOTE: Complete these steps after you have installed Telescope in Section Chapter 4:, "Install Telescope," on page 37

5.2.1 Notes on Using Oracle Databases with Telescope

- A 32-bit Oracle client (not 64-bit) must be installed on the machine where DBManager is installed, and on any machine running the Telescope Graphics Broker.
- The character set of the Oracle database server must be fully UTF8, including the one for NCHAR.

  To verify this:

  a Issue the following SQL command: `SELECT * FROM NLS_DATABASE_PARAMETERS;`

  b Verify you see:

  - `NLS_CHARACTERSET AL32UTF8`
  - `NLS_NCHAR_CHARACTERSET UTF8`
- Telescope requires the following Oracle components:
  - Oracle Java Client
  - SQL*Plus
  - Oracle JDBC/THIN Interfaces
  - Oracle Call Interface (OCI)
  - Oracle Programmer
  - Oracle Net
  - Oracle Connection Manager
  - Oracle ODBC Driver
  - Oracle SQL Developer (optional)

5.2.2 Create an Oracle Database

Use the Database Manager (DBManager) application to create an Oracle database to serve as the Telescope database server:

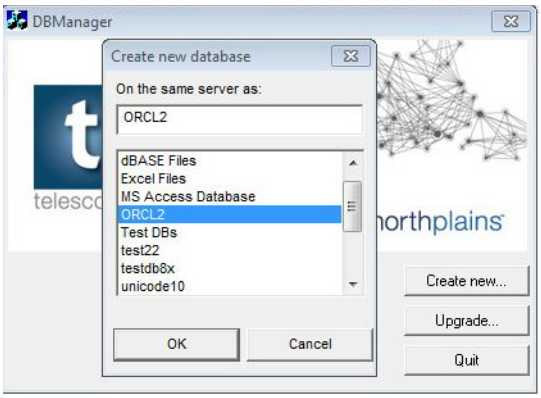
1 On the hub server, start the Telescope Database Manager:

Double-click the DBManager.exe file in the DBManager directory in the Telescope installation directory (typically, `C:/TeleScope/DBManager/DBManager.exe`).

Figure 5.5 *DB Manager*

2 Click *Create New.*

Figure 5.6 *Create New Database*



3 Select the data source you configured for the target database server in Section 2.1, "Set an ODBC Connection for the Telescope Database," on page 18.

4 Click *OK*.

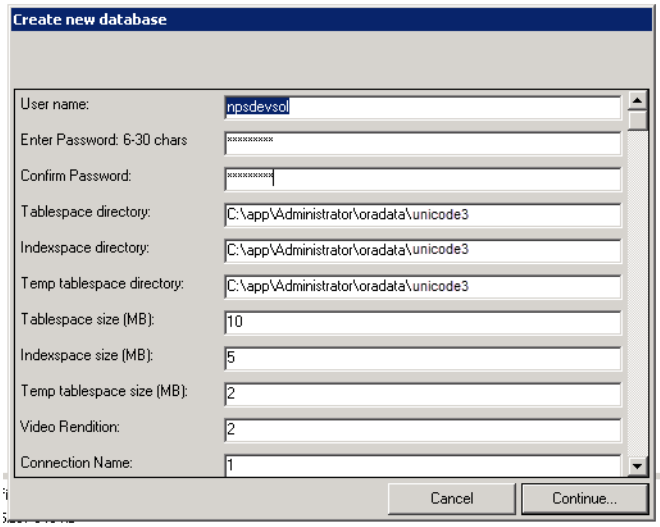
5 You may be prompted to enter your credentials. In this case, enter the database account user name and password, then click *OK*.

NOTE: Please refer to the Oracle documentation for password requirements.

Figure 5.7 *Oracle Driver Connect*

6 Complete the *Create New Database* dialog as follows:

Figure 5.8 *Create New Database*



Field	**Comment**	**Example**	**Your Site:** **(Write it down here)**
User name	Must be unique for this installation of Oracle. The user (schema) is used to qualify table names. For example: ts.mytable.	database_admin	
Enter Password	It is recommended to create a password with alphanumeric characters and mixed case letters for added security. Refer to the Oracle documentation for detailed password requirements.	AStrongPassword12!	

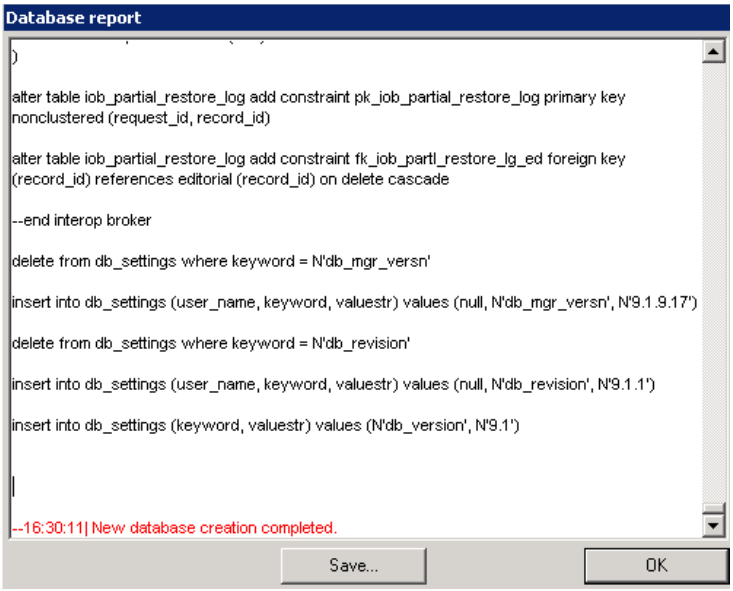
Field	Comment	Example	Your Site: (Write it down here)
Confirm Password	This field must match the Password.	AStrongPassword12!	
Tablespace directory	The full path to the location where datafiles are created for the schema. It must end with a backslash (\).	\opt\oracle\oradata\	
Indexspace directory	The full path to the location where index files are created for the schema. It must end with a backslash (\).	\opt\oracle\oradata\	
Temp tablespace directory	The full path where the temporary data file is stored. It must end with a backslash (\).	\opt\oracle\oradata\	
Tablespace size	The approximate size of the database. The default is 50 megabytes.	50	
Indexspace size	The approximate size of the indexspace (sized as 20% of the data device size). The default is 10 megabytes.	10	
Temp tablespace size	The approximate size of the temporary tablespace (sized as 20% of the data device size). The default is 10 megabytes.	10	
Video Rendition	The rendition number assigned to the QuickTime version of your video files. If you do not know which rendition is used. leave the default value. This value can be changed in the database.	2	
Connection Name	The connection name for this database; the name you chose as the `TS_CONNECTION` value in the InstallConfig file.	TelescopeDAM	

Field	Comment	Example	Your Site: (Write it down here)
Language ID	The default system language, presented to users of that system. Default is U.S. English (en_US) The language specified must exist in the file DBManager\files\extras\mssql\lan glocale	en_US * It is recommended you leave this default. See note below.	
System Language ID	The list of languages handled by the system (that is, the number of different languages supported for asset metadata and other descriptive information). For multiple languages, separate them by commas. Default is U.S. English (en_US). All languages specified must exist in the file DBManager\files\extras\mssql\lan glocale	en_US * It is recommended you leave this default. See note below.	

7 Click *Continue* then click *OK*.

8 The Database Report dialog is displayed. Error messages may appear in the report indicating that indexes have been dropped. This is normal and does not impact the database creation.

Figure 5.9 *Database Report*



9 When the database is created (or when a major error is encountered), it is recommended to save the database report by clicking the *Save* button. This information may be required later for debugging.

10 Click *OK* to close the report. The database created will have a default Telescope administrator account created with the user name *admin* with no password.

5.3 Mirroring the Database (Optional)

NOTE: This section is optional, for those wishing to mirror the Telescope database server across multiple sites.

5.3.1 Prepare the Environment for Mirroring

1. Make sure the SQL Server services are running under the same account on the principal and mirror database.
2. Enable the TCP/IP protocol in the SQL Server Network Configuration.

5.3.2 Prepare the Principal and Mirror Database for Mirroring (Backup and Restore)

1. Change the principal database to use the FULL recovery model.

```
USE master
Click GO
ALTER DATABASE telescope
SET RECOVERY FULL;
Click GO
```

2. Create a full backup of the principal database.

```
BACKUP DATABASE telescope
TO DISK = 'C:\telescope.bak'
WITH FORMAT
```

3. Click GO
4. Copy the full backup to the mirror server.
5. On the mirror server, restore the whole database with the NORECOVERY option.

```
RESTORE DATABASE telescope
FROM DISK = 'C:\telescope.bak'
WITH NORECOVERY
```

6. Click GO
7. If the path to the mirror database differs from the path to the principal database (for instance, their drive letters differ), creating the mirror database requires that the restore operation includes a MOVE clause.

```
restore database telescope
from disk='C:\telesope.bak'
with NORECOVERY,
MOVE 'telescope_DAT' TO
'C:\Program Files\Microsoft SQL
Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA\telescope_Data.mdf',
MOVE 'ftrow_telescope_CAT' TO
'C:\Program Files\Microsoft SQL
Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA\telescope_Data.ndf',
MOVE 'telescope_Log' TO
```

```
'C:\Program Files\Microsoft SQL
Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA\telescope_Log.ldf';
```

8 Backup logs from the Principal database.

```
BACKUP LOG telescope
TO DISK = 'C:\telescope_log.bak'
```

9 Click GO

10 Copy the log backup file to the mirror server and restore the logs.

```
RESTORE LOG telescope
    FROM DISK = 'C:\telescope_log.bak'
    WITH FILE=1, NORECOVERY
```

11 Click *GO*

12 If any additional log backups occur before you start mirroring, you must also restore all of those log backups, in sequence, to the mirror server using WITH NORECOVERY.

```
RESTORE LOG telescope
FROM DISK = 'C:\telescope_log.bak'
WITH FILE=2, NORECOVERY
Click GO

RESTORE LOG telescope
FROM DISK = 'C:\telescope_log.bak'
WITH FILE=3, NORECOVERY
Click GO
```

13 Connect to the principal server instance, in Object Explorer, click the server name to expand the server tree.

14 Expand *Databases*, and select the database to be mirrored.

15 Right-click the database, select *Tasks*, and then click *Mirror*.

16 To begin configuring the mirroring, click the *Configure Security* button to launch the *Configure Database Mirroring Security Wizard*.

   a Configure the security wizard without using the *witness server* option.

   b Specify the service accounts used to run the SQL Server services during configuration.

17 Once Security is configured, start the *Database Mirroring* process.

Once the mirroring process is complete the principal database shows up as *Principal, Synchronized* and the Mirror database shows up as *Mirror, Synchronized/Restoring*.)

NOTE: The Mirror database stays in the restoring state until a failover happens, then it becomes the primary database.

Chapter 6: Configure Telescope over the Web

This chapter provides information on how to configure the Telescope web server and web application server after installation. Please follow these sections in the order they are shown.

Prerequisites:

Make sure you have completed these sections before proceeding:

- Section Chapter 4:, "Install Telescope," on page 37
- Section Chapter 5:, "Install Telescope Database Server," on page 43

In this Chapter:

- Section 6.1, "Configure for Launching the WebObjects Monitor," on page 60
- Section 6.2, "Define an Encryption Passphrase," on page 72
- Section 6.3, "Next Steps," on page 75

6.1 Configure for Launching the WebObjects Monitor

After the Telescope components are installed, you must configure various settings in Internet Information Services (IIS) on the web server in order to access the WebObjects Monitor, which is the Telescope interface you use to access Telescope applications. If you are using multiple web servers, follow these steps on every web server machine.

6.1.1 Include WebObjects in ISAPI and CGI restrictions

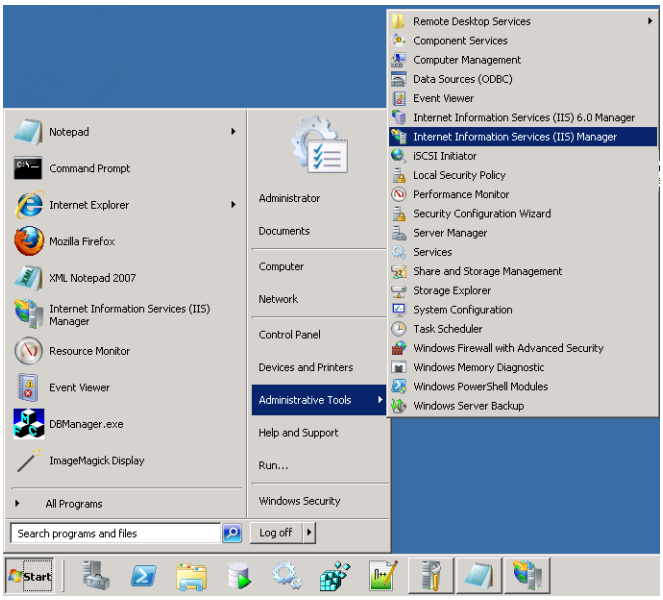
NOTE: These steps assume the default web site location, with the Scripts path `\inetpubs\scripts`. If your path is different, you will need to use it in the steps below. Check with your system administrator to verify your web site location.

To configure ISAPI and CGI restrictions for Telescope in Internet Information Services (IIS):

1. On the Web server, click *Start* > *Administration Tools* > *Internet Information Services (IIS) Manager.*

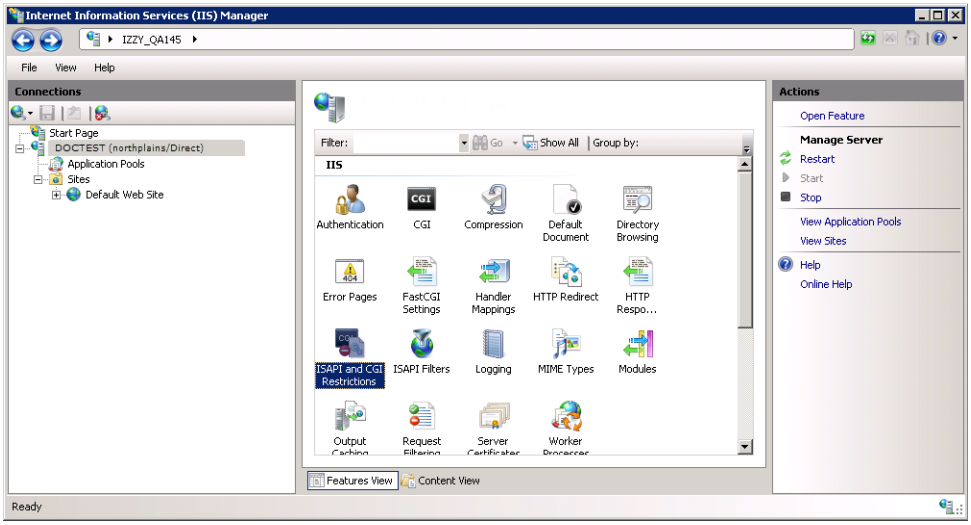
NOTE: Choose *Internet Information Services (IIS) Manager,* **not** *Internet Information Services (IIS) 6.0 Manager.* If you do not see this choice, consult documentation for your operating system to install it.

Figure 6.1 *Access IIS Manager*



2. In the Connections pane of the IIS Manager, select the host name for the IIS Server host.
3. In the main pane, double-click the "*ISAPI and CGI Restrictions"* icon.

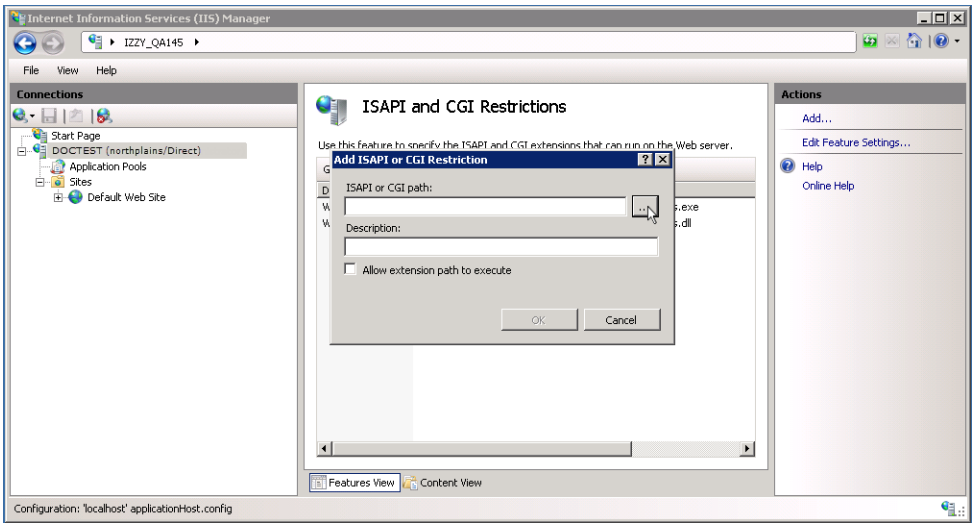
Figure 6.2 *ISAPI and CGI Restrictions*



4 In the Actions pane, click the *Add* link.

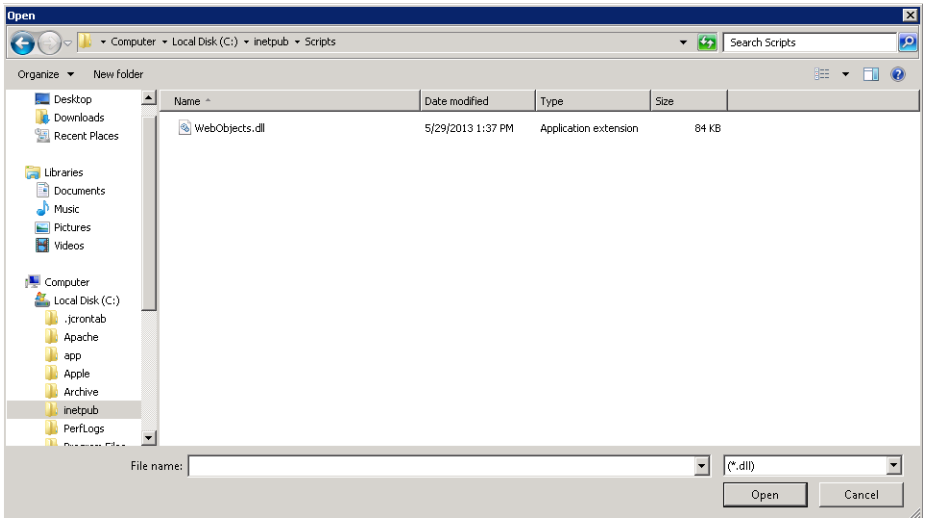
5 Click the *Browse* (...) button beside the ISAPI or CGI Path field.

Figure 6.3 *ISAPI and CGI Restrictions*



6 Navigate to and select the *inetpub\Scripts\WebObjects.dll* file. (The inetpub folder is typically at the C drive level.)

Figure 6.4 *Select WebObjects.dll file*



(If you can't see the DLL file, look at the pulldown next to the file name field to make sure you are viewing DLL files.)

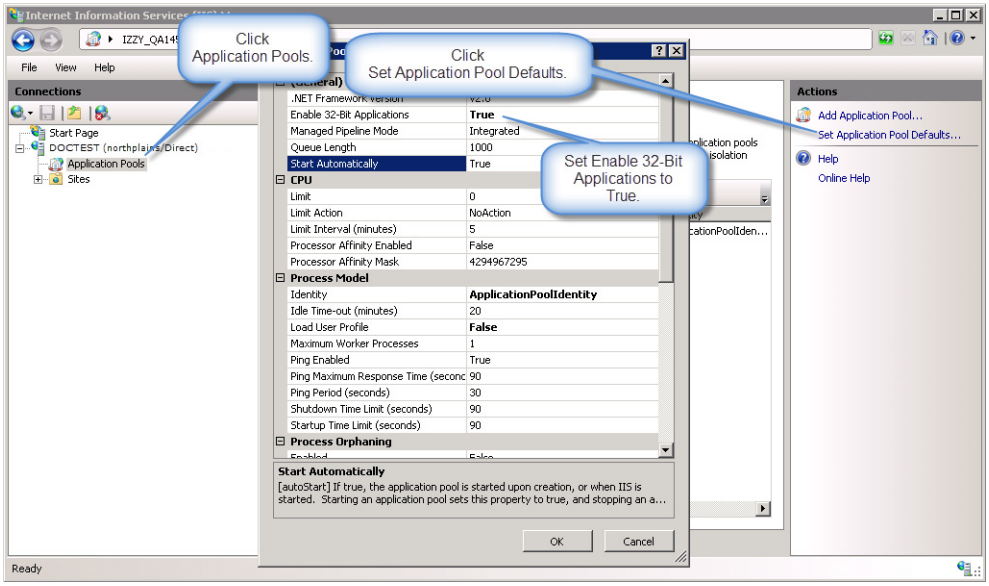
7. Click *Open*.
8. Enter a description for this file, for example "WebObjects.dll".
9. Select the *Allow extension path to execute* option and click *OK*.
10. Repeat steps 4 to 9 above to add the `inetpubs\scripts\WebObjects.exe` file. (Be sure to change the pulldown next to the file name field to make sure you are seeing EXE files.) Use the description, "WebObjects.exe".

6.1.2 Configure IIS Application Pools for 32-Bit

To configure the IIS 7 application pools for Telescope's 32-bit application requirement:

1. On the Web server, click *Start > Administration Tools > Internet Information Services (IIS) Manager.*
2. Click and expand the host name for the IIS Server host (in the Connections pane at the left).
3. In the Connections pane (to the left), select the *Application Pools* item.
4. In the Actions pane (to the right), click the *Set Application Pool Defaults* link.
5. Under General set the *Enable 32-Bit Applications* option to *True*.

Figure 6.5 *Set 32-bit Applications as Application Pool Default*



6 Click *OK*.

6.1.3 Create a Scripts Virtual Directory

The Scripts virtual directory is typically created during Telescope installation. If it does not exist, follow these steps.

1 On the web server, click *Start* > *Administration Tools*> *Internet Information Services (IIS) Manager*.

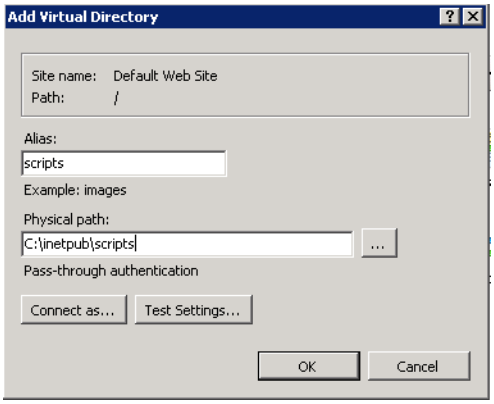
2 In Internet Information Services (IIS) Manager, in the Connections pane expand the Sites node, then expand the default web site node (or the web site where Telescope is to be installed; check with your system administrator).

3 Right-click *Default Web Site* and select *Add Virtual Directory*.

4 In the Add Virtual Directory dialog, in the Alias field, enter “Scripts”.

5 In the Physical path field, enter the location of the Scripts directory as defined in the `installConfig.xml` file. By default, the path is `C:\inetpub\Scripts`

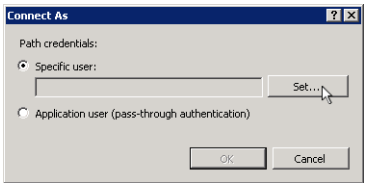
Figure 6.6 *Add Virtual Directory*



6 Click *Connect as*.

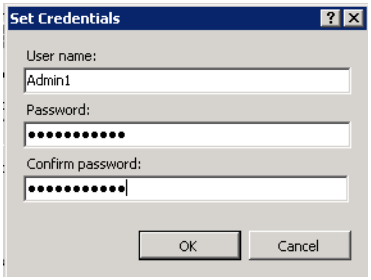
7 In the Connect As dialog, select “Specific user” then click *Set*.

Figure 6.7 *Connect As*



8 In the Set Credentials dialog, enter the valid user name and password you use to access the server machine.

Figure 6.8 *Set Credentials*



9 Click *OK* then click *Test Settings*. Verify that authentication passes for both the user name and the path.

10 Click *OK*.

6.1.4 Configure Handler Mappings for the IIS Folders

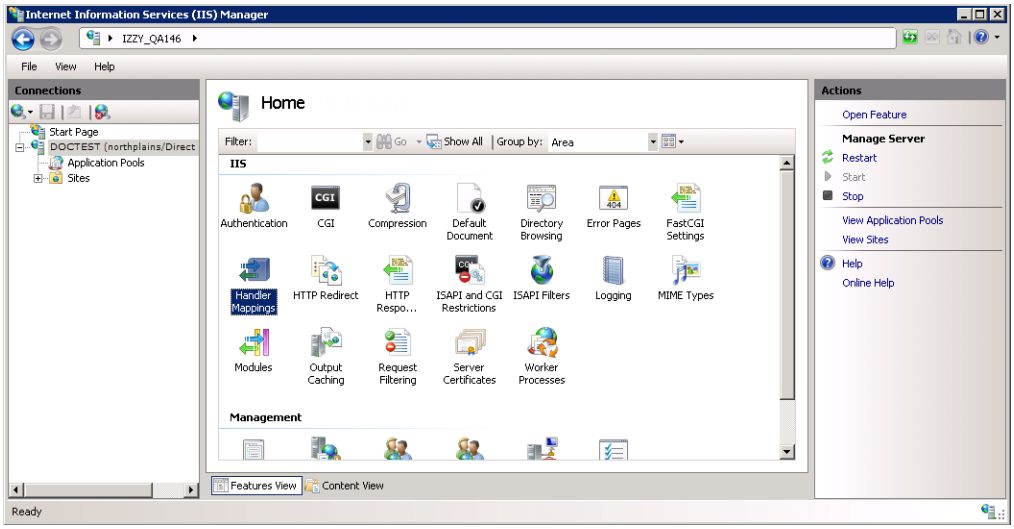
Confirm the Internet Information Services IIS 7 is configured as follows:

1 On the Web server, click *Start* > *Administration Tools* > *Internet Information Services (IIS) Manager*.

2 In Internet Information Services (IIS) Manager, click the machine name.

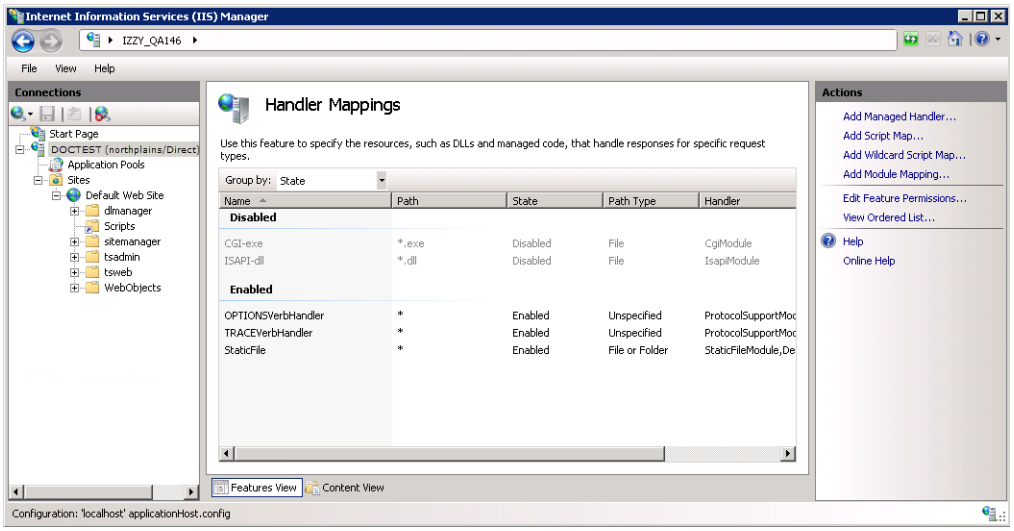
3 In the main pane, double-click the *Handler Mappings* option.

Figure 6.9 *Access Handler Mappings at machine level*



4 As shown in the following figure, ensure *CGI-exe and ISAPI-dll* **only** are disabled and all other handler mappings are enabled.

Figure 6.10 *CGI-exe Handler Mapping must be disabled at the machine level.*



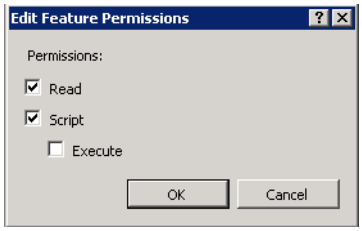
Note: If *CGI-exe* or *ISAPI-dll* are enabled, follow these steps to disable them:

a Select the *CGI-exe* entry a from the Handler Mappings pane

b Select *Edit Feature Permissions*.

c Deselect the *Execute* check mark (but leave the other check marks checked).

Figure 6.11 *Disable Handler Mappings.*



d Repeat for *ISAPI-dll* as required.

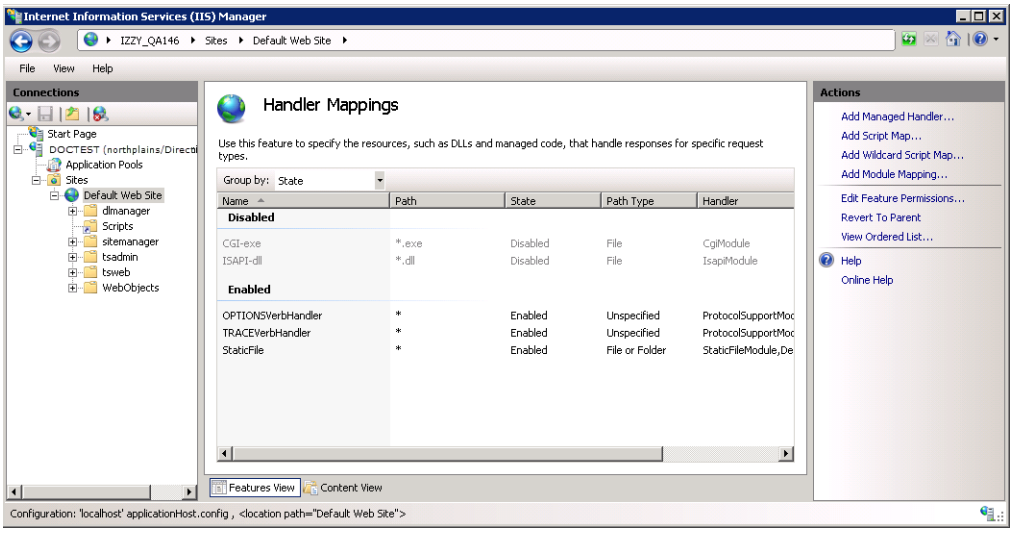
5 On the Connections pane, expand the *Sites* node and select the Default Web Site.

6 In the main pane, double-click the *Handler Mappings* option.

7 Ensure *CGI-exe* and *ISAP-dll* **only** are disabled for the Default Web Site, as in the following figure. (If they are enabled, disable them.)

Ensure that all other handler mappings are enabled, as shown in the figure.

Figure 6.12 *CGI-exe Handler Mapping must be disabled for the Default Web Site.*

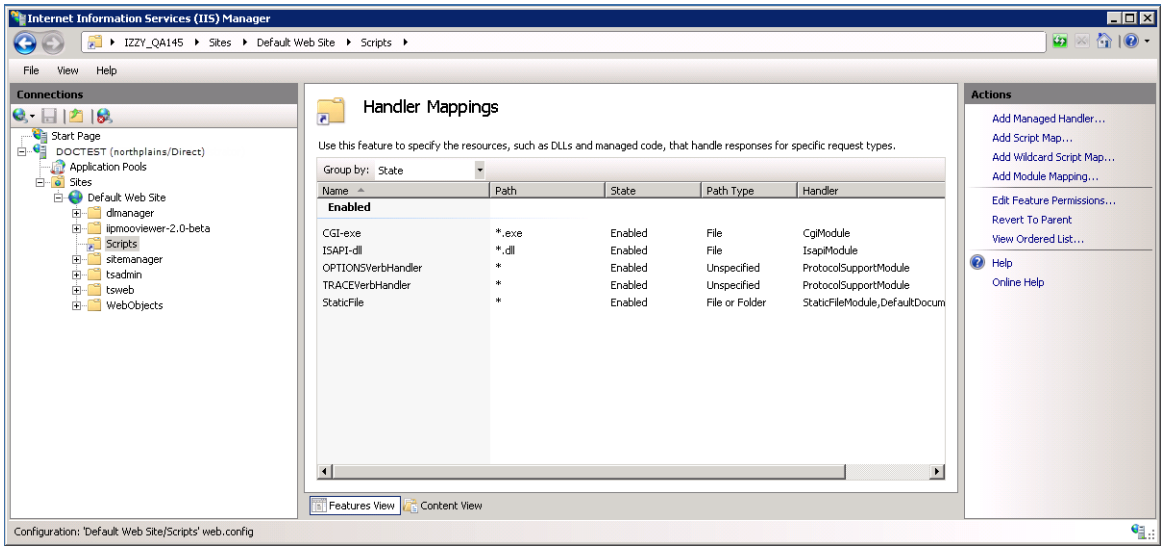


8 Expand the *Default Web Site* and click the *Scripts* folder.

9 In the main pane, double-click the *Handler Mappings* option.

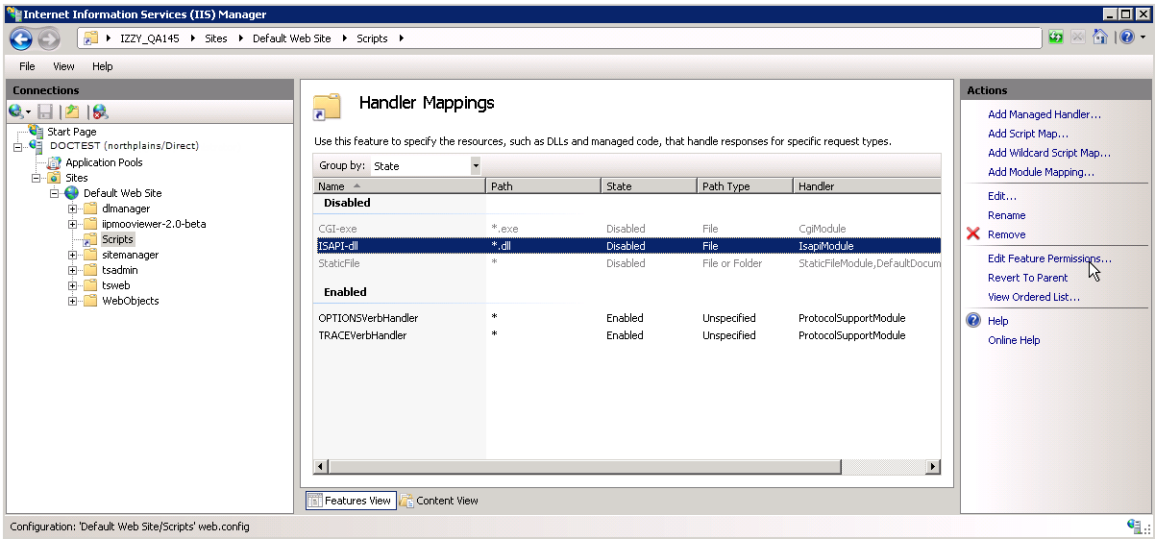
10 All Handler Mappings must be enabled for the Scripts folder, as in the following figure.

Figure 6.13 *Handler Mappings enabled for Scripts folder*



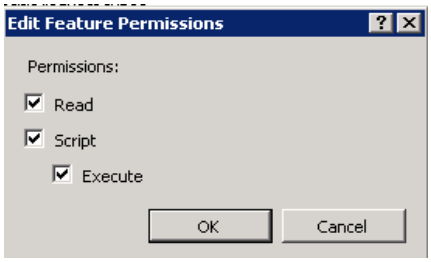
11 *If CGI-exe* and *ISAP-dll* are disabled for the Scripts folder, they will appear as in the following figure and will need to be enabled.

Figure 6.14 *Handler Mappings disabled for the Scripts folder*



To enable *CGI-exe* and ISAP-dll, select each of them in the Handler Mappings pane, click the *Edit Feature Permissions* link in the Actions pane. In the Edit Feature Permissions window, click the *Read, Script, and Execute* options, and click *OK*.

Figure 6.15 *Enable Handler Mappings*



Note: If you do not see cgi-exe in the Handler Mappings for the Scripts directory, perform these steps to add it:

a In IIS Manager, navigate to [Machine_Name] > Sites > Default Web Site > Scripts.

b Within the Scripts Home, double-click on *Handler Mappings*.

c In the Actions pane, click *Add Module Mapping*.

d In the Add Module Mapping window, specify the following details:

- Request path: `*.exe`
- Module (drop down): *CgiModule*
- Executable (optional): (Leave this field blank)
- Name: `CGI-exe`

e Click *OK*.

12 **The Handler Mappings should only be enabled for the Scripts directory.** Do a sanity check on other folders to ensure Execute is off in their Edit Features Permissions windows.

In particular, if the [Machine_Name] > Sites > Default Web Site > tsweb > default > BrowserPlugins folder is enabled, the Telescope Uploader will not initialize.

6.1.5 Enable Anonymous Authentication

1 On the Web server, click *Start* > *Administration Tools* > *Internet Information Services (IIS) Manager*.

2 In the *Connections* pane expand the Sites node, then click the Default Web Site node (or the web site dedicated to Telescope).

3 In the main pane, double-click *Authentication*.

4 In the Authentication pane, select *Anonymous Authentication*.

5 If it is disabled, go to the Actions pane, and click *Enable*.

6.1.6 Restart the World Wide Web Publishing Service

To ensure the previous settings take effect:

1 On the Web server, from the Windows *Start* menu, click *Administrative Tools* > *Services*.

2 Scroll to the bottom of the list and select *World Wide Web Publishing Service*.

3 Click *Restart* to restart the service.

6.1.7 Browser Considerations

Users can access Telescope from the supported browsers listed in the *Telescope—System Requirements* book.

Browsers must be configured with the following:

- If *Enhanced Security* is Enabled:

  Add all Telescope related internet sites to the trusted sites zone.

- Java Support:

  Make certain that *Java Support* is installed and enabled in the browser you are using. Otherwise, you may not see all user interface components. (The minimum version of Java is listed in the *Telescope—System Requirements* book.)

- Telescope Uploader plugin:

  The Telescope Uploader plugin must be installed on the client machine from a local or domain administrator's account for users to access the Telescope Uploader and full Download Cart functionality.

  See the *Telescope User's Guide* for details on how to install this plug-in for various browsers. See the *Telescope Administrator's Reference Guide* for details on how to configure this feature.

6.1.8 Firewall Configuration

You must configure the firewall on the web server to allow client browsers to connect to the server.

Configure Hub Services

The site configuration determines the ports used by the web application server and the Telescope hub and brokers.

The hub nameserver port, by default, is 12345. This port must be open on the hub server and accessible by all components of the Telescope installation. Each broker on the server listens to a port that must be accessible by the web application server. By default, these ports are not specified and cannot be known in advance. The brokers assign a port to themselves automatically.

To set the brokers to use specific ports, both the IIOP_PORT and IIOP_HOST registry keys must be configured for each broker. IIOP_HOST and IIOP_PORT are used to configure the system to use known addresses and ports which makes it possible to configure firewalls to allow communications between zones (LAN vs DMZ) or to simply allow connections into the server through the Windows Firewall. (For general information on registry keys, see Section 15.1, "Telescope Registry Keys," on page 201.)

If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address),

1. Ensure Internet Protocol Version 6 (TCP/IPv6) is disabled (not checked) in the properties for any of the active network connections (search for IPv6 in the Windows Control Panel).
2. Set the DisabledComponents to 0xff (255) in the following registry key:
   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters]
3. Restart the server.
4. Set the IIOP_HOST to the fully qualified name.
5. Restart the Brokers.

Configure Database Ports

The database port is dependent on which DBMS is in use. For more information see the documentation that came with your specific database.

Configure Web Server Ports

The following ports need to be accessible through your public firewall:

- 80 and/or 443
- If you do not configure reverse proxy, then the embedded HTTP port number needs to be accessible to the public firewall. For more information, see Section Chapter 11:, "Set Up Reverse Proxy for Downloads," on page 123

If you are using internal firewalls, the following ports must be accessible between the web server and web application server:

- Port 1085 is used by the web server to communicate to the WebObjects application server.
- Each instance of Telescope running on the WebObjects application server requires its own port. For example, TSAdmin could be configured to use port 2001, TSWeb to use port 2002, and so on.
- Two ports need to be configured for each DLManager application: a separate WebObjects application server port (for example, port 2003) as well as an embedded HTTP port number as described in Section 11.2.1, "Configure IIS to Route All Requests Through ARR," on page 125.

6.1.9 Test the WebObjects Monitor

At this point, you should be able to access the WebObjects interface from any browser as allowed by your organization's firewall:

1. Start the WebObjects Monitor.

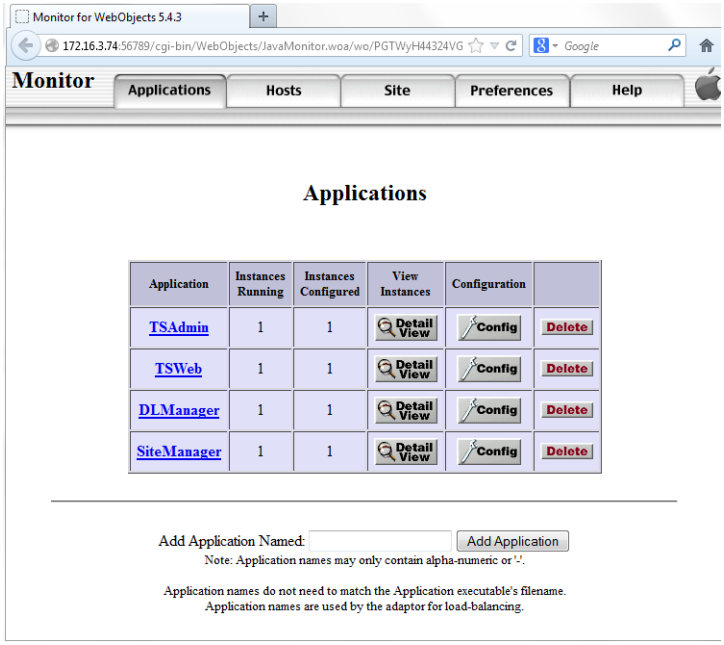
   To access this application by default, go to a web browser and type a URL consisting of the full computer name (or IP address) of the Telescope web application server, and append ":56789."

   For example:

   ```
   <your_web_app_server>:56789
   123.45.6.789:56789
   AcmeCorpTelescope:56789
   ```

   You should see the WebObjects Monitor window, which should appear like the following:

Figure 6.16 *WebObjects Monitor*



2 If you do not see the above window (including all of WebObjects Monitor applications: TSAdmin, TSWeb, DLManager, and SiteManager), review the steps listed in this chapter to ensure you have completed all configuration steps. Then go to the troubleshooting chapter, in particular Section 9.1, "Cannot Access Telescope on the Web," on page 114.

IMPORTANT! Be sure to add network passwords and use firewalls/proxies to protect the WebObjects Monitor. Only Administrators should be able to access it.

6.1.10 Next Steps

- If you cannot access the WebObjects Monitor shown above (and access all of its applications), you cannot proceed.
  - Review the steps listed in this chapter to ensure you have completed all configuration steps.
  - If you still have issues, go to Section 9.1, "Cannot Access Telescope on the Web," on page 114.
- If you did not use the -l option when you ran the Lights Out installation, you must now manually install all licenses for Telescope components. Go to Section 9.1, "Add License Keys," on page 123.
- If you did not include database configuration information in the `InstallConfig.xml` file before running the Lights Out installation, you must now manually configure the database. Go to *Telescope—Administrator's Reference Manual* to find out how.
- Otherwise, proceed to the next section.

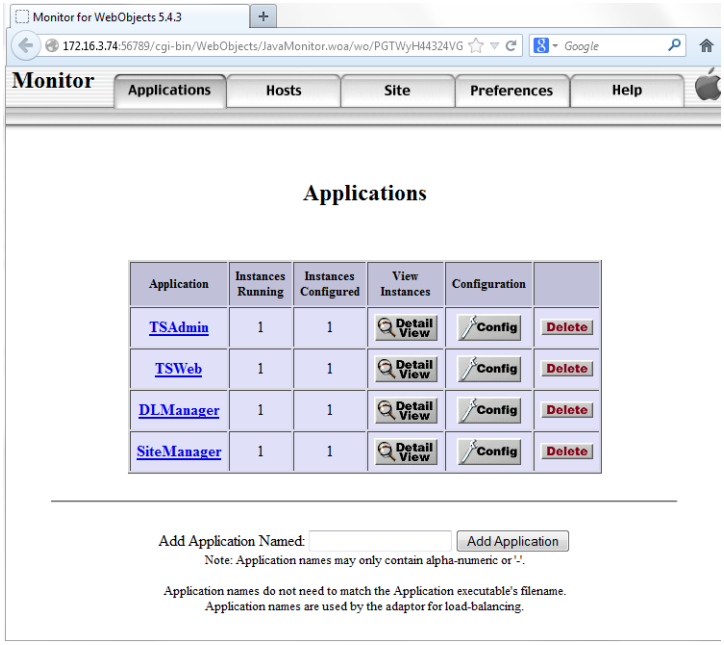
6.2 Define an Encryption Passphrase

Telescope brokers use AES-256 encryption when they provide usernames and passwords in connect requests to the Telescope database server. To enable this encryption, administrators are required to provide a unique encryption passphrase at the time of the Telescope installation or upgrade. This passphrase ensures unique encryption for your organization.

To define the encryption passphrase:

1 From the Telescope WebObjects Monitor, click *TSAdmin* to open the Telescope Administrator application.

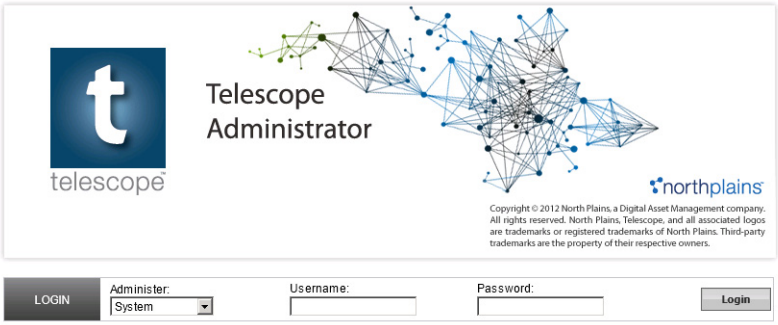
Figure 6.17 *Access TSAdmin from WebObjects Monitor*



NOTE: If you cannot access the WebObjects Monitor or the TSAdmin application, refer to Section 9.1, "Cannot Access Telescope on the Web," on page 114 in the Troubleshooting chapter.

2 A login screen appears.

Figure 6.18 *Telescope Administrator Login*



3 Select *System* from the *Administer* menu.

4 In the *Username* field enter "sysadmin".

5 In the *Password* field enter the password (if any).

NOTE: By default, the password for the sysadmin user is blank. To create a password for the sysadmin user, see the *Telescope Administrator's Guide*.

---

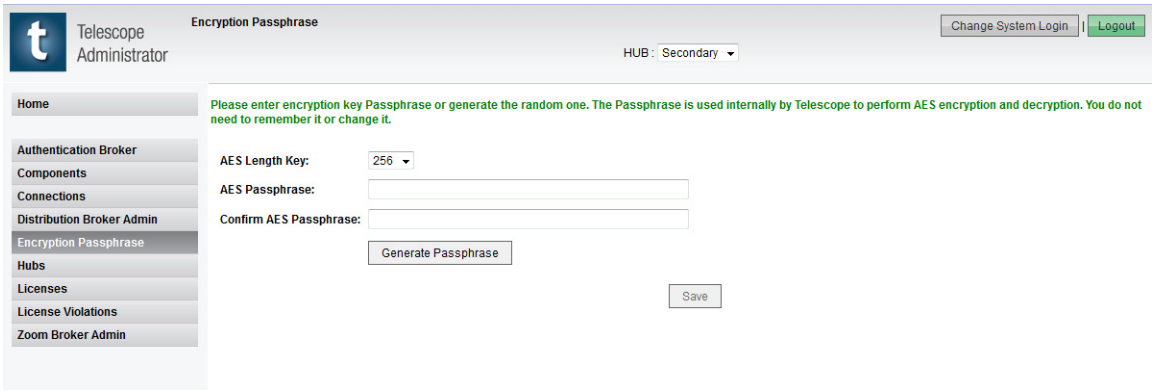
6 Click *Login*. The System Home Page appears.

NOTE: The System Home page displays information about active components and users and administrative tasks, including active users, installed hubs and databases, license pools, and so on. For more information about the administrative tasks you can perform from this interface, see the *Telescope Administrator's Guide*.

---

7 Click the *Encryption Passphrase* tab.

Figure 6.19 *Define an Encryption Passphrase*



8 Complete the following fields:

- **AES Length Key:** The block size (in bits) of the encryption key. The larger the block size, the more secure is the encryption key because of the greater number of combinations, key transformations, and rounds. Choose from 128, 192, or 256. (256 is recommended).

For AES key lengths greater than 128 bits: Key lengths of 192 and 256 require the JRE security library to be updated. This update is performed automatically on Telescope servers, but must be performed manually on the FlipFactory server. Either download the "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files" from the Oracle web site and install them on the FlipFactory server, or copy the following files from the Telescope server to the same JDK location on the FlipFactory server. For example, for Java 8:

```
C:\Program Files (x86)\Java\jdk1.8.0_40\jre\lib\security\local_policy.jar

C:\Program Files (x86)\Java\jdk1.8.0_40\jre\lib\security\US_export_policy.jar

C:\Program Files (x86)\Java\jre1.8.0_40\lib\security\local_policy.jar

C:\Program Files (x86)\Java\jre1.8.0_40\lib\security\US_export_policy.jar
```

- **AES Passphrase:** A unique alphanumeric string used in the encryption "tumbling" process to ensure unique encryption for your organization. Specify any value, and type it again in the *Confirm AES Passphrase* field. If you prefer to generate a random passphrase, click the *Generate Passphrase* button.

NOTE: The passphrase is used internally by Telescope to generate AES encryption. It is not needed to log in to any feature, so you do not need to remember it.

---

9 Click *Save*.

6.2.1 Change the Encryption Passphrase Later

It is possible to update the encryption passphrase from the command line of the hub server. For details, see the *Telescope Administrator's Guide*.

6.3 Next Steps

Use the following checklist to continue setting up your system so your users can access and search Telescope data. For more information on these items, unless otherwise specified, see the *Telescope Administrator's Guide*.

- Allow metadata fields to be visible to Telescope users. Log into TSAdmin as a database administrator and go to the *Fields* tab.
- Install and configure Solr Search. See Section 7.2, "Install Solr Search," on page 80.
- Set permissions for users and groups to access data (including to searches, renditions, fields, and so on). Log into TSAdmin as a database administrator and go to the *Users/Groups* tab.
- Ensure all I-Piece and C-Piece licenses are added to the license pool. Log into TSAdmin as a system administrator and go to the *Licenses* tab.
- Create file migration policies, then associate them to users or groups so that they will be able to import and export data. Log into TSAdmin as a database administrator and go to the *File Migration Policies* tab.

Chapter 7: Additional Configuration

This chapter provides additional configuration details for supplementary features and implementations.

In this Chapter:

- Section 7.1, "Install/Configure Telescope Brokers," on page 78
- Section 7.2, "Install Solr Search," on page 80
- Section 7.3, "Enable Telescope Video Support," on page 82
- Section 7.4, "Configure I-Pieces and C-Pieces," on page 86
- Section 7.8, "Customize your Sites," on page 95
- Section 7.6, "Install the Xinet File Broker," on page 89
- Section 7.7, "Install and Configure the Queue Broker," on page 93
- Section 7.8, "Customize your Sites," on page 95

Also:

Refer to the *Administrator's Reference Manual* for additional information on configuration. For example, you will find configuration information for:

- File migration policies
- Upload and download behavior
- Auto-ingestion (creating hot folders for automatic ingestion of files)
- Access for users and groups
- Functional rules or scripts that execute during particular actions
- Hot folder configuration
- And so on.

7.1 Install/Configure Telescope Brokers

7.1.1 Introduction to Telescope Brokers

Brokers Installed with the Hub

When you make a request of the Telescope system, the Hub co-ordinates the request. The Hub administers all of the activity of the Telescope system. Telescope Hub includes the following brokers:

- **Name Service** is a third party application by omniORB which provides name and reference lookup services in the Telescope system.
- **Session Broker** is part of the Telescope Hub server application. It provides real-time monitoring for all user actions and server component states, session information to Telescope administrators, control of server component deployment, control of Telescope user sessions, and control of I- Piece and Conversion I-Piece deployment. Users access the Session Broker through Telescope Administrator, where they add license keys and define settings such as heartbeat interval and idle time-out.
- **Connection Broker** is a centralized repository of database connection information and a "name service" for this connection information. The Connection Broker is also responsible for synchronization services at the record_id level for Telescope databases.
- **Authentication Broker** provides authentication and user management for Telescope. Authentication Broker provides database-based authentication and LDAP-based authentication, depending on the setting of the LDAP-Plug-in class and the existence of the "LDAP Server Address" entry in the Telescope database.
- **State Broker** synchronizes file access operations among multiple file brokers and provides global data storage.
- **File Conversion Broker** assists in the conversion of files from one type to another. (e.g., GIF to JPG) by storing the file conversion information of all file brokers on the system.

Separately Installed Brokers

Telescope allows for some components to be installed on multiple file servers to improve performance. The exact configuration will be unique to each implementation, but it is possible for the following brokers to be installed on a file server separate from the Telescope Hub server.

- **NTFS File Broker** manages the check out and check in functions, reports file locations to the database, and manages location links. It also manages the Conversion Broker and Conversion I-Pieces that convert files to other file types. It also supports the Xinet File Broker and/or the S3 File Broker, if either of these optional components are installed.
- **Graphics Broker** handles the generation of thumbnails and extended views for graphic files, and generates component object views (COVs) for some file types using the appropriate I-Pieces. Telescope supports multiple Graphics Brokers which allow you to deploy the Graphics Brokers together with the File Brokers to reduce network traffic. Multiple Graphics Brokers can also be deployed for load balancing.
- **Ingest Broker** is used to move files to the servers and to offload some of the processing required to generate thumbnails and extended views. The Ingest broker includes support for file migration policy, which provides the flexibility to move the files to the destination location during the ingestion process, along with the ability to configure file-name collision handling. Duplicate files are identified using MD5 signatures created from the file contents. The Ingest broker includes the Tree broker which performs tree searches.

- **Message Broker** is typically installed on the Telescope Hub machine. It handles sending, reading and responding to messages from the Telescope system. The Message Broker is also able to deliver Telescope notification messages to users by e-mail using a specified SMTP server when configured to do so.

See:

- Section 7.5, "Configure for Multiple File Brokers," on page 87

Optional (Separately Licensed) Brokers

The following brokers are available with additional licensing to extend Telescope environments:

- **Distribution Broker**—Automates and regulates file distribution, file duplication, and file conversion in Telescope. It runs invisibly in the background, fulfilling user requests automatically and without intervention. For example, it can be configured to run batch processing jobs overnight or identify assets ingested on a particular day and move them to a particular directory on the server. For more information, see the *Distribution Broker Manual*.
- **Integration Broker**—Provides a Web Services (SOAP) API into the Telescope application. Its UI Service makes it possible for external web-based applications to integrate with Telescope using a URL-based interface and a web browser on the client machine. For more information, see the *Integration Broker SDK Manual*.
- **Lookup Broker**—The Telescope Lookup Broker adds powerful functionality to Telescope, enabling users to search internal and external data sources and select values to populate metadata fields. For more information, see the *Lookup Broker Manual*.
- **Queue Broker**—The Queue Broker runs as a process that can resolve processes stored in specially created tables in the Telescope database. It is intended to improve the efficiency of the Telescope database, which can be set up to delegate nonessential tasks (such sending emails, making social media posts, running tests, and so on) to be run asynchronously. It is required to handle For Placement Only (FPO) images imported from the Xinet File Broker. For more information, contact Telescope Support.

  See: Section 7.7, "Install and Configure the Queue Broker," on page 93
- **Xinet File Broker**—manages data stored on a Xinet DAM system. Requires the NTFS File Broker, which manages data locally. For more information, contact Telescope Support.

  See: Section 7.6, "Install the Xinet File Broker," on page 89
- **S3 File Broker**—manages data stored on Amazon S3 (Simple Cloud Storage Service). Separately purchaseable. Requires the NTFS File Broker, which manages data locally. For more information, contact Telescope Support
- **Zoom Broker**—The Zoom Broker allows users to view large images at multiple levels of magnification. Users can zoom in, zoom out, and pan the image in all directions. For information, see the *Zoom Broker Manual*.

7.2 Install Solr Search

7.2.1 Install Solr on a Clean Machine (on the C: drive)

NOTE: We strongly recommend you install Solr on a clean machine that has no other applications running on it.

To install the Solr / Solr multicore on a separate machine on the C: drive:

1. From the Control Panel, check that there is an entry named "Java" to ensure that Java is installed in the machine.
2. If Java is not installed, then run the `jre-8u40-windows-i586.exe` executable, found in your 9.3 release package at `\Release\Resources`.
3. Run `Solr4.10.3.msi`, found in your 9.3 release package at `\Release\Resources`.

   When running `Solr4.10.3.msi`, ensure the path is `C:\TeleScope\Solr`
4. Run `SolrMulticore.msi`, found in your 9.3 release package at `\Release\Packages`.

   When running `SolrMulticore.msi`, ensure the path is `C:\TeleScope\Solr`
5. From Server Manager, in Services, start the NPS Indexing Broker and/or all NPS Child Indexing Brokers.

7.2.2 Install Solr on a Clean Machine on Drives other than C:

NOTE: We strongly recommend you install Solr on a clean machine that has no other applications running on it. However, you will also need to follow these instructions if you are installing Solr with the hub or other Telescope servers and those applications are not installed on the C: drive.

To install the Solr / Solr multicore on drives other than the C: drive (for example, E:), you need to install it and uninstall it to correct some hard-coded pathnames. For the following steps, assume the E: drive is being used:

1. From the Control Panel, check that there is an entry named "Java" to ensure that Java is installed in the machine.
2. If Java is not installed, then run the `jre-8u40-windows-i586.exe` executable, found in your 9.3 release package at `\Release\Resources`.
3. Run `Solr4.10.3.msi`, found in your 9.3 release package at `\Release\Resources`.

   When running `Solr4.10.3.msi`, ensure the path is `E:\TeleScope\Solr`
4. Run `SolrMulticore.msi`, found in your 9.3 release package at `\Release\Packages`.

   When running `SolrMulticore.msi`, ensure the path is `E:\TeleScope\Solr`
5. From Server Manager in Services, ensure the NPS-Jetty Service is stopped.
6. Go to `E:\TeleScope\Solr\yajsw\bat\` and run `uninstallService.bat`
7. Go to `E:\TeleScope\Solr\yajsw\conf` and open `wrapper.conf` in a text editor such as Notepad.
8. Change "C:" to the correct path (in this example, "E:") in the following two lines:

   ```
   [ wrapper.working.dir=E:/TeleScope/Solr/solr-4.10.3/telescope
   ```

```
wrapper.java.command=E:/TeleScope/Solr/solr-4.10.3/jre1.8.0_40/bin/java ]
```

9. Go to `E:/TeleScope/Solr/yajsw/bat` and run `installService.bat`.
10. From Server Manager, in Services, start the NPS Indexing Broker and/or all NPS Child Indexing Brokers.

7.2.3 Next Steps

As detailed in the *Telescope Administrator's Guide*, you need to take a variety of steps to configure the Solr search engine. For example, you need to:

- Go to `\Telescope\Applications\`**`tsweb`**`\Contents\info.plist` and change the `<search_mode>` key to `SOLR`.
- Go to `\Telescope\Applications\`**`tsadmin`**`\Contents\info.plist` and change the `<search_mode>` key to `SOLR`.
- Log in to TSAdmin as sysadmin and in the Connections tab, and specify the database connection in the recs parameter.
- Specify which metadata fields are searchable to which users.
- If you have multiple databases, configure Indexing and Child Indexing Brokers accordingly. (Single database setups do not require any modifications.)
- After all other configuration steps are complete, restart the Indexing and Child Indexing Broker services to start indexing the Solr search database. A full reindexing is required.

Complete details are provided in the *Telescope Administrator's Guide*.

7.3 Enable Telescope Video Support

Support for playback of video files in the Video Manager interface requires that the Video Manager is licensed. In addition, video support requires additional configuration steps as detailed below.

7.3.1 Install the Appropriate Media Players

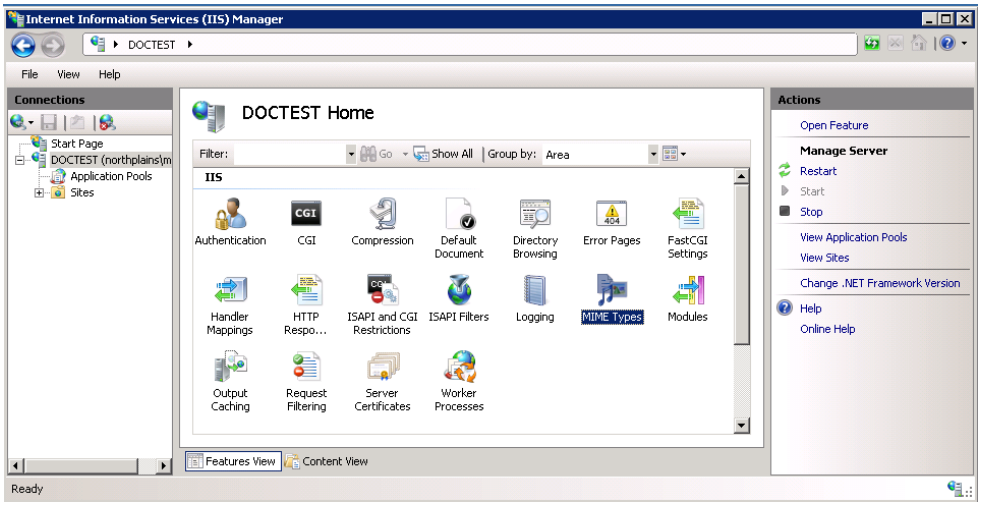
To display the extended view for a video asset, the appropriate media player for the asset file type, or a codec pack that can decode the file type, must be installed on client computers.

7.3.2 Additional Configuration for IIS 7

The QTL file type is required by the QuickTime Full Screen player running on the web application server. To add the QTL file type to the list of accepted MIME types in IIS 7:

1. From the *Start* menu of the web application server, open Internet Information Services (IIS) Manager.
2. In the Connections pane, click the machine name.
3. In the main pane, double-click the *MIME Types* option.

Figure 7.1 *MIME Types*



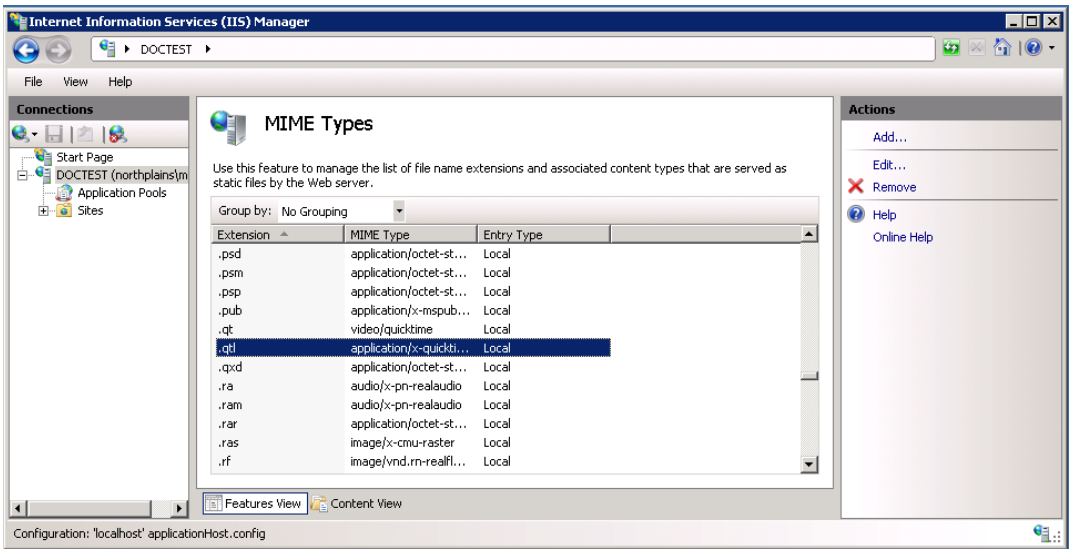
4. Scroll down and look for the *.qtl mime type*.

   If it does not appear in the list, follow these steps:

   a. In the Actions pane, click *Add*.

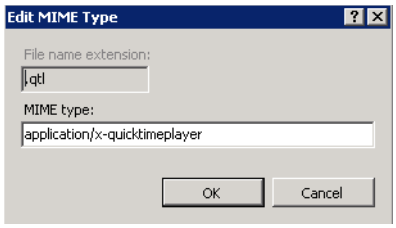
   b. In the Extension field, enter (with a preceding period): `.qtl`

Figure 7.2 *MIME Types*



c In the Mime Type field, enter: `application/x-quicktimeplayer`

Figure 7.3 *Edit MIME Type.*



d Click *OK*.

7.3.3 Configure the VideoPlayersConfig.xml File

The VideoPlayersConfig.xml configuration file (by default, in *\Telescope\aplications\tsweb.woa\Contents\Resources*) determines how video assets are displayed in the Telescope preview view.

This file is set up with default values, but you should review it and, if necessary, edit it to effectively configure video file playback in your Telescope implementation.

The VideoPlayersConfig.xml configuration file contains the following tags:

- `<pluginconfig>` – The document root tag.
- `<viewextypes>` – A list of the data_type values defined in the VIEWEX database table; by default, the list contains all the possible data_types but you should review the list to ensure it contains the data types you use.

NOTE: This is especially important if you are using Video Manager 3.0, which requires that the ViRa and TPlt data types to be present in this list.

- `<platform>` – Contains the configuration settings for the indicated browser(s); you should not need to change this.
- `<plugin>` – Defines which plug-in to use for the indicated file or MIME type based on the following attributes:

  file_type: The file type this plug-in is used for.

  mime_type: The MIME type this plug-in is used for.

  qtsrcdontusebrowser: (Optional) This tag defines the QTPlugin plug-in. Set this attribute to "true" to load the file using QuickTime's internal methods, instead of using the browser to fetch the file. This prevents the browser from caching the file, which speeds access to local movies and can help prevent copying movies over the internet. Set this attribute to "false" to allow the browser to cache the file.

  full_screen: If you are using Video Manager, this attribute indicates whether the video can be played in full screen mode.

  stream_display_name: In Video Manager 2.x, the value of this attribute is displayed in the drop-down list that allows users to select which proxy they want to view. This value is not used by Video Manager 3.0.

NOTE: If you are using Video Manager 3.0, you must set the `<plugin>` tag for all QuickTime file types to use the QTPlugin.

When a Telescope user requests the preview for a video asset, Telescope compares the asset's data type (as defined in the VIEWEX table record for the asset) with the list of data types defined in the `<viewextypes>` tag in the VideoPlayersConfig.xml file. If the asset's data type is not in the list, Telescope displays a message indicating that the preview cannot be displayed.

If the data type **is** in the list, Telescope checks the `<plugin>` tags for the user's browser to determine which plug-in to use for the asset's file type or MIME type. You can also specify a default plug-in to use for file types not explicitly defined.

NOTE: For Windows Explorer and Firefox browsers, the `<plugin>` tag that defines the default plug-in to use for all file types not explicitly defined appears near the beginning of the list of `<plugin>` tags by default. Because Telescope reads this list in order, it will use this default plug-in tag before it finds the correct plug-ins for specific file types. You should move the default `<plugin>` tag to the end of the list to ensure that Telescope first finds the correct plug-in assigned to a particular file or MIME type.

7.3.4 Video Download Performance Considerations

When a user opens a video asset, Telescope downloads a copy of the video to play in Video Manager 3 or another video player interface. If you find that this is impacting the performance of user downloads in Telescope, you can create and configure separate DLManager application instances to be used exclusively for video playback. To install and configure a Download Manager for video playback, follow the steps below:

1. Create a directory called `DLVideoManger` in your WebObjects application directory; for example, `\Telescope\Applications\DLVideoManager`

2. Copy the contents of your installed and configured Download Manager application directory into the newly created directory. For example, copy the contents of `\Telescope\applications\DLManager.woa` into `\Telescope\Applications\DLVideoManager`.
3. In the WebObjects Monitor, add an application (call it DLVideoManager) pointing to the `dlmanager.cmd` file in the new location.
4. Click the *Details* button for this new application and add the required number of instances.
5. Open the `Info.plist` file for Telescope TSWeb, located in `...\tsweb.woa\Contents` and update the `dlManagerVideo` key's value to point to the newly created DLVideoManager application.
6. Restart all TSWeb applications to force them to use the updated configuration.

7.4 Configure I-Pieces and C-Pieces

Telescope provides view / input support for customized treatment of many file types via its I-Pieces. I-Pieces are Telescope plug-ins that enable the DAM platform to handle new file formats as they emerge, providing customized support for complex previews and directly representative graphics for a wide variety of file types. This is done by either simply rendering thumbnails and previews of the file, or in some cases providing document-type specific functionality, such as managing linked assets automatically within creative applications. For example, the component object view (COV) is a special type of asset preview that displays multiple-page files that have been imported with a compatible I-Piece. These files can contain linked files, such as placed art, and text.

Conversion I-Pieces, also known as C-Pieces, are plug-in modules that perform on-demand file conversion for files before they are downloaded. For example, to particular image or video formats.

More Information

- For general information on the types of I-Pieces and C-Pieces available, and on supported file formats, see the *Telescope File Formats Guide*.
- For information on installing/configuring particular I-Pieces and C-Pieces, see their respective manuals.

General Notes

- Before they can be applied from the TSWeb interface and for predefined Migration Polices, the I-Pieces must be installed on the Graphics Broker machine and added to the license pool.
- To ensure all I-Piece and C-Piece licenses are added to the license pool, log into TSAdmin as a system administrator and go to the Licenses tab. For details, see the Telescope Administrator's Guide.
- When configuring I-Pieces, note that the connection name in their respective XML file is case sensitive. For details on using XML files, see the respective manual for the I-Piece you are configuring.
- Telescope will not generate thumbnails or previews if required third-party software is not available.

7.5 Configure for Multiple File Brokers

Site Manager automatically handles requests if there is one File Broker and that broker resides on the same machine as the hub server. If you need to configure for multiple File Brokers (or if the File Broker resides on a different machine), you must update the `site.plist` file **on the web application server** to provide information about the File Brokers available to the site.

Add the File Broker Name to site.plist

1. On the web application server, find the `site.plist` file (located in the `...\Telescope\Applications` folder) and open it with a text editor.

NOTE: You must edit this file using a text editor that will not add line breaks or other extra characters. For example, use Notepad (with wordwrap disabled) or a source code editor. DO NOT USE WordPad or Microsoft Word.

---

2. Add the file_brokers key and set it to a semicolon delimited list of File Broker servers and File Broker shares available to the site. Use the format shown in the following examples. (The first format shows one file broker; the second, multiple file brokers.)

   “file_brokers” = {“<*file broker computer name*>”=(“<*share name*>”);};

   “file_brokers” = {“<*file broker computer name*>”=(“<*share name*>”,“<*share name*>”, etc.);};

   To find the file broker computer name:

   a. Select *Start* > *Computer*.

   b. In the left column of the file browser, right-click over *Computer* and select *Properties* from the menu:

   c. From the Systems window that appears, look for the *Full Computer Name*.

   To find the share name:

   a. Open the Registry Editor (Type regedit from the command prompt).

   b. Navigate to `HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Node > North Plains Systems > NTFS File Broker > Current Version > NFTS Shares`.

   c. Use the share name shown in the Data column.

3. Restart TSWeb from the WebObjects Monitor.

NOTE: Any time you make changes to the site.plist file, you must restart TSWeb from the WebObjects Monitor.

Example:

```
{
"sites" = (
{
"sitename" = "default";
"sysadmin" = "true";
     "fn_definition" = "true";
"allow_ws" = true;
"file_brokers" = {
```

```
     "FILEBROKERMACHINE1" = ("shares1");
     "FILEBROKERMACHINE2" = ("shares2", "fb_shares2", "test_shares2");
};
"not_allowed_conv_type_codes" = ("AGS-JPEG", "PDF");
"user_pools" = ("Pool-A", "Pool-B");
"connections" = (
"1", "2"
);
}
);
"hubHost" = "127.0.0.1";
"hubPort" = "12345";
"connections" = (
{
"id" = "1";
"cb_name" = "db1";
"description" = "";
"web_name" = "database 1";
},
{
"id" = "2";
"cb_name" = "db2";
"description" = "";
"web_name" = "database 2";
}
);
}
```

7.5.1

7.6 Install the Xinet File Broker

7.6.1 Install and Configure a Xinet File Broker

Prerequisites:

- A Linux system is required. (We tested with RHEL 6.5)
- Before installing the Xinet File Broker, Xinet FullPress print spooler must be installed and configured according to the installation documentation for that product.

To remove the Xinet File Broker for 9.4.0.6.1

NOTE: This Broker was first shipped with Telescope 9.4.0.6.1. Because of the design of the Linux file system, you needed to reinstall the Xinet File Broker for 9.4.0.6.2 if you installed it for 9.4.0.6.1.

---

1. Back up the config directory from /opt/Telescope/config to a save place.
2. Go to /opt/Telescope/bin
3. Stop File Broker

```
# ./xbctl stop
```

4. Run uninstall script:

```
# ./xb.uninstall
```

5. Delete the Telescope folder under /opt

To install the Xinet File Broker:

1. Copy the NPS-XB-redhat6-9.4.0.6.2-9.4.0.5865.tar.gz into the target system. Log on to the target system as superuser (root).
2. Extract the files from the package.

```
# tar -xvf NPS-XB-redhat6-9.4.0.6.2-9.4.0.5865.tar.gz
```

NOTE: The installer filename includes the complete version number.

---

3. Install the File Broker:

```
# cd NPS-XB-redhat6
# ./install
```

4. Follow the prompts accepting the default values suggested by pressing Enter or entering values to be used for configuration in this environment.

```
[root@xinetfullpress NPS-XB-redhat6]# ./install

Enter the directory to install FileBroker package [/opt/Telescope]?
```

```
Configuring Telescope Hub...
Enter the address of Telescope Hub [127.0.0.1]?
10.24.10.151
Enter the port of Telescope HUB [12345]?

=====================================================
Telescope Primary Hub will be 10.24.10.151:12345
=====================================================

Do you want to configure Telescope Secondary Hub(s) [y/n]? n

Set up FileBroker to start automatically when machine boots up [y/n]? y
Creating directory /opt/Telescope
Creating directory /opt/Telescope/bin
Creating directory /opt/Telescope/logs
Creating directory /opt/Telescope/lib
Creating directory /opt/Telescope/config
Creating directory /opt/Telescope/var
Enter the Xinet FullPress Home Directory (Enter to skip) [/usr/etc/appletalk]?
/usr/etc/appletalk/kexportfpo utility has been generated.

Creating directory /opt/Telescope/config/FBroker/Xinet
Copying /opt/Telescope/bin/*
Copying /opt/Telescope/lib/*
generating /opt/Telescope/bin/xbctl
generating /opt/Telescope/config/FBroker/Xinet/FB_Unix.conf
generating /opt/Telescope/config/FBroker/Xinet/omniORB.cfg
generating /etc/init.d/xb_server
create /etc/rc2.d/S99npsxb ...
create /etc/rc0.d/K99npsxb ...

Configuring File Broker shares ...
```

5 Configure the File Broker share directories. As part of the FullPress configuration, you defined the high resolution and low resolution FullPress directories. You must make each FullPress high resolution directory a Telescope File Broker share directory

```
File Broker Share Directory Configuration

  1 Create New FB Share Directory
  2 Delete FB Share
  3 List FB Shares
  4 Quit

Make a Choice from the Menu above: 1

Create New FB Share Directory

Please Input the share name: FBShare

Please Input the share directory: /FBShare

New Share Entry is created
```

```
Share Name:      FBShare
Share Directory: /FBShare

Hit RETURN to continue...

File Broker Share Directory Configuration

  1 Create New FB Share Directory
  2 Delete FB Share
  3 List FB Shares
  4 Quit

Make a Choice from the Menu above: 4

  File Broker has now been successfully installed on this machine.
  You can start it with the following command.

  /opt/Telescope/bin/xbctl start
```

6. Replace the configuration files in the new installation with the ones backed up in step 1.
7. Start the Xinet File Broker:

```
# /opt/Telescope/bin/xbctl start
```

The Conversion I-Pieces are required for File Conversion capabilities and must be installed separately (if purchased). For information about the source and destination types for the Conversion I-Pieces, see the Telescope File Format Support Guide.

7.6.2 Configure the Xinet File Broker

The File Broker Admin Utility can be used to configure additional File Broker Shares, set LOGLEVEL, LOGFILE, and CleanCycle, and to check the log information. It is available on a Windows machine on which a File Broker is installed, and other File Brokers can be accessed from there.

Share Maintenance:

If the File Broker Admin Utility is not available, additional File Broker shares can be created and existing shares modified or deleted as follows:

1. Open up the xb_share.conf file.
2. Manually add the new shares or edit existing shares.

Multi-Hub Setting:

Configure the File Broker for multi-hub implementation (if required) by including the IP addresses or fully-qualified domain names of all hubs, as shown below. $NPSBASE should be the default installation location, in this case /opt/Telescope

```
# cat $NPSBASE/config/hubs.conf
192.168.0.115 12345
192.168.0.197 12345
192.168.0.222 12345
```

Broker IIOP_PORT Setting:

To enable users outside the LAN to access this File Broker (if required) through a specific port, the Broker IIOP_PORT can be specified by first opening up the configuration file as follows:

```
# cat $NPSBASE/config/FBroker/XINET/FB_Unix.conf
```

Add one line to this file as shown below, substitute the new port being specified with 12346

```
IIOP_PORT=12346
```

LOGLEVEL and LOGFILE Setting:

The LOGLEVEL and LOGFILE can also be manually configured, if required, in this conf file.

To set the log file to $NPSBASE/log/FB.log and the Log level to LOG_DEBUG, the following two lines can be added to the FB_Unix.conf file:

```
LOGFILE=$NPSBASE/log/fb.log
LOGLEVEL=LOG_DEBUG
```

LOGLEVEL can be set to one of seven levels. The column names specify what is logged at each level:

```
LOG_DEBUG, LOG_INFO – default setting, LOG _WARNING, LOG_ERR, LOG_NOTICE, LOG_ALERT,
LOG-EMERG
```

7.6.3 Starting the Xinet File Broker

1. Verify that the Telescope Hub is running. If not, start it now.
2. Once the File Broker is installed, it is set up as a daemon. This means that every time the system is rebooted, the File Broker starts automatically.
3. For now, the File Broker can be started manually by issuing the following command:

```
$NPSBASE/bin/xbctl start
```

7.6.4 Stopping the Xinet File Broker

When necessary, the File Broker can be stopped manually by issuing the following command:

```
$NPSBASE/bin/xbctl stop
```

7.7 Install and Configure the Queue Broker

7.7.1 Install the Queue Broker

Installing the Queue Broker involves copying the files to the Telescope base directory and creating the required registry entries (qb.reg may have been supplied). The database objects needed by the Queue Broker were added to the Telescope database scheme as part of the 9.4.0.6 release.

To install the Queue Broker:

1. Unzip the zipped Queue Broker package, Telescope_QueueBroker_9.4.0.6.1-9.4.0.5709.zip.
2. The following files should have been provided in the zip file, it is recommended that they be installed in a sub-directory in the Telescope installation. For example, in C:\TeleScope\QB
   - `QueueBroker.jar` - the java code
   - `qb.exe` - wrapper
   - `qbwrapper.xml` - wrapper configuration
   - `qb.reg` - registry entries for the Queue Broker
3. Edit the qb.reg file for the environment, in particular the hubip, connection, and the path of the entries in the classpath. See the section below for details on the registry key settings.
4. Install the service by running the full path to the qb executable with the i (install) option. For example:

```
c:\Telescope\QB\qb.exe -i
```

5. Ensure the two tables, qb_queue and qb_processes, are already in your Telescope DBMS. (They should have been installed with the 9.4.0.6 release.)
6. Execute the registry file qb.reg to populate the values under HKLM\Software\Wow6432Node\North Plains Systems\Queue Broker
7. Start the service.
8. Inspect the log file for errors.
9. Test the installation by populating the tables with a test process and entering a queue entry for the ping test operation. For example, (remember to replace **CONNECTION** with the correct connection name):

```
insert into qb_processes (process, type, name, location, param, payload_location, active)
values ('ping test', 'java', 'pingDB', 'com.northplains.QueueBroker.QBroker', 'String', 'cmd', 1);
insert into qb_queue values (1,'Active','ping test','CONNECTION',NULL,GETDATE());
```

   After a minute the row should show a status of "Success" and the logs will show details.

10. Examine the log and the qb_queue table for success. It should report the current version of Telescope.

7.7.2 To Remove the Queue Broker

To remove the Queue Broker follow the steps below:

1. Stop the Queue Broker Process

2. Run the uninstall command to the wrapper with the full path. For example,

```
C:\Telescope\QB\qb.exe -u
```

3. Run regedit and remove the HKLM\Software\Wow6432Node\North Plains Systems\Queue Broker registry entries
4. If retries were enabled, drop the trg_qb_queue trigger and qb_retries tables from the database
5. Drop the qb_queue and qb_processes tables from the database
6. Delete the QB subdirectory.

7.8 Customize your Sites

Site Manager automatically updates the `site.plist` file **on the web application server** with any new site you add and the connections you associate with it. You can edit the site.plist file to further customize your site.

NOTE: For more information on customizing the TSWeb site, see the *TSWeb Interface Customization Guide*.

7.8.1 Additional Site Customization

NOTE: Any time you make changes to the site.plist file, you must restart TSWeb from the WebObjects Monitor.

You can further customize your site by adding or editing the values for the following keys found in the `site.plist` file (located in the Applications folder within the Telescope installation). These keys must be added manually. If you apply these settings to a site, it will limit the visibility of the options to the site. Otherwise, the site will have all the options available to it. Site Manager updates the other keys in the file.

For information on configuring these keys, contact your North Plains Systems representative.

Key/Section	Description
blackList	Defines strings that will not be accepted as user input. Defaults are recommended. For details, see Section Chapter 11:, "Configure Web Security Features," on page 149.
passwordPolicy	Defines the password policy. Defaults are recommended. For details, see Section Chapter 11:, "Configure Web Security Features," on page 149.
fn_definition	Set the value to “true” to allow the site to use functional rules; otherwise, set to “false”.
allow_ws	Set the value to “true” to allow the site to use web services (for example, SOAP); otherwise, set to “false”.
not_allowed_conv_type_codes	A comma separated list of the conversion type codes that are NOT available to the site; the conversion type codes you can add depend on the Conversion I-Pieces you have installed.
user_pools	A comma separated list of the license pools available to the site. **Note:** If you delete or comment out the user_pools line for the default site, all license pools are visible for that site in Telescope Administrator. For any other site, only those license pools explicitly defined in the site.plist file are visible for the site in Telescope Administrator.

Chapter 8: Apply Product Upgrades

This section provides information about upgrading Telescope to a newer release.

In this Chapter:

- Section 8.1, "Upgrade the Telescope Release," on page 98
- Section 8.2, "Upgrade the Telescope Database," on page 106

8.1 Upgrade the Telescope Release

NOTE: Always consult the installation instructions in the Release Notes that are shipped with the release you are installing. Release Note instructions will take precedence over the information in this chapter.

8.1.1 Before You Start

Before you upgrade your Telescope release, you must back up files from the current release so that you can apply your configuration and other customizations after you upgrade. You must back up files on every server machine in a multi-site environment.

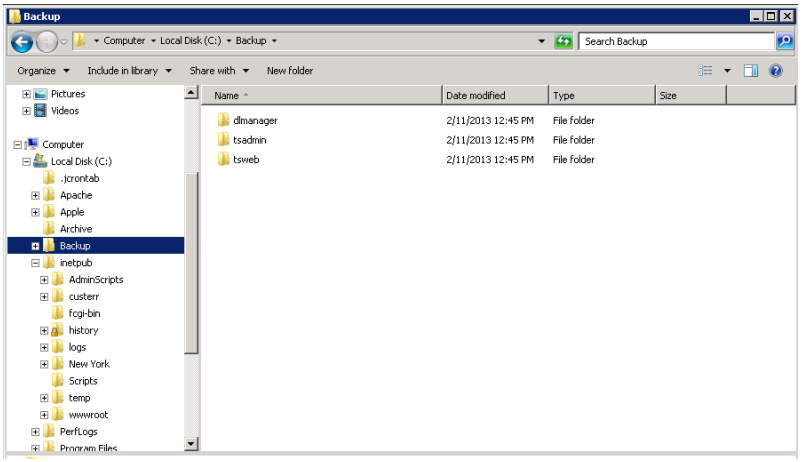
NOTE: Ensure there are no pending auto-ingest operations when updating from 9.1.4-P3. An early version of the queue state management was introduced in 9.1.4-P3. In that release, the queue management was stored within the hot folders inside each top-level hot folder in Ingest Folder\ProcessQueue. That old location is no longer used and will be ignored after installing the newer version (so any pending auto-ingest operations will be lost). The location can be safely removed after updating the environment.

Back up files:

1. Create a backup folder on every server. For example, `C:\Telescope_Backup_Site1`.
2. Before you begin any upgrade, be sure to back up the files listed below. This is a very important step. The paths listed below assume a default installation.

- For all servers, all folders and files in `\inetpub\wwwroot\`

Figure 8.1 *wwwroot configuration folders on the web application server, to be copied to backup folder*



- All customized folders across all servers
- On each web application server, the following files:
  - `...\Telescope\Applications\site.plist`
  - `...\TeleScope\Applications\dlmanager.woa\Contents\info.plist`
  - `...\TeleScope\Applications\dlmanager.woa\Contents\Resources\config.plist`

- `...\TeleScope\Applications\dlmanager.woa\Contents\Resources\aspera.prop`
- `...\TeleScope\Applications\sitemanager.woa\Contents\info.plist`
- `...\TeleScope\Applications\tsadmin.woa\Contents\info.plist`
- `...\TeleScope\Applications\tsadmin.woa\Contents\Resources\config.plist`
- `...\TeleScope\Applications\tsweb.woa\Contents\info.plist`
- `...\TeleScope\Applications\tsweb.woa\Contents\Resources\config.plist`
- `...\TeleScope\Applications\tsweb.woa\Contents\Resources\Properties`
- `...\TeleScope\Applications\tsweb.woa\Contents\Resources\aspera.prop`
- `...\Apple\Local\Library\WebObjects\Configuration\SiteConfig.xml`
- Any other customized files made for your Telescope installation (images, CSS, HTML files, and so on)

3 Back up the North Plains settings in the Windows Registry (as a precaution) on each hub and broker server:

a The `regedit` utility needs to be run from an Administrator console and may need to be run as an administrator.

b Run regedit by typing: `regedit`

c Navigate to the North Plains Systems settings:

Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Node > North Plains Systems

d Right click on North Plains Systems and select *Export* from the pop-up menu.

e Type in a file name and save the .reg file in a safe place.

f Follow the above steps for any other customization you may have made within your registries, such as the WO Adaptor registry at:
HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Node > Apple > WebObjects > Configuration.

8.1.2 Install the Upgrade

After you have completed all backup activities:

1 Unzip the zip file of the latest release.

- Do not store or unzip this file to a directory whose path includes a space. For example, do not store it in `C:\My Documents\`.
- Do not change the folder structure of the unzipped files or move any files out of the folder.
- Ensure the folder containing the unzipped files is writable.

2 Copy the unzipped files to every Telescope server machine.

3 Edit the default `InstallConfig.xml` file on each server machine to ensure the appropriate MSI components are installed.

To find out which components are installed on which servers, see Section 3.1, "Edit the Installation Configuration File," on page 23.

4 Shut down all Telescope applications and services running on all machines. In particular,

- All instances of Telescope

- All the Brokers (using Windows Services from the hub server)
- Web Objects from Windows Services on the web application server

- (If upgrading from 9.2.x and Solr is installed) Jetty-Service from Windows Services on the server where Solr Engine is installed.

5 Shut down other applications running on the machine. (The `lightsoutInstall.exe` kills all Java processes running on the machine. Other applications using these same processes will be affected, and their data may be lost.)

6 Go to the Windows Control Panel on the respective server and uninstall the following:

- Web Objects (on the web application server)
- If you are upgrading from Telescope 9.2-x and Solr is installed, uninstall the following

  - Solr Multicore (on the Server where the Solr Engine is installed)

  - Solr engine (on the server where the Solr Engine is installed)

  - Java SE Development Kit 6 Update 37 (from all servers)

  - Java 6 Update 37 (from all servers)

7 Ensure the date and time are synchronized on all servers. This will prevent potential failure of processes that need to run from one server to the next. (This may be an issue if you are using virtual environments that do not reflect your local time.)

8 Ensure that your firewall does not prevent communication between all required servers running Telescope components.

9 Run the Lights Out installation with Admin privileges for each server where you are installing (hub, web, web application, Solr). Be sure to use the -i option if the original installation is on a different drive. See Section 4.1, "Run the lightsoutInstall.exe Installer," on page 38 for details.

8.1.3 Ensure the Correct Java Version is Being Used

If you are upgrading to Version 9.3, you must follow the steps in this section to ensure Java 8 is going to be used by Telescope, and by the Solr search functionality. Follow these steps after you have installed the upgrade.

1 Verify that Java 1.8 is installed and run all Telescope 9.3 applications. In particular, ensure:

- WebObjects is re-installed pointing to Java 1.8. (From Server Manager, go to Services, select Apple WebObjects Taskd, and choose Properties from the right-click menu. Ensure you see `jre1.8.0_40` in the path to executable.)
- Jetty-Service no longer appears in the list of Services. Instead, you should see NPS Jetty-Service.
- NPS Brokers and web applications will be running under Java 1.8. (From Resource Monitor, select a Telescope executable such as cdx.exe. Ensure you see `jdk1.8.0_40` in the Handle name.)

2 Manually stop all NPS services (as applicable to your installation), in the following order. You must stop all NPS brokers on all computers.

a NPS Interoperability Broker

b NPS Zoom Builder

c NPS Zoom Broker

d NPS Distribution Broker

e NPS Ingest Broker

f NPS Graphics Broker

g NPS Lookup Broker

h NPS Message Broker

i NPS NTFS File Broker

j NPS Authentication Broker

k NPS Connection Broker

l NPS State Broker

m NPS Session Broker

n NPS Name Server

3 Stop the Apple Webobjects Taskd Service on the web application machine.

4 Back up the following files on your hub and web application server machines

```
C:\Program Files (x86)\Java\jdk1.8.0_40\jre\lib\security\local_policy.jar
C:\Program Files (x86)\Java\jdk1.8.0_40\jre\lib\security\US_export_policy.jar
C:\Program Files (x86)\Java\jre1.8.0_40\lib\security\local_policy.jar
C:\Program Files (x86)\Java\jre1.8.0_40\lib\security\US_export_policy.jar
```

5 After your backups are complete, replace the above files with the files with the same names found in the 9.3 release package:

```
\Release\Resources
```

6 At this time, upgrade the Database with latest DBManager for 9.3.0. See Section 8.2, "Upgrade the Telescope Database," on page 106.

7 Manually start all Telescope services again on all machines, in the following order (as applicable to your installation):

a NPS Name Broker

b NPS Session Broker

c NPS State Broker

d NPS Connection Broker

e NPS Authentication Broker

f NPS NTFS File Broker

g NPS Message Broker

h NPS Lookup Broker

i NPS Graphics Broker

j NPS Ingest Broker

k NPS Distribution Broker

l NPS Zoom Broker

m NPS Zoom Builder

n NPS Interoperability Broker

8.1.4 Notes on Reinstalling Solr Search

Due to a large number of improvements to the Solr functionality, you will need to reinstall Solr for this upgrade, and perform a full Solr reindex. See Section 7.2, "Install Solr Search," on page 80 for details.

After you reinstall Solr, you will see the following NPS services in the Services panel, in addition to those shown in the list above. They must be manually started to make Solr available.

a NPS Jetty-Service

b NPS Indexing Broker

c NPS Child Indexing Broker

8.1.5 Verify the Upgrade

Verify that the upgrade was successful by checking the configuration.

Verify on the Hub Server and any Broker Servers

Follow these steps on the hub server, and on broker servers if any brokers are installed on separate machines.

1. Check registry settings of ALL brokers. Compare them with the backed up registry settings.
2. If you have installed on a clean machine or upgraded from release 9.0.2 P2 or earlier, you must restart the server(s).
3. Select *Start* > *Administrative Tools* > *Services*.
4. Verify in the following order that the following brokers (if installed) are running, and manually start them if they are not started (as applicable to your installation):

NOTE: If you are upgrading from Version 9.0.x, you must stop all of these brokers in reverse order to the following, then start them again in the following exact order.

---

a NPS Name Broker

b NPS Session Broker

c NPS State Broker

d NPS Connection Broker

e NPS Authentication Broker

f NPS NTFS File Broker

g NPS Message Broker

h NPS Jetty-Service

i NPS Indexing Broker

j NPS Child Indexing Broker

k NPS Lookup Broker

l NPS Graphics Broker

m NPS Ingest Broker

n NPS Distribution Broker

o NPS Zoom Broker

p NPS Zoom Builder

q NPS Interoperability Broker

5 If any of the Brokers listed above fail to start then:

a Delete all files in the `Telescope/Logs` directory.

b Stop all brokers in reverse order to the above, then start them again in the exact order shown above. Check the log files for details.

c If a broker still fails to start, particularly in the case of an upgrade from release 9.0.3 or later, restart the server(s).

6 From the Registry Editor, navigate through to the following path:

7 Type `regedit` from a command line to use the Registry Editor. Navigate to the following settings:

HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Node > North Plains Systems

8 Browse through the various brokers to ensure the latest versions are installed.

Verify on the Web Server

Follow these steps on the web server:

1 Type `regedit` from a command line to use the Registry Editor. Navigate to the following settings:

HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Node > Apple > WebObjects > Configuration

Check that the Data value for CONF_URL points to the IP Address or Machine Name of your Web Application Server, as follows:

```
http://WEB_APP_SERVER:1085
```

(If you are running more than one application server, separate each URL by a comma.)

Verify on the Web Application Server

Follow these steps on the web application server to verify the values are correct:

1. Within the `site.plist` file which affects TSWeb configurations and is located within the `\Telescope\Applications` folder, configure the value for "hubHost" so that it points to the IP Address or the Machine Name of your Hub Server, as follows:

   ```
   "hubHost" = "HUB_SERVER";
   ```

2. Within the `Info.plist`, located within the `\Telescope\Applications\tsadmin.woa\Contents` folder:

   - Configure the <string> value of the "PrimaryHub" key so that it points to the IP Address or the Machine Name of your Hub Server, as follows:

     ```
     <key>PrimaryHub</key>
     <string>HUB_SERVER</string>
     ```

   - Configure the <string> value of the "url" key so that it points to the IP Address or the Machine Name of your Web Server, as follows:

     ```
     <key>url</key>
     <string>http://WEB_SERVER</string>
     ```

3. Access the Services console via the computer's Administrative Tools

   - Right click on Apple WebObjects Taskd and select "Restart".
   - Right click on Apple WebObjects Java Monitor and select "Restart".
   - Right click on World Wide Web Publishing Service and select "Restart".

Verify on Browsers Running TSWeb

The cache must be cleared on any browsers running TSWeb. Otherwise, the Telescope Uploader plug-in may not be updated with the latest changes.

Verify Functional Rules

Consult the *Telescope Administrator's Guide* for content on functional rules.

NOTE: User name and group name parameters were changed for Version 9.3.0. If you use functional rules to pass user names or user groups, be aware that you need to explicitly add the table name prefix to these names (for example, `user.user_name`). Details are in the *Administrator's Guide*.

8.1.6 Upgrade the Telescope Database

Consult the Release Notes shipped with the release you are installing to verify if you need to upgrade the database. If a database upgrade is required, follow the steps in Section 8.2, "Upgrade the Telescope Database," on page 106.

If you upgrade the database from earlier versions, you may be required to set the passphrase and enter the database credentials. See Section 8.2.2, "Update Telescope Database Credentials," on page 109.

NOTE: You can only upgrade the Telescope database after you have installed and verified the software in the previous sections.

8.1.7 Apply Configurations and Customizations from Backups

To restore image and configuration files for each site in your environment, you must manually copy the content from the default installation location to the site folder for each site.

1. For each server, copy the content of the Backup folder to corresponding folders in the new installation. Replace only those files that have been customized for the existing site in your environment.

   For example, copy the contents of a backed up New York folder to `\inetpub\wwwroot\tsadmin\New_York\`. Repeat this for the `tsweb` and `dlmanager` folders.

2. Update CSS and HTML files by merging the existing files in the backed up folder to the site folder in each web environment.

3. Update any image files.

NOTE: By default, the Session ID is hidden to improve your web security. If you customized your Telescope installation in earlier releases in ways that require the session ID, you will need to either redo this customization, or turn the SecureSessionID feature off in the `...\TeleScope\Applications\tsadmin.woa\Contents\Resources\Config.plist` file. For details, see Section 11.2.4, "Change the Secure Session ID," on page 156.

8.2 Upgrade the Telescope Database

NOTE: Consult the Release Notes shipped with the release you are installing to verify if you need to complete the steps in this section. Release Note instructions will take precedence over the information in this chapter.

8.2.1 Upgrade the Telescope Database

For Telescope upgrades, you may need to upgrade the Telescope database. Always check the release notes to confirm upgrade installation steps, including database updates.

Important! If upgrading to Telescope 9.4.0.7 or later, you will be able to make all database changes at once. The instructions in the release notes will tell you how you can remove a DBManager registry key to ensure all database updates occur from the beginning of 9.4.0.

To upgrade the Telescope database:

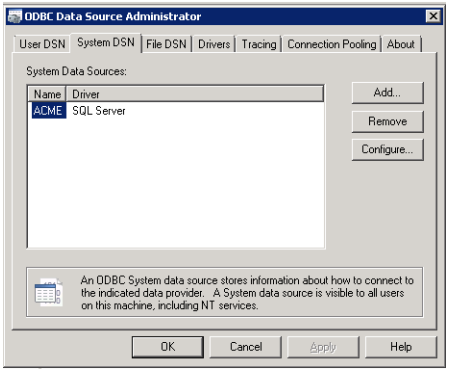
1. From a command line on the hub server, navigate to and start the following executable:

   `c:\Windows\SysWOW64\odbcad32.exe`

   The ODBC Data Source Administrator appears.

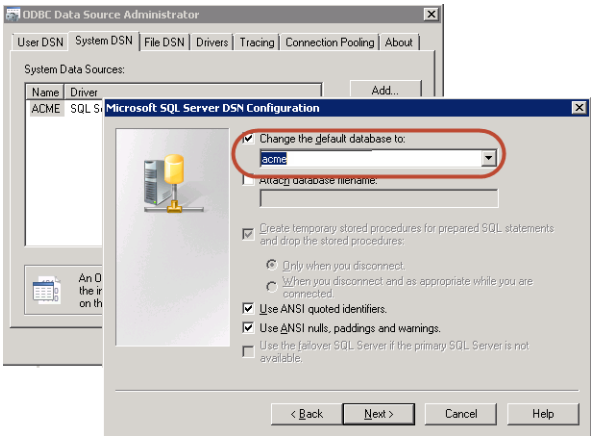
2. Select the *System DSN* tab.
3. Select the system data source of the existing Telescope database.

Figure 8.2 *Select the Telescope database data source*



4. Click *Configure*.
5. Click Next and follow the steps in the Microsoft SQL Server DSN Configuration wizard. Watch for the following screen:

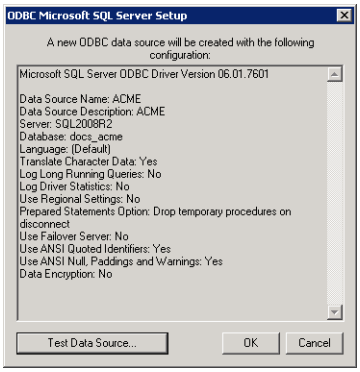
Figure 8.3 *Change the default database to the Telescope database*



6 Click the check box beside *Change the default database to:* and select your database source from the dropdown list.

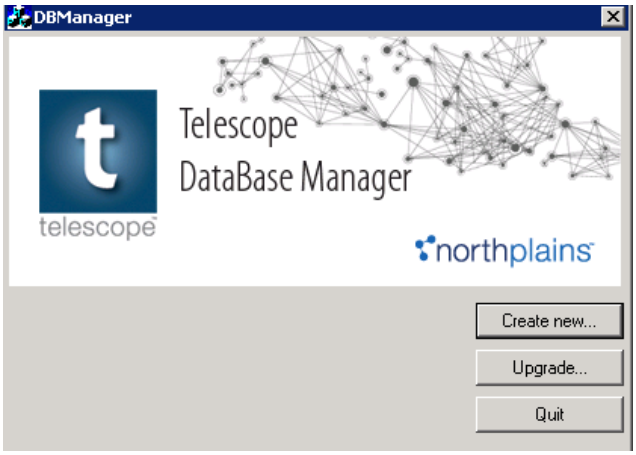
7 Click *Next* and continue until you finish the Wizard. Click *Test Data Source* to confirm your settings.

Figure 8.4 *Confirm ODBC database setup*



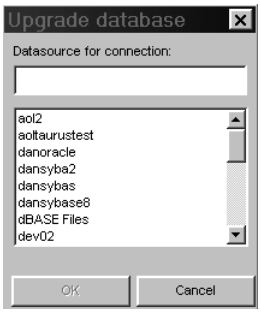
8 Open `DBManager.exe` from the Telescope installation at `\\Telescope\DBManager`.

Figure 8.5 *DB Manager*



9 Click *Upgrade*.

Figure 8.6 *Upgrade Database*



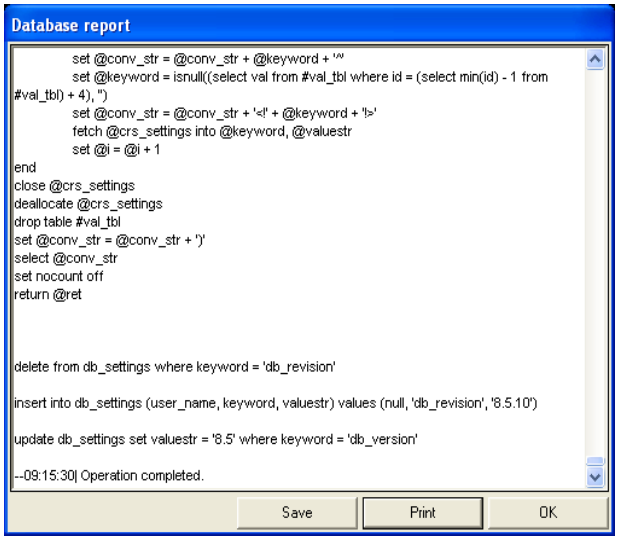
10 Select the data source of the database you created, and click *OK*.

NOTE: If upgrading from an 8.x release, you may be prompted to provide additional information required to configure the database for the current version. For example, you may be prompted to specify *Language ID*, *System Language ID*, *Video Rendition*, or *Connection Name*. For details on these database fields, see Section Chapter 5:, "Install Telescope Database Server," on page 43.

---

11 Click *Continue* to finish upgrading the database.

Figure 8.7 *Database Report*



12 Click Save to save the report log. (This log shows changes made to the database, and will be useful later if you encounter an error.)

13 Click *OK* to close the report.

Find the Upgrade Scripts

The upgrade scripts are stored in plain text format at the file system level. They can be found in the DBManager installation folder at:

- For MS SQL: `\\Telescope\DBManager\files\upgrade\mssql for SQL Server`
- For Oracle: `\\Telescope\DBManager\files\upgrade\oracle`

8.2.2 Update Telescope Database Credentials

Telescope brokers use a user name and password when connecting to the Telescope database. (These credentials are used internally by the Telescope software, and are not required for any user logins.) For extra security during every connection request, the user name and password are also encrypted by an encryption passphrase unique to your organization. As a result, these database credentials are not accessible to North Plains Systems staff.

Database credentials are required for Telescope database upgrades from releases prior to Version 9.1.4. You will also need to specify a passphrase (see Section 6.2, "Define an Encryption Passphrase," on page 72).

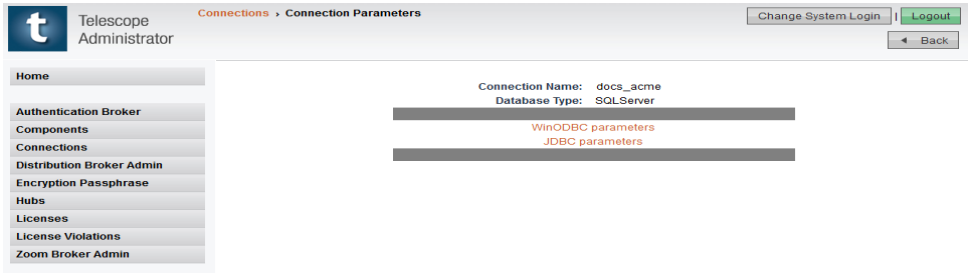
To update the Telescope database credentials:

1 Log in as sysadmin to the TSAdmin Systems application.

2 Click the *Connections* tab.

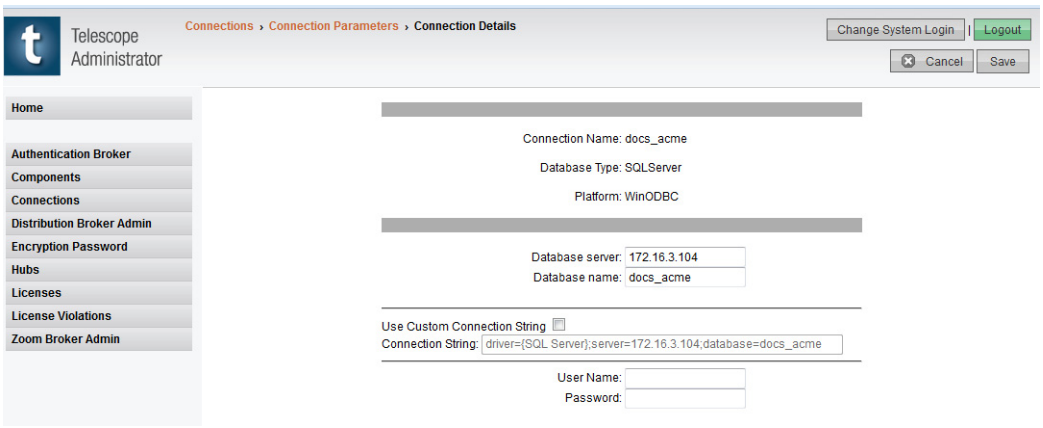
3 Click the connection name on the Connections page.

Figure 8.8 *Connection Parameters*



4 Click *WinODBC Parameters*.

Figure 8.9 *Connection Details*



5 To update the user name and password, type new values in the fields provided.

6 If your organization uses a port number for the database server different from 1433 (the default), add it to the port number in the *Database server* field, separated by a comma. For example, “172.16.3.104,1500”. (This applies to the WinODBC parameters only.)

7 If your organization prefers a custom connection string, click the check box beside *Use Custom Connection String*, then alter the connection string provided.

8 Click *Save*.

9 Repeat the above steps for the JDBC parameters.

10 When finished with the JDBC parameters, click the *Validate connection when saving* check mark.

11 Click *Save*. Your changes will be verified.

8.2.3 Back up and Restore from Oracle 11g to Oracle 12C

Follow these instructions to migrate the Telescope database when upgrading your Oracle database system from 11g to 12c.

The code below uses the following examples:

- The **source database** is on an Oracle 11g server, and is called OracleDB_1. The user name for the system database administrator for this server is “sysdba”, and the password is “Password789”.

- The **target database** is on an Oracle 12c Server, restoring the backup as OracleDB_1. The database administrator user name and password remains the same as the source database server (“sysdba”/ “Password789”).

On the source database server:

1. From Windows, create a temporary folder, `C:\temp`
2. Open the Windows command prompt as Administrator and start the SQLPLus environment:

   ```
   >sqlplus sysdba/Password789 as sysdba
   ```

3. From the SQL prompt, execute the following commands:

   ```
   SQL>create or replace directory dump_loc as 'C:\temp';
   SQL> grant read, write on directory dump_loc to OracleDB_1;
   SQL> exit (this will exit the SQL prompt)
   ```

4. From the Windows command prompt, run the following to create the dump and log files using export data pump:

   ```
   > expdp sysdba/Password789 directory=dump_loc dumpfile=OracleDB_1.dmp
   logfile=dump_loc:OracleDB_1.log schemas=OracleDB_1
   ```

   (The above command creates dump file `OracleDB_1.dmp` and log file `dump_loc` in the `C:\temp` folder.)

On the target database server:

1. Create a directory `C:\temp`, and copy the `dmp` file from the source server.
2. Open a Windows command prompt as Admininstrator and start the SQLPlus environment:

   ```
   >sqlplus sysdba/Password789 as sysdba
   ```

   (Use your system password.)

3. From the SQL prompt, execute these commands:

   ```
   SQL>create tablespace OracleDB_1_DATA datafile 'C:\Temp\OracleDB_1.dbs' size 1500M reuse
   autoextend on next 5m maxsize unlimited online default storage (initial 128k next 128k
   maxextents unlimited pctincrease 0);
   SQL>CREATE USER OracleDB_1  IDENTIFIED BY "OracleDB_1";
   SQL>alter user OracleDB_1 identified by "OracleDB_1" default tablespace OracleDB_1_DATA
   temporary tablespace temp quota unlimited on OracleDB_1_DATA;
   SQL>grant connect, resource, create session, dba to OracleDB_1;
   SQL>alter user OracleDB_1 quota unlimited on OracleDB_1_DATA;
   SQL>create tablespace OracleDB_1_IDX datafile 'C:\Temp\OracleDB_1_IDX.dbs' size 1500M
   reuse autoextend on next 5m maxsize unlimited online default storage (initial 128k next
   128k maxextents unlimited pctincrease 0);
   SQL>alter user OracleDB_1 quota unlimited on OracleDB_1_IDX;
   SQL>CREATE OR REPLACE DIRECTORY dump_loc AS 'C:\temp';
   SQL>grant read, write on directory dump_loc to OracleDB_1;
   SQL>exit  ( it will exit you from SQL prompt )
   ```

4. From the Windows command prompt, run the following to use import data pump to restore from the dmp file:

   ```
   >impdp sysdba/Password789 directory=dump_loc dumpfile=OracleDB_1.dmp
   REMAP_SCHEMA=OracleDB_1:OracleDB_1 REMAP_TABLESPACE=OracleDB_1_DATA1:OracleDB_1_DATA
   REMAP_TABLESPACE=OracleDB_1_INDEX1:OracleDB_1_IDX table_exists_action=replace
   logfile=dump_loc:OracleDB_1.log schemas=OracleDB_1
   ```

Troubleshooting: Warning when Ingesting Video Assets through FlipFactory

If your organization upgrades to Oracle 12C and is using FlipFactory video processing, a “No matching authentication protocol” warning may be issued from the FlipFactory plugin file and you will not be able to synchronize and process video assets.

According to Oracle forums, you can resolve this issue by adding the following lines to the `sqlnet.ora` file on the Oracle server and Oracle client server:

```
SQLNET.ALLOWED_LOGON_VERSION_SERVER=8
SQLNET.ALLOWED_LOGON_VERSION_CLIENT=8
```

(“8” is for the Oracle8i authentication protocol.)

Then restart the listener.

Chapter 9: Troubleshooting

In this Chapter:

- Section 9.1, "Cannot Access Telescope on the Web," on page 114
- Section 9.2, "Miscellaneous Troubleshooting," on page 121
- Section 9.3, "Add License Keys," on page 123
- Section 9.4, "Update the Master License Key," on page 124
- Section 9.5, "Contact Customer Service," on page 127

9.1 Cannot Access Telescope on the Web

Use this section if you have installed Telescope but cannot access its WebObjects Monitor, or if you can see the WebObjects Monitor but not any of its applications.

9.1.1 Initial Troubleshooting Steps

If you cannot access the WebObjects Monitor, follow these sections to check the installation and configuration.

Verify Telescope Hub is running

The default Telescope machine (Hub server) should start immediately after the installation is complete.

To check if the hub services are running,

1. Select *Start* > *Administrative Tools* > *Services* and scroll down to the following "NPS" entries to see if they are running.
   - NPS Name Server
   - NPS Session Broker
   - NPS State Broker
   - NPS Connection Broker
   - NPS Authentication Broker
2. If any of the Brokers listed above are not running, then:

   a Stop all brokers in reverse order as listed above (that is, stop NPS Authentication Broker, then NPS Connection Broker, and so on, until you finally stop the NPS Name Server).

   b Delete all files in the Log directory at `C:\TeleScope\Log`.

   c Check the logs.

   d Restart the broker(s) in the exact order listed above.
3. If a broker still fails to start, particularly in the case of an upgrade from release 9.0.3 or later, restart the server(s).
4. If any of the Brokers listed above still fail to start, then re-master the license file:

   a Open a DOS window (cmd) on the machine on which the Telescope Hub is installed and navigate to the Telescope directory, where you have the sesb.exe file, most commonly within the C:\Telescope (default) directory.

   b Re-name the sesb.dat file.

   c Run:

   ```
   sesb -remaster <new master key>
   ```

   NOTE: Substitute <new master key> with the new master key string in the license text file.

   d Remove ALL Broker log files.

   e Re-start the Brokers in the order listed above.

Check log files

The Telescope system logs all activities in various log files. Go to the Logs directory in the Telescope installation (by default, `C:\TeleScope\Logs`). There are log files for every broker. Check the time stamps for recent activity, and open recently updated log files to diagnose issues.

To diagnose current issues, you may want to delete the log files in this directory, try to start services to run Telescope again, and view the freshly created log files.

Check handler mappings

As outlined in Section 6.1.4, "Configure Handler Mappings for the IIS Folders," on page 64, ensure Handler Mappings are only enabled for the Scripts folder.

PATH Environment Variable Fix

If the Telescope services or web applications do not start, verify that the PATH environment variable is set correctly:

- The `C:\Windows\System32; C:\Windows; C:\Windows\System32\wbem` entries must be present and must be the first entries in the PATH.
- Entries must not contain double backslashes (\\); you can either remove one of the backslashes, or delete the entry entirely if it is a duplication of another entry.
- There must not be any duplicate entries.
- Make sure the correct version of Java SDK is listed and listed only once.

Install or Update Java

Java is required for most of the Telescope brokers and by the hub applications.

The `java.exe` and `javaw.exe` files might be installed in the `\Windows\System32` or `Windows\SysWOW64` directories. When the Java application is started by Windows Services it does not detect Java based on the PATH environment variable. It is detected from either the `\Windows\System32` or `\Windows\SysWOW64` directories. This could result in running Telescope using a wrong version of Java or causing an error message and the application not starting.

When updating Java, the `java.exe` and `javaw.exe` files should be removed from `\Windows\System32` and `\Windows\SysWow64`, and a PATH variable pointing to the correct Java version should be used instead.

Check Port Numbers

If you find that the Java Apple Monitor does not start in Windows Services, there may be a port number conflict.

To check which ports are being used:

1. Make sure you are using the latest version of Java.
2. Issue the command `tasklist.exe` from the Administrator Command Prompt.
3. Find all instances of "Java.exe" and note their PID number
4. Issue the following command, where xxx means the 3 digit or 4 digit PID number for each instance you found in the previous step. Continue until you find which PID is used by "Apple JavaMonitor".

   ```
   tasklist.exe /svc /FI "PID eq xxx"
   ```
5. Find which port is used by Apple JavaMonitor (by using PID number you found in the previous step) above) using the following command:

```
netstat.exe -a -n -o
```

To change the port number used by Apple JavaMonitor:

1. Stop Apple JavaMonitor (from Services)
2. With a text editor, open `\Apple\Library\WebObjects\JavaApplications\JavaMonitor.woa\yajsw\conf\wrapper.conf`
3. Change "`wrapper.tray.port = 15002`" into any port in use (for example, “12345,” used by Telescope Web Applications).
4. Try to start Apple JavaMonitor. It should fail to start
5. Change the setting to another port number that is not in use. For example, "`wrapper.tray.port = 15015`".
6. Start Apple JavaMonitor. It should start successfully. If it does not, change the port number again.

Restart WebObjects Task Daemon and WebObjects Monitor

The following procedure is necessary only if the Telescope WebObjects Monitor fails to respond.

1. Log in as an administrator **on the Telescope web application server**.
2. Go to *Start* > *Administrative Tools* > *Services*.
3. In the Services window, restart the following services:
   - Apple WebObjects Taskd (Task Daemon)
   - Apple Java Monitor
   - WorldWide Web Publishing service

If there is an error while trying to stop and restart the services, stop the “WOTaskDService.exe” and “WOMonitorService.exe” processes using the Windows Task Manager and start the service again. Alternatively, simply restart the computer to automatically restart all required services.

Restart an Application

If Telescope applications fail to respond, try stopping and restarting the application processes with the following steps:

1. Using a web browser, connect to the Telescope WebObjects interface.

   To access the WebObjects interface by default, go to a web browser and type a URL consisting of the IP address or machine name for the Telescope web application server, and append “:56789.”

   For example: `123.45.6.789:56789` or *`MymMchine.mycompany.com`*`:56789`
2. Click *Detail View* next to the application that is not responding.
3. Click the red *Stop* button to stop all applications.
4. Click the green *Start* button to restart the applications that have been stopped.

9.1.2 Troubleshooting Steps for Multiple Server Machines

If you are not able to start servers across multiple machines, follow these steps to troubleshoot.

Verify Server Status

1. From the Telescope WebObjects Monitor, click on Site Manager and log in.
2. Ensure that the Server Address for Telescope Hub matches the IP Address or Machine Name of your Hub Server.

Check Servers are Synced

1. Check that all server machines (hub, web, and web application) are synced with the same date and time. Telescope will not work if the server machines are out of sync.

Additional Checks on the Hub Server

1. Check the registry settings of ALL brokers. Compare them with the backed up registry settings.
2. Select *Start* > *Administrative Tools* > *Services*.
3. Verify the following brokers are running and manually start them if they are not started (as applicable to your installation):

NOTE: If you are upgrading from Version 9.0.x, you must stop all of these brokers in reverse order to the following, then start them again in the following exact order.

---

a. NPS Name Server
b. NPS Session Broker
c. NPS State Broker
d. NPS Connection Broker
e. NPS Authentication Broker
f. NPS NTFS File Broker
g. NPS Message Broker
h. NPS Jetty-Service
i. NPS Indexing Broker
j. NPS Child Indexing Broker
k. NPS Lookup Broker
l. NPS Graphics Broker
m. NPS Ingest Broker
n. NPS Distribution Broker
o. NPS Zoom Broker

p NPS Zoom Builder

q NPS Interoperability Broker

If any of the Brokers listed above fail to start, then:

a Stop all brokers in reverse order as listed above (that is, stop NPS Interoperability Broker, Zoom Builder and so on, until you finally stop the NPS Name Server).

b Delete all files in the Log directory at `C:\TeleScope\Log`.

c Check the logs.

d Restart the broker(s) in the exact order listed above.

e If a broker still fails to start, particularly in the case of an upgrade from release 9.0.3 or later, restart the server(s).

If any of the Brokers listed above still fail to start, then re-master the license file:

a Open a DOS window (cmd) on the machine on which the Telescope Hub is installed and navigate to the Telescope directory, where you have the sesb.exe file, most commonly within the C:\Telescope (default) directory.

b Re-name the sesb.dat file.

c Run:

`sesb -remaster <new master key>`

NOTE: Substitute <new master key> with the new master key string in the license text file.

d Remove ALL Broker log files.

e Re-start the Brokers in the following order:

i NPS Name Server

ii NPS Session Broker

iii NPS State Broker

iv NPS Connection Broker

v NPS Authentication Broker

(Other brokers will need to be relicensed.)

Additional Checks on the Web Application Server

1 Make the following changes to the `site.plist` file, which affects TSWeb configurations and is located within the `...\Telescope\Applications` folder:

a Configure the value for "hubHost" so that it points to the IP Address or the Machine Name of your Hub Server, as follows:

```
"hubHost" = "HUB_SERVER";
```

b If you are performing an upgrade install, you can include the default blackList and passwordPolicy settings. See Section 11.1, "Configure Web Security Features," on page 149.

NOTE: If you have multiple sites, the blackList and passwordPolicy sections should be copied into each site definition file.

---

2 Access the Services console via the computer's Administrative Tools.

a Right click on Apple WebObjects Taskd and select "Restart".

b Right click on Apple WebObjects Java Monitor and select "Restart".

3 Re-start the Site Manager application:

a Using a web browser, connect to the Telescope WebObjects Monitor.

To access the WebObjects interface by default, go to a web browser and type a URL consisting of the IP address or machine name for the Telescope web application server, and append ":56789." For example:

```
123.45.6.789:56789
```

b Click *Detail View* next to the Site Manager entry.

c Click the red *Stop* button to stop the application instance.

d Click the green *Start* button to restart the instance that was stopped.

4 Within the `Info.plist`, located in `\Telescope\Applications\tsadmin.woa\Contents`,

a Configure the <string> value of the "PrimaryHub" key so that it points to the IP Address or the Machine Name of your Hub Server, as follows:

```
<key>PrimaryHub</key>
<string>HUB_SERVER</string>
```

b Configure the <string> value of the "url" key so that it points to the IP Address or the Machine Name of your Web Server, as follows:

```
<key>url</key>
<string>http://WEB_SERVER</string>
```

5 Access the Services console via the computer's Administrative Tools

a Right click on Apple WebObjects Taskd and select "Restart"

b Right click on Apple WebObjects Java Monitor and select "Restart"

6 Ensure that there is only one "primary" Hub configured within the `AdminConfig.plist`. file, located at `\Telescope\Applications\tsadmin.woa\Contents\Resources`. Configure the value for "hubHost" so that it points to the IP Address or the Machine Name of your Hub Server, as follows:

```
"Hubs" = (
     {
          "primary" = "Y";
          "hubHost" = "HUB_SERVER";
```

```
        "hubPort" = "12345";
        "displayName" = "PRIMARY";
    }
```

Additional Checks on the Web Server

1. From the Registry Editor, navigate through to the following path:

   `\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apple\WebObjects\Configuration`

   Set the Data value for CONF_URL to point to the IP Address or Machine Name of your Web Application Server, as follows:

   `http://WEB_APP_SERVER:1085`

2. In the case of an upgrade installation and depending on the set up of the folder structure, you may be required to manually move Telescope Web Images from the default installation directory (`C:\inetpub\wwwroot\`) to the specific image folder.

3. Configure IIS. (See Section 6.1, "Configure for Launching the WebObjects Monitor," on page 60.)

9.2 Miscellaneous Troubleshooting

9.2.1 404 Errors for Telescope Uploader or Other Web Applications

If you cannot download the Drag and Drop plugins in Windows browsers and receive a 404 Error, ensure handler mappings are only enabled for the Scripts directory.

In particular, in IIS Manager, navigate to [Machine_Name] > Sites > Default Web Site > tsweb > default > BrowserPlugins and ensure the handler mappings are not enabled for this folder.

For information on handler mappings, see Section 6.1.4, "Configure Handler Mappings for the IIS Folders," on page 64.

Also, ensure that Java is enabled on your Windows machine. (If Java is blocked, web applications cannot be accessed.)

9.2.2 Content Search does not work with WHERE clause (Oracle)

When an Oracle Database is used at the backend, a content search may not return any results if a specific usergroup has a where clause specified. (The TSWeb log file will contain SQL Exceptions such as “invalid identifier”, “missing parenthesis”, and so on.) This situation typically occurs after an upgrade.

Workaround:

Run the following commands on the Oracle database for the Telescope database:

```
drop index ft_on_tx
create index ft_on_tx on ft_contents (ft_text) indextype is ctxsys.context
```

9.2.3 Server names with special characters not supported

If the Telescope server is installed on a machine with a name that includes an underscore (_) or other special characters, the server may not be accessible from Internet Explorer browsers. In some situations, it may also be unavailable for SSL configurations.

Workaround:

Do not install Telescope on a machine that has special characters in its name. If Telescope is already installed on such a machine, avoid Internet Explorer and use a different browser (such as Firefox).

9.2.4 Client gets "Session expired" when routing through Blue Coat Proxy

When routing through BlueCoat Proxy, a "Session expired" message is received immediately after logging in.

Workaround:

1. Add the following CPL code to the proxy policy:

   Configuration -> Policy -> Policy Files — Install Local File From: Text Editor –> Install

2. Add the following text in the text editor window:

```
<Cache> url.domain= telescopeondemand.com webpulse.categorize.mode(none)
```

3 Click *Install*.

9.2.5 Video assets do not play in Preview (QuickTime) using Firefox

The Windows Media Player does not work properly under Firefox Versions 21 and 22 browser. This may prevent the preview of video files such as mov, mp4, or m4v files in Telescope.

Workaround:

Change the Firefox setting “plugins.load_appdir_plugins” to true. For details, go to https://support.mozilla.org/en-US/kb/windows-media-or-other-plugins-stopped-working.

9.2.6 “Trust anchor missing” error in TSWeb logs

If there is a 'trust anchor missing parameter' error appearing in TSWeb logs, you need to install certificates in the “truststore”, that is, the Java CA Certificates Store and the Windows default certificate store.

Search the internet for more information; for example, go to the Microsoft website.

This error does not affect the operation of downloads, uploads, or any other feature.

9.3 Add License Keys

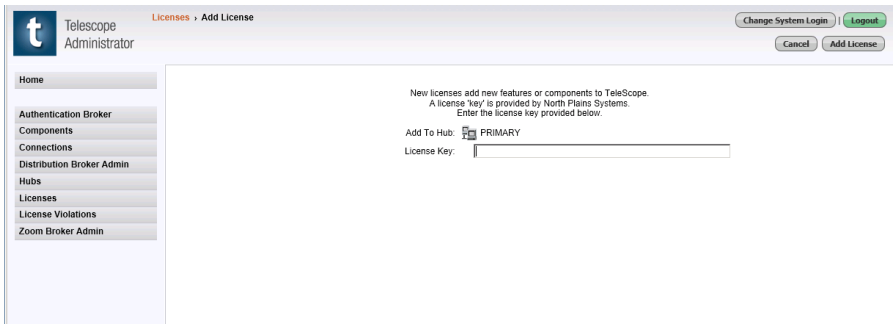
NOTE: If you used the -l option to apply the license keys during Telescope installation, this section is not required. Follow this section only if you did not use the -l option during the installation and need to manually add license keys.

To use any individual Telescope component, you must have purchased a license key. These license keys are all stored in a standard text file which includes the Master key and all purchased subkeys. Have this file ready before you start these steps.

To license Telescope components:

1. Start the WebObjects Monitor, click TSAdmin (Telescope Administrator), and log in to administer the System.
2. In the Telescope Administration page, click *Licenses* in the navigation pane.
3. In the Licenses panel, click *Add License*.
4. In the License file, copy a license key, the alpha-numeric string in between the square [] brackets.
5. Paste the key into the *License Key* field.

Figure 9.1 *Add License*



6. Click *Add License.*

   If the license key is correct and valid, the new license is added to TeleScope Administrator and appears in the Licenses panel.

7. Click *Add License* and repeat the above procedure for every license you need to add.

For More Information

For more information about license keys used in Telescope Administrator, see the *Telescope Administrator's Reference Manual*.

9.4 Update the Master License Key

If any of the following situations happen, you must obtain a new master key from North Plains Systems and update the Hub with the new key.

- The network card of the computer is changed.
- The master key needs to be applied to a different network card in a multiple-card computer.
- A temporary master key has expired.

When you have obtained the new key, follow these steps to update the Hub:

1. Stop all Telescope applications using WebObjects Monitor.
2. Turn autorecover off for all Telescope applications using WebObjects Monitor.
3. Select *Start > Administrative Tools > Services*.
4. Manually stop all NPS services (as applicable to your installation), in the following order:
   a. NPS Interoperability Broker
   b. NPS Zoom Builder
   c. NPS Zoom Broker
   d. NPS Distribution Broker
   e. NPS Ingest Broker
   f. NPS Graphics Broker
   g. NPS Lookup Broker
   h. NPS Child Indexing Broker
   i. NPS Indexing Broker
   j. NPS Jetty-Service
   k. NPS Message Broker
   l. NPS NTFS File Broker
   m. NPS Authentication Broker
   n. NPS Connection Broker
   o. NPS State Broker
   p. NPS Session Broker
   q. NPS Name Server

NOTE: You must stop all NPS brokers on all computers.

5 Open a DOS window (cmd) on the computer on which the Telescope Hub is installed and navigate to the Telescope directory (where the sesb.exe file is located, usually the Telescope installation directory) and delete the sesb.dat file. Then run:

```
sesb -remaster <new master key>
```

where <*new master key*> is the new master key string.

6 Manually start **only** the these NPS services in the following order:

   a NPS Name Server

   b NPS Session Broker

   c NPS State Broker

   d NPS Connection Broker

   e NPS Authentication Broker

7 Log in to TSAdmin (Telescope Administrator) as 'sysadmin' and add all the individual licenses from the license text file. (See Section 9.1, "Add License Keys," on page 123.)

8 Manually stop (in reverse order) the NPS services listed in step 6. That is:

   a NPS Authentication Broker

   b NPS Connection Broker

   c NPS State Broker

   d NPS Session Broker

   e NPS Name Server

9 Manually start all NPS services (as applicable) in this order:

   a NPS Name Server

   b NPS Session Broker

   c NPS State Broker

   d NPS Connection Broker

   e NPS Authentication Broker

   f NPS NTFS File Broker

   g NPS Message Broker

   h NPS Jetty-Service

   i NPS Indexing Broker

j NPS Child Indexing Broker

k NPS Lookup Broker

l NPS Graphics Broker

m NPS Ingest Broker

n NPS Distribution Broker

o NPS Zoom Broker

p NPS Zoom Builder

q NPS Interoperability Broker

10 Restart all the Telescope applications using WebObjects Monitor.

NOTE: If the command fails, close the cmd window, set the compatibility mode of sesb.exe to “Windows Server 2003” and select the “Run as Administrator” option, then repeat the steps above.

9.5 Contact Customer Service

North Plains Systems strives to make its software powerful, intuitive and easy to use. This includes allocating significant resources to Research & Development and Technical Support. If you have any questions or suggestions for improving our software, we will be pleased to assist you.

You can email a Customer Service Representative with your questions or comments to support@northplains.com

Security Considerations

Chapter 10: Configure SSL for Downloads

It is recommended that organizations use a Secure Sockets Layer (SSL). SSL uses Secure Certificates to provide security by encrypting communications between web application servers and visitors to your website.

Secure configuration should include reverse proxy for downloads so that the Download Manager is configured to download files securely.

In this Chapter:

- Section 10.1, "Configure SSL for Downloads," on page 131
- Section 10.2, "Set Up Reverse Proxy for Downloads (Using Microsoft ARR)," on page 139

See Also:

- Section Chapter 12:, "Configure LDAP," on page 160

10.1 Configure SSL for Downloads

NOTE: Before you proceed with the following steps, Telescope must already be installed and working.

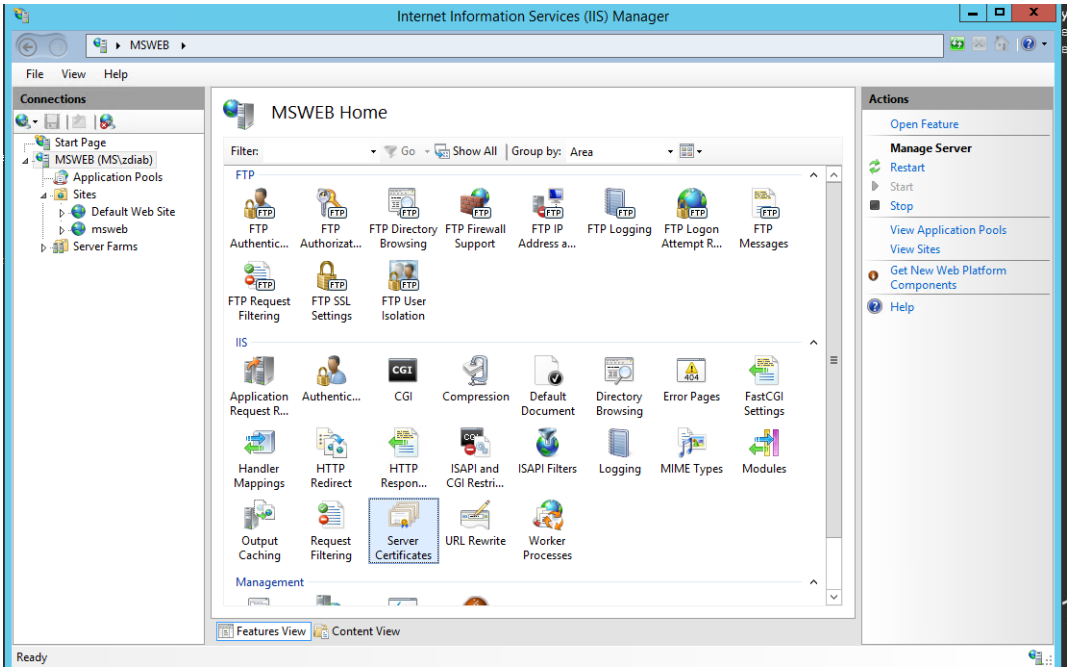
- Section 10.1.1, "Prerequisites," on page 131
- Section 10.1.2, "Install the Certificate on the Web Server," on page 131
- Section 10.1.3, "Add the Site Binding," on page 134
- Section 10.1.4, "Configure plist Files," on page 136
- Section 10.1.5, "Restart and Verify," on page 138
- Section 10.1.5, "Restart and Verify," on page 138

10.1.1 Prerequisites

- For Windows, the web server uses Internet Information Services (IIS). Apache is not supported on Windows.
- The web server is SSL-enabled
- A valid SSL certificate is required. The SSL certificate must be fully signed and come from a known source with commercial root signing authority (for example, COMODO). For installation instructions, see Section 10.1.2, "Install the Certificate on the Web Server," on page 131
- Microsoft Internet Information Services (IIS) Application Request Routing (a Windows reverse proxy application) is required. Installation/configuration steps are provided in Section 10.2, "Set Up Reverse Proxy for Downloads (Using Microsoft ARR)," on page 139.

10.1.2 Install the Certificate on the Web Server

1. Open Internet Information Services (IIS) Manager.
2. Double click the web server's name.
3. Double click on the *Server Certificates* icon.



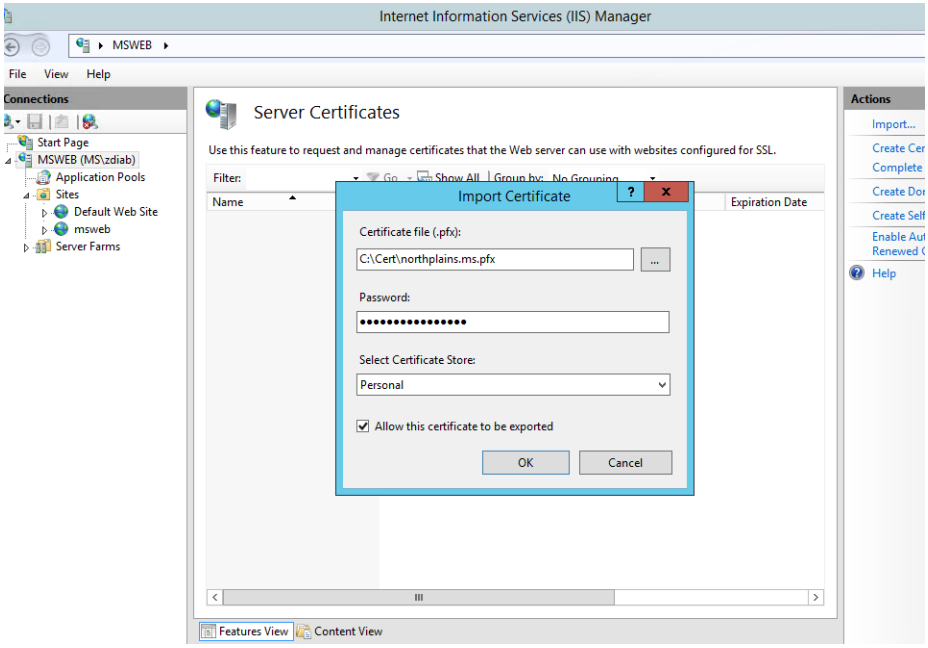
4 The Server Certificates panel appears.

5 Click the *Import* link in the right panel.

6 Click the three dots beside the Certificate file (.pfx) field to browse to the certificate file in its path location. It must be a PFX file.

7 Specify the password and select the certificate store.

8 Click *OK* to import the certificate.



9 Leave the IIS window open while you complete the next steps to verify the SSL certificate in the next section.

Verify the SSL Certificate

To view details about the certificate you installed on the web server:

1 Find the Encrypting File System window in your Control Panel (search for this window from your system's search facility).

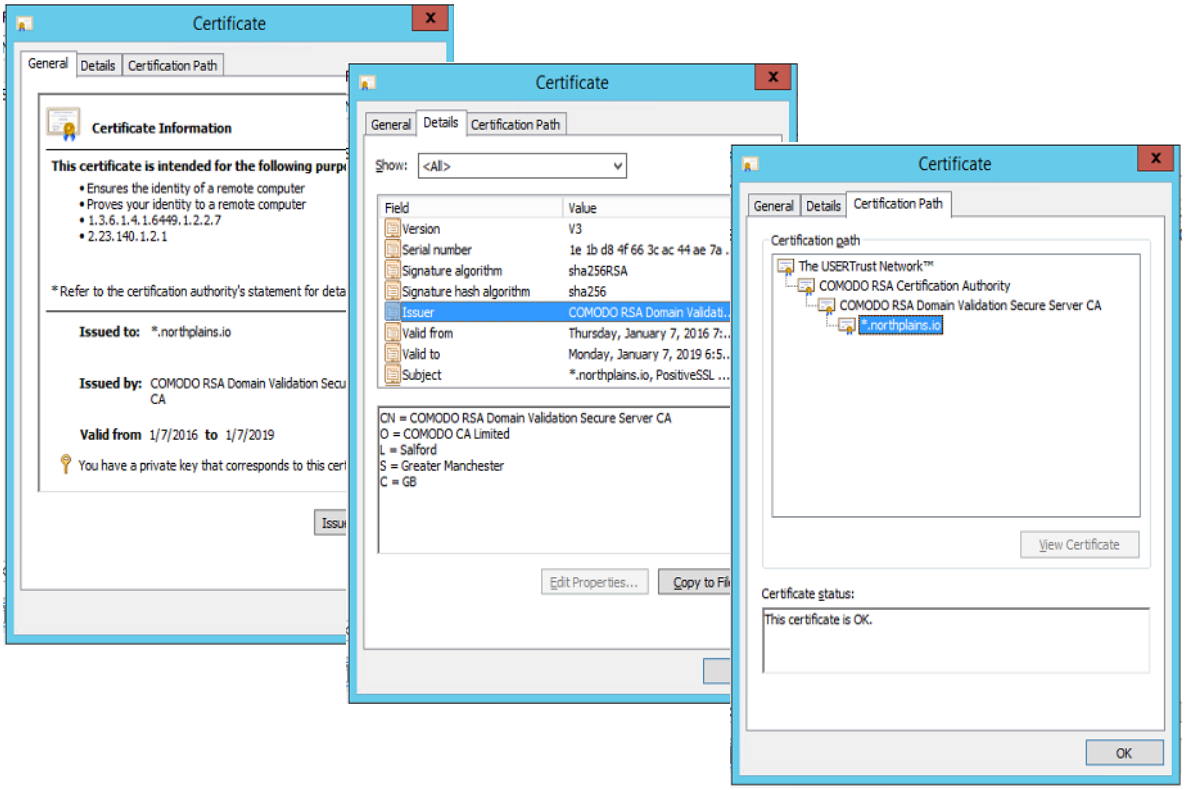
2 Click the *View certificate* button.

3 The Certificate properties window should show the following:

General tab: Verify the certificate comes from the expected source with commercial root signing authority (for example, COMODO).

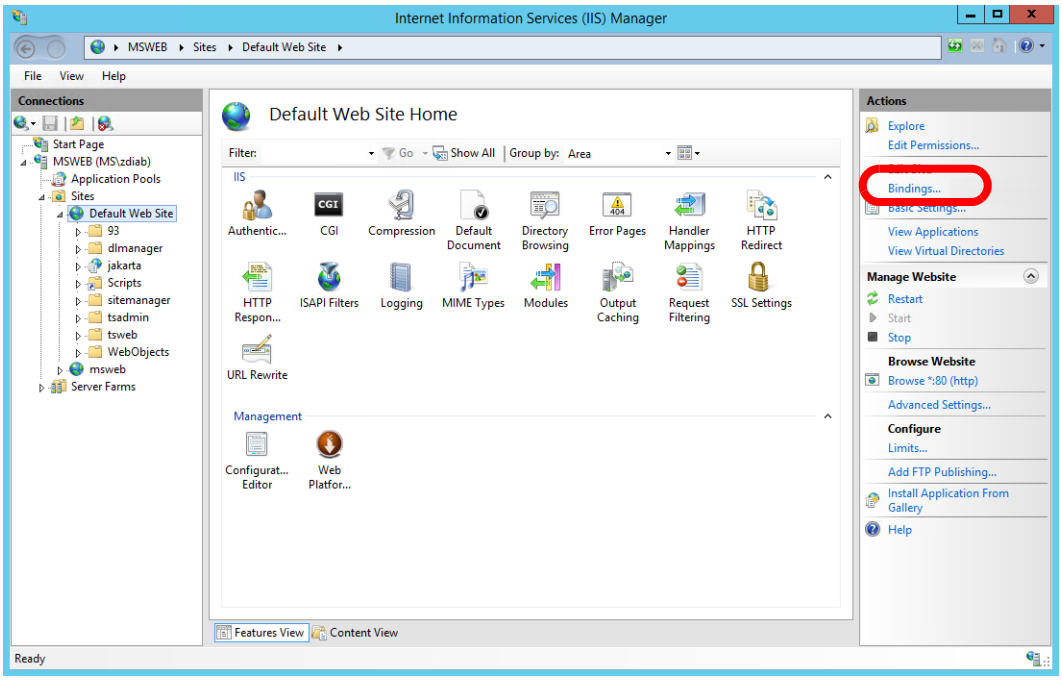
Details tab: This tab gives you more details on the Issuer.

Certification Path tab: The Certification Path must be accessible and the Certificate status should read, "This certificate is OK".

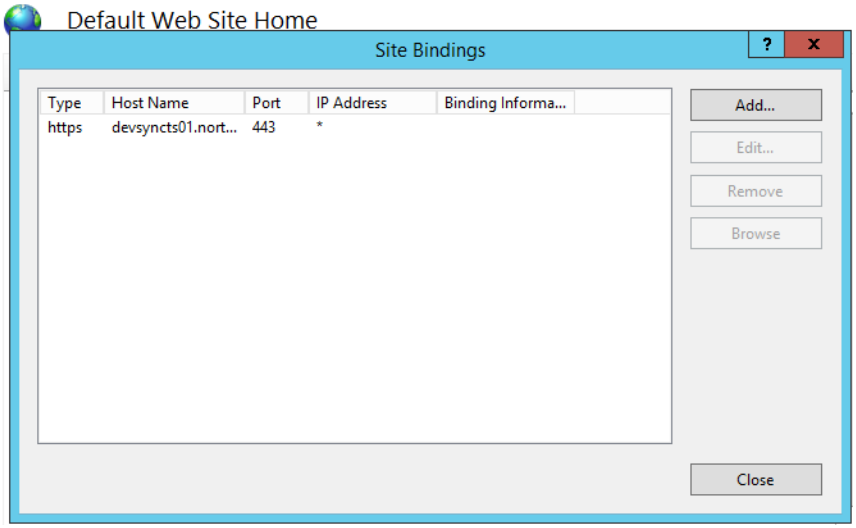


10.1.3 Add the Site Binding

1. Return to the IIS window you used to install the certificate.
2. In the tree structure in the left panel, navigate to *Sites* > *Default Web Site (for web server)*. The Default Web Site Home panel appears.
3. Click on *Bindings* in the *Actions* tab on the right-hand side.

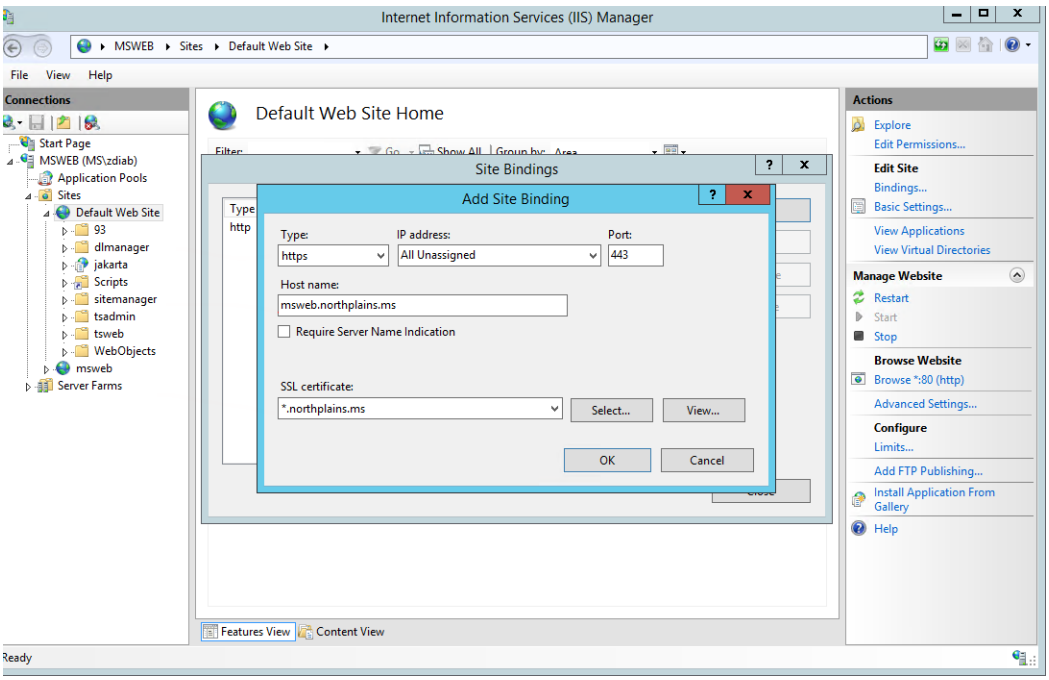


The Site Bindings panel appears.



4 Click the *Add* button.

5 In the Add Site Binding panel, set *Type* to “https” and *Port* to “443”. Specify your Host Name, select the SSL Certificate, then click *OK*.



6 Click OK again to save your Site Bindings changes.

7 Restart the IIS service. (Restart, under the Manage Website section in the right panel.)

8 Go to the WebObjects Monitor.

9 Click the Site tab.

10 In the URL to Adaptor field, change the URL from “http” to “https.” Also, update the URL to be the host name from step 5 above and not the local web server name. Then click the *Update HTTP Adaptor URL* button.

10.1.4 Configure plist Files

1 Stop all instances of TSAdmin, TSWeb, DLManager, and Site Manager. Go to the WebObjects Monitor and follow these steps for each of TSAdmin, TSWeb, DLManager, and SiteManager:

   a Click the Detail View button for the applications.

   b Stop every instance.

2 On the web application server, use a text editor to open each of the info.plist and config.plist files listed below. Ensure the listed values use “https” as shown (NOT “http”).URLs should be set to use the host name associated with the SSL certificate (from step 5 in the previous section). Save and close the files when finished with each one.

NOTE: It is highly recommended that you use SSL for all external communication. If you are setting up an internal environment for testing or development and are not using SSL, you can replace “HTTPS” with “HTTP” in all places below. (In other words, remove the “S” if you are not using SSL, but this is not recommended.)

Legend:

[WEB_SERVER_HOST] – The server where the web server software (ISS) is installed. Use a fully qualified domain name or IP address. Do not use the local server name; instead, use the host name associated with the SSL certificate.

[WEB_APPLICATION_SERVER_HOST] – The server where the WebObjects software is installed. The DLManager should also run on this server. This server might be the same as the web server host (but this is not recommended). Use a fully qualified domain name or IP address.

NOTE: If the WEB_SERVER_HOST and the WEB_APPLICATION_SERVER_HOST are on the same server, then use the WEB_SERVER_HOST name in the configuration below.

In this file (in C:\Telescope\Applications by default)	**The following keys should be:**
TSAdmin info.plist: ...\tsadmin.woa\Contents\info.plist	<key>protocol</key> <string>https://</string>url <key>url</key> <string>https://[WEB_SERVER_HOST]]/[your_path_to_images]</string>
TSWeb info.plist ...\tsweb.woa\Contents\info.plist Note: exitURL may not need to be set	<key>dlManager</key> <string>https://[WEB_SERVER_HOST]/Scripts/WebObjects.dll/DLManager.woa/wa/download</string> <key>dlManagerVideo</key> <string>https://[WEB_SERVER_HOST]/Scripts/WebObjects.dll/DLManager.woa/wa/downloadNow</string> <key>protocol</key> <string>https://</string> <key>exitURL</key> <string>https://[WEB_SERVER_HOST]/Scripts/WebObjects.dll/TSWeb</string> <key>url</key> <string>https://[WEB_SERVER_HOST]/[your_path_to_images]</string>

TSWeb config.plist ...\tsweb.woa\Contents\Resources\Config.plist	HostURL = "https://[WEB_SERVER_HOST]"; internalSpacerImage = "https://[WEB_SERVER_HOST]/tsweb/default/common/spacer.gif"; externalSpacerImage = "https://[WEB_SERVER_HOST]/tsweb/default/common/spacer.gif";
Site Manager info.plist ...\sitemanager.woa\Contents\info.plist	<key>url</key> <string>https://[WEB_SERVER_HOST]/[your_path_to_images]</string>
DLManager info.plist ...\dlmanager.woa\Contents\info.plist **Notes:** 1. DO NOT use “https” for the protocol key. 2. You may want to take the time to make the additional changes required for Reverse Proxy. See Section 10.2.5, "Configure DLManager for ARR," on page 145	<key>protocol</key> <string>http://</string> <key>http_host</key> <string>https://[WEB_APPLICATION_SERVER_HOST]</string> <key>http_video_host</key> <string>https://[WEB_APPLICATION_SERVER_HOST]</string> <key>url</key> <string>https://[WEB_SERVER_HOST]/[your_path_to_images]</string>
DLManager Config.plist ...\dlmanager.woa\Contents\Resources\Config.plist	HostURL="https://[WEB_SERVER_HOST]";

10.1.5 Restart and Verify

All Telescope instances must be restarted again. Go to the WebObjects Monitor and follow these steps for each of TSAdmin, TSWeb, DLManager, and SiteManager:

1. Click the Detail View button for all services.
2. Start every instance.
3. Verify you can access the HTTPS URLs for TSAdmin and TSWeb.

Users may need to install the certificate on their local browser and assign it to the Trusted Authority Storage. Make sure there are no errors when the site is accessed; otherwise, asset download and video manager playback will not work.

10.2 Set Up Reverse Proxy for Downloads (Using Microsoft ARR)

10.2.1 What is Reverse Proxy?

It is recommended that you use reverse proxy HTTPS communication routing between web clients and embedded HTTP servers for more secure HTTPS downloads.

Client requests with specific patterns are redirected to the internal HTTP port but responses are delivered through the standard HTTP port. For example, all requests with the pattern “http://172.16.3.242/dlm:12103/” are redirected internally to “http://172.16.3.242:12103”.

The reverse routing from port 12103 performs the response to the client from /dlm:12103/ Therefore we retain the ability to communicate with the internal HTTP server through ports 80 or 443 only.

10.2.2 Set Up Microsoft ARR (Overview)

For reverse proxy on Windows, use Microsoft Internet Information Services (IIS) Application Request Routing (ARR) Server Farm and URL Rewrite rules to establish HTTP communication between the client and the embedded HTTP server of DLManager.

Prerequisites

- Section 10.1, "Configure SSL for Downloads," on page 131

Steps

The following steps are detailed in this section:

1. Section 10.2.3, "Determine the Embedded Port Number," on page 139
2. Section 10.2.4, "Configure IIS to Route All Requests Through ARR," on page 140
3. Section 10.2.5, "Configure DLManager for ARR," on page 145
- Section 10.2.6, "Troubleshooting Microsoft ARR," on page 147

10.2.3 Determine the Embedded Port Number

Before you start, make sure DLManager is up and running and you can use it to perform basic download and video previews.

A prerequisite to reverse proxy configuration is to determine the port number of the embedded HTTP server. This embedded HTTP server uses embedded Apache Tomcat (which is installed at the time DLManager is installed).

On the Web Application Server:

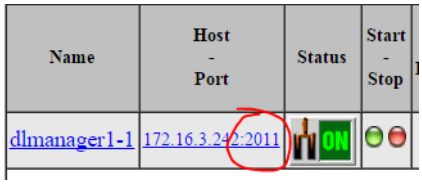
1. In the DLManager installation directory on the web application server machine, navigate to the `info.plist` file located in:

   `.../Telescope/Applications/dlmanager.woa/Contents`
2. Find the `port_threshold` key:

```
<key>port_threshold</key>
<string>10100</string>
```

3 Go to WebObject Monitor and open details of DLManager to see the port number:

Figure 10.1 *DLManager host port number*



4 Take this port number and add it to the number from the `port_threshold` string in step 2 above.

Based on the above, the DLManager HTTP port is 10100 + 2011 = 12111

So the embedded HTTP port for our example is 12111.

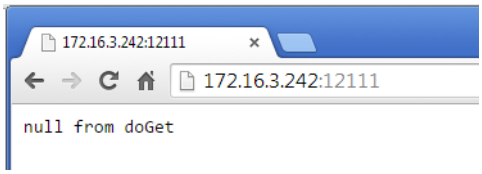
5 To make sure you have the correct HTTP port, open a browser accessible on your network and use the port number you calculated along with the DLManager IP address or host name:

http://[my_server]:12111

For example, http://172.16.3.242:12111

6 The browser should respond with a plain text error. (Otherwise, it will report the web page can't be found.)

Figure 10.2 *Plain text response is shown when the web application server URL and HTTP port number is correct*



10.2.4 Configure IIS to Route All Requests Through ARR

Important! Before you start these instructions, be sure you have completed the steps in Section 10.2.3, "Determine the Embedded Port Number," on page 139 and have the port number of the embedded HTTP server handy.

On the Web Server:

1 Install the Microsoft Application Request Routing (ARR) extension for IIS. You can download it from the following URL:
http://www.iis.net/downloads/microsoft/application-request-routing

If the Web Server does not have Internet access, use the following link to find out how to install ARR manually:

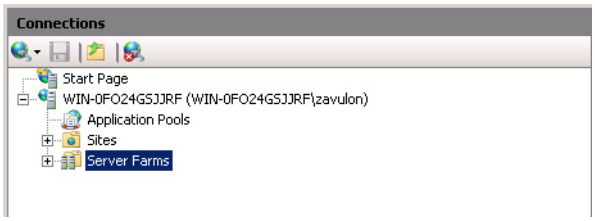
https://blogs.technet.microsoft.com/erezs_iis_blog/2013/11/27/installing-arr-manually-without-webpi/

2 After you install ARR, restart IIS management console. (Click *Start* > *Administrative Tools* > *Internet Information Services (IIS) Manager*.)

NOTE: You must start IIS from its own management console as described above, and not restart it from the Services panel.

3 Expand the server in the console and you should see a new configuration option: Server Farms.

Figure 10.3 *Server Farms Configuration Option*



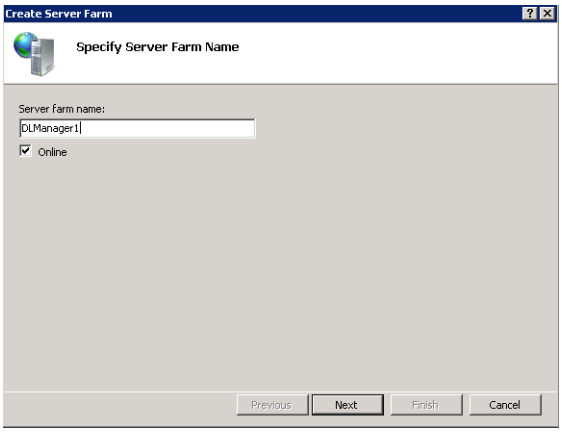
4 You need to create a separate server farm for each DLManager instance:

a Right-click on *Server Farms* and select *Create Server Farm* from the menu.

b Type the name of the new Server Farm.

For the first DLManager instance, type DLManager1. For the second, you will type DLManager2, and so on, for each DLManager instance you have, because each instance requires a distinct server farm.

Figure 10.4 *Specify Server Farm Name*



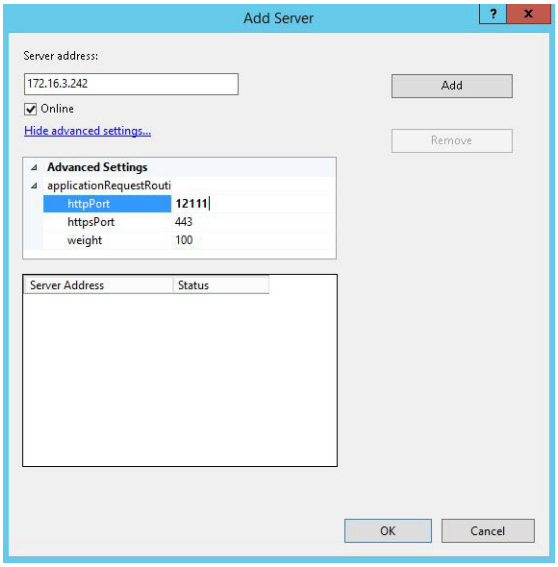
c Click the *Next* button.

d Type the web application server address, WEB_APPLICATION_SERVER_HOST. This is the internal IP address or fully qualified domain name of the application server host where DLManager is running.

e Click the *Advanced settings* link (if it's not already expanded).

f Expand the *Advanced Settings* entry.

Figure 10.5 *Server Farm, Advanced Settings*

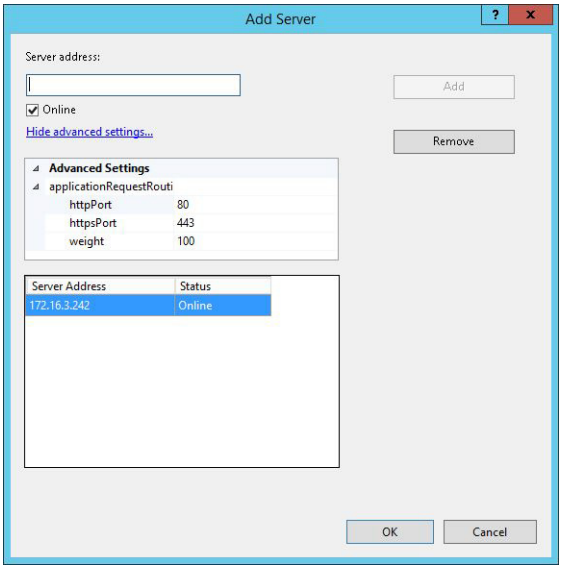


g Type the embedded port number (12111) in the *httpPort* field. (You calculated this value in the previous section, Section 10.2.3, "Determine the Embedded Port Number," on page 139.)

h Click the *Add* button.

The new server address should appear with “online” status in the bottom list.

Figure 10.6 *Specify Ports*



i Click *OK*.

j Click *Finish*.

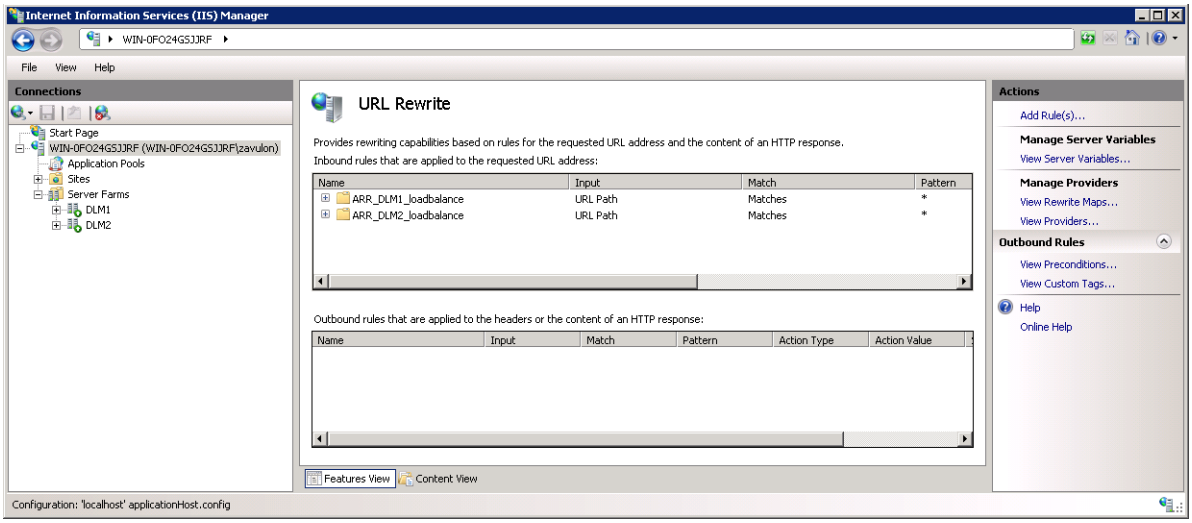
k A pop-up window appears asking you to allow rules. Click *Allow.*

l Repeat the above steps for each DLManager instance in your Telescope environment.

5 From the IIS management console, open the URL Rewrite options to configure the rules for parsing URL patterns.

Because you have configured one Server Farm for each instance, you should see pre-defined rules for each Server Farm you created.

Figure 10.7 *URL Rewrite*



6 Double-click on the first rule to edit the Rule Configuration.

7 Expand the *Conditions* section.

8 Select *Match Any* in the Logical grouping dropdown.

9 Click *Add* to add the new Condition. The Edit Condition window appears. Use the following values:

Condition Input:

{HTTP_HOST}{REQUEST_URI}

Check if input string:

Matches the Pattern

Pattern:

*[WEB_SERVER_HOST]*DLM*

This IP address or fully qualified domain name should match the external IP address or external fully qualified domain name of the web server (use the host name associated with the SSL certificate).

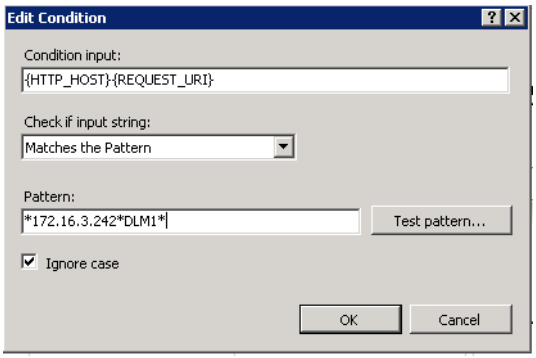
For example:

*172.16.3.242*DLM1*

NOTE: If you have multiple servers with names that can't be differentiated with the wildcard characters (for example, "DLM1" and "My_DLM1" would both be identified with "*DLM1") you will need to add the port numbers

to the pattern. See the troubleshooting section, Section , "Add Port Numbers Information to Patterns to Differentiate between Server Names," on page 148.

Figure 10.8 *Edit condition*

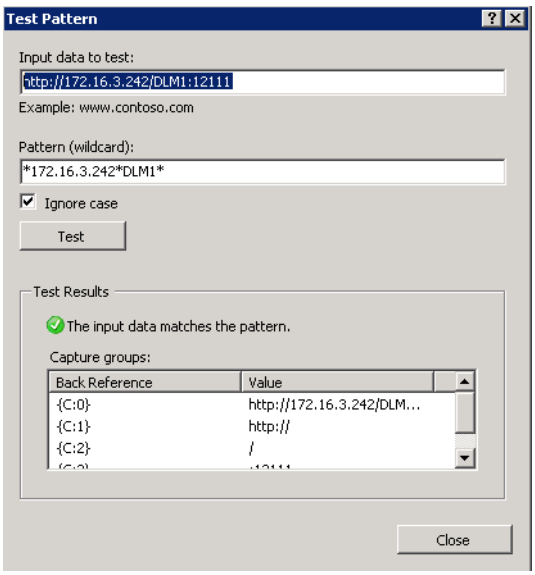


NOTE: The "DLM1" in the example above is taken from and should match the HTTP_HOST and HTTP_VIDEO_HOST settings in the DLManager `info.plist` file.

10 You can test the pattern to see if the logic is performed.

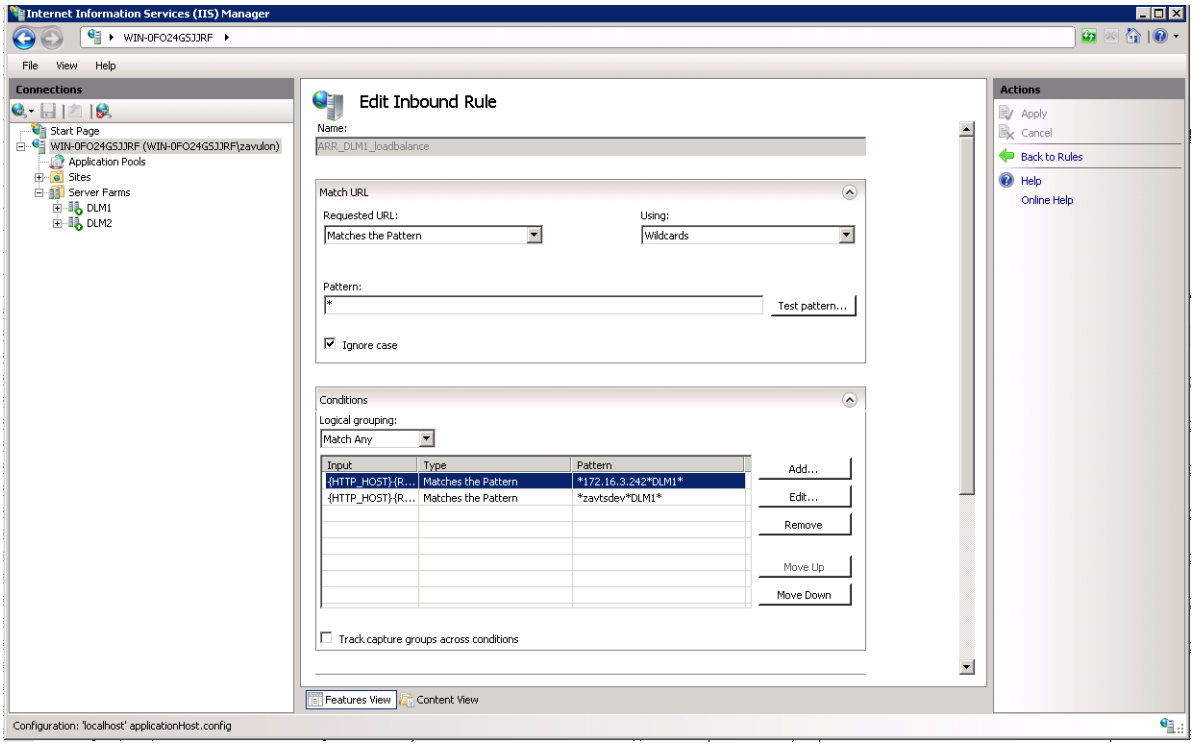
Click Test Pattern, then type (for example) `http://[WEB_APPLICATION_SERVER]/DLM1:12111` in the *Input data to test* field.

Figure 10.9 *Test Pattern*



11 If you are observing the correct behavior, close the Test Pattern window and click *OK* to create a new rule.

Figure 10.10 *Edit inbound rule*



12 Click *Apply Action* to save the rule.

13 Repeat the same configuration for each rule of the Server Farm.

14 Restart IIS when done.

10.2.5 Configure DLManager for ARR

Changes are required in the DLManager `info.plist` file. When finished making your changes, restart the DLManager instance.

NOTE: You may make these changes earlier in the process, at the same time you were making other plist changes for SSL configuration. See Section 10.1.4, "Configure plist Files," on page 136.

In this file (in C:\Telescope\Applications by default)	The following keys should be:
DLManager info.plist ...\dlmanager.woa\Contents\info.plist	<key>protocol</key> <string>http://</string> <key>http_host</key> <string>https://[WEB_APPLICATION_SERVER_HOST]/DLM1</string> <key>http_video_host</key> <string>https://[WEB_APPLICATION_SERVER_HOST]/DLM1</string> <key>url</key> <string>https://[WEB_SERVER_HOST]/DLM1</string>

Notes:

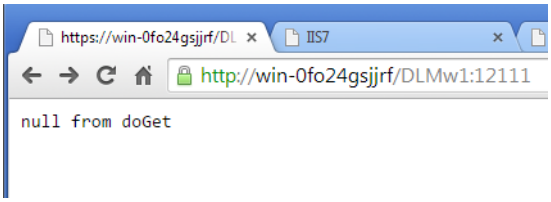
- DO NOT use "https" for the protocol key.
- You must add a unique DLManager identifier (the "`/DLM1`" in the examples above) for each instance. Use an identifier name that different from the application name to make it easier to distinguish for the rewrite rules. This identifier must match the one added to the Pattern above.
- Use the URL pattern you configured in the Inbound URL rewrite rule. For example, if the rule is *172.16.3.242*DLM1* (where "172.16.3.242" represents the external IP address or external fully qualified domain name of the Web Server), then the `http_host` key should be:

```
<key>http_host</key>
<string>http://172.16.3.242/DLM1</string>
```

To test success:

If everything is configured correctly you should be able to place the `http_host` key URL plus the port number into the browser and see the same response as in Section 10.2.3, "Determine the Embedded Port Number," on page 139:

Figure 10.11 *Test Pattern*



If you see the null message, the download will work through ports 80 or 443.

10.2.6 Troubleshooting Microsoft ARR

Use appcmd to see Full Configuration

If the server routing is not performing correctly, check the Server Farm configuration using the `appcmd` command, located at `%windir%\system32\inetsrv`:

```
>cd %windir%\system32\inetsrv
>appcmd list config /section:webFarms
```

The `appcmd` result outputs the full Server Farm configuration for all configured farms:

```
<webFarms>
    <applicationRequestRouting>
        <hostAffinityProviderList>
            <add name="Microsoft.Web.Arr.HostNameRoundRobin" />
            <add name="Microsoft.Web.Arr.HostNameMemory" />
        </hostAffinityProviderList>
    </applicationRequestRouting>
<webFarm name="DLM1" enabled="true">
    <applicationRequestRouting>
        <protocol>
            <cache />
        </protocol>
        <healthCheck />
        <affinity>
        </affinity>
        <loadBalancing />
    </applicationRequestRouting>
    <server address="zavtsdev" enabled="true">
        <applicationRequestRouting httpPort="12111" />
    </server>
</webFarm>
<webFarm name="DLM2" enabled="true">
    <applicationRequestRouting>
        <protocol>
            <cache />
        </protocol>
        <healthCheck />
        <affinity>
        </affinity>
        <loadBalancing />
    </applicationRequestRouting>
    <server address="zavtsdev" enabled="true">
        <applicationRequestRouting httpPort="12112" />
    </server>
</webFarm>
</webFarms>
```

Use this output to check that all addresses and required ports are configured correctly.

If any configuration is missing, you can add it using the same `appcmd` command. Use the following command to see the list of options available:

```
>appcmd.exe set config -section:webFarms -?
```

For example, to set the port number for specific Server Farm, use:

```
>appcmd.exe set config /section:webFarms /"[name='DLM2'].[address='zavtsdev']".httpPort:12112
```

Add Port Numbers Information to Patterns to Differentiate between Server Names

This section provides steps on how to add port number information to condition patterns, in order to differentiate between server names. For more information on the steps to define patterns in the Edit Condition window, go to Section 10.2.4, "Configure IIS to Route All Requests Through ARR," on page 140

- Example for when port number information is not required because the patterns can be differentiated:

  ```
  *172.16.3.242*DLM1*
  *172.16.3.242*DLM2*
  ```

- Example for when port number information is required because the wildcards in the patterns mean the names cannot be differentiated and the two servers may be confused on startup:

  ```
  *172.16.3.242*DLM1*
  *172.16.3.242*My_DLM1*
  ```

  ("*DLM1" could include "My_DLM1")

Ideally, you should use server names that will be clearly differentiated despite wildcards. However, if the host names have already been defined, you can include the sum of the port threshold with the respective port numbers in the pattern entry, as described in the following steps. The example above, with server names "DLM1" and "My_DLM1," is used to illustrate.

1. Find the port_threshold value in the DLManager `Info.plist` file, located at `...\dlmanager.woa\Contents\info.plist`. For example,

   ```
   <key>port_threshold</key>
    <string>10100</string>
   ```

2. In WebObjects Monitor, find the port number used by each of the DLManager hosts. These are shown in the Host-Port column. For example, DLM1:2003 and My_DLM:2005

3. Include the sum of the port threshold value with the respective port number in the patterns. For example:

   For DLM1, 10100+2003=12103 to make the pattern:

   ```
   *172.16.3.242*DLM1*12103*
   ```

   For My_DLM1, 10100+2005=12105 to make the pattern:

   ```
   *172.16.3.242*My_DLM1*12105*
   ```

Chapter 11: Configure Web Security Features

Cross Site Scripting (XSS) introduces some vulnerabilities that, if appropriate precautions are not taken, could potentially have a serious impact on business security if exploited by malicious parties.

Northplains installs security features to protect against various types of XSS security attacks. This section describes these attacks, and how users can configure the security features to suit their Telescope environment.

In this Chapter:

- Section 11.1, "What are XSS Security Attacks?," on page 150
- Section 11.2, "Change XSS Configuration," on page 152

11.1 What are XSS Security Attacks?

XSS security attacks occur when malicious scripts are injected into trusted web sites. The malicious party sends ("injects") XSS code to the web site, where it is stored and later sent on to an unsuspecting user. Because the malicious script is sent from and runs from a trusted source, the user's browser executes the script and grants it access to cookies, session tokens, and other sensitive information retained by the browser and used with that site.

11.1.1 Types of XSS Security Attacks

The following types of XSS security attacks have been addressed by Telescope:

Stored XSS Attacks

In this type of attack, injected code is permanently stored on target servers, such as in a database, a message forum, visitor log, or comment field. The unsuspecting user retrieves malicious script from the server when making a request for the stored information.

Reflected XSS Attacks

In this type of attack, injected code is reflected off the web server, through an error message, search result, or other response that includes malicious code sent to the server as part of the request. Reflected attacks are delivered to unsuspecting users via an out-of-bounds route, such as in an e-mail message or chat client. If the user is tricked into clicking on a malicious link or submitting a specially crafted form, the injected code travels to the vulnerable web server, which reflects the attack back to the user's browser.

Phishing attacks

An HTTP parameter submitted to the server may contain a URL value designed to cause the web application to redirect the request to a specified URL. By modifying the URL value to point to a malicious site, an attacker may successfully launch a phishing scam where the unsuspecting user is redirected to an untrusted page that contains malware.

No bounds checking

If large character strings are allowed on input, they provide attackers with the space they require to inject long and complex scripts to deliver XSS attacks. Unlimited character buffers on the server also provide the potential for buffer overflow attempts against servers, applications and clients.

11.1.2 Telescope Security Features

Telescope uses following security features to counter XSS security attacks.

Regular Expression (RE) blacklisting

For every input text field, validation scripts automatically check for characters and patterns that may indicate strings that could contain attacks. Such attacks could include SQL commands, file inclusions, HTTP code, URLs, commented code, and so on.

If such strings are found, they are "blacklisted"; the user request is ignored. See the next section for details on the blacklisted strings and how to configure them.

Password requirements

Telescope passwords now require at least 6 characters, including one digit, one character, and one special character. See the next section for details on how to change these defaults or remove this requirement.

Bounds limits

Bounds limits have been added according to the Telescope data model. These limits cannot be changed, except for the custom side bar width. (To change the custom side bar width, which is 32 characters by default, update the "CustomPanelLength" variable in the Home.strings file, located at `.../tsweb.woa/Contents/Resources/`.)

11.2 Change XSS Configuration

The default XSS security configuration is added automatically when you install Telescope. (If you configured XSS security settings in a previous release, your settings are preserved when you upgrade.)

We recommend that you do not change the default configuration provided by Telescope. However, if your organization uses special characters in filenames or XSS commands or has special password requirements, you may need to change the code as described in this section. **To ensure accuracy, please contact North Plains Customer Support before proceeding with your changes.**

11.2.1 Default XSS Code Example

XSS configuration is defined in the `blackList` and `passwordPolicy` sections in the following files, located on the web application server:

- `site.plist`, which sets TSWeb configurations and is located within the `...\Telescope\Applications` folder. If you have multiple sites, this code should be included in each site definition.
- `Config.plist` (for TSAdmin), which sets TSAdmin configurations and is located within the `...\TeleScope\Applications\tsadmin.woa\Contents\Resources` folder on the Web Application server.

The following `site.plist` code example shows the configuration code for these sections.

```
{
"sites" = (
   {
          "sitename" = "default";
          "sysadmin" = "true";
          "connections" = (
          "1",
          );

 "blackList" = (
     {
           NAME = "XSS_SCRIPT";
           REG_EXP = "(((\\%3C)|<)((\\%2F)|/)*[a-z0-9\\%]+((\\%3E)|>)";
           REQUIRED = "Y";
     },
     {
          NAME = "XSS_IMA";
          REG_EXP = "(((\\%3C)|<)((\\%69)|i|(\\%49))((\\%6D)|m|(\\%4D))((\\%67)|g|(\\%47))[^\n]+((\\%3E)|>)";
          REQUIRED = "Y";
     },
     {
          NAME = "SSI_CMD";
          REQUIRED = "Y";
          REG_EXP = "\\<\\!-\\#";
     },      {
          NAME = "XPATH_CHARACTER";
          REG_EXP = "^((((\\%3C)|<)\\!(--))(S|s|[a-z0-9\\%])*";
```

```
          REQUIRED = "Y";
     },
     {
          NAME = "SQL_CMD";
          REG_EXP = "((\\%3D)|(=))|((\\%27)|(\\')|(\\-\\-)|(\\%3B)|(;))";
          REQUIRED = "Y";
     },
     {
          NAME="HTML_TAG";
          "REG_EXP"="((\\%3C)|<)(\\\"[^\\\"]*\\\"|\\'[^\\']*\\'|[^'\\\">])*((\\%3E)|>)";
          REQUIRED = "Y";
     },
     {
          NAME = "META_CHARACTER";
          REG_EXP = "[(\\~)(\\!)(\\#)(\\$)(\\%)(\\^)(\\&)(\\+)(\\[\\])(\\{\\})(\\|)(\\?)]";
          REQUIRED = "Y";
     }
 );
"blackListForSearches" =(
     {
          NAME="SSI_CMD";
          REG_EXP="\\<\\!-\\#";
          REQUIRED = "Y";
     },
     {
          NAME="SQL_CMD";
          REG_EXP="((\\%3D)|(=))|((\\%27)|(\\-\\-)|(\\%3B)|(;))";
          REQUIRED = "Y";
     },
     {
          NAME="HTML_TAG";
          REG_EXP="((\\%3C)|<)(\\\"*\\\"|)*((\\%3E)|>)";
          REQUIRED = "Y";
     },
     {
          NAME="META_CHARACTER";
          REG_EXP="[\\~\\$\\%\\^\\+\\[\\]\\{\\}\\?]"; REQUIRED= "Y";
      }
 );
"passwordPolicy" = {
     REG_EXP = "((?=.*\\d)(?=.*[!@\\#$%&])(?=.*[a-zA-Z]).{6,})";
     NAME = "PASSWORD_POLICY";
     REQUIRED = "Y";
};
},
{
```

```
     "customMenuA" = ();
     "customMenuB" = ();
     "sysadmin" = "true";
     "connections" = ();
     "sitename" = "FF";
}
);
     "hubHost" = "127.0.0.1";
     "hubPort" = "12345";
     "connections" = (
{
     "id" = "1";
     "cb_name" = "sql_902_1";
     "description" = "";
     "web_name" = "sql_902_1";
}
);
}
```

11.2.2 Interpret and Change the Configuration File for Blacklisted Strings

We recommend that you do not change the default configuration provided by the Telescope. However, if your organization uses special characters in filenames or XSS commands, you may need to change the code as described in this section.

The following scripts, identified by "NAME" in the blackList section of the configuration code shown above, check for various special characters or phrases and blacklist (deny) the user request if any of these characters or phrases are found.

To turn any of these scripts off, change REQUIRED = "Y" to REQUIRED = "N". (Again, for your website security, this is not recommended.)

blackList Name	Blacklisted String, with Explanation
XSS_SCRIPT	((\\%3C)|<)((\\%2F)|/)*[a-z0-9\\%]+((\\%3E)|>) Blacklists strings (between <string> and </string> tags) containing the following HTTP tags and their hexadecimal equivalents: < /[text] > (where "[text]" is any alphanumeric string)
XSS_IMA	((\\%3C)|<)((\\%69)|i|(\\%49))((\\%6D)|m|(\\%4D))((\\%67)|g|(\\%47))[^\n]+((\\%3E)|>) Blacklists images; strings with the following HTTP tag and its hexadecimal equivalent: <img>

blackList Name	Blacklisted String, with Explanation
SSI_CMD	\\<\\!-\\# Blacklists command strings with the following meta-characters: <!-# These characters could indicate common Server-Side Include (SSI) commands intended to execute external CGI scripts or system commands, such as <!#exec cmd="/bin/ls/"->
XPATH_CHARACTER	^((((\\%3C)|<)\\!(--))(S|s|[a-z0-9\\%])* Blacklists HTML comments; that is, strings with the following HTTP tag and its hexadecimal equivalent: < !--[text] (where "[text]" is any character, including whitespace and periods (.)
SQL_CMD	((\\%3D)|(=))|((\\%27)|(\\'))|(\\-\\-)|(\\%3B)|(;)) Blacklists strings with any of the following characters and their hexadecimal equivalents that may indicate SQL injections: = ' -- ;
HTML_TAG	((\\%3C)|<)(\\\"[^\\\"]*\\\"|\\'[^\\']*\\'|[^'\\\">])*((\\%3E)|>) Blacklists strings with any of the following special characters or their hexadecimal strings, which may indicate HTML tags: <" "> <' '> (These tags could spill to multiple lines.)
META_CHARACTER	[\\~\\!\\$\\%\\^\\&\\+\\[\\]\\{\\}\\?] Blacklists the following special characters that may indicate meta-characters: ~ ! $ % ^ & + [ ] { } ?

11.2.3 Change the Configuration File to Allow Search for Special Characters

By default, Telescope searches do not support the use of particular special characters. (See the lists below.)

We recommend that you do not change the default configuration provided by the Telescope. However, if your organization uses special characters in filenames or metadata, you may need to change the code as described in this section to enable searching for these characters.

The following scripts, identified by "NAME" in the blackListForSearches section of the configuration code shown above, check for various special characters or phrases and blacklist (deny) the user request if any of these characters or phrases are found.

To turn any of these scripts off, change REQUIRED = "Y" to REQUIRED = "N". (Again, for your website security, this is not recommended.)

blackListForSearches Name	Blacklisted String, with Explanation
SSI_CMD	\\<\\!-\\# Blacklists strings with the following meta-characters: <!-# These characters could indicate common Server-Side Include (SSI) commands intended to execute external CGI scripts or system commands, such as <!#exec cmd="/bin/ls/"->
SQL_CMD	((\\%3D)|(=))|((\\%27)|(\\-\\-)|(\\%3B)|(;)) Blacklists strings with any of the following characters and their hexadecimal equivalents that may indicate SQL injections: = -- ;
HTML_TAG	((\\%3C)|<)(\\\"*\\\"|)*((\\%3E)|>) Blacklists strings with any of the following special characters or their hexadecimal strings, which may indicate HTML tags: <" "> <' '> (These tags could spill to multiple lines.)
META_CHARACTER	[\\~\\$\\%\\^\\+\\[\\]\\{\\}\\?] Blacklists the following special characters that may indicate meta-characters: ~ $ % ^ + [ ] { } ?

11.2.4 Change the Secure Session ID

By default, the Session ID is hidden.

We recommend that you do not change the default configuration provided by the Telescope. However, if your organization requires the session ID to be exposed (due to onsite customization, multiple TSWeb application servers, or some other reason), you can change the SecureSessionID to “False” (by default, it is “True”).

This setting is located in the following file:

`...\TeleScope\Applications\tsadmin.woa\Contents\Resources\Config.plist` file.

Update the line to the following:

```
"secureSessionID" = "false";
```

11.2.5 Change the Password Policy

We use stringent password requirements for your security.

However, if your organization requires the ability to create users without an associated password, you will need to remove the new password policy settings within the Site.plist and Config.plist configuration files.

```
To remove the settings, set the requirement for passwordPolicy to "N", as shown here:
"passwordPolicy" = {
```

```
    REG_EXP = "((?=.*\\d)(?=.*[!@\\#$%&])(?=.*[a-zA-Z]).{6,})";
    NAME = "PASSWORD_POLICY";
    REQUIRED = "N";
};
```

PasswordPolicy Name	Blacklisted String, with Explanation
REG_EXP	`((?=.*\\d)(?=.*[!@\\#$%&])(?=.*[a-zA-Z]).{6,})` Imposes the following requirements when validating passwords: `(?=.*d)` at least one digit `!@#$%&` at least one of these special characters `(? =.*[a-zA-Z])` at least one character (either case) `{6,}` at least 6 characters

11.2.6 Regular Expression Syntax

The backslash character (\) in a regular expression indicates that the character that follows it either is a special character (as shown in the following table), or should be interpreted literally.

In Java and UNIX systems, special characters also need to escape with another "\".

Regular Expression	Meaning
.	A single character (except newline)
^	Beginning of line
$	End of line
[...]	Range of characters
*****	Zero or more duplicates
\<	Beginning of word
\>	End of word
_+	One or more duplicates
?	Zero or one duplicate
(...|...)	Shows alteration
\w	Matches a letter in a word
\W	Opposite of \w

11.2.7 Grouping Expressions

Regular Expression	Meaning
(subexpression)	Captures the matched subexpression and assigns it a zero-based ordinal number.
(?= subexpression)	Zero-width positive assertion
(?! subexpression)	Zero-width negative assertion
(?<= subexpression)	Zero-width positive assertion.

11.2.8 For More Information

For more information on the standards used to implement these solutions:

https://www.owasp.org/index.php/XSS_%28Cross_Site_Scripting%29_Prevention_Cheat_Sheet

For more information on regular and grouping expressions:

http://msdn.microsoft.com/en-us/library/az24scfc.aspx

http://www.regular-expressions.info/reference.html

Enterprise Considerations

Chapter 12: Configure LDAP

Lightweight Directory Access Protocol (LDAP) is an internet protocol used by email and other programs to store and access data from a central server. This chapter shows how to set up LDAP to work with Telescope.

In this Chapter:

- Section 12.1, "Set up LDAP to Work with Telescope," on page 161
- Section 12.2, "Set Up LDAPS (LDAP over SSL, Secure LDAP)," on page 165
- Section 12.3, "Identify Base Authentication Using the LDAP Browser Tool," on page 167
- Section 12.4, "LDAP Troubleshooting Tips," on page 172

12.1 Set up LDAP to Work with Telescope

12.1.1 Before You Start ...

To set up LDAP to work with Telescope, you need:

- An LDAP Browser Tool.

  Download the free browser tool at http://www.ldapadministrator.com/download.htm. (You will need this tool to identify base authentication. The steps shown in the following sections are based on version 4.5 of this tool.)

- Acquire your LDAP Service Account Credentials, including username/password/base DN.

  (To find the base DN on your own, see Section 12.3, "Identify Base Authentication Using the LDAP Browser Tool," on page 167)

- LDAP server name and port
- A normal user account in the Active Directory forest that you can test with
- A Telescope LDAP Plugin License.

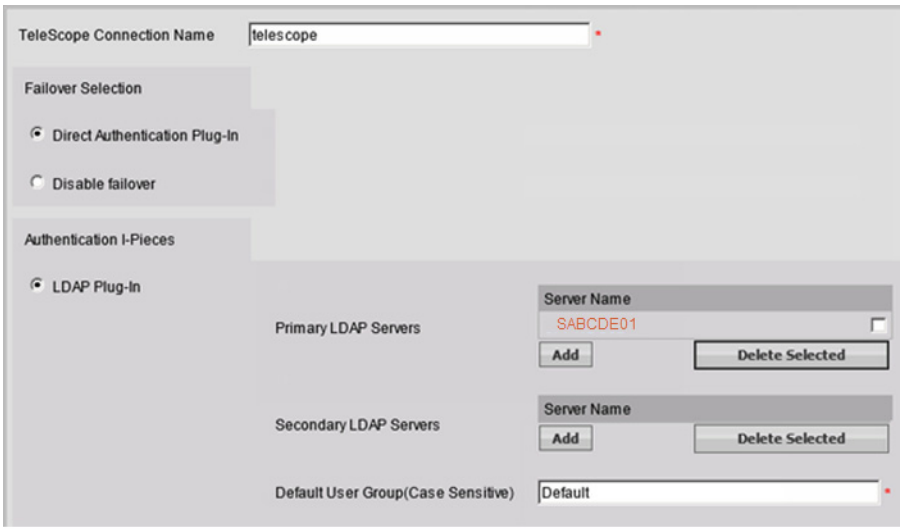
12.1.2 Configure the LDAP Plugin

1. Log in to TSAdmin as a system administrator. (Ensure *Administer* is set to *System*.)
2. Click the *Authentication Broker* link in the left navigation panel.
3. In the *Telescope Connections* section, click *Add*.
4. Referencing the screenshot below, set the following:

   a. Set *TeleScope Connection Name* to the connection name used by Telescope to connect to the database. Locate it by clicking the *connections* link in the left navigation panel of the TSadmin screen.

   b. If you need access to the Telescope database of users, set *Failover Selection* to "Direct Authentication Plug-In"; otherwise set it to disabled.

   c. *LDAP Parameter Directory* (at the bottom of the window) can be either `C:\Temp` or `\\server\path`.

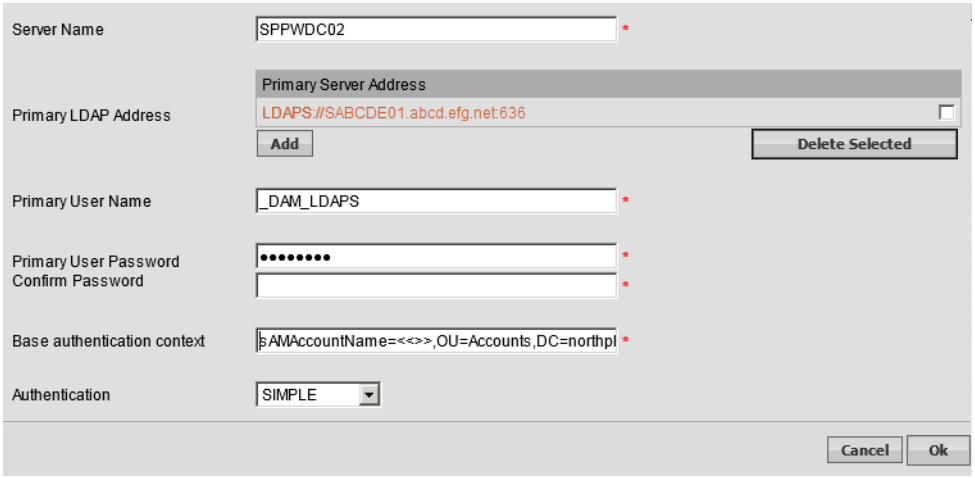


Notes:

- The purpose of the LDAP parameter directory is for the Authentication Broker to be able to write the group membership file to the hard drive for processing, in the event the number of characters in your group membership string reaches over 4000 characters (this limit is used in Functional Rules, like login and create rules).
- If you use a UNC path, you will need to start the Authentication Broker with domain credentials.
- If you are using a functional rule to process the group information to make decisions on what Telescope group the user belongs to, you'll need to have a windows share for the parameter directory. Both the user running the Authentication Broker and the user running the SQL Server will need to be granted access at both the share level and the folder level.
- If security is an issue, remove the "everyone" permissions from the share, as well as the security permissions from the folder, and then assign Read/Write access to the Authentication Broker user, and Read Access to the SQL Server users.

5 In the same window shown above, click “Add” in the "Primary LDAP Server" section.

In the panel that appears, provide values as illustrated in the screenshot below:



a Fill in the *Server Name* field.

In Single Domain instances, set the server name to the actual LDAP server name.

In Multiple Domain instances, set each domain server name to the domain name itself. This setting can then be used as the identifier "hint" on login for when you want Telescope to find your user in a particular domain.

Set up each domain independently of the others (even if their servers are the same).

Once the domains are set up, your users will need to use the domain qualifier to log in (for example, NPS\username). The Authentication Broker will use "NPS" against the "server name" field (also called NPS in this scenario) and then look up the user on the domain forest defined by the configuration contained within it.

b To set the Primary LDAP Address, click *Add*. Use the following format:

```
ldap://servername:port
```

(for example, `ldap://npsldap.northplains.com:389`)

c Primary User Name is the **read-only** service account, which can access and enumerate the entire domain structure. This name is created and used within your organization. The primary username may need to be your FQN or prequalified with a domain (for example, NPS\username or username@nps). You can validate your settings in an LDAP Browser tool, to help speed up the process.

d Primary User Password is the password for the primary user account described in the previous step.

e Base Authentication Context will sometimes be given to you as follows:

```
uid=<<>>,OU=Users,DC=Northplains,DC=Com
sAMAccountName=<<>>,OU=Users,DC=Northplains,DC=com
```

You will need to use the LDAP Browser tool to validate the Base DN to ensure you are using the correct user name lookup field. The field can be either UID or sAMAccountName, and you will need to check which on is used. While you are validating, ensure that you are using the correct DN to begin with.

See Section 12.3, "Identify Base Authentication Using the LDAP Browser Tool," on page 167 to determine this setting.

The <<>> section of the base context is considered a replacement parameter for the passed in user name of the person logging in.

f Leave Authentication as "Simple". If you require a different setting, contact the North Plains Systems Professional Services Group.

6 Click *OK* to commit your changes.

7 If you get no error messages, proceed to click on all of the *OK* buttons.

8 Be sure to click the *Save* option in the main page of TSAdmin to commit your settings to the broker.

If all settings are correct, you will see a "save successful" message.

9 Attempt to log into "Telescope.Web" with your domain user and password.

If you get a message indicating your username or password is incorrect, proceed to the troubleshooting tips section at the end of this section.

12.2 Set Up LDAPS (LDAP over SSL, Secure LDAP)

12.2.1 Before You Start ...

Ensure you have gathered the following information from your organization:

- LDAP Over SSL servername and port.
- Root Certificate, Internal Certificate (if applicable), LDAP certificate in X.509 format (.cer should be sufficient).
- Username and password for the Primary Account.

12.2.2 Set up LDAP Plugin for LDAP over SSL

1. Follow the steps in Section 12.1, "Set up LDAP to Work with Telescope," on page 161 to first get LDAP authentication working, then proceed with the next steps to add in LDAPS after you know everything else functions.
1. Log in to TSAdmin as a system administrator. (Ensure *Administer* is set to *System*.)
2. Click the *Authentication Broker* link in the left navigation panel.
3. In the *Telescope Connections* section, click the connection you set up already (it opens in a new window).
4. Click the Primary LDAP Server link (it opens in a new window).
5. Click on the "Primary LDAP Address" link.
6. Use your LDAP Over SSL server name and port to modify the settings as follows:

   `ldaps://servername:port`

   For example: `ldaps://NPSLDAP:636`

   (Note that both the "S" and the secure port are required
7. Click *OK* for all of the open windows. Click *Save* in the main window to commit to the broker.
8. Install the certificates into the Java (JRE & SDK) Certificate Store.

NOTE: Having the certificates in the Operating System Certificate Store is not enough. The certificates MUST reside in the Java certificate store for this to work. Read the section below on using the Java keytool to find out more on how to do this.

Using the Java keytool

Review the following notes before performing the certificate installation, so that you know the answers to questions you will face while installing the certificates.

- The "-Alias" name is arbitrary and must be unique for each of the certificates.
- Add the key to both the JRE and JDK sections.
- If there are spaces in your string, wrap them in double quotes.

- The Java keytool only works with .cer X.509 files. Other formats will not import as expected as of the publication date of this document. (Section 12.4, "LDAP Troubleshooting Tips," on page 172 reviews how to make .cer files from a p7k file provided by certificate vendors.)
- The default password for the java keystore is "changeit". You will be asked for this password during the key import. You will be asked to enter it twice, for each time a key is inserted into the keystore.

With the above points in mind, continue with the next steps to add in the certificates you gathered.

9 Open a command prompt as an administrator.

10 Enter the following commands (modify the paths to the certificate as appropriate).

For the Internal Certificate:

```
keytool -import -alias InternalCert -file "c:\Internal CA.cer" -keystore "C:\Program Files
(x86)\Java\jdk1.6.0_37\jre\lib\security\cacerts"
```

```
keytool -import -alias InternalCert -file "c:\Internal CA.cer" -keystore "C:\Program Files
(x86)\Java\jre6\lib\security\cacerts"
```

For the Root Certificate:

```
keytool -import -alias RootCert -file "c:\Root CA.cer" -keystore "C:\Program Files
(x86)\Java\jre6\lib\security\cacerts"
```

```
keytool -import -alias RootCert -file "c:\Root CA.cer" -keystore "C:\Program Files
(x86)\Java\jdk1.6.0_37\jre\lib\security\cacerts"
```

For the LDAP Server Handshake Certificate:

```
keytool -import -alias serverCert -file c:\SERVERNAME.cer -keystore "C:\Program Files
(x86)\Java\jdk1.6.0_37\jre\lib\security\cacerts"
```

```
keytool -import -alias serverCert -file c:\SERVERNAME.cer -keystore "C:\Program Files
(x86)\Java\jre6\lib\security\cacerts"
```

11 Attempt to log in to Telescope.

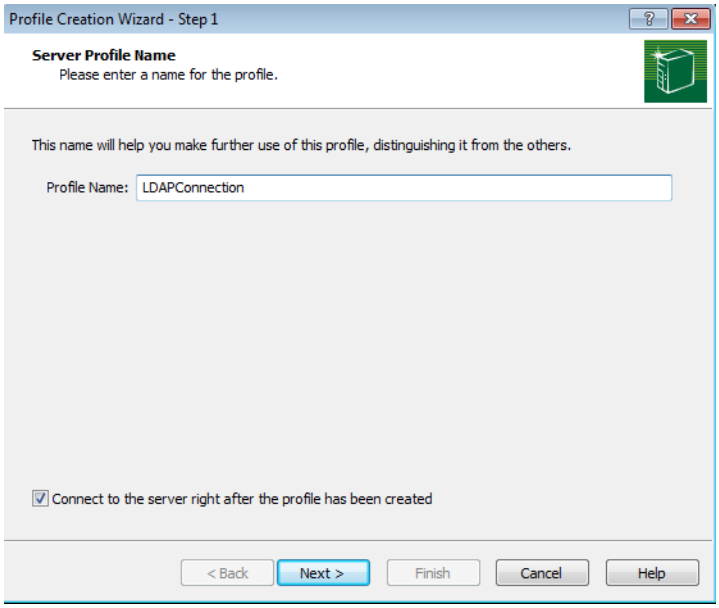
- If the login is successful, you are logging in with LDAPS. (The authentication may be noticeably slower due to the extra handshake measures performed by the certificate.)
- If the login is not successful, go to Section 12.4, "LDAP Troubleshooting Tips," on page 172.

12.3 Identify Base Authentication Using the LDAP Browser Tool

You will need to use the LDAP Browser tool to identify your base authentication, including your DN name.

1. Download and install the Free version of LDAP Browser 4.5 from the following website:

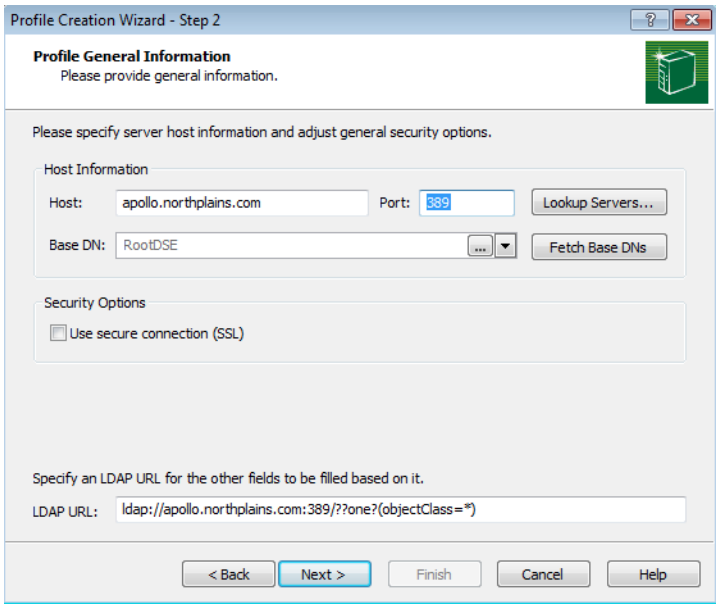
   http://www.ldapadministrator.com/download.htm
2. Launch the tool.
3. Click the *New* button to create a new connection.
4. Give it any name, and then click *Next*.



5. Set the Host Name and Port.

   (Leave the Base DN alone. The LDAP URL at the bottom of the panel will self-populate.)

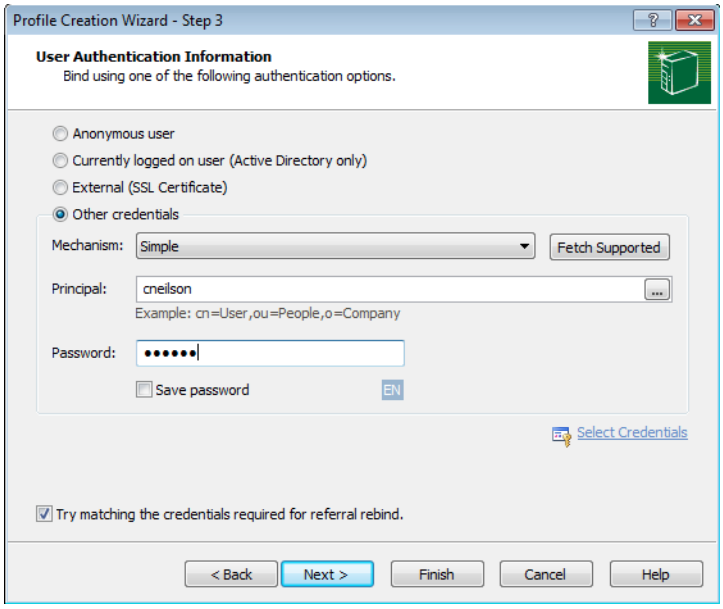
   Click the *Next* Button.



6 Set the radio button to *Other Credentials* and the Mechanism to *Simple*.

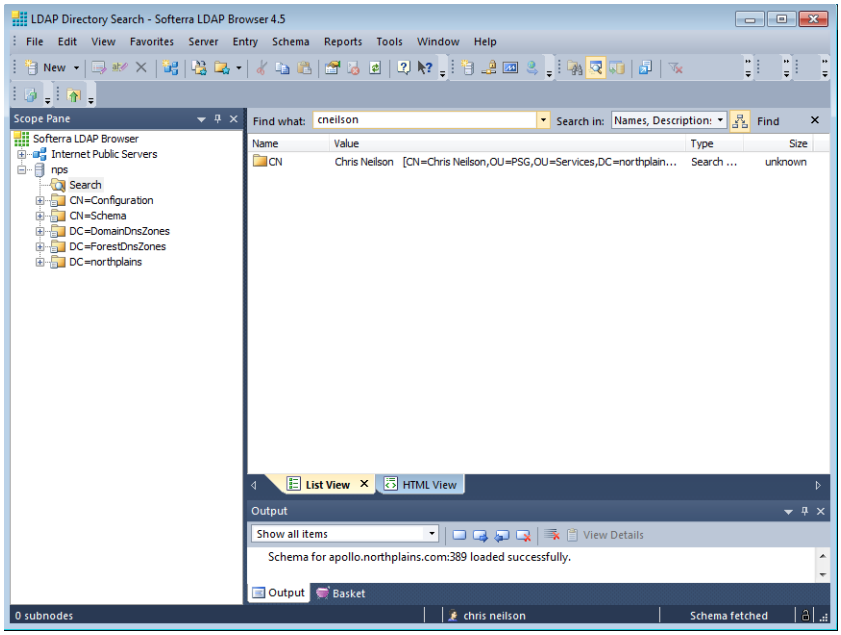
Type in the user name and password of the service account.

Click *Finish* to make the connection.

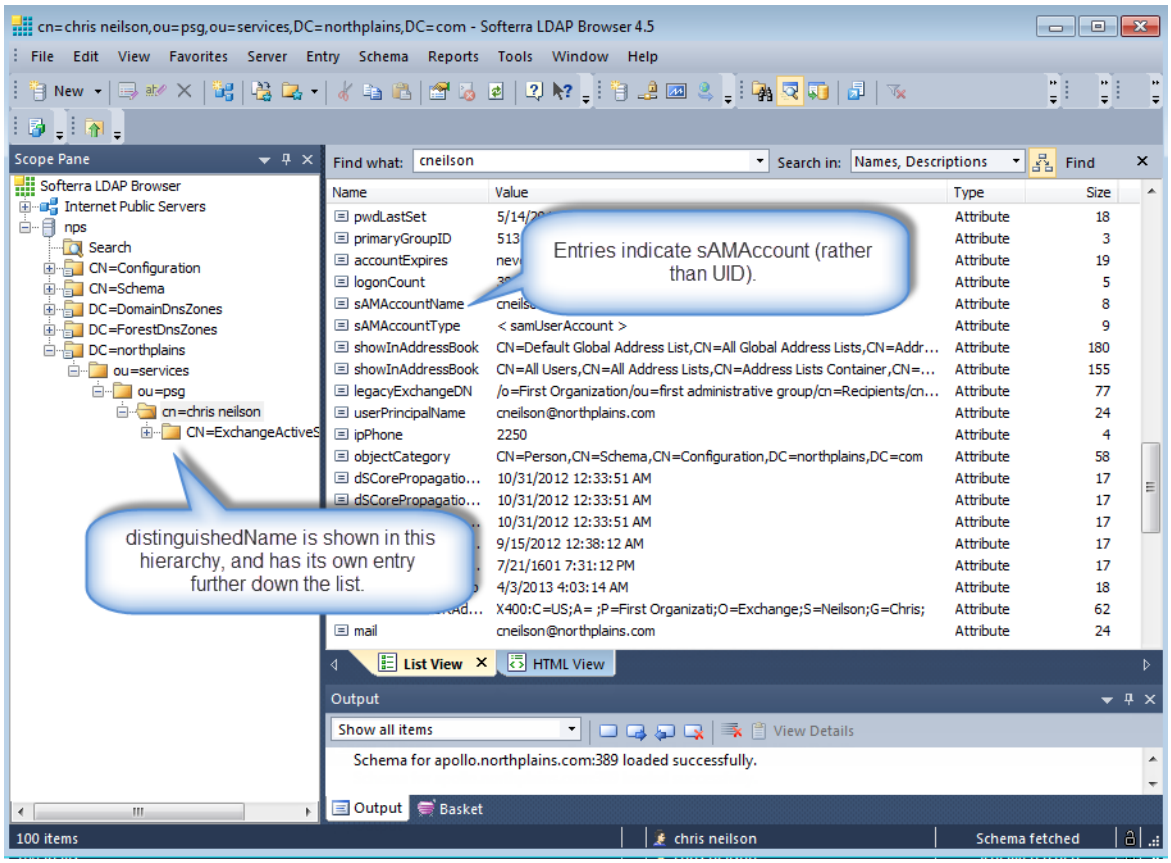


NOTE: If this authentication fails at this point, then so will the Authentication Broker, so make sure you can connect before continuing with these instructions. If you are having difficulties, see Section 12.4, "LDAP Troubleshooting Tips," on page 172.

7 Find your user account by typing it into the Find What box, then click *Find*. If the service account is set up correctly, your user account will appear. This step confirms that the Authentication Broker will find you when you attempt to log in.



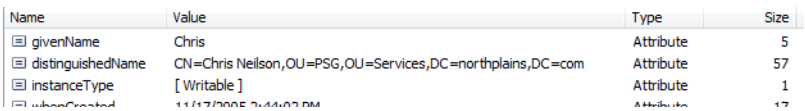
8 Double-click on your user name and scroll through the available options.



The *Name* column will help you set up the mappings later on. Use these entries to take note of mappings for department, phone number, email, first name, last name, and other values stored about users. The values in the name field are case sensitive, so take note of the case as well.

You will also need to determine if your environment is using sAMAccountName or UID to look up usernames. This method will determine how you set up your base authentication context within the TSAdmin LDAP Plugin. In this example, we are using sAMAccountName.

9 Within your profile, scroll down to locate your distinguishedName entry. This will also be critical in assisting you with building out the Base Authentication Context



Name	Value	Type	Size
givenName	Chris	Attribute	5
distinguishedName	CN=Chris Neilson,OU=PSG,OU=Services,DC=northplains,DC=com	Attribute	57
instanceType	[Writable]	Attribute	1

10 With the information we have, we can construct the base authentication context for the LDAP Plugin as follows

```
sAMAccountName=<<>>,DC=northplains,DC=com
```

(Explanation: We have determined it is a sAMAccountName. <<>> is a replacement parameter to pass the name typed by the user in Telescope The DC entries were derived from the distinguishedName entry. OU entries may also be required; see below.)

Note: OU entries

In the example above, the plugin will look across the **entire** domain from the top down (the top to bottom is read from the end to the beginning of the distinguished name). In very large Environments this search will take a long time to return results, and will result in extended login times.

To reduce the extent of the search, Organizational Unit (OU) entries may be added to the base context in very large environments. The OU entries in users' distinguishedName entries serve to subdivide users into various groups. Adding the OU will eliminate areas of the directory tree that do contain users, so they won't need to be processed.

In the example above, an added OU would look like this:

```
sAMAccountName=<<>>,OU=Services,DC=northplains,DC=com
```

In this example, the LDAP Plugin will only look for users found in the "Services" branch of the Active Directory Tree (in other words, the `com\northplains\services` folder of the directory tree). Adding in `OU=PSG` would further limit the search to only the PSG group, eliminating any lookup of users from elsewhere in the directory.

11 You now have everything needed to validate and finalize the LDAP Plugin configuration.

You may wish to leave the LDAP browser application open and use it to validate your user mappings.

12.4 LDAP Troubleshooting Tips

If you are having difficulties setting up LDAP for use with Telescope, follow these steps to verify you have the correct setup.

1

2 Look in the Authentication Broker log file (`ab.log`) because most issues around setting up LDAP Plugins are recorded here. You will locate this file in the logs directory of the Telescope installation (typically, `c:/telescope/logs/ab.log`).

NOTE: The Telescope Web log file will also have errors propagated from the Authentication Broker log file.

---

   a The first entry in the log shows that the Primary Service Account User attempts to log in. This attempt is only logged after the user's first attempt to log in.

   b If the primary service account user can't log in, an error is listed immediately after the attempt. Go into the LDAP Browser tool and validate the credentials, adjusting as necessary. Sometimes this is a necessary step in verifying the credentials.

3 If your primary user authenticates successfully, you will see a lot of extra information in the log file. The extra details will relate to the AD profile of the user who attempted to log in through the TS.Web interface.

   a If you do not see this profile information, look for a validation that the DN search can find the user account logging in. This will almost always happen when your base context is too deep. Try adjusting the context higher than your user profile and try logging in again.

   b Another situation, which is common, is that the AD server information is incorrect, or you are trying to authenticate against an invalid domain.

4 Once your account has been found, you should then see your entire profile information in the log file and you should be able to log in successfully.

5 If you encounter problems, use an Internet search on the error being reported in the log. The error code, while possibly cryptic, should have an MSDN article about it and be easily resolvable.

6 Remember: to get logged in with a base setup, all you need to do is have the service account login working and your profile found in the directory tree.

7 For setting up LDAP over SSL, ensure that all of the certificates are installed.

   Note that Java cannot handle P7b files, which have all of the certificates inside one store. For P7b files, you need to export the enclosed files to separate .cer X.509 certificate files. To do this,

   a Double-click the P7b file. It will open in a console window. Right-click on each certificate, choose "all tasks," then "Export", then follow the prompts for the remaining steps.

   b Use the Java keytool to put the certificates in both the JRE and the JDK keystores.

   c Ensure that the ports are correct for the SSL socket:

   The default port for LDAPS is 636; the default port for LDAP is 389.

   Also ensure you have LDAPS in the URL and not LDAP.

Chapter 13: Install Telescope in a Clustered Environment

This section provides information about installing Telescope in a cluster environment.

- Section 13.1, "Overview," on page 174
- Section 13.2, "Create a Cluster," on page 175
- Section 13.3, "Create a Failover Cluster," on page 178
- Section 13.4, "Set Up the Cluster," on page 179

13.1 Overview

Telescope server components such as Remote File Store serve multiple Telescope clients at the same time. Not only must server components be stable at the application level, they must also be reliable at the system level.

If a server computer goes down, the Telescope server components can automatically switch to a redundant server in a failover procedure that is transparent to Telescope clients.

A failover occurs in the following scenario:

Before a failover there are two Hub computers running, but only the primary computer is considered active. The secondary computer is in a passive state. The two computers have their own internal IP addresses, but they share the same virtual IP address. At any time, the client user can use the virtual IP address to connect to the active Hub computer.

When a failure occurs, the Hub applications are shut down on the primary computer (the server is changed to a passive state) and the cluster virtual IP is then switched to the secondary computer's IP address. The Hub applications are restarted on the secondary computer, and the secondary computer changes to active state.

To see which instance is being used:

To see which instance is being used (so you can identify where to retrieve the correct log files from for any issue that is being logged), click on the icon in the upper left corner of the TSWeb screen. In the About screen that appears, the Instance ID is shown with the version number. (If the instance ID is "1", it will not appear.)

To change the instance being used, go to the WebObjects Monitor, click on the *Detail View* button beside the TSWeb application. From the Details view, stop the application, click the *Config* button, change the ID number, click Update Instance Settings, then start the TSWeb application again.

13.2 Create a Cluster

13.2.1 Install a Failover Cluster

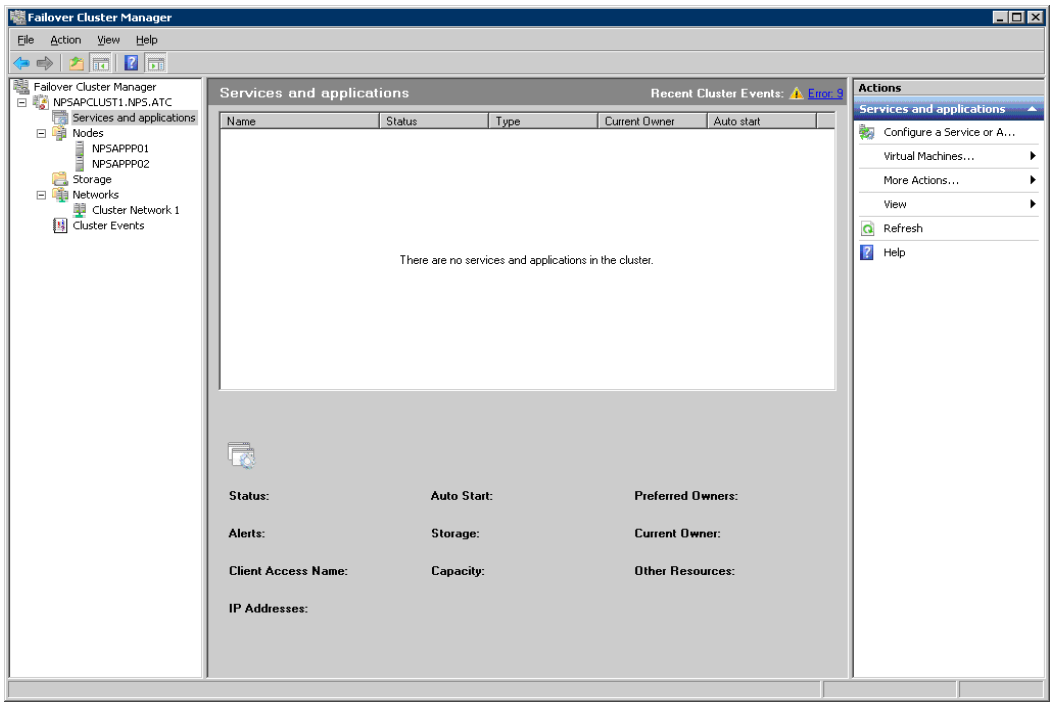
1. Click *Start> Administrator Tools> Server Manager.*
2. Scroll down to Features Summary and click *Add Features*.
3. In the Add Features Wizard select *Failover Clustering* then click *Install*.

13.2.2 Validate the Cluster Configuration

It is recommended that the cluster is validated to confirm the servers, network, and storage meets the failover cluster requirements.

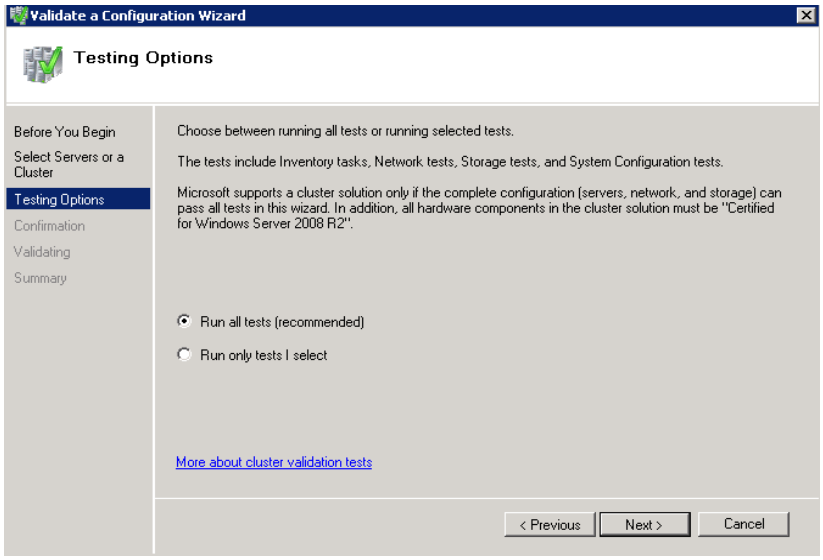
1. Click *Start> Administrator Tools> Failover Cluster Manager.*

Figure 13.1 *Failover Cluster Manager*



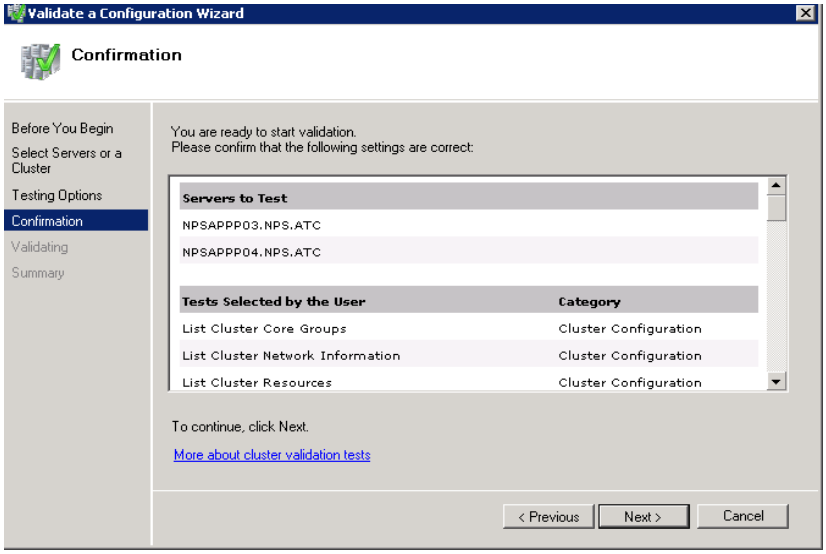
2. Under Management click *Validate a Configuration*.
3. In the Validate a Configuration Wizard click *Next*.
4. In the Select Servers dialog, enter the server name(s) then click *Next*.
5. In the Testing Options dialog, select *Run all tests (recommended)*.

Figure 13.2 *Validate a Configuration: Testing Options*



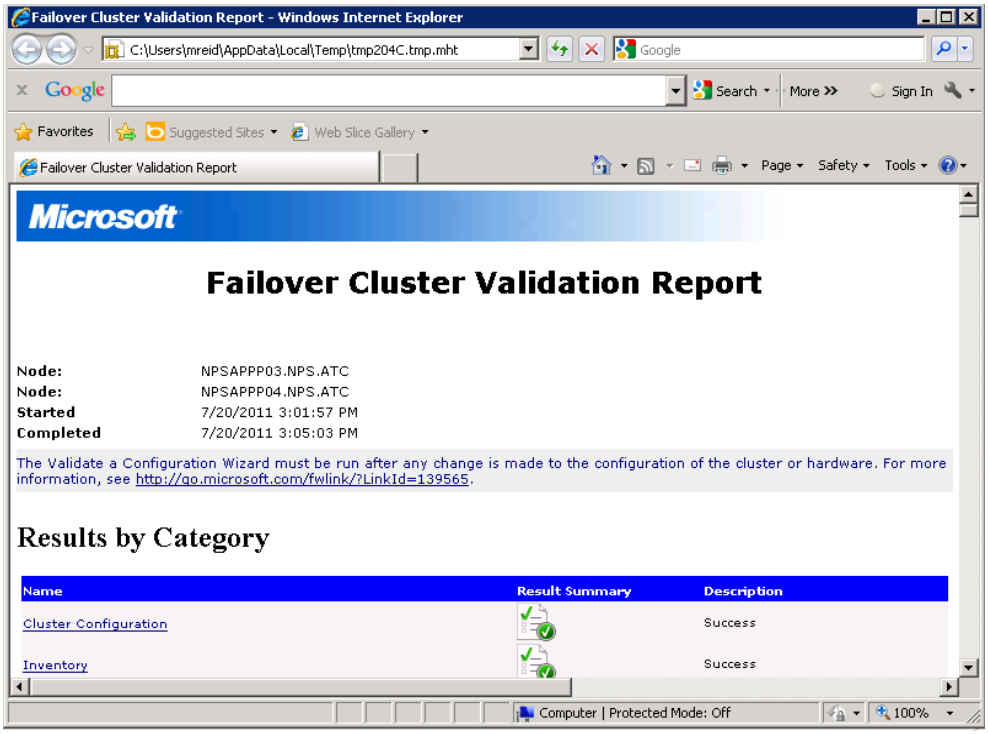
6 In the Confirmation dialog click *Next*. All tests run and are shown in a Confirmation panel (shown below).

Figure 13.3 *Validate a Configuration: Confirmation*



7 In the Summary dialog click *View Report* to see results of the validation tests. (These will take time to generate.)

Figure 13.4 *Failover Cluster Validation Report*

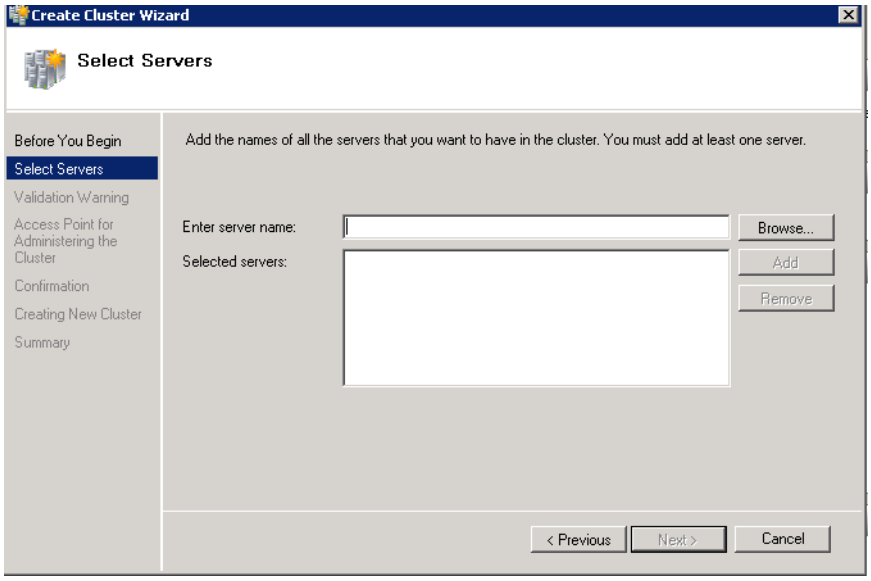


8 Click *Finish* to end the Validation wizard.

13.3 Create a Failover Cluster

1. Click *Start> Administrator Tools> Failover Cluster Manager.*
2. Under Management click *Create a Cluster* and click *Next*.
3. In the Create a Cluster Wizard click *Next*.
4. In the Select Servers dialog, enter the server name(s) and click *Next*.

Figure 13.5 *Select Servers*



5. In the Validation Warning dialog, click *Next*.
6. In the Access Point for Administering the Cluster dialog enter the required information then click *Next*.
7. In the Confirmation dialog click *Next*.
8. In the Creating New Cluster dialog click *Next*. The new cluster is created.
9. In the Summary dialog click *Review Report* to see the results of the cluster creation.
10. Click *Finish* to end the Create a Cluster wizard.

13.4Set Up the Cluster

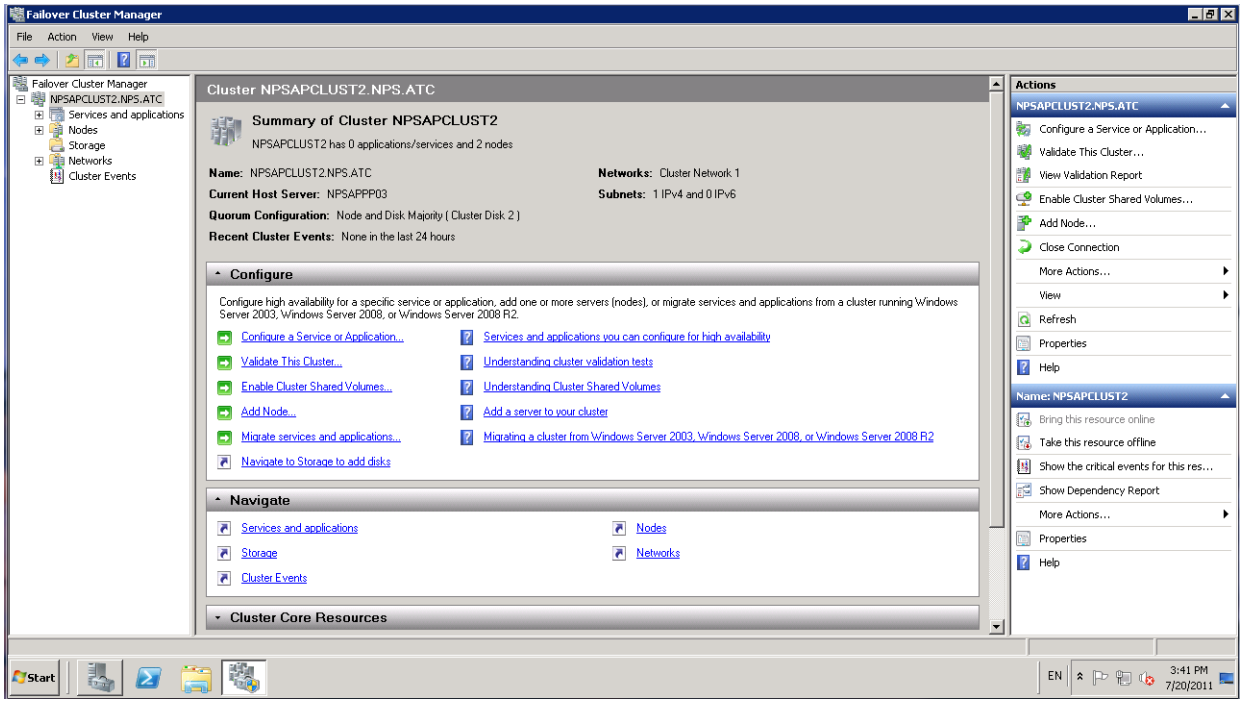
Cluster Manager must be installed first; then launch the Cluster Manager Application.

13.4.1 Set up the Generic Server

Set up a Generic Server to represent a "grouping" of services. This allows all the Telescope services to be dependent on one another.

1. Click *Start> Administrator Tools> Failover Cluster Manager.*
2. Under Management click *Manage a Cluster* and click *Next*.

Figure 13.6 *Manage a Cluster*



3. Click *Configure a Service or Application* (the first entry with the green arrow).
4. In the resulting window, click *Other Server* and click *Next*.
5. Give the Server a Name and an IP Address and click *Next*.

NOTE: You will need this name for the setup of the Name Service below (ORBendPoint Parameter), and it will be the "hub name" when setting up the rest of the product.

---

6. Select *Storage* if necessary, and click *Next* to continue.
7. Confirm the Setup and click *Next*.
8. Allow the Server to configure itself and click *Finish* to continue.

13.4.2 Set up the NPS Name Service

Setup of the Name Service is slightly different from other Telescope Services:

1. Open the Registry and navigate to the following location:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NPS Name Server\`

2. Locate the "ImagePath" variable and set it to:

```
C:\Telescope\omniNames.exe -runsvc -start 12345 -logdir "C:\TeleScope" -errlog "C:\TeleScope\omniNames.errlog" -
ORBendPoint giop:tcp:[Generic_Servername]:12345 -ignoreport
```

3. Click *OK* and save the registry.
4. Locate and delete the 2 omninames files in `C:\Telescope\` directory. They are called:

   `omninames-[Generic_Servername].bak`

   `omninames-[Generic_Servername].log`

5. The omninames files will be rebuilt automatically and correctly on the first start of the service

13.4.3 Set Up All the Services

Click inside the "Generic Server" you created earlier, then set up the remaining Telescope services as follows:

1. Click *Add a Resource* and select *4 - Generic Service*.
2. Select the Service from the List, which you are setting up.
3. Confirm the Settings and click *Finish*.
4. Perform the same steps until all of the Telescope services have been added to the Cluster Manager.

13.4.4 Set Up the Broker Service Dependencies

Once all of the services are added to the Generic Server, set the Dependencies tab of the respective tab as per the following. This order is selected to allow the brokers to start as quickly as possible during a restart of the server, and represents the recommended manual startup order.

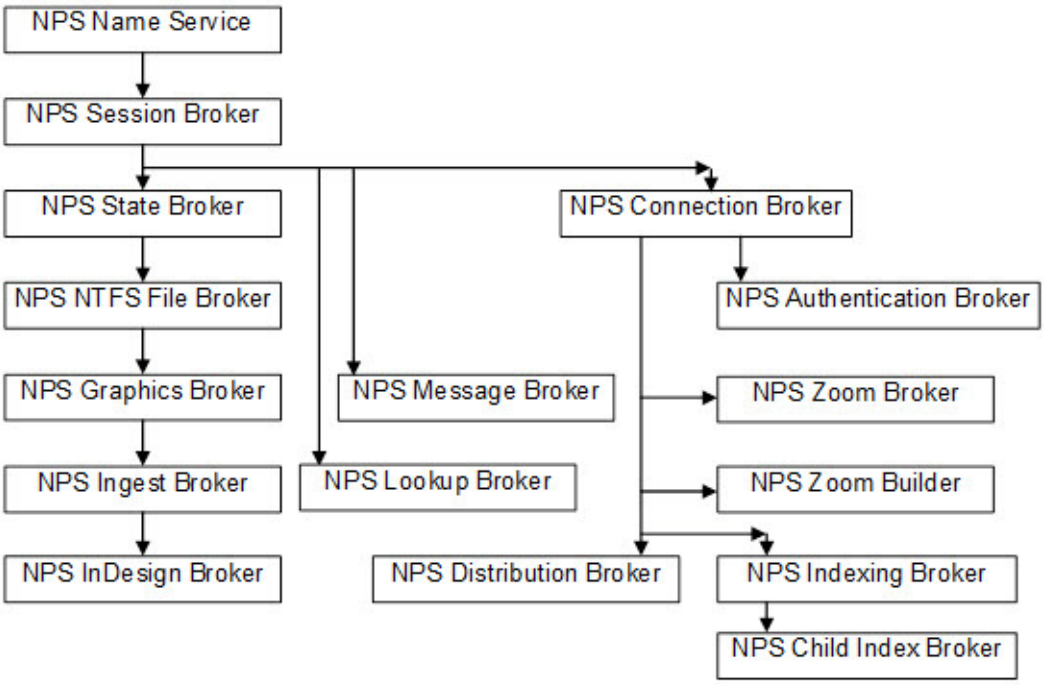
Service	Dependencies
NPS Name Server	Name: [Generic_ServerName] AND IP Address: [Cluster_IP]
NPS Session Broker	NPS Name Server
NPS State Broker	NPS Session Broker
NPS Connection Broker	NPS Session Broker
NPS Authentication Broker	NPS Connection Broker
NPS NTFS File Broker	NPS State Broker
NPS Message Broker	NPS Session Broker
NPS Jetty-Service	No dependency.

Service	Dependencies
NPS Indexing Broker	NPS Jetty-Service NPS Connection Broker
NPS Child Indexing Broker	No dependency to start up, but requires the NPS Indexing Broker to be operational.
NPS Lookup Broker	NPS Session Broker
NPS Graphics Broker	NPS NTFS File Broker
NPS Ingest Broker	NPS Graphics Broker
NPS Distribution Broker	NPS Connection Broker
NPS InDesign Broker	NPS Ingest Broker
NPS Zoom Builder	NPS Connection Broker
NPS Zoom Broker	NPS Connection Broker
NPS Interoperability Broker	NPS Connection Broker

Broker Dependency Map

This dependency map shows the service dependencies for when the machine is restarted. These dependencies can be coded into the registry settings so they can be followed during a reboot of the machine.

Figure 13.7 *Telescope Broker Dependency Map*



13.4.5 Notes on Clustering

1. After the clustering is set up, go into both sides of the cluster and launch the service control manager (services.msc). For all of the NPS services, set them to "Manual". The Cluster Manager will be launching these services from this point on, and they should not be launching on their own with the next system restart.
2. After the clustering is set up on the one side, RDC to the second side and perform the instructions in Section 13.4.2, "Set up the NPS Name Service," on page 180 to ensure omninames are generating correctly on failover. After you finish, perform a failover at your convenience.
3. Add your licenses to the first side of the cluster. Then fail over to the second side from within Cluster Manager. Logout/Login to TSAdmin again and add all the licenses to the second side of the cluster. Fail back to the first side if you desire.

Appendixes

Chapter 14: Telescope Configuration Parameters

The following sections provide information about the Telescope Configuration Parameters:

- Section 14.1, "Telescope Administrator Configuration Parameters," on page 185
- Section 14.2, "Download Manager Configuration Parameters," on page 188
- Section 14.3, "Site Manager Configuration Parameters," on page 191
- Section 14.4, "TSWeb Configuration Parameters," on page 193
- Section 14.5, "Other Settings," on page 198
- Section 14.6, "Java Applets," on page 200

14.1 Telescope Administrator Configuration Parameters

This section describes the parameters used to configure Telescope Administrator. These parameters affect Telescope Administrator's behavior in the same way on all platforms. The default settings are acceptable for most systems. User-specific settings, such as IP addresses and paths, require user configuration. The parameters are stored in two files, info.plist and config.plist. Edit these files where applicable.

14.1.1 Info.plist (TSAdmin)

NOTE: By default, the TSAdmin `Info.plist` file is located on the Web Application Server at `C:\Telescope\Applications\tsadmin.woa\Contents\info.plist`

AllowCCUsers – This key should be set to "Y" or "True" if a Browse and Download User license has been purchased. If this flag is "Y" or "True", then TSWeb asks the Session Broker if a Browse and Download User access license is available.

CFBundleDevelopmentRegion – Automatically generated, do not modify.

CFBundleExecutable – Automatically generated, do not modify.

CFBundleGetInfoString – Automatically generated, do not modify.

CFBundleIconFile – Automatically generated, do not modify.

CFBundleIdentifier – Automatically generated, do not modify.

CFBundleInfoDictionaryVersion – Automatically generated, do not modify.

CFBundleName – Automatically generated, do not modify.

CFBundlePackageType – Automatically generated, do not modify.

CFBundleShortVersionString – Automatically generated, do not modify.

CFBundleSignature – Automatically generated, do not modify.

CFBundleVersion – Automatically generated, do not modify.

Java – Automatically generated, do not modify.

JVMVersion – Automatically generated, do not modify.

NSExecutable – Automatically generated, do not modify.

NSJavaClientRoot – Automatically generated, do not modify.

NSJavaNeeded – Automatically generated, do not modify.

NSJavaPath – Automatically generated, do not modify.

NSJavaPathClient – Automatically generated, do not modify.

NSJavaRoot – Automatically generated, do not modify.

PrimaryHub, PrimaryName, PrimaryPort – These 3 parameters define the [PRIMARY] Hub which is used to register the application and all sessions. If this parameter is missing from AdminConfig.plist, it is added automatically when the application starts up.

doLogInfo – Specifies whether or not debug information is to be stored in the Telescope log files. Possible values are 1 to turn on debugging, or 0 to turn off debugging.

exitURL – URL of a page to be redirected to when the user logs out. By default this parameter is not included or is empty and the logout redirects the user to the default Telescope Login page. To redirect the user to a different location when logged out or session timeout, this parameter needs to be edited or created.

faultsBatchFetchLimit – Used for prefetching records by using faults. This value should not be a big number because the maximum length of SQL queries varies between different databases.

maxDbChannels – The maximum database channels opened by Telescope. The default value is 5.

maximumPopupItems – The maximum number of items in the popup lists. By default, this is 300.

minDbChannels – The minimum database channels opened by Telescope. By default, these channels are opened when Telescope starts up.

protocol – http:// or https://

search_mode – The Solr search method is the default. Do not modify.

tempDirectory – The full path to a temporary directory for Telescope Administrator.

url – The URL to the Web server where the Telescope Admin images are installed.

sessionTimeOut – The session timeout interval in seconds. (Deprecated)

14.1.2config.plist (TSAdmin)

NOTE: By default, the TSAdmin `Config.plist` file is located on the Web Application Server at `C:\Telescope\Applications\tsadmin.woa\Contents\Resources\Config.plist`

RestrictionFields – Defines the fields that determine whether an asset should be treated as restricted.

RestrictionColor – The background color to display behind a restricted asset's thumbnail, expressed as a hexadecimal value.

MinimumBrowserVersions, ExcludedBrowserVersions – These parameters list the included and excluded browsers in the following format: {M(ac)|
W(in);NS(Netscape)|IE(InternetExplorer)|SA(Safari);MAJOR_VER;MINOR_VER}

AdminWatermarkBatchSize –The number of watermarks displayed at one time to the administrator in the Watermark Administration page.

SystemDisplayName – The Name used to display to the user the "System" connection for administering System source.

SystemDefaultLoginName – Default user name/password for System connection if not set in the State Broker.

SystemDefaultPassword – The Default connection user password for System connection if not already set in the State Broker.

allowMultipleSubAdmins – The following parameter defines whether multiple sub-admins with overlapping visible groups are allowed to log in at the same time. Values: “Y” or “N”. Default is “N”.

WelcomePagesHTMLDir – This location is relative to $APPROOT\tsadmin.woa\Resources and indicates where the HTML files for the Welcome Pages are stored.

DefaultContentEncoding – Automatically generated, do not modify.

BlackList – Denies a user request if any of the listed characters or phrases exist. For details, see Section 11.2.2, "Interpret and Change the Configuration File for Blacklisted Strings," on page 154.

WhiteList – Permits a user request if any of the listed characters or phrases exist (not recommended).

phoneNumberPolicy – Sets the standard phone number format (by default, North American), and whether or not phone numbers are a required User Preference Field.

passwordPolicy – Allows the ability to create users without an associated password (not recommended). For details, see Section 11.2.5, "Change the Password Policy," on page 156.

Secure session ID – Exposes the session ID. For details, see Section 11.2.4, "Change the Secure Session ID," on page 156.

14.2Download Manager Configuration Parameters

This section describes the parameters used to configure Download Manager applications. These parameters affect the behavior of the Download Manager in the same way on all platforms. The default settings are acceptable for most systems. User-specific settings, such as IP addresses and paths, require user configuration. The parameters are stored in two files, info.plist and config.plist. Edit these files where applicable.

14.2.1Info.plist (Download Manager)

NOTE: By default, the DLManager `Info.plist` file is located on the Web Application Server at `C:\Telescope\Applications\dlmanager.woa\Contents\info.plist`

CFBundleDevelopmentRegion – Automatically generated, do not modify.

CFBundleExecutable – Automatically generated, do not modify.

CFBundleGetInfoString – Automatically generated, do not modify.

CFBundleIconFile – Automatically generated, do not modify.

CFBundleIdentifier – Automatically generated, do not modify.

CFBundleInfoDictionaryVersion – Automatically generated, do not modify.

CFBundleName – Automatically generated, do not modify.

CFBundlePackageType – Automatically generated, do not modify.

CFBundleShortVersionString – Automatically generated, do not modify.

CFBundleSignature – Automatically generated, do not modify.

CFBundleVersion – Automatically generated, do not modify.

Java – Automatically generated, do not modify.

JVMVersion – Automatically generated, do not modify.

NSExecutable – Automatically generated, do not modify.

NSJavaClientRoot – Automatically generated, do not modify.

NSJavaNeeded – Automatically generated, do not modify.

NSJavaPath – Automatically generated, do not modify.

NSJavaPathClient – Automatically generated, do not modify.

NSJavaRoot – Automatically generated, do not modify.

agent_url – The following parameter indicates where the agent servlet is configured: "http://192.168.0.231:8080/DLMExt/DLAgent". Note that DLAgent was deprecated in version 9.3.

buffer_size – The size, in bytes, of buffer used to stream files to client.

conversionTimeout – The amount of time, in seconds, that the Download Manager waits for the Conversion Broker to complete a conversion. The default value is 60 seconds, but if you are working with very large files, or performing complex conversions, you should increase this value.

doLogInfo – When used together with the Debugging enabled and Output Path settings in Monitor, a full debug log is created as a separate file. Set to 1 to enable debug logging or 0 for standard logging.

duplicateFileDirSeparator – Index separator for duplicate files, for example, if there is a duplicate file the directory name is Duplicate file, example.jpg_1.

duplicateFileDirectory – Specifies a directory name for duplicate files. {0} is replaced with the file name.

duplicateFileMaxDirLength – Specifies the maximum directory length for duplicate files. Duplicate files fail to download if this parameter is exceeded.

duplicateFileNumberOfAttempts – Specifies the maximum number of attempts for creating a directory for duplicate files. Duplicate files will fail to download if this parameter is exceeded.

file_server_as_servlet – Switch between the lite-http download file-serving mechanism and the "woresponse" file-serving mechanism implemented in version 6.2.3.

http_host –

Defines the host (name or IP address) that is used to construct the URL for the built-in http server for downloading. If provided, include the protocol identifier, i.e. "http://". If empty, then the IP address assigned to the host should be used.

If a host name is supplied, DNS entries must be configured so that internal and/or external clients can access the host by the given name. If the Application server is behind a firewall, an external (public) DNS entry should exist for external clients and an internal DNS entry should exist for internal clients inside the same firewall.

http_video_host –

Defines the host (name or IP address) that is used to construct the URL for the built-in http server for downloading video files.

If provided, include the protocol identifier, i.e. "http://". If empty, then the IP address assigned to the host should be used.

If a host name is supplied, DNS entries must be configured so that internal and/or external clients can access the host by the given name. If the Application server is behind a firewall, an external (public) DNS entry should exist for external clients and an internal DNS entry should exist for internal clients inside the same firewall.

maxDbChannels – The maximum database channels opened by Telescope. The default is 5.

minDbChannels – The minimum database channels opened by Telescope. By default, these channels are opened when Telescope starts up.

param_cookie_name – The following parameter is used to define the name of a cookie if cookies are enabled or else uses this as a GET parameter with this value defined.

port_threshold –

The value of this parameter is used to calculate the port number on which the built-in http server for the DLManager listens.

The port on which each DLManager instance is running must be known. This can be found by looking in the Configuration page for each instance in Monitor. The sum of the DLManager instance port number and the port_threshold defines the port on which the built-in http server is started for this instance.

For example, if there are 3 instances of the DLManager running on ports 2005, 2006 and 2007 and the value set as the port_threshold is 5005, then the three built-in http servers are started at 7010, 7011 and 7012 respectively. If the port_threshold is changed to 10000, then the three built-in servers now start at ports 12005, 12006 and 12007 respectively.

The value specified for the port-threshold is chosen to ensure that the ports used by the http servers do not conflict with any other services on the computer.

Note: Client browsers are connected to the application server on these ports and a firewall rule might need to be created to allow this communication.

protocol – "http://" or, for SSL security, “https://”

shouldCompressFiles – This flag specifies whether or not to compress the files when there is only one file downloaded. Allowed values “Y” or “y” for YES and “N” or “n” for NO.

siteFilePath – Provides the full path to site.plist. A typical value would be “c:\site.plist”.

ssl_keystores_file – The path and file name of the private certificate keystore file used for SSL security.

ssl_keystore_password – The keystore password for the keystore file.

tempDirectory – The full path to a directory where DLManager delivers downloaded files.

url – The URL to the Web server, where the DLManager images are installed.

use_agent – The following parameter is used to indicate that the download agent has to be used for downloading. “true” or “false” are possible values.

zipBufferSize – The size, in bytes, of the zip buffer used to stream files to client.

14.2.2config.plist (Download Manager)

NOTE: By default, the DLManager `Config.plist` file is located on the Web Application Server at `C:\Telescope\Applications\dlmanager.woa\Contents\Resources\Config.plist`

HostURL – Because a WebObjects adaptor can be located on a different computer than an actual application instance and the application instance cannot directly communicate with the adaptor, this value provides a real WebObjects adaptor URL. If this value is an empty string, an IP address of the application instance is used instead. For example: http://www.northplains.com. This value is required by different services within the application that need to provide a URL to connect to those services through the WebObjects adaptor. The protocol type (like http or https) for this value should be the same as defined in the Info.plist file for the key protocol.

NoZipFileTypes – When calling Download Now the files of the specified file type (file extensions) will not be zipped. DO NOT put blank spaces between file types.

DefaultContentEncoding – Leave as “UTF-8”

14.3 Site Manager Configuration Parameters

This section describes the parameters used to configure SiteManager applications. These parameters affect the behavior of SiteManager in the same way on all platforms. The default settings are acceptable for most systems. User-specific settings, such as IP addresses and paths, require user configuration.

14.3.1 Info.plist (Site Manager)

NOTE: By default, the Site Manager `Info.plist` file is located on the Web Application Server at `C:\Telescope\Applications\sitemanager.woa\Contents\info.plist`

CFBundleDevelopmentRegion – Automatically generated, do not modify.

CFBundleExecutable – Automatically generated, do not modify.

CFBundleGetInfoString – Automatically generated, do not modify.

CFBundleIconFile – Automatically generated, do not modify.

CFBundleIdentifier – Automatically generated, do not modify.

CFBundleInfoDictionaryVersion – Automatically generated, do not modify.

CFBundleName – Automatically generated, do not modify.

CFBundlePackageType – Automatically generated, do not modify.

CFBundleShortVersionString – Automatically generated, do not modify.

CFBundleSignature – Automatically generated, do not modify.

CFBundleVersion – Automatically generated, do not modify.

Java – Automatically generated, do not modify.

JVMVersion – Automatically generated, do not modify.

NSExecutable – Automatically generated, do not modify.

NSJavaClientRoot – Automatically generated, do not modify.

NSJavaNeeded – Automatically generated, do not modify.

NSJavaPath – Automatically generated, do not modify.

NSJavaPathClient – Automatically generated, do not modify.

doLogInfo – When used together with the Debugging enabled and Output Path settings in Monitor a full debug log is created as a separate file. Set to 1 to enable debug logging or 0 for standard logging.

NSJavaRoot – Automatically generated, do not modify.

siteFilePath – Provides the full path to site.plist. A typical value is “c:\site.plist”.

url – The URL to the Web Application server, where the Site Manager images are installed.

14.3.2Config.plist (Site Manager)

NOTE: By default, the Site Manager `Config.plist` file is located on the Web Application Server at `C:\Telescope\Applications\sitemanager.woa\Contents\Resources\Config.plist`

DefaultContentEncoding – Leave as “UTF-8”

14.4TSWeb Configuration Parameters

This section describes the parameters used to configure Telescope Web (TSWeb) applications. These parameters affect the behavior of Telescope in the same way on all platforms. The default settings are acceptable for most systems. User-specific settings, such as IP addresses and paths, require user configuration. The parameters are stored in two files, info.plist and config.plist. Edit these files where applicable.

NOTE: Case must be considered when typing in TSWeb URLs. If the URLs are not exactly the same, the TSWeb interface may work but the Telescope Uploader will time out. For example, if URLs in the TSWeb info.plist and config.plist files use "/script/", then these URLs when specified in the browser must also use "/script/" (not "/Script/")

14.4.1Info.plist (TSWeb)

NOTE: By default, the TSWeb `Info.plist` file is located on the Web Application Server at `C:\Telescope\Applications\tsweb.woa\Contents\info.plist`

AllowCCUsers – This key should be set to "Y" or "true" if a Browse and Download User license has been purchased. If this flag is "Y" or "true", then Telescope asks the Session Broker if a Browse and Download User access license is available.

CFBundleDevelopmentRegion – Automatically generated, do not modify.

CFBundleExecutable – Automatically generated, do not modify.

CFBundleGetInfoString – Automatically generated, do not modify.

CFBundleIconFile – Automatically generated, do not modify.

CFBundleIdentifier – Automatically generated, do not modify.

CFBundleInfoDictionaryVersion – Automatically generated, do not modify.

CFBundleName – Automatically generated, do not modify.

CFBundlePackageType – Automatically generated, do not modify.

CFBundleShortVersionString – Automatically generated, do not modify.

CFBundleSignature – Automatically generated, do not modify.

CFBundleVersion – Automatically generated, do not modify.

Java – Automatically generated, do not modify.

JVMVersion – Automatically generated, do not modify.

NSExecutable – Automatically generated, do not modify.

NSJavaClientRoot – Automatically generated, do not modify.

NSJavaNeeded – Automatically generated, do not modify.

NSJavaPath – Automatically generated, do not modify.

NSJavaPathClient – Automatically generated, do not modify.

NSJavaRoot – Automatically generated, do not modify.

TSLimiterURL – URL for connection to TSLimiter (optional).

allowDirectLogin – Defines whether or not users are allowed to access the Login page and log in directly using the Telescope interface. With this feature turned on, your organization can use its own Login page and pass the required login parameters to Telescope using the faceless login interface. If the key is set to "N", the exitURL key is used to retrieve the location to which a user is directed if an attempt to access the Login page is made.

dlManager – The url to the Download Manager valid for your environment. This should be similar to: http://191.158.0.6/scripts/WebObjects.dll/DLManager.woa/wa/download.

dlManagerVideo – Contains the URL for the DLManager serving requests to download video files for progressive and full-screen viewing. Typical values are "http://192.168.0.6/scripts/WebObjects.dll/ DLManagerNow.woa/wa/downloadNow".

doLogInfo – When used together with the Debugging enabled and Output Path settings in Monitor a full debug log is created as a separate file. Set to 1 to enable debug logging or 0 for standard logging.

exitURL – URL of a page to be re-directed to when the user logs out. By default this parameter is not included or is empty and the logout redirects the user to the default Telescope Login page. To redirect the user to a different location upon logout or session timeout, this parameter needs to be created or edited.

faultsBatchFetchLimit – Used for pre-fetching the array of faults. This number should be a big number as multiple databases support different lengths of SQL queries. Do not modify this value without a solid understanding of Apple frameworks.

maxDbChannels – The maximum database channels opened by Telescope. The default is 5.

maximumPopupItems – The maximum number of items in the popup lists. By default, this is 300.

minDbChannels – The minimum database channels opened by Telescope. By default, these channels are opened when Telescope starts up. This value cannot be less than 2.

param_cookie_name – The following parameter is used to define the name of a cookie if cookies are enabled or else it is used as a GET parameter with this value defined.

protocol – "http://" or, for SSL security, "https://"

search_mode – Leave as "SOLR"

sessionTimeOut – The session timeout interval in seconds.

siteFilePath – Provides the full path to site.plist. A typical value would be "c:\site.plist".

tempDirectory – The full path to a temporary directory for Telescope.

userUploadLimit – The upload limit on the applet side (in bytes).

watermarkAlphaChannel – Multiplier for alpha channel image watermarking.

url – The URL to the Web server where the Telescope images are installed.

14.4.2config.plist (TSWeb)

NOTE: By default, the TSWeb `Config.plist` file is located on the Web Application Server at `C:\Telescope\Applications\tsweb.woa\Contents\Resources\Config.plist`

KeywordSearchFields – The default search fields for simple search in Telescope.

DocTemplateSize – Size in bytes of the Templates, in MIMIX format; default is 10K up to a max of 2199023255552 bytes (2GB).

HomeCatalogTableView, HomeMessageTableView, TasksListPage – These keys are used to define the number of records per batch that should be displayed by the batch navigator defined on the page of the same name as each key. To omit the batch navigator, specify a value of zero.

HostURL – Because a WebObjects adaptor can be located on a different computer than the actual application instance and the application instance cannot directly communicate with the adaptor, this value provides the real WebObjects adaptor URL. If this value is an empty string, the IP address of the application instance is used instead. For example**:** http://www.northplains.com. This value is required by different services within the application that need to provide a URL to connect to these services through the WebObjects adaptor. The protocol type (like http or https) for this value should be the same as defined in the TSAdmin Info.plist file for the key protocol.

defaultLanguage – Defines the default language used by the system (which can be changed as a preference by users, if a multilanguage system is implemented). This parameter has the value “en_US” (U.S. English) by default. You can replace this language-country code with another value, but make sure to use a language that is included as a folder at the following path:
`C:\TeleScope\Applications\tsweb.woa\Contents\Resources\Sites\default\Resources\Language`

previewMetaOnTop – If this parameter is set to false, a legend of metadata is shown under images in the extended view (rather than at the top of the view). If it is missing from config.plist, it is assumed this value equals "true".

internalSpacerImage, externalSpacerImage –

Parameters used to detect internal users (behind the firewall) and external users (facing the firewall). The host name portion of the URL in both parameters should:

- contain a hostname which is resolvable internally only (for internalSpacerImage parameter).
- contain a hostname which is resolvable externally (for externalSpacerImage parameter).

Setting a hostname for internalSpacerImage, which is resolvable both internally and externally, declares all users internal. This parameter works together with the parameter http_video_host from DLManager, from file Info.plist.

EDLClassName – This parameter indicates the concrete class name to be used for generating an EDL If the parameter is missing, is empty or the class is not found, a default EDL generator is used instead.

maxmultirecords — The upper limit of the number of record_ids that can be passed to the GetDataMultiple SOAP API call. Optional configuration, the default value is 1000.

RegistrationSenderEmail – The email address used as a sender email (email indicated as "from") for the self-registration page to notify a user for the successful registration by email. This value is mandatory if the self-registration page is in use.

SelfRegistrationGroupName – The group name for the self-registered users. If the group specified here exists in the database, self-registration is enabled for Telescope, if the group does not exist in the database, self-registration is disabled.

DefaultContentEncoding – This is the HTML encoding. If not set, WebObjects encoding ISO-8859-1 (ISO Latin 1). Examples: DefaultContentEncoding = "Cp1252" DefaultContentEncoding = "UTF-8"

PredefinedPassword – The predefined password that is stored in the Telescope database users table when the LDAP plugin is being used. If users have this password value and request password updates from Telescope, they are provided a pre-defined message to use LDAP to change their password. It is recommended that you leave this value as is. (Contact Professional Services if you want to change it.)

secureSessionID – By default, “true” (meaning the session ID is hidden). Set to “false” to expose the session ID (due to onsite customization, multiple TSWeb application servers, or some other reason).

RelatedFileTypeList — Optional attribute that associates related file type extensions in Telescope Uploader, for the check-in process. This allows TSWeb users to check in a docx file (for example), even if the checked out file had a "doc" extension. By default this parameter has the following values (add others using the same format shown in this default): RelatedFileTypeList = (("doc", "docx"), ("xls", "xlsx"), ("ppt", "pptx"));

TelescopeUploaderVersion – Specifies the version of the Telescope Uploader to be used by TSWeb clients. This value needs to be updated when a service pack is installed that includes updates to the Uploader. If the version on their machine is out of date, users will be prompted to install the latest version.

TelescopeUploaderType – Versioning information that identifies which version of the Telescope Uploader needs to be used.

TelescopeUploaderName – Versioning information that identifies which version of the Telescope Uploader needs to be used.

TelescopeUploaderClassid – Versioning information that identifies which version of the Telescope Uploader needs to be used.

TelescopeUploaderSecure – Encrypts user names, passwords and session IDs when they are sent across the network to/from the Telescope Uploader. By default this preference is on ("TRUE"), for your enhanced security.

UploadMaxChunkSize – For the Telescope Uploader, the maximum data chunk size that can be processed during the upload stream.

downloadNonZippedAssets – Enables Download Cart users to download files. Enabled by default.

downloadZippingControl – Enables Download Cart users to choose whether or not to zip multiple files. Enabled by default.

NOTE: Multiple files are typically zipped into a download.zip file. To prevent this behavior, change the following settings: unless the following settings are set in the TSWeb config.list file:

```
downloadNonZippedAssets="true";
downloadZippingControl="NEVER";
```

In addition, the DLManager info.plist file must have the following setting:

```
<key>shouldCompressFiles</key>
  <string>N</string>
```

---

useHTML5Player – Leave as is.

anyUserCanAdminAdvanceSearch – Enables TSWeb users to create and update their own private advanced searches (off—”false”—by default). For details, see the *Telescope Administator's Reference Manual*.

MaxDownloadCartAssets – Enforces a limit for the number of items in the Download Cart. For details, see the *Telescope Administator's Reference Manual*.

We have added functionality to hide the submit and skip buttons that appear on challenge forms (some organizations may have changed these buttons to read “Continue” or some other phrase). Often, these buttons are not required because there is already an OK button for users to exit the form.

challengeFormSubmitButton – Enables the removal of the Submit and/or Skip buttons from challenge forms. By default, the challengeFormSubmitButton option is “true” and forces both buttons to appear by default. You must explicitly add this option and set it to “false” before you can hide the buttons:

challengeFormSubmitButton = “false”;

With this option set to false, you can then go to any Metadata Update Functional Rule and leave an empty string between quotation marks for either or both of these options; that is, submit=”” or skip=””. For example,

<?xml version=”1.0” encoding=”UTF-8” standalone=”yes”?> <challengeform> <displayattrs heading=”Asset Security” submit=”” skip=”” abort=”OK”/> <html><div style=”text-align: center;”>”You are not allowed to edit the asset metadata.”
 </html> </challengeform>

maxAssetSelectionLimit – Limits the number of assets that can be selected by TSWeb users from a set of search results. By default, it is 1900, but you can edit the value and change it to a higher value. For example, maxAssetSelectionLimit = "50000". 50,000 is the recommended maximum.

As of version 9.4.0.7, larger values will work fine with most actions performed on selected assets, such as change multiple, add to collection, import, attach renditions, download. It is not recommended to use a value greater than 2500 if there will be delete actions of this large number of assets (although this restriction may change in future releases.

14.5 Other Settings

14.5.1DBUtils

These options help prevent full Solr re-indexing.

com.northplains.dbutils.xml

NOTE: By default, this configuration file is at `C:\TeleScope\com.northplains.dbutils.xml`

---

queryTimeoutInterval

The maximum time to wait for an SQL query to complete (default 1000 milliseconds)

queryRetryAttempts

The number of attempts before giving up (default 1)

Note that the timeout value will increase by its own value every retry. That is, if the timeout is 3000 milliseconds and the number of attempts is set to 3, then the query timeouts would be as follows:

- 1st attempt = 3000 milliseconds (total aggregated wait time 3000 seconds)
- 2nd attempt = 2*3000 = 6000 milliseconds (total aggregated wait time 9000 seconds)
- 3rd attempt = 3*3000 = 9000 milliseconds (total aggregated wait time 18000 seconds)

14.5.2Annotation Stroke Width Configuration

The default setting for the annotation stroke width is 2 pixels. This can be changed to either 5 or 10 pixels.

To change the stroke width default setting

1. Using a text editor, open `DocInfoViewContainer.strings` file located in *\Telescope\Applications\tsweb.woa\Contents\Resources*
2. Locate **AnnotationStrokeWidth** and change it to the desired value.

14.5.3Update Maximum Number of Assets Viewable in Filmstrip and Side-by-Side Views

Users may find the Filmstrip View and Side-by-Side Views disabled, with the message “View inactive due to over limit assets.” This situation occurs when users try to view more than the maximum number of assets for these views. By default, this maximum value is 500.

This maximum value is configurable on a site-by-site basis, and is set with the `MaxAssetInPhotoPortal` setting in each site’s `CatalogViewWrapper.strings` file.

NOTE: Since there is no pagination for filmstrip view, as the number of items approaches and exceeds the default (even if configured for more than the default) performance reduces as all thumbnails must be populated in the filmstrip. **It is not recommended to exceed the default.**

Example:

For example, update the following value:

```
MaxAssetInPhotoPortal = "500";
```

In **all** `CatalogViewWrapper.strings` files that are being used. For example (default installation paths are shown):

- For the new "mktdemo" skin

  ```
  D:\Apps\TeleScope\Applications\tsweb.woa\Contents\Resources\Sites\mktdemo\Resources\Languag
  e\default\CatalogViewWrapper.strings
  ```

- For the original "default" skin:

  ```
  D:\Apps\TeleScope\Applications\tsweb.woa\Contents\Resources\Sites\default\Resources\Languag
  e\default\CatalogViewWrapper.strings
  ```

- For any language skin, such as:

  ```
  D:\Apps\TeleScope\Applications\tsweb.woa\Contents\Resources\Sites\mktdemo\Resources\Languag
  e\fr_CA\CatalogViewWrapper.strings
  ```

14.6 Java Applets

There are five Java applets installed with Telescope:

TSWFileDropCollect.jar – This drag-and-drop applet is used when you drag a file to the import icon in-order to import a file.

TSWUploadCollect.jar – Shows when you click on the import icon in order to import a file.

TSWLocate.jar – Used when you do a Locate Document.

TSWUpload.jar – Used by the Check-in operation to upload a binary file.

TSWUploadApplet.jar – The first ingest-progress-bar page that shows when you import a file. This applet is the first in a series of 2 or 3 HTML pages. Also called the long response page.

NOTE: Both TSWFileDropCollect and TSWUploadCollect are used to collect the XML info about the files being imported. For example, the filenames, sizes, and location. These applets only collect the basic information and do not import the actual binaries.

Chapter 15: Telescope Registry Keys

The registry keys settings for the various Telescope brokers are can be found from the Registry Editor, at *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\North Plains Systems*.

15.1 Authentication Broker

Key	Description	Default Value
CLASSPATH	The Java JVM class path setting.	
HUBIP	The IP, hostname, or fully qualified domain name of the Telescope Hub computer.	
HUBPORT	The port number of the Telescope Hub computer.	
LOGFILE	The path to Authentication Broker log file. If omitted, the default is <*install directory*>\logs\authb.log.	
LOGLEVEL	The level of message logging in the log file.	Valid values are: LOG_EMERG, LOG_ALERT, LOG_CRIT, LOG_ERR, LOG_WARNING, LOG_NOTICE, LOG_INFO,CPP_LOGLEVEL, and LOG_DEBUG. If omitted, the default is LOG_NOTICE
IIOP_PORT	Authentication Broker's listening port. If omitted, Authentication Brokers use a system assigned port.	
IIOP_HOST	The Internet Inter ORB Protocol host name used by the Authentication Broker. If the host name has not been set, then the local IP address is used. If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address), instructions are provided under the "Firewall Configuration" section in the *Telescope Installation and Configuration Guide for Windows Server Edition*.	
MAX_CONNECTION_IN_POOL	Maximum DB connection pool size.	Default is 2.
MIN_CONNECTION_IN_POOL	Minimum DB connection pool size.	1
PLUGIN_DIRECTORY	The path to the Authentication Broker's plugins folder.	Default value is: <*install directory*>\ABPlugins.
PREFSML_FILE	The file name and path to the Authentication Broker's PrefsML file.	Default value is: <*install directory*>\com.northplains.authenticationbroker.xml.
CONN_NAME_IDLE_TIMEOUT	The idle timeout limit for a connection name, in seconds.	Default is 3600.

Key	Description	Default Value
CONNECTION_IDLE_TIMEOUT	The idle timeout limit for a database connection, in seconds.	Default is 3600.
JVM_HEAP_SIZE	Each Java application has a default heap size. If a particular application uses a lot of memory, the heap size, specified in megabytes, can be changed via this variable. For example, if you want a heap size of 512 megabytes, then type “512M” (without the quotes).	Recommended maximum setting is 1024M.

15.2 Connection Broker

Key	Description	Default Value
CLASSPATH	The Java JVM class path setting.	
HUBIP	The IP, hostname, or fully qualified domain name of the Telescope Hub computer.	
HUBPORT	The port number of the Telescope Hub computer.	
LOGFILE	The path to the Connection Broker log file.	If omitted, this defaults to <*install directory*>\Logs\cb.log.
LOGLEVEL	The level of message logging in the log file.	Valid values are: LOG_EMERG, LOG_ALERT, LOG_CRIT, LOG_ERR, LOG_WARNING, LOG_NOTICE, LOG_INFO, and LOG_DEBUG. If omitted, the default is LOG_NOTICE.
IIOP_PORT	Connection Broker's listening port. If omitted, Connection Brokers use a system assigned port.	
IIOP_HOST	The Internet Inter ORB Protocol host name used by the Connection Broker. If the host name has not been set, then the local IP address is used. If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address), instructions are provided under the "Firewall Configuration" section in the *Telescope Installation and Configuration Guide for Windows Server Edition*.	
NOTIFY_FAIL_TIMEOUT	The amount of time, in milliseconds, the Connection Broker waits before terminating the connection with a subscriber.	If omitted, the default is 1000ms.
NUMBER_OF_WORKERS	The number of workers the notification message is dispatched to.	If omitted, the default is 3.
XML_DATA_FILE	The path to the XML data file.	If omitted, the default is <*install directory*>\cb_data.xml.

15.3 Distribution Broker Configuration

The Distribution Broker configuration parameters are set under the registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\North Plains Systems\Distribution Broker\CurrentVersion

During installation, the Distribution Broker creates a default set of configuration parameters in the above registry key.

The following is the list of configurable parameters for the Distribution Broker.

Key	Description	Default Value
CLASSPATH	The Java JVM class path setting.	
CONV_WORKER_IDLE_TIMEOUT	Specifies the timeout, in seconds, of the conversion worker thread.	If omitted, the default is 3600.
DISTB_PREFSML	Points to the Distribution Broker's XML Configuration File. The XML file name is: com.northplains.distributionbroker.xml This step is performed by the installer.	
DPIECE_DIRECTORY	The full path to the Distribution Broker's Destination I-Pieces directory. This step is performed by the installer.	$InstallationDirectory\DPieces
HUBIP	The IP, hostname, or fully qualified domain name of the Telescope Hub server.	
HUBPORT	The port number of the Telescope Hub server. Typically 12345.	
IIOP_PORT	The Internet Inter ORB Protocol port number used by the Distribution Broker. If the port number has not been set, then a random open port is used.	
IIOP_HOST	The Internet Inter ORB Protocol host name used by the Distribution Broker. If the host name has not been set, then the local IP address is used. If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address), instructions are provided under the “Firewall Configuration” section in the *Telescope Installation and Configuration Guide for Windows Server Edition*.	
JVM_HEAP_SIZE	Each Java application has a default heap size. If a particular application uses a lot of memory, the heap size, specified in megabytes, can be changed via this variable. For example, if you want a heap size of 512 megabytes, then type “512M” (without the quotes).	Recommended maximum setting is 1024M.
LOGFILE	If an error is encountered by Telescope, then a log file is generated for the Telescope developers to examine. This is the Log file name. This step is performed by the installer.	InstallationDirectory\Logs\distb.log

Key	Description	Default Value
LOGLEVEL	This setting determines the type of information and the level of detail that is included in the log file. The various log levels are in the following hierarchy, and each level contains all of the information included in the previous levels. the default value is “LOG_NOTICE”. This step is performed by the installer. **LOG_CRIT**: Only the critical errors are included in the log file. **LOG_ERR**: Critical errors plus errors. **LOG_WARNING**: Critical errors, errors and warnings. **LOG_NOTICE**: Critical errors, errors, warnings and notices. **LOG_INFO**: Critical errors, errors, warnings, notices and general information. **LOG_DEBUG**: Critical errors, errors, warnings, notices, general information and debugging information. **Note**: If the LOGLEVEL is set to LOG_DEBUG then the XML configuration file is copied into the log file each time that a contract is executed, saved or modified. This can result in a very large log file.	
LOG_SQL	Set to “y”, every time the Distribution Broker prepares a SQL statement. The statement is then logged into the standard Distribution Broker log file.	
NUMBER_OF_WORKERS	The number of sub-processes issued by the Distribution Broker. The number of workers configured defines the maximum number of contracts that can run simultaneously, in parallel. Increasing it will allow more, different contracts to run at the same time, but also will consume more system resources. The default value is the DISTB_NUM_WORKERS value, from the Distribution Broker's XML Configuration File set during installation.	
MAX_CONV_WORKERS	Specifies the maximum number of Conversion Request Handling workers. You can use the maximum number to limit the number of worker threads for the distribution broker.	
REQUEST_IDLE_TIMEOUT	The timeout limit for determining whether a communication with a client is lost. The timeout request skips any interaction part with the client and continues processing, assuming communication with the client has been lost.	Default is 300.

Key	Description	Default Value
USE_TIMESTAMP_SUBFOLDER	Whether to use time stamped distribution sub-folders or not. When this value is set to 0, the Distribution Broker does not create time stamped sub-folders.	When set to 1, the default, the Distribution Broker creates time stamped sub-folders.
WORKER_START_PORT	The Distribution Broker uses separate processes for its workers to perform work. The Distribution Broker communicates with these workers via a socket. When the Distribution Broker starts up, it creates a number of workers, each with a specific port number. The first worker gets the port number specified by this setting. Each subsequent worker is assigned a port that is an increment relative to the first worker. For example, if the first worker uses port 30000 and the Distribution Broker creates 3 workers, the subsequent ports used are 30001, 30002, and 30003, respectively.	
XML_DATA_FILE	The path of the PrefsML (XML) file for the Distribution Broker	If omitted, the default is <*installdirectory*>\db_data.xml.

15.4 File Broker

Key	Description	Default Value
BINDING_NAME	The File Broker binding name on the NameServer, if not set, will use the localhost name for the File Broker.	
CONVERSION_TIMEOUT	The timeout, in seconds, that the File Broker waits for a conversion to complete.	Default value for this key is 3600.
CONVERTER_IDLE_TIMEOUT	The timeout setting for the FBConverter subpress to stop when idle for the specified the timeout period.	
CONVERTER_RSS_MAX	The Maximum RSS setting for the FBConverter process.	
CONVERTER_VMEM_MAX	The Maximum VMEN setting for the FBConverter process.	

Key	Description	Default Value
FBCOPY_CHUNKSIZE	(NTFS File Broker **only**) The size of the “chunks” in kilobytes the File Broker will break a file into when copying files to and from the File Broker computer. The maximum value, under standard installations, must be less than 2048. A value of 1792 would be considered allowable. The limitation comes from the omniORB library that the File Broker uses. It has a default maximum message size of 2048 KB. The copy chunk size must fit within that message size, taking into account message overhead. **To increase the omniORB message size:** The omniORB message size can be increased to allow values of FBCOPY_CHUNKSIZE greater than 2048, but the customer does so at their own risk as this is not fully tested configuration by Northplains. To increase the omniORB message size to allow FBCOPY_CHUNKSIZE to be greater than the default maximum, add an entry in the registry here: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\omniORB Add a new string entry as follows: giopMaxMsgSize = <size in bytes> For example, for FBCOPY_CHUNKSIZE of 3072, the omniorb maximum message size would need to be larger, say 4MB. giopMaxMsgSize = 4194304 Further information on this and other omniORB configuration options can be found in the ominORB 4.1 documentation guide at this URL: http://omniorb.sourceforge.net/omni41/omniORB/omniORB004.html	By default the chunk size is 768KB. Increasing this value may speed up file transfer if network overhead is causing a delay. The maximum value, under standard installations, must be less than 2048. (See Description.)
FB_CONVERTER_PATH	Full directory path location of the fbconverter executable file. This path is set by the installer, and generally should not need to be adjusted manually.	By default, the same directory location as the file broker executable file.
FILEINFO_FILE_SUFFIX	Set the Fileinfo file extension for non-NTFS file systems.	
HUBIP	The IP, hostname, or fully qualified domain name of the Telescope Hub computer.	

Key	Description	Default Value
HUBPORT	The port number of the Telescope Hub computer.	
IIOP_PORT	The File Broker's listening port. If omitted the File Broker uses a system assigned port.	
IIOP_HOST	The Internet Inter ORB Protocol host name used by the File Broker. If the host name has not been set, then the local IP address is used. If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address), instructions are provided under the "Firewall Configuration" section in the *Telescope Installation and Configuration Guide for Windows Server Edition*.	
INIT_CHILD_READY_TIMEOUT	The waiting timeout, in seconds, of the first subprocesses to be ready on the Broker parent process.	Default is 30.
IOR_LOGGING	A log will start for the IOR string for debugging purposes if set to "y".	
LEAVE_FILE_OPEN	Set to "Y" to keep the physical file open when the File Broker is in a read/write operation.	
LOGFILE	The path to File Broker log file.	Default is <*install directory*>\logs\fb.log.
LOGLEVEL	The level of message logging in the log file.	Valid values are: LOG_EMERG, LOG_ALERT, LOG_CRIT, LOG_ERR, LOG_WARNING, LOG_NOTICE, LOG_INFO, and LOG_DEBUG. If omitted, the default is LOG_NOTICE.
MAX_ERR_LIST_LENGTH	The maximum length of the error list.	
MAX_NUMBER_OF_CONVERTER	The maximum number of FBConverter subpress can be created.	
NON_NTFS	Set to "Y" if the file system is not NTFS.	
REFRESH_CYCLE	The interval in seconds that the File Broker communicates with secondary hubs in a multi-hub scenario to refresh the conversion options cache.	Default value is "600".

Key	Description	Default Value
RESOURCE_FILE_SUFFIX	The resource file extension for non-NTFS file systems. **Note:** Resource files must be opened in text editors that preserve their UTF-8 character set.	
SIZE_SELECT_QUEUE	Used on Solaris systems only. Sets the file path pointing to a converter Queue configuration file.	
STARTUP_TIMEOUT	Timeout for the process to start.	
TEMP_DIR	The temporary directory used by the file broker for file conversion.	Default is *C*:\Temp.
TEMP_FILE_DELETE_TIMEOUT	The time between deletes of temporary files created by other components (C-Pieces), in the event they crash or time out. If a temporary file is older than this setting, it is deleted.	Default is 14,400 (4*60*60) seconds (that is, 4 hours). Minimum is 3600 (1*60*60) seconds (that is, 1 hour).

15.5Graphics Broker

Key	Description	Default Value
BINDING_NAME	The Graphics Broker binding name on the NameServer.	If not set, will use the local hostname for the Graphics Broker.
BYPASS_FB_4_LOCAL_FILE	A flag to make the Graphics Broker access files directly when it can translate a file location to a local path. Valid values are "y" or "n", case insensitive. If set to "n", the Graphics Broker will always access and download files from the File Broker.	If omitted, the default is "y"
DB_ACCESS_IDLE_LIMIT	The timeout limit for an idle connection, in seconds.	Default is 3600. Recommended not to change the default setting.
DB_IPIECE_CHECK_INTERVAL	The interval that the Graphics Broker sub-process scan from newer I-Pieces, in seconds	Default is 1800. Recommended not to change the default setting.
DB_SCAN_INTERVAL	The interval that connections are scanned for idling, in seconds.	Default is 300. Recommended not to change the default setting.
DEFAULT_GB	This flag registers Graphics Broker as a default Graphics Broker. Valid values are “y” or “n”, case insensitive.	Default is “n”.
DUMP_THUMBNAIL	When a thumbnail is created “_thumbnail” is appended to the suffix of a jpg format file.	
ENCRYPT_PREVIEW	Controls whether thumbnails and viewex previews are encrypted in the database. Valid values are “y” or “n”, case insensitive.	Default is N if not set.
FB_CONFIG	(Internal Use Only.)	

Key	Description	Default Value
FILE_ACCESS_RETRY_TIMEOUT	The specified time, in full seconds, that will pass before another attempt is made to access files ingested into Telescope that need preview processing. Increasing this setting is sometimes necessary when a file broker share is a remotely mounted network volume. Values of 10-30 seconds may be necessary. Local disk broker shares generally don't need this value to be changed. An indication that this setting may need to be increased is if there is a Graphics Broker log entry like the following, even when you know the file was just placed there in an ingest process: [WARNING] FBClient::GetFileLocal(): The Locally resolved file [\\NETWORK_SERVER\Volume\Share1\file.mov] does not exist ...	Default is 2.
GENERATE_WATERMARK	This flag generates a watermark on extended views.	Valid values are “y” or “n”, case insensitive. If omitted, the default is “n”.
GRAPHICS_TIMEOUT	The timeout (in seconds) for the Graphics Broker to give up on a preview request for a file.	Default (and minimum enforced value) is 600 seconds, no maximum is specified.
HUBIP	The IP, hostname, or fully qualified domain name of the Telescope Hub computer.	
HUBPORT	The port number of the Telescope Hub computer.	
IIOP_PORT	Graphics Broker’s listening port.	If omitted, Graphics Brokers use the system assigned port.
IIOP_HOST	The Internet Inter ORB Protocol host name used by the Graphics Broker. If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address), instructions are provided under the “Firewall Configuration” section in the *Telescope Installation and Configuration Guide for Windows Server Edition*.	Default is the local IP address is used.
INIT_CHILD_READY_TIMEOUT	The waiting timeout, in seconds, of the first sub-processes to be ready on the Graphics Broker parent process.	Default is 30.

Key	Description	Default Value
INIT_CHILD_STARTUP_TIMEOUT	Timeout for the 1st child process to start.	Minimum value is 10 seconds. Recommended not to change the default setting.
IPIECE_DIR	Location of the directory for the I-Piece.	
IPIECE_SCAN_INTERVAL	The interval that the Graphics Broker sub-process scan from newer I-Pieces, in seconds.	Default is 1800.
LOG_CALLBACK	Log information about callback functions.	Valid values are “y” or “n”, case insensitive. If omitted, the default is “n”.
LOG_IOR	Log information about CORBA.	Valid values are “y” or “n”, case insensitive. If omitted, the default is “n”.
LOG_SQL	Log information about SQL query or database connection.	Valid values are “y” or “n”, case insensitive. If omitted, the default is “n”.
LOGFILE	The path to Graphics Broker log file. It is recommended to specify this path as <*install directory*>\GB\logs\gb.lo.	If omitted, the default is C:\gb.log.
LOGLEVEL	The level of message logging in the log file.	Valid values are: LOG_EMERG, LOG_ALERT, LOG_CRIT, LOG_ERR, LOG_WARNING, LOG_NOTICE, LOG_INFO, and LOG_DEBUG. If omitted, the default is LOG_NOTICE.
MAX_NUMBER_OF_WORKER	The maximum number of sub-processes in Graphics Broker. Valid values are integers that are greater than or equal to one, or a negative number. A negative value means maximum value of six. If omitted, the default is three.	Default is 3. Maximum is 6.
PROPERTY_TIMEOUT	The timeout (in seconds) for the Graphics Broker to give up on a property request for a file.	Default (and minimum enforced value) is 600 seconds, no maximum is specified.
SERVING_HOSTS	The Graphics Broker’s serving host. Valid values are comma separated of File Broker host names, in upper case.	Default is the local host name.

Key	Description	Default Value
TEMP_DIR	The temporary folder path the Graphics Broker uses to store temporary files while a file is being downloaded from the File Broker. The provided path will be to the TMP directory environment variable in Windows, or the TMPDIR environment variable in Unix. The path must be a valid path on the machine.	
TEMP_FILE_DELETE_TIMEOUT	The time between deletes of temporary files created by other components (I-Pieces), in the event they crash or time out. If a temporary file is older than this setting, it is deleted.	Default is 14,400 (4*60*60) seconds (that is, 4 hours). Minimum is 3600 (1*60*60) seconds (that is, 1 hour).
WATERMARK_FONT	The font name that is used to display the text in the watermark.	Default is an empty string.
WATERMARK_ON_THUMBNAIL	This flag generates a watermark on thumbnails.	Valid values are “y” or “n”, case insensitive. If omitted, the default is “n”.
WATERMARK_POSITION	The position of the watermark against its background.	Valid values are “TOP”, “MIDDLE” and “BOTTOM”. If omitted, the default is “MIDDLE”
WATERMARK_TEXT	The text that appears in the watermark.	Default is an empty string.
WORKER_IDLE_TIMEOUT	The timeout limit for an idle Graphics Broker sub-process, in seconds. Sub-processes cease when this value is met, unless it is the last process.	Default is 21600 (6 hours). Recommended not to change the default setting.

15.6 InDesign Server

For the InDesign Server registry settings, see the *Telescope – InDesign I-Piece and Conversion I-Piece Manual*.

15.7 Indexing Broker and Child Indexing Brokers

For details on configuring the Indexing Broker and its Child Indexing Brokers for Solr Search functionality, see the *Telescope Administrator's Reference Manual*.

Key	Description
CLASSPATH	The Java JVM class path setting.
HUBIP	The IP, hostname, or fully qualified domain name of the Telescope Hub computer.
HUBPORT	The port number of the Telescope Hub computer.
IIOP_HOST	The Internet Inter ORB Protocol host name used by this Broker. If the host name has not been set, then the local IP address is used. If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address), instructions are provided under the "Firewall Configuration" section in the *Telescope Installation and Configuration Guide for Windows Server Edition*.
IIOP_PORT	This Broker's listening port. If omitted, uses a system assigned port.
LOGFILE	The path to this Broker's log file. If omitted, the default is <*install directory*>\logs\idx.log.
LOGLEVEL	The level of message logging in the log file. Valid values are: LOG_EMERG, LOG_ALERT, LOG_CRIT, LOG_ERR, LOG_WARNING, LOG_NOTICE, LOG_INFO,CPP_LOGLEVEL, and LOG_DEBUG. If omitted, the default value is LOG_NOTICE
PREFSML_FILE	The file name and path to this Broker's PrefsML file. Default value is: <*install directory*>\com.northplains.authenticationbroker.xml.

15.8 Ingest Broker

Key	Description	Default Value
AUTO_INGEST_CONFIG_FILE	Auto-ingest configuration file path.	
AUTO_QUEUE_PATH	Configures where to store auto-ingest, run-time state information. This state information is used to track files queued for processing in an auto-ingest folder. It is also used to keep track of the queue state in order to resume pending operations if the broker is shut down while there are still files to process. UPGRADE NOTE: Ensure there are no pending auto-ingest operations when updating from 9.1.4-P3 to 9.2.1 or later. An early version of the queue state management was introduced in 9.1.4-P3. In that release, the queue management was stored within the hot folders inside each top-level hot folder in Ingest Folder\ProcessQueue. That old location is no longer used and will be ignored after installing the newer version (so any pending auto-ingest operations will be lost). The location can be safely removed after updating the environment.	The following path: [Telescope IngestBroker directory]\var\ AutoIngestQueues
BROADCAST_INCOMPLETE_CAT	Set this value to 1 to configure the Ingest Broker to send a Telescope message when an incomplete catalog is created. Otherwise, set to 0 or omit this entry.	
CLASSPATH	The Java JVM class path setting.	
CONN_NAME_IDLE_TIMEOUT	The idle timeout limit for a connection name, in seconds.	Default is 3600.
CONNECTION_IDLE_TIMEOUT	The idle timeout limit for a database connection, in seconds. If omitted, the	Default is 3600.
GB_OBJ_REFRESH_TIMEOUT	Time interval to refresh Graphics Broker object reference from the Name Service. The Graphics Broker objects whose age exceeds this timeout are purged and a new reference is fetched from the Name Service.	Default is 1800.
GB_TIMEOUT	The timeout limit for waiting on Ingest related Graphics Broker operations to complete. If the Graphics Broker processes large files it might not get back to the Ingest Broker in time to complete creating a catalog. If this happens, increase the timeout setting.	Default 1800.
GRAPHICS_RETRY_PAUSE	The length of time between tries for Graphics Broker calls, in milliseconds. The number of calls is determined by MAX_GRAPHICS_TRIES.	1000 (one second).

Key	Description	Default Value
HUBIP	The IP, hostname, or fully qualified domain name of the Telescope Hub computer.	
HUBPORT	The port number of the Telescope Hub computer.	
IIOP_PORT	The Internet Inter ORB Protocol host name used by the Ingest Broker. If the host name has not been set, then the local IP address is used.	
IIOP_HOST	The Internet Inter ORB Protocol host name used by the Ingest Broker. If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address), instructions are provided under the "Firewall Configuration" section in the *Telescope Installation and Configuration Guide for Windows Server Edition*.	Default is the local IP address is used.
INDEXING_WAIT	A configurable delay in the processing of asset deletions by the Ingest Broker, to better avoid race conditions and ensure the assets are removed from the Telescope database. This delay happens only while deleting data from Telescope after a functional rule failure.	2 seconds.
JDBC_CLASS_ORACLE	Oracle JDBC Class name.	Default value is "oracle.jdbc.driver.OracleDriver".
JDBC_CLASS_SQLSERVER	MS SQL Server JDBC Class name. Set it to "net.sourceforge.jtds.jdbc.Driver" for jtds-1.1.jar or jtds-1.2.jar.	
JDBC_CLASS_SYBASE	Alternative Java Class name for Sybase JDBC driver.	Default: com.sybase.jdbc22.jdbc2.SybDriver
JVM_HEAP_SIZE	Each Java application has a default heap size. If a particular application uses a lot of memory, the heap size, specified in megabytes, can be changed via this variable. For example, if you want a heap size of 512 megabytes, then type "512M" (without the quotes).	Recommended maximum setting is 1024M.
LOGFILE	The path to Ingest Broker log file.	Default is <*install directory*>\logs\ib.log.

Key	Description	Default Value
LOGLEVEL	The level of message logging in the log file.	Valid values are: LOG_EMERG, LOG_ALERT, LOG_CRIT, LOG_ERR, LOG_WARNING, LOG_NOTICE, LOG_INFO, and LOG_DEBUG. If omitted, the default is LOG_NOTICE.
LOG_REQUEST	Writes new Ingest Broker requests to the Ingest Broker request file (IBRequest.'ID".data located in the Log file directory.	
LOG_SQL	Logs SQL database query statements at the LOG_INFO level.	Valid values are "y" or "n", case insensitive. If omitted, the default is "n".
MAX_GRAPHICS_TRIES	The maximum number of times a Graphics Broker method is called again (retried). By default, there is a one second (1000 millisecs) pause between calls. (The time of the pause between retries can be adjusted with the key GRAPHICS_RETRY_PAUSE.)	Valid values are 1 or more. The default is 2 (meaning a total of 3 tries).
MIN_CONNECTION_IN_POOL	The minimum number of database connections in a connection name. Valid values are integers that are greater than or equal to 0.	If omitted, the default is 0.
MIN_NUMBER_OF_WORKERS	The minimum number of worker threads. Valid values are integers that are greater than or equal to 1.	If omitted, the default is one.
MAX_CONNECTION_IN_POOL	The maximum number of database connections in a connection name. Valid values are integers that are greater than MIN_CONNECTION_IN_POOL value or a negative number. Negative values mean unlimited.	Default is unlimited.
MAX_NUMBER_OF_WORKERS	The maximum number of worker threads. By default there is an unlimited number of Ingest Broker worker threads possible. The limit should be determined by the number of cores in the server for this configuration attribute. Be aware the number of workers for all Brokers when setting these parameters. A client's usage pattern will determine the best settings for the environment. If there is a small number of people responsible for imports along with a few hot folders, then a smaller number of Ingest Broker workers is required.	Valid values are integers that are greater than MIN_NUMBER_OF_WORKERS value or a negative number. Negative values mean unlimited. If omitted, the default is unlimited.

Key	Description	Default Value
MAX_USER_CACHE	Instructs the Ingest Broker to stop caching the user's data from the Telescope database. This setting may be required to disable caching if user privileges are being updated through LDAP (to ensure new settings take effect and are not ignored due to caching). To disable caching, use "MAX_USER_CACHE=0." A positive integer will limit the number of pieces of user data cached to that number. A negative integer will use unlimited caching. By default, this key is not specified (meaning that unlimited caching is used).	Default is unlimited.
METADATA_VALIDATION	If set to "N", it disables all metadata validation on Ingest regardless of any individual field settings.	Valid values are "Y" or "N", case insensitive. If omitted, the default is "Y".
NEW_DOC_THUMBNAIL_FILE	The path to the new-document thumbnail JPEG file.	
PROGRESS_THUMBNAIL_FILE	The path to the in-progress thumbnail JPEG file.	
REQUEST_IDLE_TIMEOUT	The timeout limit for determining whether a communication with a client is lost. The timeout request skips any interaction part with the client and continues processing, assuming communication with the client has been lost.	Default is 300.
SUPPRESS_USER_VALIDATION_ERRS	If set to "Y" it does not report server-side Ingest Metadata field validation errors to the user client.	Valid values are "Y" or "N", case insensitive. If omitted, the default is "N".
WORKER_IDLE_TIMEOUT	The idle timeout limit for a worker thread, in seconds. Timeout workers are removed from the pool and deleted.	Default is 3600.

* If the Graphics Broker processes large files it might not get back to the Ingest Broker in time to complete creating a catalog. If this happens, increase the timeout setting.

** By default there is a unlimited number of Ingest Broker worker threads possible. The limit should be determined by the number of cores in the server for this configuration attribute. Be aware the number of workers for all Brokers when setting these parameters. A client's usage pattern will determine the best settings for the environment. If there is a small number of people responsible for imports along with a few hot folders then a smaller number of Ingest Broker workers is required.

15.9 Lookup Broker Configuration

The Lookup Broker is installed as part of the Telescope installation process. A new key for the Lookup Broker created in the Windows registry:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\North Plains Systems\Lookup Broker\CurrentVersion]

The registry key defines several values that affect the execution of the Lookup Broker.

The following table lists the possible configuration entries and their default values.

Key	Description	Default Value
CLASSPATH	The Java JVM class path setting.	
HUBIP	IP of the machine hosting the Telescope Hub.	The IP you entered in the installation wizard.
HUBPORT	Port number of the machine hosting the Telescope Hub.	12345
JDBC_CLASS_SQLSERVER or JDBC_CLASS_ORACLE	The jdbc driver you are using to connect to the database.	net.sourceforge.jtds.jdbc.Driver or oracle.jdbc.driver.OracleDriver
LOGFILE	Path to the log file.	C:\Telescope\Logs\lb.log
LOGLEVEL	Logging level, which can be: LOG_ERR LOG_WARNING LOG_INFO LOG_DEBUG	LOG_INFO
QUERY_TIMEOUT	Number of seconds before the Lookup Broker aborts the current SQL query attempt. The minimum setting is 5 seconds.	Default is 600 seconds.
XMLFILE	Path to the XML configuration file.	C:\Telescope\lookup.xml
IIOP_PORT	Lookup Broker's listening port. If omitted, the system assigned port is used.t.	
IIOP_HOST	Internet Inter ORB Protocol host name used by the Lookup Broker. If the host name has not been set, then the local IP address is used. If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address), instructions are provided under the “Firewall Configuration” section in the *Telescope Installation and Configuration Guide for Windows Server Edition*.	

Key	Description	Default Value
DISABLE_SQUAREBRACKET_WILDCARD	When set to “Y” the left bracket character ‘[‘ is escaped in lookup quires. This allows the ‘[‘ to be used as a literal search character in lookup queries instead of being treated as the opening bracket in a wildcard search as supported by SQL Server. This has no impact for Oracle databases.	Default “N”.

15.10Message Broker

Key	Description	Default Value
CLASSPATH	The Java JVM class path setting.	
CONN_NAME_IDLE_TIMEOUT	The idle timeout limit for a connection name, in seconds.	Default is 3600.
CONNECTION_IDLE_TIMEOUT	The idle timeout limit for a database connection, in seconds. If omitted, the	Default is 3600.
HUBIP	The IP, hostname, or fully qualified domain name of the Telescope Hub computer.	
HUBPORT	The port number of the Telescope Hub computer.	
IIOP_PORT	Message Broker's listening port. If omitted, Graphics Brokers use the system assigned port.	
IIOP_HOST	Message Broker's Host Name (or IP). If not set, it uses the local IP. If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address), instructions are provided under the "Firewall Configuration" section in the *Telescope Installation and Configuration Guide for Windows Server Edition*.	
JDBC_CLASS_ORACLE	Oracle JDBC Class name. If not set, the default value is "oracle.jdbc.driver.OracleDriver".	
JDBC_CLASS_SYBASE	Alternative Java Class name for Sybase JDBC driver.	Default: com.sybase.jdbc22.jdbc2.SybDriver
JDBC_CLASS_SQLSERVER	MS SQL Server JDBC Class name. Set it to "net.sourceforge.jtds.jdbc.Driver" for jtds-1.1.jar or jtds-1.2.jar.	
JVM_HEAP_SIZE	Each Java application has a default heap size. If a particular application uses a lot of memory, the heap size, specified in megabytes, can be changed via this variable. For example, if you want a heap size of 512 megabytes, then type "512M" (without the quotes).	Recommended maximum setting is 1024M.
LOGFILE	The path to Message Broker log file.	Default is <*install directory*>\logs\mb.log.

Key	Description	Default Value
LOGLEVEL	The level of message logging in the log file.	Valid values are: “LOG_DEBUG”, “LOG_INFO”, “LOG_NOTICE”, “LOG_WARNING”, “LOG_ERR”, and “LOG_CRIT”. If omitted, the default is LOG_NOTICE.
LOG_SQL	If set to “y”, it logs SQL Database query statements at the LOG_INFO level.	
MIN_CONNECTION_IN_POOL	The minimum number of database connections in a connection name. Valid values are integers that are greater than or equal to 0.	If omitted, the default is 0.
MAX_CONNECTION_IN_POOL	The maximum number of database connections in a connection name. Valid values are integers that are greater than MIN_CONNECTION_IN_POOL value or a negative number. Negative values mean unlimited.	Default is unlimited.
SMTP_SERVER	SMTP server address of the Mail Server to be used for external messaging. To be specified in the format “mail.mycompany.com” (without quotes).	
TSWEB_LOGIN_PAGE	URL of Telescope login page in the format “Telescope.mycompany.com/scripts/WebObjects.dll/tsweb82”.	

15.11 Multi-Hub Settings

To allow the File Broker to register to multiple Hubs:

1. On the computer running the File Broker, start RegEdit and locate the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\North Plains Systems\MultiHubs

2. Add a DWORD value for each Hub you want the File Broker to register. Set the value name to the Hub's IP address and the value data to the Hub's port number.

15.12Queue Broker Registry Keys

When the Queue Broker is installed, a new key is created for it in the Windows registry:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\North Plains Systems\QueueBroker\CurrentVersion]

The registry key defines values that affect the execution of the Queue Broker, as summarized in the following table.

Key	Description	Default Value
CLASSPATH	The Java JVM class path setting.	
HUBIP	The IP, hostname, or fully qualified domain name of the Telescope Hub server.	
HUBPORT	The port number of the Telescope Hub server. Typically 12345.	
JVM_HEAP_SIZE	Each Java application has a default heap size. If a particular application uses a lot of memory, the heap size, specified in megabytes, can be changed via this variable. For example, if you want a heap size of 512 megabytes, then type “512M” (without the quotes).	Recommended maximum setting is 1024M.
LOGFILE	The path to Queue Broker log file.	Default is <*install directory*>\logs\qb.log.
LOGLEVEL	The level of message logging in the log file. Valid values are: “LOG_DEBUG” (very verbose, use only for short time spans), “LOG_INFO”, “LOG_NOTICE”, “LOG_WARNING”, “LOG_ERR”, and “LOG_CRIT” (critical errors only).	If omitted, the default is LOG_NOTICE.
IIOP_HOST	Queue Broker’s Host Name (or IP). If not set, it uses the local IP. If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address), instructions are provided under the “Firewall Configuration” section in the *Telescope Installation and Configuration Guide for Windows Server Edition*.	
IIOP_PORT	Message Broker’s listening port. If omitted, Graphics Brokers use the system assigned port.	
CONNECTION	The name (as defined in cb_data) for the default database for the Queue Broker to connect to.	
LICENSE	The type of licensing used - "USER" to use a content creator license - "BROKER" to use the Queue Broker license	

Key	Description	Default Value
BROKER_ID	The identifier for the Queue broker if multiple brokers are needed to run against the same database.	
THREADS	The maximum number of threads that will run at the same time.	
PREFSML_FILE	The file name and path to the Queue Broker's PrefsML file.	Default value is: <install directory>\com.northplains.broker.queue.xml.

15.13Session Broker

Key	Description	Default Value
HUBIP	The IP, hostname, or fully qualified domain name of the Telescope Hub computer.	
HUBPORT	The port number of the Telescope Hub computer.	
LOGFILE	The path to Session Broker log file.	Default is <*install directory*>\logs\sesb.log.
LOGLEVEL	The level of message logging in the log file. **Note:** When the Telescope system starts up, it checks for a CONSUMERACCESS license in the Session Broker. Telescope no longer requires this license, and users can ignore the error message that is shown in the Session Broker log file warning that this license is missing.	Valid values are: LOG_EMERG, LOG_ALERT, LOG_CRIT, LOG_ERR, LOG_WARNING, LOG_NOTICE, LOG_INFO, and LOG_DEBUG. If omitted, default to be LOG_NOTICE.
SESSION_BROKER_ID	The Session Broker ID. Valid values are integers between 1 and 127.	
IIOP_PORT	Session Broker's listening port. If omitted, the system assigned port is used.	
IIOP_HOST	The Internet Inter ORB Protocol host name used by the Session Broker. If the host name has not been set, then the local IP address is used. If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address), instructions are provided under the "Firewall Configuration" section in the *Telescope Installation and Configuration Guide for Windows Server Edition*.	
HEARTBEAT_INTERVAL	Component heartbeat call interval, in seconds. Valid values are integers that are greater than or equal to 15.	Default to 30.
IDLE_TIMEOUT	Component idle timeout, in seconds. Valid values are integers that are greater than or equal to two times the HEARTBEAT_INTERVAL value. If omitted, default to be 1800 or twice the HEARTBEAT_INTERVAL value, which ever is greater.	
SESSION_LOGGING_INTERVAL	The interval for session information to be mirrored to disk, in seconds. If omitted, default to 15.	

Key	Description	Default Value
LOG_HEARTBEAT	Used to get more information about the IDL session.	Valid values are “Y”, “y”, “N”, or “n”.
SESB_CLOCK_YEAR	Session Broker clock year. Valid value is 2003 to the current year.	Default value is 2003.
LOG_LICENSE	Used for log information about the license.	Valid values are “Y”, “y”, “N”, or “n”.
ENABLE_MONITOR	Enables the monitor process in the Session Broker.	Valid values are “Y”, “y”, “N”, or “n”.
TOLERANCE	Used to allow for time difference (in minutes) between system clocks in a distributed environment. There are several types of events that the TOLERANCE setting accounts for: - latency events between Telescope servers (network latency) - system time events, for example network time updates, typically in milliseconds, that may occur monthly as directed by the universal GMT time clock. A TOLERANCE setting of 1 (1 minute) is recommended. This setting cannot exceed the amount of time of the HEARTBEAT_INTERVAL. With a default value of 30 seconds, the HEARTBEAT_INTERVAL would need to be changed to "60" to accommodate a 1-minute tolerance.	1 minute.

15.14State Broker

Key	Description	Default Value
HUBIP	The IP, hostname, or fully qualified domain name of the Telescope Hub computer.	
HUBPORT	The port number of the Telescope Hub computer.	
LOGFILE	The path to State Broker log file.	If omitted, the default is <*install directory*>\logs\sb.log.
LOGLEVEL	The level of message logging in the log file.	Valid values are: LOG_EMERG, LOG_ALERT, LOG_CRIT, LOG_ERR, LOG_WARNING, LOG_NOTICE, LOG_INFO, and LOG_DEBUG. If omitted, the default is LOG_NOTICE.
FCB_DIR	The File Conversion Broker directory.	
IIOP_PORT	State Broker's listening port. If omitted, the system assigned port is used.	
IIOP_HOST	The Internet Inter ORB Protocol host name used by the State Broker. If the host name has not been set, then the local IP address is used. If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address), instructions are provided under the "Firewall Configuration" section in the *Telescope Installation and Configuration Guide for Windows Server Edition*.	
STATE_LOGGING	Enable/disable logging for file state changes.	Valid values are "Y" or "N". If omitted, the default is "N".
GLOBAL_VAR_LOG_DIR	The path to the folder in which the global variable data file is created and maintained.	Default is "."
GLOBAL_VAR_LOG_INTERVAL	The interval (in seconds) to flush global variable data to the data file. If omitted, the default is 15 seconds.	

Key	Description	Default Value
RECORD_SCAN_INTERVAL	The interval (in seconds) to remove stale file state records. If omitted, the default is 3600 seconds.	
OPEN_RECORD_TIMEOUT	The timeout (in seconds) for an open file state record to be considered stale and be removed in the next record scan. If omitted, the default is 86400 seconds (one day).	
IDLE_RECORD_TIMEOUT	The timeout (in seconds) for a closed file state record to be considered stale and be removed in the next record scan. If omitted, the default is 604800 seconds (one week).	
CONV_REC_LOGGING	Enable/disable logging for conversion record changes.	Valid values are “Y” or “N”, If omitted, the default is “N”.

15.15Zoom Broker Configuration

The Zoom Broker must be installed before you can perform the following configuration procedure.

Set the following values in the Windows registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\North Plains Systems\Zoom Broker\CurrentVersion

The following is a list of configurable parameters for the Zoom Broker.

Key	Description	Default Value
HUBIP	The IP address, machine name, or DNS of the Hub to register the Zoom Broker with.	localhost
HUBPORT	The Hub IP Port number.	12345
LOGFILE	The log file name.	InstallationDirectory\Logs \zoomb.log
LOGLEVEL	The log file name. The log level options are: **LOG_CRIT**: Only the critical errors are included in the log file. **LOG_ERR**: Critical errors plus errors. **LOG_WARNING**: Critical errors, errors and warnings. **LOG_NOTICE**: Critical errors, errors, warnings and notices. **LOG_INFO**: Critical errors, errors, warnings, notices and general information. **LOG_DEBUG**: Critical errors, errors, warnings, notices, general information and debugging information.	InstallationDirectory\Logs \zoomb.log
IIOP_PORT	Zoom Broker's listening port. If omitted, the system assigned port is used.	
IIOP_HOST	The Zoom Broker's IIOP Host Name (or IP). If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address), instructions are provided under the "Firewall Configuration" section in the *Telescope Installation and Configuration Guide for Windows Server Edition*.	If there is no host name, the local IP address is used.

15.16Zoom Builder Configuration

The Zoom Builder must be installed first before performing the following configuration procedure. See Zoom Builder Installation for installation instructions.

Set the following values in the Windows registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\North Plains Systems\Zoom Builder\CurrentVersion

Key	Description	Default Value
HUBIP	The IP address, machine name, or DNS of the Hub to register the Zoom Builder with.	localhost
HUBPORT	The Hub IP Port number.	12345
LOGFILE	The log file name.	InstallationDirectory\Logs \zb.log
LOGLEVEL	The log level. The log level options are: LOG_CRIT: Only the critical errors are included in the log file. LOG_ERR: Critical errors plus errors. LOG_WARNING: Critical errors, errors and warnings. LOG_NOTICE: Critical errors, errors, warnings and notices. LOG_INFO: Critical errors, errors, warnings, notices and general information. LOG_DEBUG: Critical errors, errors, warnings, notices, general information and debugging information.	LOG_NOTICE
IIOP_PORT	Zoom Builder's listening port. If omitted, the system assigned port is used.	
IIOP_HOST	The Zoom Builder IIOP Host Name (or IP). If you want to use a fully-qualified name for the IIOP_HOST registry key (rather than an IP address), instructions are provided under the "Firewall Configuration" section in the *Telescope Installation and Configuration Guide for Windows Server Edition*.	If there is no host name, the local IP address is used.
ZB_PREFSML	The path to the PrefsML file.	C:\Telescope\com.northplains.zoombuilder.xml

Key	Description	Default Value
IMAGEMAGICK_DIR	Path to ImageMagick. This value allows a user to specify a full path to an ImageMagick directory. For example, C:\Program Files (x86)\ImageMagick-6.9.0-Q16 If the value is not set, Telescope attempts to read the value from the registry settings for ImageMagick (installed with Telescope), at HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ImageMagick\Current The C: drive is assumed for this default, so if your ImageMagick directory resides in a different drive or different location, you need to update this registry key.	
DEFAULT_ZB	The default Zoom Builder.	
SERVING_HOSTS	This is the Zoom Builder's serving host. Valid values are a comma-separated list of Telescope Hub host names, in upper case. This value is required if the Zoom Builder is installed on a machine other than the machine acting as the Telescope Hub.	The default is the local host name.
MAX_NUMBER_OF_WORKER	The number of the worker processes, for example, 3.	Default value is 3.
WORKER_IDLE_TIMEOUT	The timeout limit for an idle Graphics Broker sub-process, in seconds. Sub-processes cease when this value is met, unless it is the last process.	Default is 21600 (6 hours).
DB_ACCESS_IDLE_LIMIT	The timeout limit for an idle connection, in seconds.	Default is 3600.
DB_SCAN_INTERVAL	The interval that connections are scanned for idling, in seconds.	Default is 300.
FB_CONFIG	(Internal Use Only.)	
BYPASS_FB_4_LOCAL_FILE	A flag to make the Zoom Builder access files directly when it can translate a file location to a local path. Valid values are "y" or "n", case insensitive. If set to "n", the Graphics Broker will always access and download files from the File Broker.	If omitted, the default is "y"
TEMP_DIR	The temporary folder path the Graphics Broker use to store the temporary files when a file is downloaded from File Broker.	
BUILD_TIMEOUT	The timeout setting for the build zoom image process.	Default is 1800 seconds.

15.16.1 Add a New Field to the EDITORIAL Table

You must add a new field to the EDITORIAL table in the Telescope database to store a value to indicate the status of the Zoom Builder processing: For example, add a field called “zoomable” with a data type of integer. The values might be 1 to indicate that a zoom build is in progress. Zero (0) indicates that the zoom information has been created and is ready to display. The default NULL value means that no zoom information has been created for the imgae.

NOTE: Since the “zoomable” field is a system field updated by Telescope, you should not have edit permission for this field. To prevent confusion, you can remove the “See” permission for this field.

15.16.2Create a Folder to Store Zoom Images

The hard drive to contain the folder must have sufficient spare to store a reasonable number of very large TIFF files. The default number of cached zoom images is 10,000. The folder must also be a network share with the following permissions:

- Read/Write for the account the Zoom Broker and Zoom Builder are starting up as on the Hub server.
- Read for the web server account.

NOTE: Make a note of the zoom image folder path and the name and data type of the field you added to the EDITORIAL table. This information is needed when you configure the Zoom Broker settings for a connection in Telescope Administrator.

Chapter 16: Third-Party License Acknowledgements

Use of your software is subject to the terms and conditions of the North Plains Systems Software License Agreement. Third-party software license acknowledgements also apply, as listed in this chapter.

- Section 16.1, "MediaInfo(Lib) License Acknowledgement," on page 238
- Section 16.2, "ZenLib License Acknowledgement," on page 239
- Section 16.3, "zlib Data Compression Library," on page 240
- Section 16.4, "MD5 (from RSA Data Security, Inc.)," on page 242

16.1 MediaInfo(Lib) License Acknowledgement

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Third party libraries

The software relies on third party libraries. Such libraries have their own license. Telescope uses the following libraries (see their license acknowledgements elsewhere in this chapter):

Base classes library: ZenLib, zlib license.

Contributors

Jérôme Martinez (main developper)

16.2ZenLib License Acknowledgement

16.3zlib Data Compression Library

zlib 1.2.5 is a general purpose data compression library. All the code is thread safe. The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files http://www.ietf.org/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format) and rfc1952.txt (gzip format).

All functions of the compression library are documented in the file zlib.h (volunteer to write man pages welcome, contact zlib@gzip.org). A usage example of the library is given in the file example.c which also tests that the library is working correctly. Another example is given in the file minigzip.c. The compression library itself is composed of all source files except example.c and minigzip.c.

To compile all files and run the test program, follow the instructions given at the top of Makefile.in. In short "./ configure; make test", and if that goes well, "make install" should work for most flavors of Unix. For Windows, use one of the special makefiles in win32/ or contrib/vstudio/ . For VMS, use make_vms.com.

Questions about zlib should be sent to <zlib@gzip.org>, or to Gilles Vollant <info@winimage.com> for the Windows DLL version. The zlib home page is http://zlib.net/ . Before reporting a problem, please check this site to verify that you have the latest version of zlib; otherwise get the latest version and check whether the problem still exists or not.

PLEASE read the zlib FAQ http://zlib.net/zlib_faq.html before asking for help.

Mark Nelson <markn@ieee.org> wrote an article about zlib for the Jan. 1997 issue of Dr. Dobb's Journal; a copy of the article is available at http://marknelson.us/1997/01/01/zlib-engine/ .

The changes made in version 1.2.5 are documented in the file ChangeLog.

Unsupported third party contributions are provided in directory contrib/ .

zlib is available in Java using the java.util.zip package, documented at http://java.sun.com/developer/technicalArticles/Programming/compression/ .

A Perl interface to zlib written by Paul Marquess <pmqs@cpan.org> is available at CPAN (Comprehensive Perl Archive Network) sites, including http://search.cpan.org/~pmqs/IO-Compress-Zlib/ .

A Python interface to zlib written by A.M. Kuchling <amk@amk.ca> is available in Python 1.5 and later versions, see http://www.python.org/doc/lib/module-zlib.html .

zlib is built into tcl: http://wiki.tcl.tk/4610 .

An experimental package to read and write files in .zip format, written on top of zlib by Gilles Vollant <info@winimage.com>, is available in the contrib/minizip directory of zlib.

Notes for some targets:

- For Windows DLL versions, please see win32/DLL_FAQ.txt
- For 64-bit Irix, deflate.c must be compiled without any optimization. With -O, one libpng test fails. The test works in 32 bit mode (with the -n32 compiler flag). The compiler bug has been reported to SGI.
- zlib doesn't work with gcc 2.6.3 on a DEC 3000/300LX under OSF/1 2.1 it works when compiled with cc.
- On Digital Unix 4.0D (formely OSF/1) on AlphaServer, the cc option -std1 is necessary to get gzprintf working correctly. This is done by configure.
- zlib doesn't work on HP-UX 9.05 with some versions of /bin/cc. It works with other compilers. Use "make test" to check your compiler.
- gzdopen is not supported on RISCOS or BEOS.

- For PalmOs, see http://palmzlib.sourceforge.net/

Acknowledgments:

The deflate format used by zlib was defined by Phil Katz. The deflate and zlib specifications were written by L. Peter Deutsch. Thanks to all the people who reported problems and suggested various improvements in zlib; they are too numerous to cite here.

Copyright notice:

Jean-loup Gailly Mark Adler

jloup@gzip.org madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes. Please read the FAQ for more information on the distribution of modified source versions.

16.4MD5 (from RSA Data Security, Inc.)

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.